SMART SECURITY SYSTEM BASED ON BIOMETRIC

A project report submitted in partial fulfillment of the requirement for award of the Degree of

BACHELOR OF TECHNOLOGY

In

ELECTRONICS AND COMMUNICATION ENGINEERING

is a bonafide of record work done by

M.NAVYAKA	22KP5A0411
P.VANAJA	21KP1A0488
A.SANJAY	22KP5A0417
P.KAVITHA	21KP1A04A0

Under the Esteemed Guidance of

E.V.SANTHI

Assistant Professor

Department of Electronics and Communication Engineering

NRI INSTITUTE OF TECHNOLOGY
(Approved by AICTE, Affiliated to JNTU, KAKINADA)
VISADALA (P.O.), MEDIKONDURU MANDAL, GUNTUR-522 438
ANDHRA PRADESH

2021-2025

NRI INSTITUTE OF TECHNOLOGY

(Approved by AICTE, Affiliated to JNTU, KAKINADA) VISADALA (P.O.), MEDIKONDURU MANDAL, GUNTUR ANDHRA PRADESH.

CERTIFICATE

This is to certify that the project report entitled "SMART SECURITY SYSTEM BASED ON BIOMETRIC" is a Bonafide record of work carried out by the members. M.NAVYAKA(22KP5A0411), P.VANAJA(21KP1A0488), A.SANJAY(22KP5A0417) ,P.KAVITHA(21KP1A04A0)is in under our guidance and supervision in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in ELECTRONICS AND COMMUNICATION ENGINEERING for the academic year 2021-2025.

PROJECT GUIDE
E.V SANTHI
Assistant Professor

HEAD OF DEPARTMENT
Dr. K. SRIHARI RAO Ph.D
Professor &HOD

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We are highly indebted to our guide E.V SANTHI Assistant Professor Department of ELECTRONICS AND COMMUNICATION ENGINEERING, NRI INSTITUTE OF TECHNOLOGY, VISADALLA, MEDIKONDURU, GUNTUR for her valuable guidance in the successful completion of our project work. We are very much indebted to her for suggesting this interesting topic and helping us at every stage for its successful completion.

It is a great pleasure to convey our sincere thanks to our Honourable Chairman Dr. Alapati Ravindra Prasad garu and Hon'ble Secretary and Correspondent Sri Alapati Rajendra Prasad garu for providing excellent facilities and everything for our success. Our sincere thanks to respected Principal, Dr.KOTA.SRINIVASU garu for his co – operation and valuable suggestions during our stay in this institute. We thank our respected Executive director, Chie Executive Officer, Chief Finance Officer and Administrative Officer for their co- operation and valuable support during our stay in this institute.

We thank respected Vice Principal for his valuable suggestions and motivation during our stay. Our heartfelt thanks to beloved HOD of our department Dr. K. SRIHARI. RAO for his motivation, care and valuable guidance at every step of our project work and in every aspect for our success.

We thank wholeheartedly our project coordinators Dr. C. KALAI SELVAN Professor and Dr.B.SAIDAIAH Professor For their special care towards completion of our project in smooth manner.

It's our pleasure to thank all the faculty members of ECE department for extending their constant co-operation and support during our stay in NRIIT.

Our heartiest thanks to our beloved parents who are well behind us for all our success as well as achievements. Finally we thank all our friends who helped either directly or indirectly to achieve our GOAL.

M.NAVYAKA 22KP5A0411

P.VANAJA 21KP1A0488

A.SANJAY 22KP5A0417

P.KAVITHA 21KP1A04A0

DECLARATION

We hereby declare that the work which is being presented in the Dissertation Entitled "SMART SECURITY SYSTEM BASED ON BIOMETRIC" submitted towards the partial fulfillment of requirements for the award of the degree in Bachelor of Technology and authentic record of our work carried out under the supervision of Dr.B.SAIDAIAH Professor in Department of Electronics and Communication Engineering, at NRI Institute of Technology , Guntur.

The matter embodied in this dissertation report has not been submitted by us for the award of any other degree. Further the technical details furnished in the various chapters in this report are purely relevant to the above project and there is no deviation from the theoretical point of view for design, development and implementation.

PROJECTMEMBERS

M.NAVYAKA	22KP5A0411
P.VANAJA	21KP1A0488
A.SANJAY	22KP5A0417
P.KAVITHA	21KP1A04A0

NRI INSTITUTE OF TECHNOLOGY

(Approved by AICTE, Approved by JNTU, Kakinada) Visadala (P.O), Medikonduru (M), Guntur-522438, Andhra Pradesh.

INSTITUTE VISION:

To become reputed institution of Engineering & Management programs, producing competitive, ethical & socially responsible professionals.

INSTITUTE MISSION:

IM1: Provide quality education through best teaching and learning practices of committed staff.

IM2: Establish a continuous interaction, participation and collaboration with industry to provide solutions.

IM3: Provide the facilities that motivate/encourage faculty and students in research and development activities.

IM4: Develop human values, professional ethics, and interpersonal skills amongst the individuals.

(Alapati Rajendra Prasad)
Secretary & Correspondent

(Dr. Kota Srinivasu)
PRINCIPAL

NRI INSTITUTE OF TECHNOLOGY

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

DEPARTMENT VISION:

To become a center of excellence by bringing out the professional competence in the core areas of electronics and communication engineering.

DEPARTMENT MISSION:

DM1: To provide conducive environment that impart electronics & communication knowledge through quality teaching and self-learning.

DM2: To serve the needs of electronics, telecommunication and allied industries through industry interaction.

DM3: To encourage innovative thinking, continuous learning among the stakeholders and creates new techniques in IOT & VLSI.

DM4: To groom students in communication and interpersonal skills.

DM5: To Inculcate human values and ethics to make learners sensitive towards social issues.

PROGRAMME EDUCATIONAL OBJECTIVES

PEO1: Graduates with competences in the area of electronics and communication engineering.

PEO2: Graduates with continuous learning ability in hardware and software system.

PEO3: Graduates with successful career in industry, research with technical and interpersonal skills.

PEO4: Graduates with professional and ethical values.

PEO5: Graduate shall contribute to organizational goals with individual and teamwork.

(Alapati Rajendra Prasad)
Secretary & Correspondent

(Dr. Kota Srinivasu)
PRINCIPAL

NRI INSTITUTE OF TECHNOLOGY

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

PROGRAMME SPECIFIC OUTCOMES

PSO1: Professional Knowledge: Apply the concepts of electronics and communications to arrive cost effective and appropriate solutions.

PSO2: Problem-solving skills: Apply the principles of analog, digital and signal processing systems for consumer electronics, medical and radar systems.

PSO3: Software usage: Use VHDL, MATLAB, MULTISIM, and MENTOR GRAPHICS to design integrated circuits and analyze signals.

Signature of the HOD

NRI INSTITUTE OF TECHNOLOGY

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

Program Outcomes (PO's)

1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. Problem analysis: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

6. The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

11. Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

ABSTRACT

A door locking system with biometric authentication is an advanced security solution that enhances access control by using unique biological traits such as fingerprints, facial recognition, or iris scans. Traditional locking systems, which rely on keys or passwords, are vulnerable to theft, duplication, or unauthorized access. In contrast, biometric authentication provides a high level of security, as biometric data is unique to each individual and difficult to replicate. This system ensures that only authorized persons can gain entry, thereby reducing the risks associated with unauthorized access and enhancing overall safety.

The system operates by capturing and storing biometric data of authorized users. When access is requested, the system scans the provided biometric input and compares it with the stored data. If a match is found, the door unlocks; otherwise, access is denied. Modern biometric door locking systems integrate with smart technology, allowing for remote monitoring, real-time access logs, and seamless integration with home automation or corporate security frameworks. Additionally, these systems may include fail-safe mechanisms such as backup power supply, multi-factor authentication, or emergency access options to ensure reliability in all situations.

Biometric door locking systems are widely used in residential, commercial, and institutional settings where security is a priority. They offer convenience by eliminating the need for physical keys or remembering passwords. Furthermore, advancements in biometric technology have improved the accuracy, speed, and affordability of these systems, making them accessible to a broader range of users. However, challenges such as data privacy concerns, potential spoofing attempts, and environmental factors affecting biometric recognition still need to be addressed. Despite these challenges, biometric door locking systems continue to evolve, providing an efficient and secure solution for modern access control needs.

INDEX

SMART SECURITY SYSTEM BASED ON BIOMETRIC

CHAPTER-1

INTRODUCTION

A door locking system with biometric authentication is a modern security solution designed to provide enhanced access control by using biological characteristics such as fingerprints, facial recognition, or iris scans. Traditional locking mechanisms, such as mechanical locks and password-based systems, have been widely used for securing residential and commercial properties. However, these conventional methods have significant limitations, including the risk of key duplication, password breaches, or unauthorized access. As security threats continue to evolve, there is an increasing need for more reliable and foolproof authentication systems. Biometric authentication addresses these concerns by offering a highly secure and user-friendly method for verifying an individual's identity before granting access.

The concept of biometric authentication is based on the uniqueness of biological traits, which ensures that only authorized individuals can access a secured area. Unlike conventional locks, which can be easily compromised, biometric systems rely on distinctive human features that cannot be easily replicated or stolen. This makes biometric-based door locking systems a preferred choice for high-security environments, including homes, offices, government institutions, and research facilities. By eliminating the need for physical keys or passwords, these systems also reduce the chances of unauthorized entry due to lost, stolen, or shared credentials. Additionally, biometric locks offer greater convenience, as users do not have to remember passwords or carry keys, making the system both secure and efficient.

A biometric door locking system typically consists of several key components, including a biometric scanner, a microcontroller, a locking mechanism, and a database for storing and verifying biometric data. The biometric scanner captures the user's fingerprint, facial features, or other biological markers and converts them into a digital template. This template is then compared with stored records in the system's database. If a match is found, the microcontroller sends a signal to the locking mechanism, granting access.

One of the primary advantages of a biometric door locking system is its ability to provide real- time monitoring and access logs. These systems can be connected to centralized security networks, allowing administrators to track entry and exit times, identify unauthorized access attempts, and generate reports for security analysis. In corporate environments, such features enhance workforce management by ensuring that only authorized personnel have access to restricted areas. In residential settings, homeowners can monitor who enters and leaves their property, adding an extra layer of security and peace of mind. Additionally, modern biometric locks can be integrated with smart home automation systems, enabling users to control access remotely via mobile applications or voice commands.

Despite the numerous advantages, biometric door locking systems also present certain challenges that need to be addressed. One of the major concerns is data privacy, as biometric information is highly sensitive and requires secure storage to prevent unauthorized access or misuse. If biometric data is compromised, it cannot be changed like a password or a PIN, raising concerns about long-term security. To mitigate this risk, biometric systems employ encryption and secure storage techniques to protect user data. Another challenge is the potential for biometric spoofing, where attackers attempt to trick the system using fake fingerprints, photos, or synthetic biometric data. Advanced biometric systems incorporate liveness detection technologies, such as pulse detection and 3D imaging, to counter such threats.

Environmental factors can also impact the performance of biometric authentication systems. For instance, fingerprint scanners may struggle to recognize prints if the user's fingers are wet, dirty, or injured. Similarly, facial recognition systems may face difficulties in poor lighting conditions or when the user is wearing accessories like glasses or masks. To address these limitations, manufacturers continuously improve sensor technologies and implement adaptive algorithms that enhance recognition accuracy under varying conditions. Moreover, backup authentication methods, such as PIN codes or mechanical key overrides, are often included to ensure access in case of system failures or emergencies.

The adoption of biometric door locking systems has been steadily increasing due to advancements in technology and a growing awareness of security needs. Many organizations and homeowners are transitioning to biometric-based access control due to its

superior security, ease of use, and ability to prevent unauthorized access. Governments and businesses are also investing in biometric authentication for securing sensitive data centers, research labs, and confidential facilities. As the cost of biometric technology decreases, these systems are becoming more accessible to the general public, further driving their popularity.

In addition to security benefits, biometric door locking systems contribute to operational efficiency by reducing reliance on traditional key management. In corporate settings, lost or misplaced keys can lead to security vulnerabilities and financial losses associated with rekeying or replacing locks. With biometric authentication, access rights can be easily managed, updated, or revoked without the need for physical key replacements. This is particularly useful in large organizations where employee access needs frequently change based on job roles or project assignments. Similarly, in rental properties and shared accommodations, biometric locks offer a convenient solution for granting temporary access to tenants or guests without the need for duplicate keys.

Looking ahead, the future of biometric door locking systems is expected to be driven by innovations in artificial intelligence, machine learning, and sensor technologies. AI-powered biometric systems can improve accuracy by learning from user patterns and adapting to changes in appearance over time. With the rise of smart cities and connected infrastructure, biometric authentication is likely to become a standard feature in access control systems, further revolutionizing security practices across various industries.

In conclusion, a door locking system with biometric authentication is a highly secure and efficient solution for modern access control needs. By leveraging unique biological traits, these systems offer a level of security that surpasses traditional locks and password- based mechanisms. With features such as real-time monitoring, remote access, and seamless integration with smart technologies, biometric locks provide both security and convenience. However, challenges related to data privacy, spoofing threats, and environmental factors must be addressed to ensure the widespread adoption of biometric authentication. As technology continues to evolve, biometric door locking systems will play an increasingly vital role in shaping the future of security, making them an essential investment for homes, businesses, and high-security facilities.

PROBLEM STATEMENT

A door locking system with biometric authentication aims to address the limitations and vulnerabilities associated with traditional access control methods. Conventional locking mechanisms, such as mechanical locks and password-based systems, have been in use for centuries, but they come with several security flaws that make them susceptible to unauthorized access. Physical keys can be lost, stolen, or duplicated, while passwords and PIN codes can be forgotten, shared, or hacked. These limitations highlight the need for a more secure and reliable authentication method to prevent security breaches and unauthorized entry into restricted areas. Biometric authentication offers a solution to these challenges by utilizing unique biological characteristics that cannot be easily replicated, providing a higher level of security. However, despite its advantages, biometric authentication also comes with its own set of challenges that must be addressed to ensure its effectiveness and reliability in real-world applications.

One of the primary problems with traditional door locking systems is the risk of unauthorized access due to key duplication or password breaches. In commercial and residential environments, lost or stolen keys pose a significant security threat, as they can be used to gain unauthorized entry. Similarly, passwords and PIN codes can be guessed, stolen through social engineering attacks, or shared among individuals, making them less reliable for security purposes. Moreover, traditional locking mechanisms require constant key management, which can be cumbersome in organizations where access rights frequently change. The reliance on physical keys or passwords creates security loopholes that can be exploited by intruders, making it necessary to explore more advanced and foolproof security measures.

Biometric authentication presents a promising alternative by utilizing unique human features such as fingerprints, facial recognition, or iris scans to grant access.Unlike keys and passwords, biometric traits cannot be easily duplicated or shared , making them a more secure option for access control. However, despite its potential, biometric authentication systems face several challenges that hinder their widespread adoption.One of the major concerns is the accuracy and reliability of biometric recognition.

Another critical issue associated with biometric door locking systems is data privacy and security. Biometric data is highly sensitive and, once compromised, cannot be changed like a password or a key. Unlike passwords, which can be reset in the event of a breach, biometric traits are permanent, making them a valuable target for cybercriminals. If a hacker gains access to a database containing biometric information, they could potentially use the stolen data for identity theft or unauthorized access. Ensuring the secure storage and encryption of biometric data is crucial to prevent such security breaches. Additionally, concerns about data privacyRegulations and user consent must be addressed to ensure compliance with legal and ethical standards.

Another challenge that biometric door locking systems face is the possibility of spoofing and fraudulent access attempts. Advanced hacking techniques, such as using fake fingerprints, high-resolution images, or 3D-printed facial models, have demonstrated the potential to bypass biometric security measures. While modern biometric systems incorporate liveness detection features to differentiate between real and fake biometric inputs, sophisticated spoofing attacks remain a concern. Continuous research and development are required to enhance biometric security mechanisms and prevent unauthorized access through fraudulent means.

Compatibility issues between biometric systems and existing security frameworks can lead to technical complications, making the transition complex and costly. Additionally, users may require training to familiarize themselves with the new authentication process, as biometric systems may not be as intuitive as traditional keys or PIN codes for some individuals.

Biometric authentication systems also require reliable power sources and internet connectivity for remote access and monitoring features. In the event of a power outage or network failure, access control mechanisms may become temporarily inoperative, potentially causing inconvenience or security vulnerabilities. Implementing backup power solutions and offline authentication capabilities is essential to ensure the continuous functionality of biometric door locking systems in all circumstances.

Despite these challenges, biometric authentication remains one of the most secure and efficient methods for access provided that its limitations are effectively addressed. Ongoing technological advancements in artificial intelligence, machine learning, and sensor technology

are improving the accuracy and security of biometric recognition. AI-powered biometric systems can learn and adapt to changes in a user's biometric features over time, reducing false rejection rates and improving overall reliability. Additionally, innovations in blockchain technology offer promising solutions for secure and decentralized biometric data storage, minimizing the risks associated with data breaches.

To maximize the benefits of biometric door locking systems, it is crucial to implement multi- layered security measures. Combining biometric authentication with additional security features, such as PIN codes, RFID cards, or mobile-based authentication, can enhance security and provide alternative access methods in case of biometric system failures. Furthermore, continuous security updates and firmware upgrades are necessary to address emerging threats and improve system performance over time.

The demand for biometric door locking systems is expected to increase as security concerns continue to grow in both residential and commercial sectors. Businesses, government institutions, and homeowners are recognizing the importance of adopting advanced security solutions to protect their assets and personal information. However, successful implementation requires careful consideration of potential challenges, including reliability, data privacy, integration complexity, and cost. Addressing these concerns through technological advancements, regulatory compliance, and user education will be key to ensuring the widespread adoption and effectiveness of biometric door locking systems.

In conclusion, while biometric authentication offers a highly secure and efficient solution for access control, several challenges must be addressed to ensure its reliability and security. The vulnerabilities associated with traditional locking systems, such as key duplication and password breaches, make biometric authentication an attractive alternative. However, concerns related to accuracy, data privacy, spoofing threats, and system integration must be carefully managed. As technology continues to evolve, biometric door locking systems have the potential to become the standard for modern security solutions, offering enhanced protection and convenience in various applications. By implementing robust security measures and continuously improving biometric recognition technology, these systems can play a vital role in shaping the future of access control and security management.

MOTIVATION

The motivation behind developing a door locking system with biometric authentication stems from the increasing need for advanced security measures in residential, commercial, and institutional settings. Traditional door locking mechanisms, such as mechanical keys, PIN codes, and password-based systems, have long been used for access control. However, these conventional methods are prone to various security vulnerabilities, including key duplication, unauthorized access, password breaches, and theft. The limitations of traditional security systems highlight the need for a more robust and reliable solution that ensures maximum protection against security threats. Biometric authentication offers a promising alternative by leveraging unique human characteristics, such as fingerprints, facial recognition, or iris scans, to grant access. This system enhances security by eliminating the risks associated with lost keys, forgotten passwords, and unauthorized access attempts, providing a more efficient and user-friendly security solution.

One of the primary motivations for implementing a biometric door locking system is the growing concern over security breaches and unauthorized access. In both residential and commercial environments, unauthorized entry poses a significant threat to people's safety and property. Burglaries, data theft, and physical intrusions are on the rise, making it essential to adopt more secure access control methods.A biometric door locking system addresses these concerns by using unique biological traits that cannot be easily replicated, significantly reducing the risk of security breaches.

Another strong motivation for this project is the need for convenience and efficiency in access control systems.The advancement of biometric technology also serves as a strong motivation for adopting this system. Over the years, biometric recognition systems have become more accurate, affordable, and widely available. The increasing adoption of biometric authentication in smartphones, banking services, and government identification programs demonstrates its effectiveness and reliability. As technology continues to evolve, biometric systems are becoming more sophisticated, offering faster recognition, enhanced security features, and improved resistance to spoofing attacks

Another significant motivation is the ability of biometric door locking systems to provide real- time monitoring and access tracking. Unlike traditional locks, which do not provide any record of entry and exit, biometric systems can log every access attempt, creating a detailed record of who entered and when.The motivation for this project also arises from the growing adoption of smart home and IoT (Internet of Things) technologies. As more homes and businesses integrate smart devices for security and automation, biometric door locking systems can seamlessly fit into this ecosystem. These systems can be connected to mobile applications, allowing users to manage access remotely, receive security alerts, and integrate with other smart home features such as surveillance cameras and alarm systems. The ability to control access through smartphones or voice commands enhances convenience while maintaining a high level of security.

The project aims to incorporate robust encryption and secure authentication protocols to ensure that biometric data is stored safely and cannot be accessed by unauthorized entities. Additionally, implementing multi-factor authentication, such as combining biometrics with PIN codes or RFID cards, can further enhance security and provide alternative access methods in case of system failures.

The motivation to develop this system is also driven by the need for accessibility and inclusivity in security solutions. Traditional locks and password-based systems may pose difficulties for certain individuals, such as the elderly or those with disabilities, who may struggle with handling physical keys or remembering passwords. A biometric door locking system provides a more inclusive solution by allowing users to gain access effortlessly through fingerprint or facial recognition. The ease of use makes biometric authentication a suitable security option for a wide range of users, including those who may have difficulty operating traditional locking mechanisms.

Additionally, the increasing reliance on technology in modern security systems motivates the development of a biometric door locking system that is adaptable to future innovations. As new security threats emerge, traditional access control methods may become obsolete, necessitating the adoption of more advanced technologies.

advancements. By incorporating these features, the system can remain effective in addressing security challenges and adapting to changing user needs.

The environmental impact of traditional locking systems also serves as motivation for developing a biometric alternative. Traditional locks and keys require metal components, manufacturing, and replacement over time, contributing to material waste. Lost keys and the need for rekeying add to this environmental impact. In contrast, biometric locks minimize the reliance on physical materials, reducing waste and making them a more sustainable security solution. As the world moves towards eco-friendly technologies, biometric access control systems align with efforts to reduce environmental footprints in security infrastructure.

In conclusion, the motivation for developing a door locking system with biometric authentication arises from the need for enhanced security, convenience, efficiency, and technological advancement. The shortcomings of traditional locking mechanisms, such as vulnerability to theft, unauthorized access, and key mismanagement, underscore the importance of adopting biometric authentication. The ability to provide real-time monitoring, seamless integration with smart home technology, and improved accessibility further supports the motivation for this project. Additionally, addressing concerns related to data security and privacy while ensuring adaptability to future technological advancements makes biometric door locking systems a valuable investment for modern access control. By leveraging cutting- edge biometric recognition and security protocols, this system has the potential to revolutionize access control and contribute to a safer and more secure environment for residential, commercial, and institutional applications.

OBJECTIVE

The primary objective of developing a door locking system with biometric authentication is to enhance security and improve access control through the use of unique biological traits such as fingerprints, facial recognition, or iris scans. Traditional security measures, including mechanical locks, PIN codes, and passwords, have long been used for access control but come with several vulnerabilities, such as key duplication, unauthorized access, and security breaches. This project aims to provide a more secure and reliable solution by implementing biometric authentication, which eliminates the risks associated with lost keys and forgotten passwords. By ensuring that only authorized individuals can access a secured area, this system significantly enhances safety in residential, commercial, and institutional settings.

One of the key objectives of this project is to develop a biometric authentication system that is highly accurate and reliable. Biometric recognition systems must be able to accurately distinguish between authorized users and unauthorized individuals while minimizing false acceptance and false rejection rates. The system should incorporate advanced biometric sensors and algorithms capable of handling various environmental conditions. By improving the accuracy of biometric authentication, this project aims to provide a security solution that works efficiently in diverse real-world conditions.

The project also aims to enhance data security and privacy by implementing robust encryption and secure storage mechanisms for biometric data.The system should employ encryption techniques and secure authentication protocols to ensure that biometric data is stored safely and cannot be exploited by cybercriminals. Moreover, the project seeks to comply with data privacy regulations and ethical standards by implementing secure data management practices and ensuring that users have control over their biometric information.

Another objective is to develop a biometric door locking system that supports real- time monitoring and access tracking. Unlike traditional locks, which do not provide any record of entry and exit, biometric authentication systems can log every access attempt and generate detailed reports. This feature is particularly useful in corporate offices, research facilities, and high-security institutions, where monitoring access is essential for security and operational efficiency. The system should be able to track access in real-time, notify

administrators or homeowners of unauthorized attempts, and provide remote access control through mobile applications or smart home integration.

The project also aims to incorporate multi-factor authentication for enhanced security. While biometric authentication provides a high level of security, adding additional authentication layers can further strengthen the system. The biometric door locking system should support secondary verification methods such as PIN codes, RFID cards, or mobile-based authentication to provide an extra layer of security in case of biometric system failures or attempted spoofing attacks. This approach ensures that even if a biometric scanner fails to recognize a user's fingerprint or face due to environmental factors, an alternative authentication method is available to grant access securely.

Another key objective is to ensure the durability and robustness of the biometric door locking system. Security systems should be designed to withstand harsh environmental conditions, such as extreme temperatures, humidity, dust, and physical tampering attempts. The biometric sensors, locking mechanisms, and electronic components should be built using high-quality materials to ensure long-term functionality and reliability. Additionally, the system should include backup power options or offline authentication capabilities to ensure continuous operation during power outages or network failures.

The objective is to develop a biometric door locking solution that is affordable without compromising on security and reliability. By making this technology more accessible, the project aims to encourage wider adoption in homes, small businesses, and educational institutions, improving security across different sectors.

Another important goal is to implement anti-spoofing measures to prevent fraudulent access attempts. One of the challenges of biometric authentication is the possibility of spoofing attacks, where hackers attempt to gain unauthorized access using fake fingerprints, high- resolution images, or 3D-printed facial models. The system should incorporate liveness detection features, such as pulse detection, 3D imaging, and motion analysis, to differentiate between real and fake biometric inputs. By enhancing the security of biometric recognition, the project aims to prevent unauthorized access and make the system more resilient against sophisticated hacking attempts.

Furthermore, the project seeks to provide scalability and flexibility in access control management. In commercial and institutional environments, access requirements often change based on employee roles, visitor permissions, or security updates. The biometric door locking system should allow administrators to easily manage user access levels, add or remove users, and update authentication settings as needed. The system should also support different levels of access control, such as granting temporary access to guests or contractors without compromising security.

Lastly, the project aims to contribute to the advancement of biometric authentication technology by exploring new innovations and potential improvements. The use of artificial intelligence and machine learning can enhance the accuracy and adaptability of biometric recognition, while blockchain technology could provide secure and decentralized storage of biometric credentials. By researching and implementing the latest advancements in biometric security, this project seeks to develop a cutting-edge access control solution that remains effective in the face of evolving security threats.

In conclusion, the objectives of this project focus on enhancing security, improving convenience, ensuring data privacy, and integrating advanced technology into access control systems. The biometric door locking system aims to provide a secure, user-friendly, and efficient solution for residential and commercial applications by utilizing unique biological traits for authentication. By addressing challenges such as data security, spoofing prevention, environmental adaptability, and system integration, this project seeks to develop a comprehensive security solution that meets the needs of modern access control. With continuous technological advancements, the biometric door locking system has the potential to revolutionize security practices and provide a safer, more efficient alternative to traditional locking mechanisms.

THESIS ORGANISATION

The organization of this thesis is structured to systematically present the development, implementation, and evaluation of the biometric door locking system. The thesis is divided into multiple chapters, each focusing on specific aspects of the project, including background information, problem definition, system design, implementation, testing, and conclusions. The following sections provide an overview of the structure of the thesis, highlighting the key components discussed in each chapter.

The first chapter introduces the project by providing an overview of the increasing need for secure access control systems. It discusses the limitations of traditional door locking mechanisms, such as mechanical keys, PIN codes, and password-based authentication, which are prone to security vulnerabilities such as key duplication, theft, and unauthorized access. The chapter also introduces biometric authentication as an effective alternative, emphasizing its advantages in terms of security, convenience, and reliability. Additionally, this chapter outlines the objectives of the project, the scope of the biometric door locking system, and the significance of implementing biometric authentication for access control.

The second chapter provides a comprehensive literature review on biometric authentication and door locking systems. This section explores existing security technologies, including traditional locking mechanisms, electronic locks, and smart locks. It also discusses different biometric authentication methods, such as fingerprint recognition, facial recognition, and iris scanning, along with their respective advantages and limitations. The literature review examines previous research and studies related to biometric access control systems, highlighting key findings, challenges, and technological advancements. Additionally, this chapter discusses the role of artificial intelligence and machine learning in improving biometric authentication accuracy and security.

The third chapter presents the problem statement and research methodology.The methodology section outlines the approach taken to design, develop, and evaluate the proposed system. It includes details on the selection of biometric authentication technology, hardware and software components, system architecture, and data collection methods. This chapter also

discusses the evaluation criteria used to assess the system's performance, including security effectiveness, accuracy, responsetime, and user experience.

The fourth chapter focuses on the system design and architecture of the biometric door locking system. It describes the overall framework of the system, including the hardware and software components used for biometric authentication and access control. The chapter discusses the integration of biometric sensors, microcontrollers, locking mechanisms, and communication modules to create a fully functional security system. It also provides a detailed explanation of the biometric authentication process, covering user enrollment, feature extraction, template storage, and access verification. Additionally, the chapter presents system flowcharts, block diagrams, and use case scenarios to illustrate the functionality and operation of the system. The goal of this chapter is to provide a comprehensive understanding of how the biometric door locking system is structured and how its components work together to ensure secure access control.

The fifth chapter delves into the implementation and development of the biometric door locking system. It provides an in-depth discussion of the software development process, including programming languages, algorithms, and tools used for biometric recognition. The chapter also details the hardware assembly, sensor integration, and microcontroller programming required to build the system. Furthermore, it explains the communication protocols used to enable remote access and real-time monitoring through mobile applications or cloud-based platforms. This section also discusses challenges encountered during the implementation phase and the solutions employed to address them. By presenting the technical details of the system's development, this chapter serves as a guide for understanding how the biometric door locking system was constructed and deployed.

The final chapter, which serves as the conclusion, summarizes the key findings and contributions of the research. It revisits the objectives outlined in the first chapter and evaluates whether they have been successfully achieved. The chapter highlights the strengths of the biometric door locking system, including its enhanced security, user convenience, and technological advancements. It also discusses the limitations of the current system and suggests potential improvements for future research. Additionally, this chapter provides recommendations for further development, such as the integration of

biometrics for enhanced accuracy. The conclusion emphasizes the significance of biometric authentication in modern access control systems and its potential to transform security practices in residential, commercial, and institutional settings.

In summary, the organization of this thesis is designed to provide a clear and comprehensive exploration of the biometric door locking system. Each chapter systematically addresses different aspects of the project, from background research and problem identification to system design, implementation, testing, and evaluation. By following this structured approach, the thesis effectively presents the development process, challenges, and outcomes of the biometric door locking system while offering insights into its real-world applications and future enhancements. The overall objective of the thesis is to contribute to the field of biometric security by demonstrating the effectiveness of biometric authentication in improving access control and addressing security challenges associated with traditional locking mechanisms.

CHAPTER-2
LITERATURE SURVEY

The advancement of security systems has led to the development of various access control mechanisms, ranging from traditional key-based locks to sophisticated biometric authentication systems. Biometric authentication has emerged as a promising solution to enhance security in door locking systems, eliminating the limitations associated with traditional locking mechanisms. This literature survey provides an overview of existing door locking technologies, biometric authentication methods, and previous research conducted in this domain. The survey examines different biometric modalities, security challenges, and technological advancements that have contributed to the development of biometric-based access control systems.

Traditional Door Locking Systems and Their Limitations

Conventional door locking systems primarily rely on mechanical keys, PIN codes, and RFID (Radio Frequency Identification) cards for access control. While these methods have been widely used, they come with several vulnerabilities. Mechanical keys can be lost, stolen, or duplicated, making unauthorized access relatively easy. PIN-based systems and password authentication, though commonly used, are prone to security risks such as shoulder surfing, brute-force attacks, and password forgetfulness. RFID card-based systems, while more secure than traditional keys, are susceptible to cloning and unauthorized duplication, compromising security. These limitations have driven the need for more advanced security measures, leading to the adoption of biometric authentication for access control.

Biometric Authentication in Security Systems

Biometric authentication leverages unique biological characteristics such as fingerprints, facial features, iris patterns, and voice recognition for identity verification. Unlike passwords or physical keys, biometric traits are difficult to replicate, offering a higher level of security. Several biometric authentication techniques have been developed and integrated into access control systems.

Fingerprint Recognition

Fingerprint recognition is one of the most widely used biometric authentication methods due to its accuracy and ease of implementation. Fingerprint scanners capture the unique ridges and patterns of an individual's finger and store them as templates for authentication. Several studies have demonstrated the effectiveness of fingerprint-based door locking systems.

Research by Maltoni et al. (2019) highlights the reliability of fingerprint recognition in various security applications, emphasizing its high accuracy and resistance to forgery. However, challenges such as environmental factors, skin conditions, and sensor durability

must be addressed to improve performance.

Facial Recognition

Facial recognition technology analyzes unique facial features such as the distance between eyes, nose shape, and jaw structure for authentication. Recent advancements in artificial intelligence and deep learning have significantly improved the accuracy of facial recognition systems. Studies by Zhang et al. (2020) demonstrate the efficiency of convolutional neural networks (CNNs) in facial recognition, making it a viable option for door locking systems. However, facial recognition faces challenges such as changes in lighting conditions, facial obstructions (e.g., glasses or masks), and spoofing attacks using high-resolution images.

Iris Recognition

Iris recognition is another highly secure biometric authentication method that captures unique patterns in the human iris. Daugman (2018) highlights the near-perfect accuracy of iris recognition, making it ideal for high-security applications. Iris-based authentication is resistant to forgery and can function effectively under different lighting conditions. However, the high cost of iris recognition sensors and the need for close-range scanning limit its widespread adoption in consumer-based door locking systems.

Voice Recognition

Voice recognition analyzes vocal characteristics such as pitch, tone, and speech patterns for identity verification. Research by Rabiner and Schafer (2021) emphasizes the potential of

voice biometrics in access control systems. While voice recognition provides a hands-free authentication method, it is susceptible to environmental noise, voice changes due to illness, and spoofing attacks using recorded audio.

Multi-Factor Authentication for Enhanced Security

To address the limitations of single biometric authentication methods, researchers have explored multi-factor authentication (MFA), which combines multiple verification techniques for increased security. MFA integrates biometric authentication with secondary security measures such as PIN codes, RFID cards, or mobile-based authentication. Studies by Li et al. (2021) suggest that combining fingerprint recognition with facial recognition enhances the robustness of access control systems, reducing the likelihood of false acceptance or rejection.

Security Challenges in Biometric Authentication

Despite the advantages of biometric authentication, several security challenges must be addressed to ensure reliable implementation in door locking systems. One major concern is spoofing attacks, where unauthorized individuals attempt to bypass authentication using artificial biometric data such as fake fingerprints or 3D-printed facial models. Research by Sun et al. (2020) explores anti-spoofing techniques, such as liveness detection and 3D depth analysis, to mitigate these threats.

Another critical issue is biometric data security and privacy. Unlike passwords, biometric data is immutable, meaning that once compromised, it cannot be changed. Therefore, secure encryption and storage mechanisms are necessary to prevent unauthorized access to biometric templates. Studies by Jain and Ross (2019) propose the use of blockchain technology and decentralized biometric storage to enhance data security.

Integration of Artificial Intelligence and Machine Learning

Artificial intelligence (AI) and machine learning (ML) play a significant role in improving biometric authentication accuracy and efficiency. AI-powered algorithms

enhance the ability of biometric systems to adapt to variations in biometric traits, such as aging, facial hair growth, and minor injuries. Research by He et al. (2022) highlights the application of deep learning models in fingerprint and facial recognition, significantly reducing false rejection and false acceptance rates. AI-based biometric authentication also enables continuous learning, allowing the system to improve over time based on user interactions.

Smart Home Integration and IoT-Based Security Systems

With the rise of smart home technology, biometric door locking systems are increasingly being integrated with Internet of Things (IoT) platforms. IoT-enabled security systems allow remote access control, real-time monitoring, and instant notifications in case of unauthorized access attempts. Studies by Chen et al. (2021) demonstrate how IoT-based biometric security systems can enhance convenience by enabling users to control access through mobile applications and cloud-based services. However, IoT integration also introduces cybersecurity risks, such as hacking attempts and network vulnerabilities, which must be addressed through robust encryption and secure communication protocols.

The literature survey highlights the evolution of door locking systems from traditional mechanical locks to advanced biometric authentication systems. While fingerprint, facial, iris, and voice recognition offer improved security, challenges such as spoofing attacks, environmental conditions, and biometric data security must be addressed. Multi-factor authentication, AI integration, and IoT-based security solutions have been explored to enhance biometric authentication reliability and usability. This study serves as a foundation for developing a secure and efficient biometric door locking system that leverages state-of-the-art authentication techniques while addressing existing security concerns. Future research should focus on improving anti-spoofing mechanisms, enhancing biometric recognition accuracy, and ensuring the ethical and secure use of biometric data in access control applications.

METHODOLOGY

The methodology for designing and implementing a biometric door locking system with authentication is structured to ensure security, reliability, and efficiency. The system follows a step-by-step approach that includes problem analysis, hardware selection, software development, system integration, testing, and evaluation. This methodology provides a clear framework for developing the system, ensuring that each component works harmoniously to achieve a secure access control solution.

System Design and Architecture

The biometric door locking system is designed to provide a secure and user-friendly authentication mechanism for access control. The design process involves the selection of biometric technology, hardware components, and software frameworks necessary to develop the system. The architecture consists of three primary components:

1. **Biometric Authentication Module** – Responsible for capturing, processing, and verifying biometric data such as fingerprints or facial recognition.
2. **Control Unit** – The microcontroller or processor that manages access control and communication between different system components.
3. **Locking Mechanism** – The electronic lock that physically controls door access based on authentication results.

The system is also integrated with additional security features such as encrypted data storage, remote access control, and a mobile application for monitoring access logs.

Selection of Biometric Authentication Technology

Choosing the right biometric authentication method is crucial to the success of the project. The system primarily employs fingerprint recognition due to its accuracy, ease of implementation, and cost-effectiveness. Facial recognition is considered as an additional feature for multi-factor authentication. The key factors in selecting a biometric technology include:

- **Accuracy and reliability** – The chosen biometric method should have a low false rejection rate (FRR) and false acceptance rate (FAR).

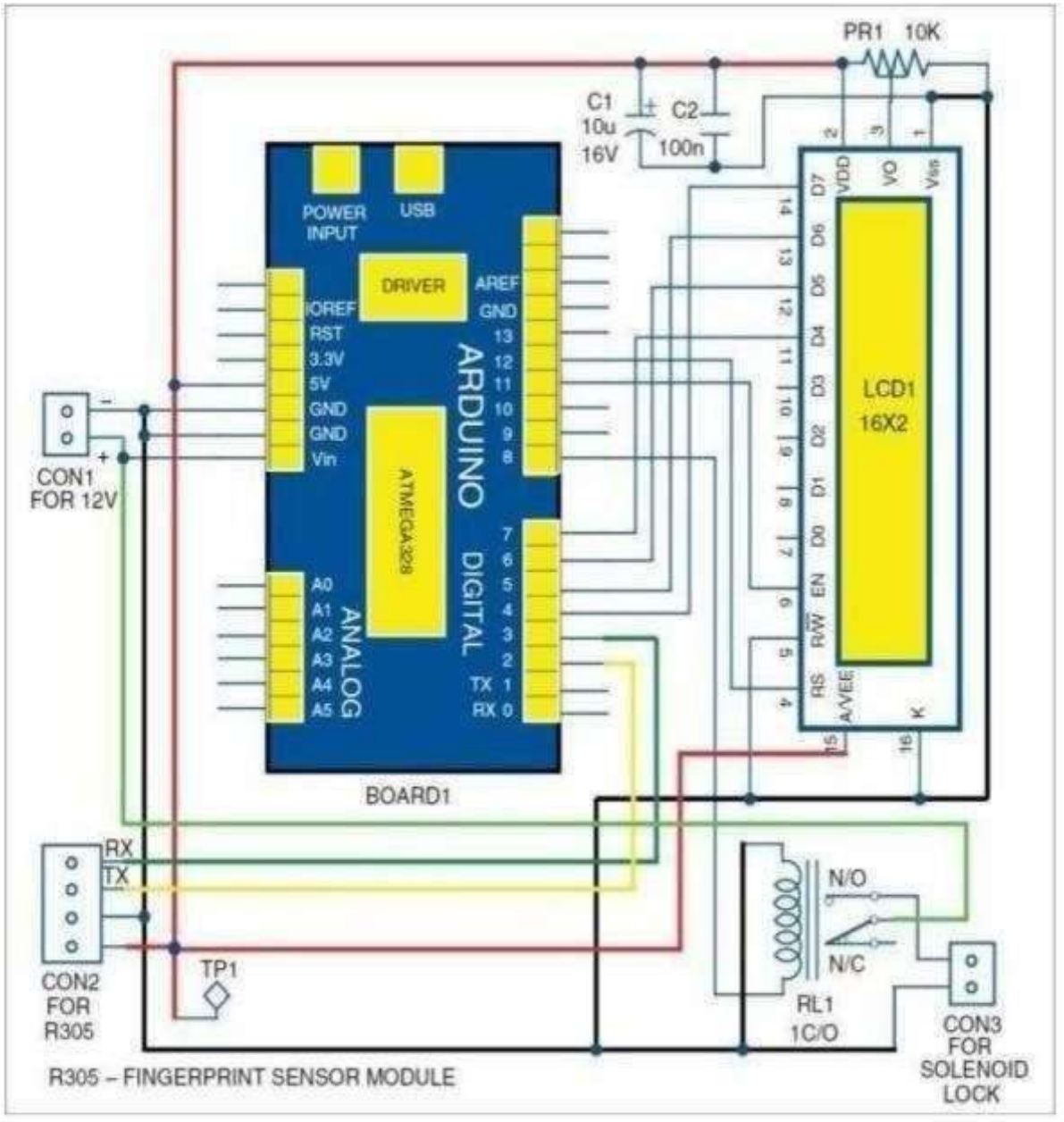


Figure: Architecture Of Fingerprint Door Lock System

- **Speed and efficiency** – Authentication should be performed in real-time with minimal delay.
- **Security considerations** – The biometric data should be encrypted and securely stored to prevent unauthorized access.

Fingerprint sensors are widely available and provide high accuracy, making them an ideal choice for this project. Advanced image processing techniques are used to enhance fingerprint recognition performance under varying conditions.

Hardware and Component Selection

The hardware selection is based on compatibility, efficiency, and security. The main hardware components include:

1. **Fingerprint Scanner** – Used to capture and authenticate fingerprint data. A capacitive or optical fingerprint sensor is selected based on accuracy and durability.
2. **Microcontroller Unit (MCU)** – Responsible for processing authentication requests and controlling the electronic lock. An Arduino or Raspberry Pi is used as the processing unit.
3. **Electronic Lock** – A solenoid or electromagnetic lock is chosen for its reliability and fast response time.
4. **Display and Keypad** – A small LCD screen and keypad are included for system interaction, user registration, and manual authentication options.
5. **Power Supply** – A backup power source, such as a rechargeable battery, is integrated to ensure the system functions during power outages.

Software Development and Algorithm Implementation

The software development process involves writing the necessary code to capture, process, and authenticate biometric data. The software is developed using a combination of programming languages such as Python (for image processing and facial recognition) and C++ (for microcontroller programming). The main steps in software development

1. **Fingerprint Enrollment and Storage** – Users register their fingerprints, which are processed and stored securely in an encrypted format.
2. **Authentication Algorithm** – When a user places a finger on the scanner, the captured fingerprint is compared with stored templates using a matching algorithm such as the Minutiae-based approach.
3. **Access Control Decision** – If the fingerprint matches, the system grants access by unlocking the door. If authentication fails, access is denied, and an alert is triggered.
4. **Remote Access and Monitoring** – A mobile application or web interface allows users to monitor access logs and remotely control the locking system.

The software is designed with error-handling mechanisms to ensure smooth operation and security against spoofing attempts.

Integration and System Testing

The integration phase involves assembling the hardware and software components into a fully functional biometric door locking system. The system is tested under different conditions to evaluate its performance, security, and usability.

1. **Unit Testing** – Each component (fingerprint scanner, microcontroller, electronic lock) is tested individually to ensure functionality.
2. **Integration Testing** – The complete system is tested to ensure seamless interaction between hardware and software.
3. **Security Testing** – Various attack scenarios, such as fake fingerprints and brute-force attempts, are simulated to assess the system's resistance to unauthorized access.
4. **Performance Testing** – Authentication speed, accuracy, and response time are measured to ensure real-time operation.
5. **User Testing** – The system is tested with multiple users to evaluate usability, enrollment ease, and overall experience.

Security Measures and Data Protection

To protect biometric data and prevent unauthorized access, the system incorporates the following security measures:

- **Liveness Detection** – The system includes anti-spoofing techniques to detect fake fingerprints and facial images.
- **Two-Factor Authentication** – For enhanced security, an optional secondary authentication method (PIN or RFID) is included.
- **Access Logs and Monitoring** – The system maintains a log of all access attempts and alerts users in case of suspicious activity.

Deployment and Real-World Application

After successful testing, the system is deployed in a real-world environment such as a residential home, office, or high-security area. Deployment involves:

1. **Installation of the Biometric Lock** – The biometric doorlock is installed on an actual door and connected to the control unit.
2. **User Registration** – Authorized individuals are enrolled into the system.
3. **Live Testing and Adjustments** – The system undergoes final testing to fine-tune authentication settings and ensure optimal performance.

Evaluation and Future Enhancements

The final step involves evaluating the system's effectiveness and identifying potential improvements. Key evaluation criteria include:

- **Authentication Accuracy** – Ensuring a high success rate for legitimate users while minimizing false rejections.
- **User Convenience** – The ease of use and registration process is assessed to ensure a smooth experience.
- **Security Performance** – The system's resistance to various attack scenarios is analyzed.
- **Scalability and Upgradability** – Future enhancements such as integrating cloud-based storage, AI-based authentication improvements, and additional biometric methods are considered.

The methodology for developing a biometric door locking system follows

structured approach that ensures security, accuracy, and usability. By integrating biometric authentication with advanced security measures, the system enhances access control while eliminating the risks associated with traditional locking mechanisms. The hardware and software components are carefully selected and tested to ensure seamless functionality. Security testing and encryption techniques protect biometric data from potential threats. Future enhancements, including AI-driven improvements and cloud-based access control, can further enhance the system's reliability and efficiency. The biometric door locking system serves as a modern and secure alternative for residential and commercial security applications, providing a robust solution against unauthorized access.

CHAPTER-3

EXISTING SYSTEM

Security has always been a fundamental concern for homes, offices, and various establishments. Traditional door locking mechanisms have been in place for centuries,

evolving from simple mechanical locks to electronic access control systems. However, despite advancements in security technology, conventional systems still have vulnerabilities that make them susceptible to unauthorized access, security breaches, and inconvenience. The existing systems used for door locking include mechanical key locks, PIN-based locks, RFID-based systems, and basic biometric authentication systems. Each of these systems has its advantages and limitations, which necessitate the development of a more robust and secure biometric door locking system.

BLOCK DIAGRAM

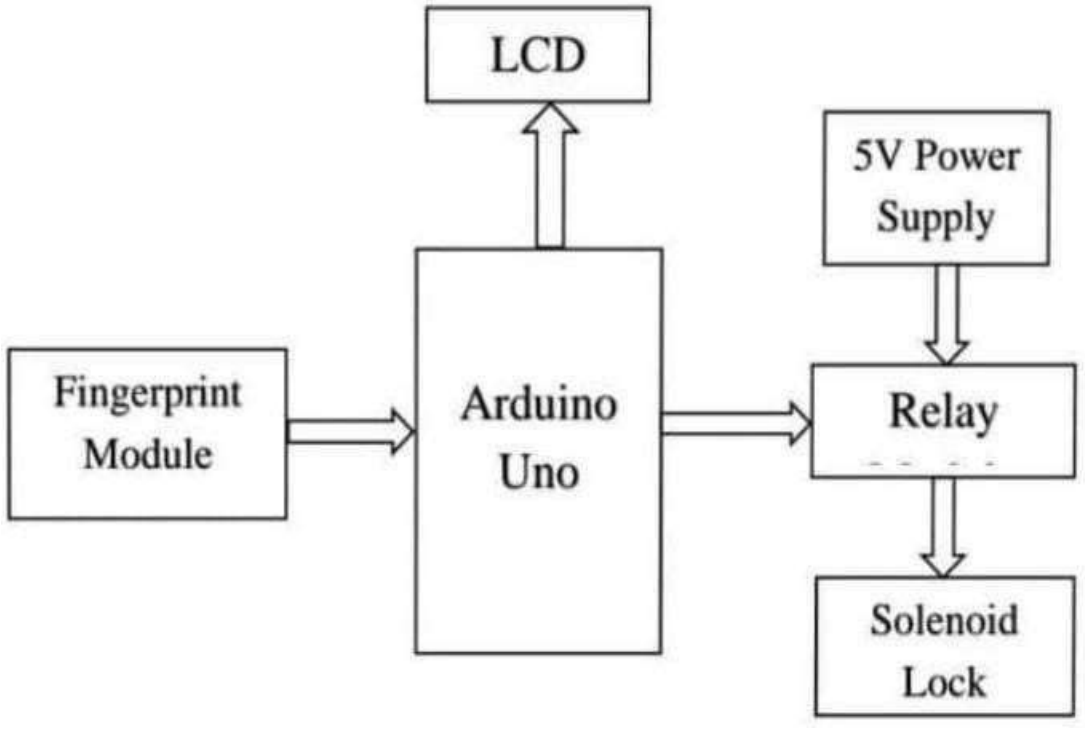


Fig: ARDUINO UNO

Mechanical Key Locks

Mechanical locks are the most widely used form of door security, relying on a key-and-lock mechanism. These locks work by inserting a uniquely shaped key into a cylinder that aligns with internal pins, allowing the lock to be turned and opened. Despite their simplicity and affordability, mechanical key locks have several drawbacks that limit their effectiveness in modern security applications.

One major issue with traditional locks is that keys can be lost, stolen, or duplicated, compromising security. Unauthorized individuals can easily make copies of keys, leading to potential security threats. Additionally, mechanical locks require physical interaction, which can be inconvenient, especially in cases where multiple users need access. Lock picking and bumping techniques have also become more sophisticated, making it easier for burglars to bypass mechanical locks without leaving traces of forced entry.

PIN-Based Electronic Locks

To address the limitations of mechanical locks, electronic PIN-based locks were introduced. These locks require users to enter a pre-defined numerical code to gain access. PIN-based systems eliminate the need for physical keys and provide a more convenient way to manage access control. They are commonly used in residential buildings, office spaces, and commercial establishments.

While PIN-based locks offer better security than mechanical locks, they are still prone to several vulnerabilities. One significant issue is that PIN codes can be easily forgotten, shared, or guessed by unauthorized individuals. Shoulder surfing, where an attacker observes the PIN entry process, is a common security threat in these systems. Additionally, users often choose weak or easily predictable PINs, making brute-force attacks feasible. If a PIN is compromised , there is no way to verify the identity of the individual entering the code, making it less secure than biometric authentication.

RFID-Based Access Control Systems

RFID (Radio Frequency Identification) technology has been widely adopted in access control systems. RFID-based locks use a card or key fob that contains an embedded microchip. When the card is brought near the RFID reader, it transmits a unique identifier to the system, which then grants or denies access based on stored credentials. This technology is commonly used in hotels, office buildings, and high-security areas.

RFID-based locks offer advantages such as contactless access, convenience, and faster authentication compared to mechanical and PIN-based locks. However, these systems are not without security concerns. RFID cards can be lost, stolen, or cloned using advanced hacking techniques. Attackers can use RFID skimming devices to capture card data and create duplicate access cards. Additionally, if an RFID card is misplaced, access control becomes challenging until a replacement card is issued.

Biometric Authentication in Existing Systems

To overcome the limitations of mechanical, PIN-based, and RFID-based locks,biometric authentication has been introduced in modern access control systems. Biometric door locks use unique biological traits such as fingerprints, facial recognition, iris scans, or voice recognition to verify a user's identity. These systems provide a higher level of security because biometric data is unique to each individual and cannot be easily duplicated.

Fingerprint recognition is one of the most widely used biometric authentication methods in existing security systems. Many modern smartphones, laptops, and smart door locks are equipped with fingerprint scanners that allow users to unlock their devices or doors with a simple touch. Facial recognition has also gained popularity due to advancements in artificial intelligence and machine learning, allowing access to be granted based on a user's facial features.

Despite the improved security offered by biometric authentication, existing biometric door locking systems still face several challenges. One of the primary concerns is spoofing, where attackers use fake fingerprints, high-resolution photos, or 3D-printed facial models to bypass authentication. Some biometric systems lack liveness detection, making them vulnerable to these attacks. Environmental factors such as lighting conditions, skin dryness, or sensor wear and tear can also affect the accuracy of biometric recognition.

Challenges in Existing Systems

The existing security systems, whether mechanical, electronic, or biometric, come with several challenges that need to be addressed to ensure optimal security. Some of the key issues include:

1. **Vulnerability to Unauthorized Access** – Traditional mechanical locks can be picked or duplicated, PIN codes can be guessed or stolen, RFID cards can be cloned, and biometric systems can be fooled by spoofing techniques.
2. **User Inconvenience** – PIN-based systems require users to remember codes, and RFID cards can be lost or forgotten. In biometric systems, environmental conditions can sometimes lead to authentication failures, causing inconvenience.
3. **Security Threats and Breaches** – RFID-based systems are susceptible to hacking, PIN codes can be leaked, and some biometric systems lack adequate protection against spoofing attacks.
4. **Data Privacy Concerns** – Biometric authentication involves storing sensitive user data, which raises concerns about data security, privacy, and potential misuse if biometric information is compromised.

The Need for an Improved Biometric Door Locking System

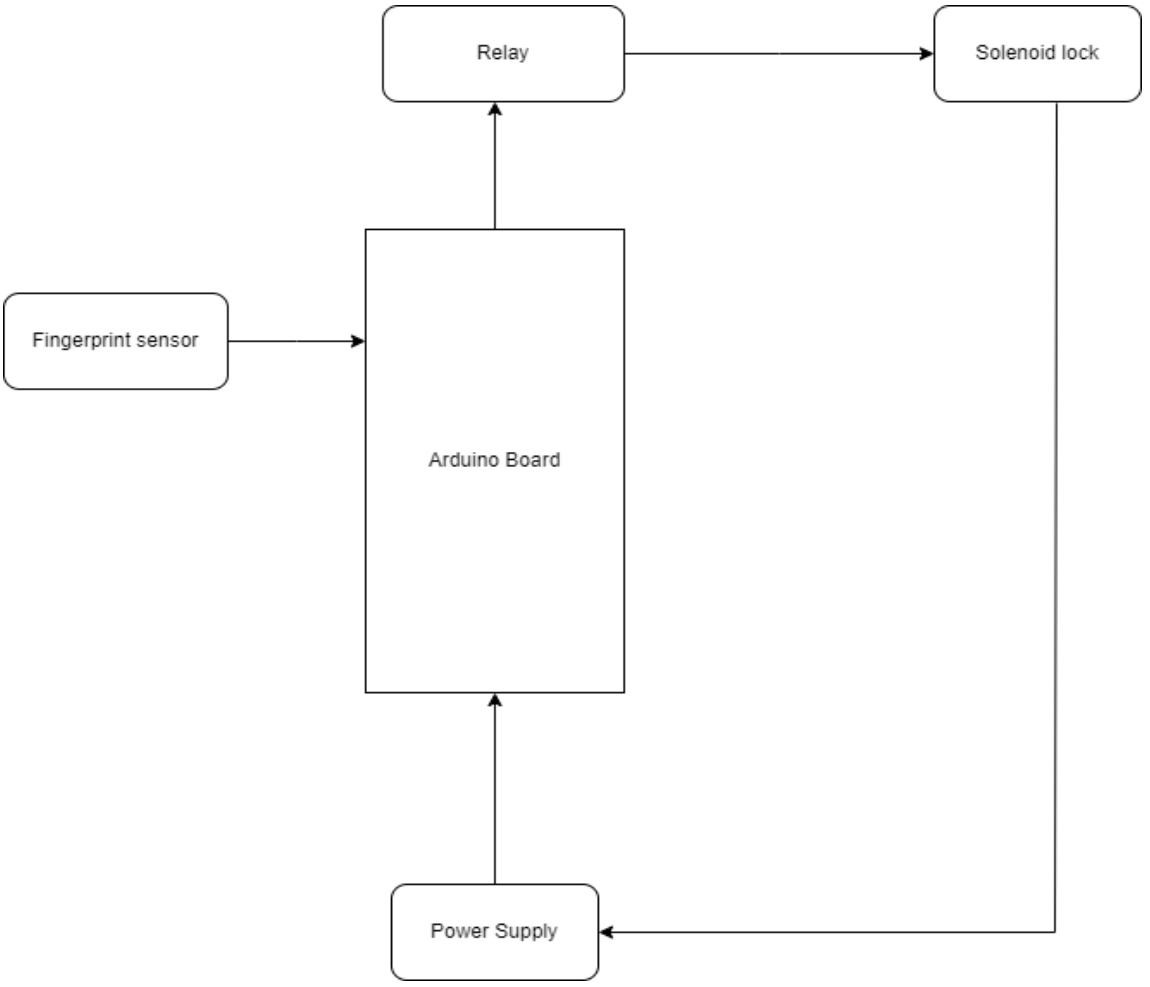
The limitations of existing door locking systems highlight the need for a more advanced and secure biometric authentication-based access control system. The proposed system should address the challenges faced by traditional and current biometric authentication methods by incorporating additional security features such as:

1. **Multi-Factor Authentication** – Combining fingerprint recognition with a secondary authentication method, such as a PIN or RFID card, can enhance security and prevent unauthorized access.
2. **Liveness Detection and Anti-Spoofing Mechanisms** – Advanced biometric systems should implement liveness detection to ensure that only real, live biometric samples are accepted, preventing spoofing attacks.
3. **Encrypted Biometric Data Storage** – To protect user privacy, biometric data should be encrypted and stored securely using advanced cryptographic techniques to prevent unauthorized access or data breaches.
4. **Remote Monitoring and Access Control** – Integrating the biometric system with a mobile application or web interface can allow users to monitor access logs, grant or revoke access remotely, and receive real-time alerts in case of suspicious activity.
5. **AI-Based Biometric Recognition** – Using artificial intelligence and machine learning can improve the accuracy of biometric authentication, reducing false rejection rates and enhancing system performance under various conditions.

The existing door locking systems, including mechanical locks, PIN-based systems, RFID access control, and biometric authentication, each have their own strengths and weaknesses. While biometric authentication provides a higher level of security compared to traditional methods, current biometric systems still face challenges related to spoofing, environmental conditions, and data security. To address these issues, an improved biometric door locking system must integrate advanced security features, multi-factor authentication, encrypted biometric storage, and remote monitoring capabilities. By overcoming the limitations of existing systems, the proposed biometric authentication-based door lock can provide a highly secure, reliable, and user-friendly solution for modern access control needs.

CHAPTER-4
PROPOSED SYSTEM

The proposed biometric door locking system with authentication is designed to enhance security by integrating biometric technology with advanced access control mechanisms. Traditional door locking systems, such as mechanical locks and password-based authentication, are susceptible to security vulnerabilities, including unauthorized key duplication, password breaches, and unauthorized access. The proposed system aims to overcome these challenges by implementing fingerprint recognition, a highly secure and user- friendly authentication method. By incorporating biometric authentication, the system ensures that only authorized individuals can access restricted areas, making it an ideal solution for residential, commercial, and institutional security applications.



Block Diagram

Overview of the Proposed System

The biometric door locking system consists of several key components, including a fingerprint scanner, microcontroller unit, electronic lock mechanism, power supply, and an optional mobile or web-based interface for remote access control. The system works by capturing the user's fingerprint, processing it to extract unique features, and comparing it with stored biometric templates. If a match is found, access is granted, and the door lock is activated. If authentication fails, access is denied, and the system can trigger an alert if multiple unauthorized attempts are detected. The system also includes an administrative interface for managing users, monitoring access logs, and configuring security settings.

Features of the Proposed System

1. **Biometric Authentication** – The system uses fingerprint recognition technology to verify user identities. Fingerprint patterns are unique to each individual, making this method more secure than traditional password-based or key-based access systems.
2. **User Management** – The system allows administrators to register, update, and remove users from the database. Role-based access control can be implemented to restrict access based on user permissons.
3. **Automatic Locking Mechanism** – The door lock automatically engages after a specified time interval to ensure security, even if users forget to lock the door manually.
4. **Real-Time Access Logs** – The system maintains a database of all access attempts, recording user identity, timestamp, and authentication status. Administrators can review these logs for security audits.
6. **Remote Access Control** – Through an integrated mobile or web application, authorized users can monitor and control the system remotely, granting or revoking access as needed.

7. **Intrusion Detection and Alerts** – If multiple failed authentication attempts occur, the system can trigger an alert, notify the administrator, and temporarily disable authentication to prevent brute-force attacks.
8. **Power Backup and Fail-Safe Mode** – A backup battery ensures continued operation in case of power failure. Additionally, an emergency override feature allows manual access if the system malfunctions.
9. **Encryption and Security Measures** – All biometric data and communication between system components are encrypted to prevent unauthorized access and data breaches.

System Architecture

The proposed biometric door locking system follows a structured architecture consisting of hardware and software components that work together seamlessly.

Hardware Components

1. **Fingerprint Scanner** – Captures the user's fingerprint and extracts biometric features for authentication.
2. **Microcontroller Unit (MCU)** – Acts as the system's processing unit, handling biometric data processing, user authentication, and communication with other components.
3. **Electronic Lock** – A solenoid or electromagnetic lock is used to secure the door and is controlled by the microcontroller.
4. **Power Supply Unit** – Ensures continuous operation of the system, with a backup battery for reliability during power outages.

1. **LCD Display or LED Indicators** – Provides visual feedback on authentication status and system alerts.
2. **Buzzer or Alarm System** – Produces sound alerts for successful authentication, failed attempts, or security breaches.
3. **Communication Modules (Wi-Fi/Bluetooth/GSM)** – Enables remote monitoring and control of the system via a smartphone or web interface.

Software Components

1. **Biometric Processing Algorithm** – Extracts and matches fingerprint features against stored templates for authentication.
2. **User Management System** – Allows administrators to enroll, update, or remove users from the system.
3. **Database Management** – Stores biometric data, access logs, and user information securely.
4. **Remote Access Application** – A web or mobile-based interface for monitoring and controlling the system remotely.
5. **Security Protocols** – Implements encryption and secure communication to protect biometric data and prevent cyber threats.

Working of the Proposed System

The system operates in multiple phases, including enrollment, authentication, access control, and monitoring.

1. **User Enrollment** – New users must be registered by the administrator. The fingerprint scanner captures and processes the user's fingerprint, storing a unique biometric template in the database.
2. **Authentication Process** – When a user attempts to access the door, they place their finger on the scanner. The system extracts fingerprint features and compares them with stored biometric templates.
3. **Access Control Decision** – If authentication is successful, the microcontroller activates the electronic lock, granting access. If authentication fails, access is denied, and the system logs the attempt.

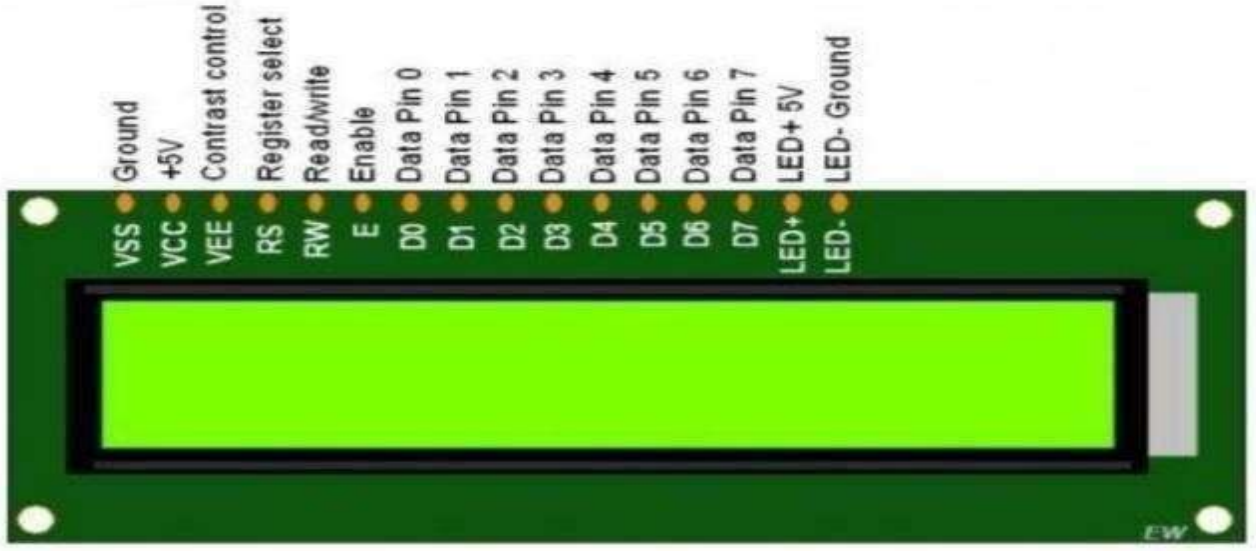


Figure:16X2 LCD Display

Figure:Solenoid Electric Door Lock

4. **Security Measures** – Multiple failed authentication attempts trigger security alerts and temporarily lock the system to prevent unauthorized access.
5. **Remote Monitoring and Control** – Administrators can use a mobile or web application to monitor access logs, modify user permissions, and unlock doors remotely.

Advantages of the Proposed System

1. **Enhanced Security** – Biometric authentication eliminates the risk of lost keys or password breaches, providing a highly secure access control method.
2. **Convenience** – Users do not need to carry keys or remember passwords, as access is granted based on their unique fingerprint.
3. **Automated Access Management** – The system maintains access logs and provides real-time monitoring, reducing the need for manual security checks.
4. **Scalability** – The system can be expanded to accommodate additional users and integrate with other security solutions.
5. **Remote Accessibility** – Administrators can monitor and control the system remotely, making it ideal for modern security applications.
6. **Intrusion Prevention** – The system detects unauthorized access attempts and alerts administrators, enhancing overall security.

Challenges and Mitigation Strategies

While biometric authentication offers significant security benefits, certain challenges must be addressed:

1. **False Rejections and Acceptances** – Advanced biometric algorithms with high accuracy rates will minimize authentication errors.
2. **Privacy Concerns** – Biometric data will be encrypted and stored securely to comply with data protection regulations.

3. **Power Dependency** – A backup battery system will ensure continued operation during power failures.

3. **Wear and Tear of Fingerprint Scanners** – High-quality fingerprint sensors with long- term durability will be used.
4. **Environmental Factors** – The system will be designed to function effectively under varying environmental conditions, such as humidity and temperature changes.

The proposed biometric door locking system with authentication is an advanced security solution that enhances traditional access control mechanisms. By utilizing fingerprint recognition, it ensures a secure, reliable, and convenient method for granting access to authorized individuals. The system is designed to integrate with modern security infrastructures, providing features such as remote monitoring, intrusion detection, and multi- factor authentication. With a focus on security, usability, and scalability, the proposed system addresses the limitations of traditional locking systems while meeting the needs of residential, commercial, and high-security applications. Implementing this system will significantly enhance security and provide a robust solution for preventing unauthorized access.

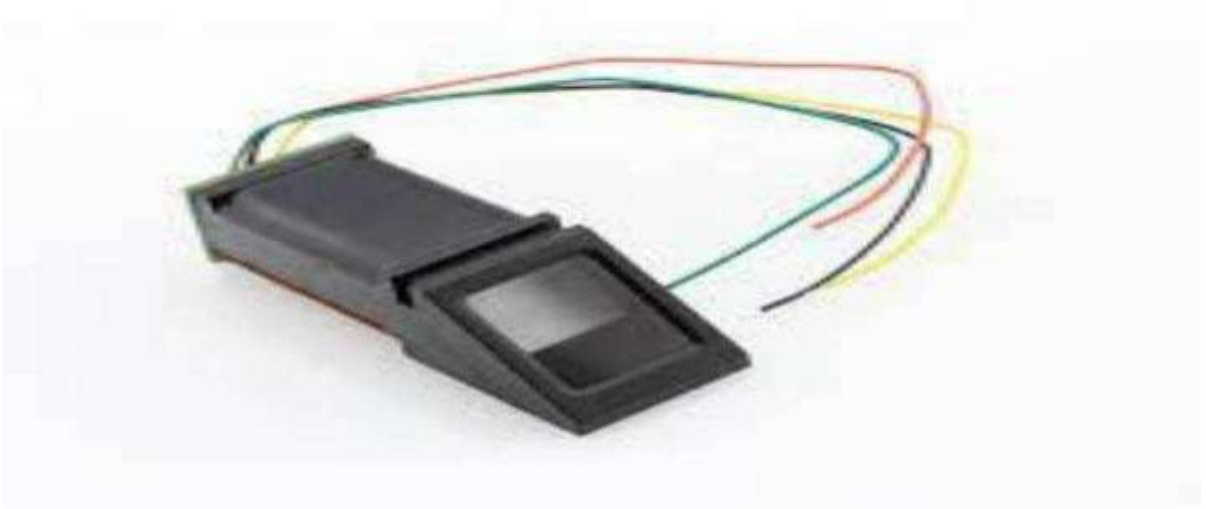


Fig: Finger Print Sensor

CHAPTER-5

REQUIREMENTS

FUNCTIONAL REQUIREMENTS

A biometric door locking system with authentication is designed to enhance security and ensure controlled access. The system relies on biometric verification, such as fingerprint recognition, to authenticate users and grant or deny access accordingly. The functional requirements define the essential features, behaviors, and operations of the system. These requirements are categorized into authentication, user management, security, hardware control, data storage, system administration, and remote access functionalities. Each aspect of the system must function seamlessly to provide a secure and user-friendly experience.

User Authentication and Access Control

- The system must capture and process fingerprint data for authentication.
- It must verify the user's identity by comparing the captured fingerprint with stored biometric templates.
- If authentication is successful, the system should unlock the door and grant access.
- If authentication fails, access should be denied, and an alert should be triggered after multiple failed attempts.
- The system must support multi-factor authentication by allowing an optional PIN code or RFID card for additional security.
- A liveness detection mechanism should be implemented to prevent unauthorized access using fake fingerprints or 3D-printed replicas.
- If an unauthorized access attempt is detected, the system should log the attempt and notify the administrator.

User Registration and Management

- The system should allow authorized administrators to enroll new users by capturing and storing their fingerprint data securely.
- Each registered user should be assigned a unique ID to differentiate between users.

- The system must allow multiple users to be enrolled, supporting at least 100 fingerprint templates to accommodate different levels of access.
- Users should be able to update or remove their biometric data upon administrator approval.
- The system must include role-based access control, allowing administrators to grant or restrict access based on user roles (e.g., administrator, regular user, temporary user).
- Temporary access should be configurable for guests or employees, ensuring access is revoked after a specified period.

Security and Data Protection

- The system should encrypt all stored biometric data to prevent unauthorized access or data breaches.
- Secure communication protocols, such as SSL/TLS, should be used for data transmission to ensure security.
- The system must implement a fail-safe mechanism to handle power failures, ensuring data is not lost.
- An intrusion detection system should be integrated to detect and alert administrators about potential security threats.
- Audit logs should be maintained for all authentication attempts, including timestamps, user IDs, and access status (granted or denied).
- The system should include an emergency override function for situations where biometric authentication fails, allowing administrators to unlock the door manually with a master PIN or key.
- The system must automatically lock after a certain period of inactivity to prevent unauthorized access.

Hardware and Door Lock Mechanism

- The system should integrate with an electronic lock mechanism, such as a solenoid or electromagnetic lock.
- It must provide a real-time response to unlock the door within two seconds of successful authentication.
- The lock should automatically engage when the door is closed to maintain security.

- A backup power supply, such as a rechargeable battery, should be included to keep the system operational during power outages.
- The fingerprint scanner should be durable and resistant to wear and tear, ensuring long-term usability.
- A touchscreen or LCD display should be integrated to show system status messages, authentication results, and error notifications.
- An LED or buzzer should provide audible and visual feedback for successful or failed authentication attempts.
- The system should detect if the door remains open after authentication and trigger an alert if it is not closed within a specified time.

Data Storage and Log Management

- The system must store biometric data securely in an encrypted format to protect user privacy.
- A database should be used to store user details, access logs, and system configurations.
- Access logs should include details such as user ID, timestamp, authentication result, and access location.
- The system must retain access logs for a minimum period of 90 days for security audits.
- The administrator should be able to export access logs for further analysis or compliance reporting.
- Automatic log deletion should be configured to remove outdated logs while maintaining a backup for reference.
- The system should generate alerts for suspicious activities, such as multiple failed authentication attempts or unauthorized access attempts.

System Administration and Configuration

- The system should provide an administrative dashboard for configuring user roles, access settings, and security policies.
- Administrators should be able to add, remove, or update user credentials through a secure interface.
- The system must allow customization of security settings, including authentication timeouts, lockout periods, and alert notifications.

- The administrator should be able to reset user credentials in case of forgotten PINs or lost RFID cards.
- The system should support remote configuration and maintenance to allow updates and troubleshooting without physical access.
- The administrator should receive notifications about system status, hardware malfunctions, or software updates.

Remote Access and Monitoring

- The system must support remote access control via a mobile application or web-based interface.
- Users should be able to monitor real-time access logs from a remote location.
- The administrator should have the ability to revoke access remotely in case of security threats.
- The mobile application should support push notifications for security alerts and system updates.
- Remote unlocking should be available for emergency situations, provided the administrator authorizes it.
- The system should support integration with smart home security systems for enhanced monitoring.
- Users should receive alerts if an unauthorized person attempts to tamper with the biometric scanner or lock mechanism.

Performance and Reliability

- The system must authenticate users within two seconds to provide fast and seamless access.
- It should support a minimum of 100,000 authentication cycles without hardware failure.
- The fingerprint scanner should maintain an accuracy rate of at least 99% to minimize false rejections.
- The system should function efficiently in various environmental conditions, including temperature variations and humidity.
- It should automatically perform self-diagnostics and notify administrators of any hardware malfunctions.

- The biometric scanner should have an error tolerance mechanism to handle minor.

Integration with Other Systems

- The system should support integration with existing security infrastructures, such as CCTV cameras or alarm systems.
- It should be compatible with smart home automation systems for centralized security management.
- The system should allow third-party API integration for advanced security applications.

The biometric door locking system with authentication must incorporate comprehensive functional requirements to ensure secure, efficient, and user-friendly access control. By integrating biometric authentication with advanced security features, the system enhances traditional locking mechanisms while addressing vulnerabilities present in existing access control systems. The inclusion of data encryption, remote monitoring, and fail-safe mechanisms ensures the system's reliability in various environments. By adhering to these functional requirements, the biometric door locking system will provide an effective security solution for homes.

NON-FUNCTIONAL REQUIREMENTS

The biometric door locking system with authentication must not only meet functional requirements but also adhere to several non-functional requirements to ensure security, efficiency, reliability, and user satisfaction. These requirements define the overall quality attributes of the system, including performance, usability, security, maintainability, scalability, and compliance. Implementing these non-functional requirements will enhance the system's robustness and usability while ensuring long-term efficiency.

Performance Requirements

- The system must authenticate users within two seconds to provide a seamless and

quick access experience.

- The fingerprint scanner should have an accuracy rate of at least 99% to minimize false rejections and false acceptances.
- The system must support at least 100,000 authentication cycles without hardware degradation.
- It should handle multiple authentication attempts simultaneously without performance degradation.
- The system should have an uptime of 99.9%, ensuring continuous availability for users.
- The database should process authentication requests in real time without noticeable delays.
- The system should detect unauthorized access attempts within one second and trigger appropriate security measures.
- Data retrieval from the database should not exceed one second to ensure smooth operation.

Usability and User Experience

- The system interface should be user-friendly, with intuitive navigation for both administrators and regular users.
- The fingerprint scanner should be ergonomically placed for easy access and usability.
- The system should provide clear visual and audio feedback, such as LED indicators or buzzer sounds, for authentication success or failure.
- The user interface should be designed with a simple and clear layout, ensuring ease of use for individuals with minimal technical knowledge.
- A touchscreen or LCD display should be included for displaying instructions, error messages, and system status updates.
- The system should provide a multi-language option for wider accessibility.
- Users should be able to enroll and update their biometric data with minimal steps and without requiring extensive training.
- The mobile application interface should be responsive and work seamlessly on different screen sizes.

Security Requirements

- The system should use encryption algorithms such as AES-256 to secure stored

biometric data and prevent unauthorized access.

- All communication between system components, including mobile applications and remote servers, should be encrypted using SSL/TLS.
- The system should implement role-based access control (RBAC) to restrict administrative functions to authorized personnel only.
- Liveness detection should be incorporated to prevent spoofing attacks using fake fingerprints or 3D models.
- The system should automatically lock after three consecutive failed authentication attempts to prevent brute-force attacks.
- Users should be required to re-authenticate after a defined period of inactivity.
- The system must support secure remote access to prevent unauthorized controlof door locks.
- Regular security audits should be performed to identify and mitigate vulnerabilities.
- The system should comply with data privacy regulations to ensure user biometric information is securely stored and not misused.

Maintainability and Support

- The system should be modular in design, allowing easy updates and component replacements without affecting the entire system.
- Errorlogs should be stored for troubleshooting and diagnostic purposes.
- The system should have built-in self-diagnostics to detect and notify administrators about hardware malfunctions.
- Administrators should be able to reset user credentials and restore system configurations without system downtime.
- Software updatesshould be remotely deployable to address security vulnerabilities and system enhancements.
- Maintenance should require minimal effort, with clear documentation available for troubleshooting and upgrades.
- The system should automatically alert administrators about software or firmware updates.
- Fault-tolerant mechanisms should be in place to ensure that the system continues

operating even during minor failures.

Scalability and Extensibility

- The system should support scalability by accommodating an increasing number of registered users and stored biometric data.
- It should be possible to integrate additional authentication methods, such as facial recognition or iris scanning, in future updates.
- The system should be compatible with other security solutions, such as CCTV surveillance and access control software.
- The database should be designed to handle an increasing number of access logs and biometric records without performance degradation.
- The system should support the addition of new security policies and configurations without requiring significant architectural changes.
- Cloud-based storage options should be available for storing biometric data securely while ensuring scalability.
- The mobile application should support multiple platforms, including Android and iOS, for wider accessibility.

Reliability and Fault Tolerance

- The system should have a backup power supply to ensure continued operation during power outages.
- It should perform authentication even if the network connection is temporarily lost, ensuring offline access control.
- In the event of hardware failure, the system should fail safely, allowing emergency access while maintaining security.
- A redundant database system should be implemented to prevent data loss in case of unexpected failures.
- The system should perform regular backups to ensure data recovery in case of corruption or accidental deletions.
- The biometric scanner should maintain performance across varying environmental Conditions.

Compliance and Legal Requirements

- The system should comply with international security standards such as ISO 27001 for information security management.
- It must adhere to GDPR, CCPA, or other applicable data privacy laws regarding the collection and storage of biometric data.
- Users should be informed about how their biometric data is collected, stored, and used to ensure transparency.
- The system should provide an option for users to request the deletion of their biometric data in compliance with privacy regulations.
- The system should ensure that biometric data is not stored in plain text but rather in encrypted or hashed formats.
- Audit logs should be available for legal and compliance purposes, ensuring accountability and traceability.

Power and Energy Efficiency

- The system should consume minimal power to ensure efficiency, especially in battery-operated models.
- The biometric scanner should enter a low-power mode when idle to conserve energy.
- The backup battery should provide at least 24 hours of operation in case of power failure.
- The system should use energy-efficient components to reduce overall power consumption.

Environmental Considerations

- The biometric scanner should be resistant to dust, moisture, and temperature fluctuations for long-term durability.
- The system enclosure should be made from durable materials to withstand physical impact and environmental wear.
- The system should comply with electronic waste disposal regulations to ensure environmentally friendly disposal of outdated hardware.

The non-functional requirements of the biometric door locking system are essential in ensuring its reliability, security, usability, and maintainability. These requirements go beyond core functionalities to enhance the overall performance, scalability, and user experience. By meeting these standards, the system will provide a robust, efficient, and secure access control solution suitable for residential, commercial, and high-security environments. Implementing these non- functional requirements will ensure that the biometric door locking system operates seamlessly, remains secure, and meets the evolving needs of users and security compliance regulations.

Software Requirements

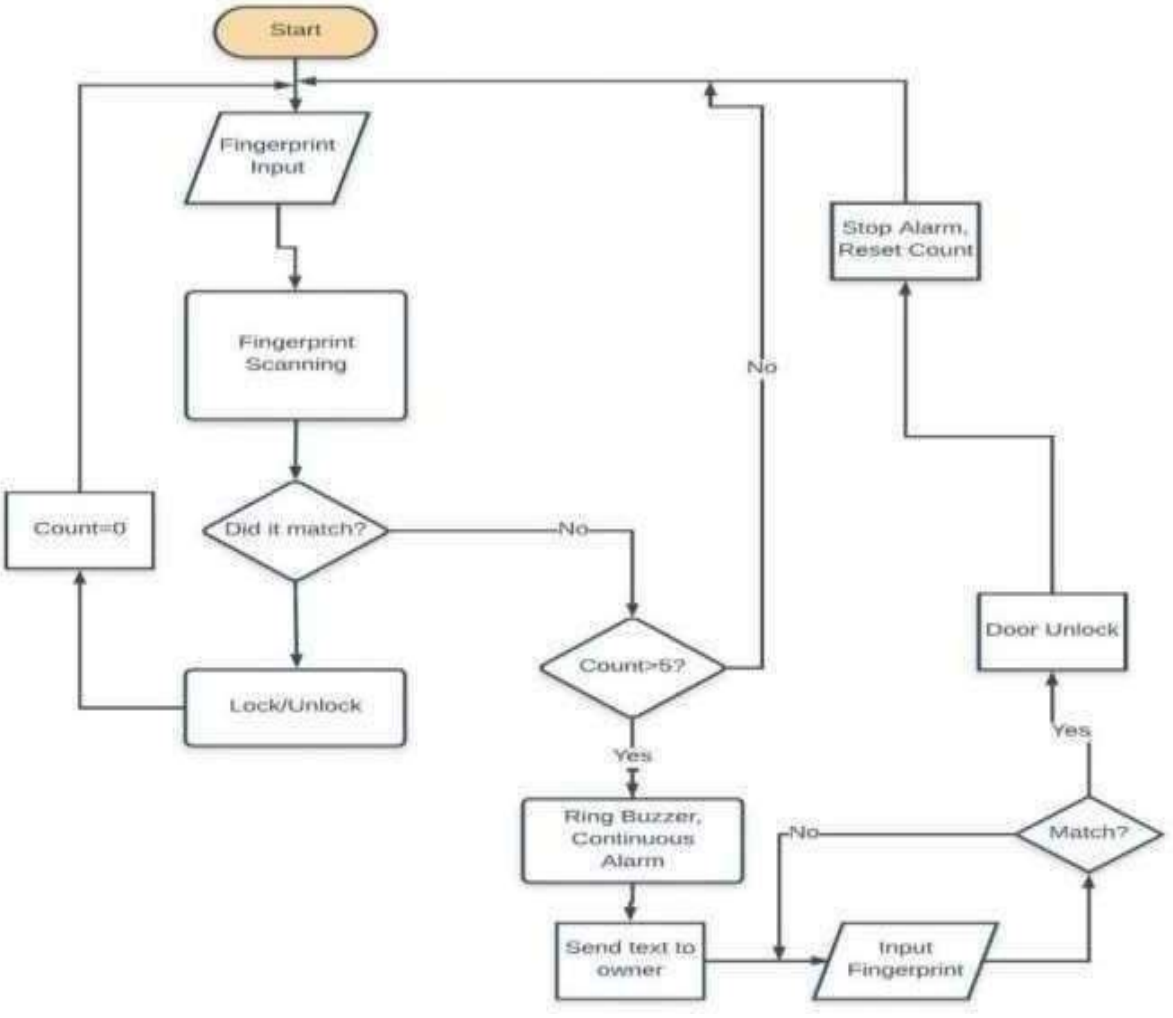
- Robust biometric data processing and storage
- Secure authentication algorithms
- User interface for managing access
- Integrationwith other security systems

CHAPTER-6

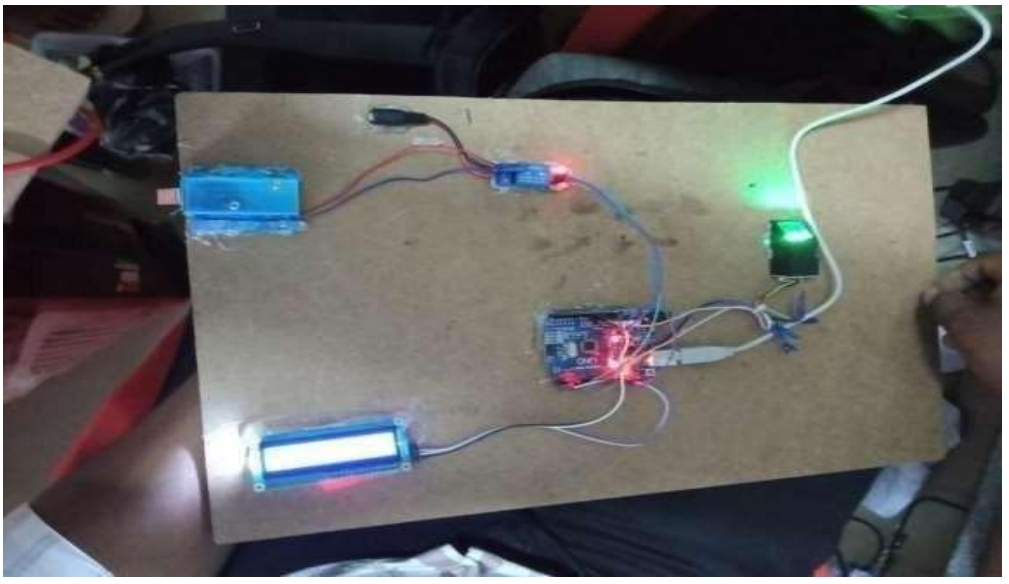
RESULTS

The Fingerprint door lock using Arduino, we are showing the components and connected them to the power supply. This system is based for improving the security which will register the owner's fingerprint into the Arduino using the fingerprint sensor, and this system we have given 5v power supply to Arduino through the code uploading wire. When you put your thumb on fingerprint sensor after registering yourself the lock will be unlocked and you repeat this process again then the solenoid lock will be got locked. The process of locking and unlocking requires less than 1second so this is why the Solenoid lock is used inside project

Figure:Flowchat



- After completing all the connections the system was powered up using the testing station of the university laboratory.
- 12v electricity was fed to the system.
- Then the fingerprint scanner started to illuminate it's green light.
- The lock was in a closed position.
- So,to test the functionality the finger was placed on the scanner,the fingerprint of which was already saved in the system.
- As the fingerprint matched, the lock will be opened.
- Then another finger was placed on the scanner which fingerprint was not saved before, then the lock will be remained lock.
- This way the functionality of the system was tested.



After the sensor is found then only the process is started. Later it shows like, ready to scan Place the finger and then we can give the access 0-127.Acess is given to 8 then to that finger only access is granted. It displays as Access Granted ID#8.In case of access is not granted then again it displays as ready to scan Place the finger.

CONCLUSION

The biometric door locking system with authentication represents a significant advancement in security and access control technology. Traditional locking mechanisms, such as mechanical keys and password-based authentication, have several vulnerabilities, including unauthorized duplication, theft, and hacking. The proposed system overcomes these challenges by integrating biometric fingerprint recognition, which provides a highly secure, reliable, and user-friendly method of authentication. By leveraging biometric technology, this system ensures that only authorized individuals can gain access, making it an ideal solution for residential, commercial, and institutional applications.

The primary objective of the biometric door locking system is to enhance security by eliminating the risks associated with traditional authentication methods. Fingerprint recognition is one of the most secure authentication techniques available because it is unique to each individual and cannot be easily replicated. The proposed system captures a user's fingerprint, extracts unique features, and compares them with stored biometric templates. If a match is found, access is granted; otherwise, access is denied. This process ensures that unauthorized users are prevented from gaining entry, reducing the risk of security breaches.

One of the key advantages of the proposed system is its ability to provide real- time authentication. Unlike traditional key-based or password-based systems that require users to carry physical keys or remember passwords, biometric authentication relies solely on an individual's fingerprint. This eliminates the risk of lost keys or forgotten passwords, providing a seamless and efficient access control solution. Additionally, the system is designed to be user- friendly, with an intuitive interface that allows for easy enrollment, authentication, and management of users.

The system also incorporates additional security measures, such as multi-factor authentication, real-time access logs, and intrusion detection alerts. Multi-factor authentication adds an extra layer of security by requiring users to verify their identity using a secondary method, such as a PIN code or RFID card. This feature enhances security by ensuring that even if an unauthorized individual gains access to a fingerprint, they will still need an additional form of authentication to enter.

Furthermore, the system maintains detailed access logs, allowing administrators to track entry attempts and monitor security activity in real time. If multiple unauthorized access attempts are detected, the system can trigger alerts and temporarily disable authentication to prevent brute-force attacks.

Power dependency is another consideration, as biometric systems require a continuous power supply to function effectively.The overall impact of the biometric door locking system is significant in terms of improving security and access control. Traditional security methods are becoming increasingly obsolete due to the rise in security threats and technological advancements. The proposed system provides a modern and secure alternative that enhances safety while maintaining user convenience. By integrating biometric authentication, real-time monitoring, and remote access control, the system offers a comprehensive security solution that meets the needs of various applications.

In conclusion, the biometric door locking system with authentication is a highly effective security solution that enhances access control by utilizing fingerprint recognition technology. While challenges such as false rejections, data privacy concerns, and power dependency exist, they can be effectively mitigated through advanced algorithms, secure data encryption, and backup power solutions. By implementing these measures, the biometric door locking system ensures a high level of security, accuracy, and reliability.

The future of security lies in biometric authentication, as it offers unparalleled security compared to conventional methods. With ongoing advancements in biometric technology, the proposed system has the potential to be further enhanced with features such as facial recognition, iris scanning, and AI-driven security analytics.Ultimately, the biometric door locking system represents a step forward in modern security solutions, providing a practical and effective way to enhance access control. Its implementation can significantly improve security standards across various sectors, making it an essential technology for the future of access management.

FUTURE SCOPE

The biometric door locking system with authentication represents a major step forward in security and access control. However, as technology continues to evolve, there are numerous opportunities for further development and improvement. The future scope of this system involves advancements in biometric authentication methods, integration with other smart security systems, increased automation, enhanced security features, and expanded applications across various industries. With continuous research and development, the system can become even more secure, efficient, and user-friendly, adapting to the changing needs of individuals and organizations.

One of the key areas of future development is the integration of multiple biometric authentication methods. While fingerprint recognition is highly secure, it is not foolproof. Factors such as injuries, dirt, or worn fingerprints can sometimes affect accuracy. To enhance reliability, future versions of the system can incorporate additional biometric authentication techniques, such as facial recognition, iris scanning, or voice recognition. A multi-biometric system would provide an extra layer of security, reducing the risk of unauthorized access and improving authentication accuracy.

Another important advancement is the use of artificial intelligence (AI) and machine learning (ML) algorithms in biometric authentication. AI can enhance fingerprint recognition by continuously learning and adapting to variations in fingerprint patterns over time. It can also detect spoofing attempts by analyzing skin texture, blood flow, or other unique characteristics. Additionally, AI-powered anomaly detection can identify unusual access patterns and trigger alerts in case of suspicious activities, further improving security.

The future of biometric door locking systems also lies in seamless integration with smart home and smart office technologies. As the Internet of Things (IoT) continues to grow, biometric authentication can be linked with home automation systems to control lighting, HVAC systems, and surveillance cameras based on user identity. For example, when an authorized user enters their home, the system could automatically adjust the lighting and temperature to their preferences. In an office environment, the system could be connected to employee attendance tracking, automatically logging working hours based on biometric authentication.

Incorporating cloud-based biometric authentication is another promising direction for future development. Cloud storage can allow users to access the system remotely and manage access permissions from anywhere. Cloud-based biometric databases can also enable cross-platform authentication, allowing users to use their biometric credentials across multiple locations or devices securely. However, strong encryption and data protection measures will be essential to ensure that biometric data remains secure and protected from cyber threats.

Enhancements in security measures will also play a crucial role in the future evolution of biometric door locking systems. Advanced encryption techniques, blockchain technology, and decentralized authentication mechanisms can further strengthen data security and prevent

unauthorized access. Implementing blockchain technology can ensure that biometric data is tamper-proof, providing an additional layer of protection against cyberattacks.

Another future possibility is the development of completely keyless entry systems that eliminate the need for physical backup keys or PIN codes. Advanced biometric sensors embedded in smartphones or wearables could be used for authentication, allowing users to unlock doors simply by approaching them. This concept could be extended to smart glasses or augmented reality (AR) devices that scan the user's biometric features for authentication.

The expansion of biometric authentication beyond door locking systems is another exciting area of exploration. This technology can be used for access control in various sectors, including banking, healthcare, and transportation. For example, biometric authentication can be integrated into ATMs to enable secure transactions without requiring a bank card or PIN. In hospitals, biometric access control can be used to restrict entry to sensitive areas, such as operating rooms or medication storage, ensuring that only authorized medical personnel can gain access. Similarly, biometric authentication can be employed in public transportation systems to allow seamless and secure ticketless travel.

The development of energy-efficient biometric systems is another important aspect of future research. As biometric door locking systems become more widespread, ensuring that they operate with minimal power consumption will be crucial. Researchers are exploring low-power biometric sensors that can function efficiently using solar energy or kinetic

energy from user interactions. Energy-efficient solutions will be particularly valuable for large-scale deployments in smart cities, where sustainability is a key concern.

Future iterations of the biometric door locking system can also incorporate voice-controlled authentication and natural language processing (NLP). Users could unlock doors by speaking a unique passphrase, adding another level of convenience to the authentication process. NLP technology can further improve security by analyzing voice patterns and detecting anomalies in real time.

One of the challenges that future biometric systems must address is the issue of privacy and data protection.Future biometric systems will need to comply with strict regulations, such as the General Data Protection Regulation (GDPR), to ensure that user data is stored and processed securely.The adaptability of biometric systems to different environments is another area of future research.

In conclusion, the future of biometric door locking systems is filled with exciting possibilities. From multi-biometric authentication and AI-powered security enhancements to IoT integration and cloud-based authentication, there are numerous ways in which this technology can evolve. Ensuring data privacy, improving energy efficiency, and expanding applications across various industries will be key focus areas for future development. As research and innovation continue, biometric authentication systems will become more secure, efficient, and versatile, revolutionizing the way access control and security are managed in homes, businesses and public spaces.

REFERENCES

1. Jain, A. K., Flynn, P., & Ross, A. (2007). Handbook of Biometrics. Springer.
2. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of Fingerprint Recognition. Springer.
3. Wayman, J. L., Jain, A. K., Maltoni, D., & Maio, D. (2005). Biometric Systems: Technology, Design and Performance Evaluation. Springer.
4. Ross, A., Nandakumar, K., & Jain, A. K. (2006). Handbook of Multibiometrics. Springer.
5. Ratha, N. K., & Bolle, R. M. (2003). Automatic Fingerprint Recognition Systems. Springer.
6. Mishra, P., & Gupta, P. (2019). Biometric Security and Privacy: Opportunities & Challenges in the Big Data Era. CRC Press.
7. Liu, S., Jiang, X., & Kot, A. C. (2014). Biometrics and Kanade-Lucas-Tomasi Feature Tracker for Human Authentication. IEEE Transactions on Information Forensics and Security.
8. Zhang, D. (2000). Automated Biometrics: Technologies and Systems. Kluwer Academic Publishers.

APPENDIX

```
#include <Adafruit_Fingerprint.h>
#include <LiquidCrystal_I2C.h>
#include <SoftwareSerial.h>
// Pins
#define RELAY_PIN 4            // Relay connected to pin 4
#define RX_PIN 2               // RX pin for fingerprint sensor
#define TX_PIN 3               // TX pin for fingerprint sensor
// LCD settings
LiquidCrystal_I2C lcd(0x27, 16, 2); // Set the LCD address to 0x27 for a 16 chars
and 2 line display
// Fingerprint sensor
SoftwareSerial mySerial(RX_PIN, TX_PIN); Adafruit_Fingerprint
finger = Adafruit_Fingerprint(&mySerial);
// Constants
const unsigned long DOOR_OPEN_TIME = 5000; // Door stays open for 5 seconds
// Variables
unsigned long doorOpenTime = 0; bool
doorOpen = false;
void setup() {
  // Initialize Serial Monitor
  Serial.begin(9600);  while
  (!Serial);
  // Initialize LCD
  lcd.init();
  lcd.backlight();
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Fingerprint  Lock");
  lcd.setCursor(0, 1);
  lcd.print("Initializing...");
  // Initialize fingerprint sensor
  finger.begin(57600);  delay(5);
  // Check if fingerprint sensor is found if
  (finger.verifyPassword()) {  lcd.clear();
    lcd.setCursor(0, 0); lcd.print("Sensor
    found!");
    Serial.println("Found  fingerprint  sensor!");
  } else {
    lcd.clear();
    lcd.setCursor(0, 0); lcd.print("Sensor
    not found");
    Serial.println("Did not find fingerprint sensor :("); while
    (1) { delay(1);  }
  }
  // Initialize  relay pin
  pinMode(RELAY_PIN,  OUTPUT);
```

```
digitalWrite(RELAY_PIN, HIGH); // Ensure door is locked initially
  // Display ready message
  delay(2000);
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Ready to scan");
  lcd.setCursor(0, 1);
  lcd.print("Place finger");

  // Printmenu
  printMenu();
}
void loop() {
  // Check if the door should be locked after the open time
  if (doorOpen && (millis() - doorOpenTime > DOOR_OPEN_TIME)) { lockDoor();
  }
// Check for commands from Serial Monitor if
  (Serial.available() > 0) {
    char command = Serial.read();

    switch (command) {
      case 'e': // Enroll a fingerprint
        enrollFingerprint();
        break;
      case 'd': // Delete a fingerprint
        deleteFingerprint();
        break;
      case '?': // Print menu
        printMenu();
        break;
    }
  }

  // Check for fingerprint scan if
  (!doorOpen) {
    int fingerprintID = getFingerprintID();
    if (fingerprintID != -1) {
      // Valid fingerprint detected
      lcd.clear();  lcd.setCursor(0,
      0);
      lcd.print("Access  Granted!");
      lcd.setCursor(0, 1); lcd.print("ID
      #"); lcd.print(fingerprintID);
      // Unlock the door
      unlockDoor();
    }
  }
```

```
delay(100); // Small delay to avoid excessive CPU usage
}

void printMenu() {
  Serial.println("\n========= Fingerprint Door Lock System =========");
  Serial.println("Commands:");
  Serial.println("e - Enroll a new fingerprint");
  Serial.println("d - Delete a fingerprint"); Serial.println("?
  - Print this menu");
  Serial.println("================================================");
}

void unlockDoor() {
  digitalWrite(RELAY_PIN, LOW); // Activate relay to unlock door
  doorOpen = true;
  doorOpenTime = millis();
  Serial.println("Door unlocked!");
}
void lockDoor() {
  digitalWrite(RELAY_PIN, HIGH); // Deactivate relay to lock door
  doorOpen = false; Serial.println("Door
  locked!");
  // Update LCD
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Ready to scan");
  lcd.setCursor(0, 1);
  lcd.print("Place finger");
}
int getFingerprintID() {
  uint8_t p = finger.getImage();
  if (p != FINGERPRINT_OK) return -1;
  p = finger.image2Tz();
  if (p != FINGERPRINT_OK) return -1;
while (true) {
    while (!Serial.available());
    // Get the ID from Serial Monitor id
    = Serial.parseInt();
    if (id > 0 && id < 128) {
      break;
    } else {
      Serial.println("ID must be between 1-127");
    }
  }

  Serial.print("Enrolling ID #");
```

```
Serial.println(id);

  // Update LCD lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Enrolling ID #");
  lcd.print(id);

  // Get the first fingerprint image
  while (getFingerprintEnroll(id, 1) != true);

  // Get the second fingerprint image while
  (getFingerprintEnroll(id, 2) != true);

  // Store the fingerprint in the database
  storeFingerprint(id);
  // Return to main state
  lcd.clear(); lcd.setCursor(0,
  0); lcd.print("Ready to
  scan"); lcd.setCursor(0, 1);
  lcd.print("Place finger");
}
bool getFingerprintEnroll(int id, int step) {
  int p = -1;
  if (step == 1) {
    lcd.setCursor(0, 1);
    lcd.print("Place finger");
    Serial.println("Place your finger on the sensor...");
  } else {
    lcd.setCursor(0, 1); lcd.print("Place
    same finger");
    Serial.println("Place same finger again...");
  }
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
      case FINGERPRINT_OK:
        Serial.println("Image taken");
        break;
      case FINGERPRINT_NOFINGER:
        Serial.print(".");
        break;
      case FINGERPRINT_PACKETRECIEVEERR:
        Serial.println("Communication error");
        break;
      case FINGERPRINT_IMAGEFAIL:
        Serial.println("Imaging error");
```

```
break;
      default:
        Serial.println("Unknown error");
        break;
    }
  }

  // OK success!
  p = finger.image2Tz(step);
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image converted"); break;
    case FINGERPRINT_IMAGEMESS:
      Serial.println("Image too messy");
      return false;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Communication error");
      return false;
    case FINGERPRINT_FEATUREFAIL:
      Serial.println("Could not find fingerprint features");
      return false;
    case FINGERPRINT_INVALIDIMAGE:
      Serial.println("Could not find fingerprint features");
      return false;
default:
      Serial.println("Unknown error");
      return false;
  }
  if (step == 1) {
    Serial.println("Remove finger");
    lcd.setCursor(0, 1);
    lcd.print("Remove finger  ");
    delay(2000);
  }
  return true;
}

void storeFingerprint(int id) { int
  p = finger.createModel();
  if (p == FINGERPRINT_OK) {
    Serial.println("Prints matched!");
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Communication error");
    return;
  } else if (p == FINGERPRINT_ENROLLMISMATCH) {
    Serial.println("Fingerprints did not match");
    lcd.setCursor(0, 1);
```

```
lcd.print("Prints didn't match");
delay(2000);
     return;
   } else {
    Serial.println("Unknown error");
    return;
   }
  p = finger.storeModel(id);
  if (p == FINGERPRINT_OK) {
    Serial.println("Fingerprint stored!");
    lcd.setCursor(0, 1);
    lcd.print("Fingerprint stored");
delay(2000);
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Communication error");
    return;
  } else if (p == FINGERPRINT_BADLOCATION) {
    Serial.println("Could not store in that location");
    return;
  } else if (p == FINGERPRINT_FLASHERR) {
    Serial.println("Error writing to flash"); return;
 } else {
    Serial.println("Unknown error");
    return;
 }
}
void deleteFingerprint() {
  int id = 0;
  Serial.println("Please type in the ID # (1-127) you want to delete...");

  while (true) {
    while (!Serial.available());
    // Get the ID from Serial Monitor id
    = Serial.parseInt();
    if (id > 0 && id < 128) {
      break;
    } else {
      Serial.println("ID must be between 1-127");
    }
  }
  Serial.print("Deleting ID #");
  Serial.println(id);
// Update LCD
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Deleting ID #");
```

```
  lcd.print(id);

  uint8_t p = finger.deleteModel(id);
  if (p == FINGERPRINT_OK) {
    Serial.println("Fingerprint deleted!");
    lcd.setCursor(0, 1); lcd.print("Fingerprint
    deleted"); delay(2000);
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Communication error");
  } else if (p == FINGERPRINT_BADLOCATION) {
    Serial.println("Could not delete from that location");
  } else if (p == FINGERPRINT_FLASHERR) {
    Serial.println("Error writing to flash");
  } else {
    Serial.print("Unknown error: 0x"); Serial.println(p, HEX);
  }

  // Return to main state
  lcd.clear(); lcd.setCursor(0,
  0); lcd.print("Ready to
  scan"); lcd.setCursor(0, 1);
  lcd.print("Place finger");
}
```

NRI INSITUTE OF TECHNOLOGY

DEPARTMENTS OF ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE OUTCOMES

COURSE CODE	COURSE OUTCOMES	Taxonomy
C426.1	Apply Subject Knowledge for given problem	Apply(L3)
C426.2	Understand the existed work done and extend by incorporating the novelty for proposed work	Understand(L2)
C426.3	Divide the work and execute consolidate it for given project	Evaluate(L5)
C426.4	Perform calculations analyze the results and provide solutions	Analyze(L4)
C426.5	Develop or design and simulate system for a given project	Evaluate(L5)
C426.6	Able to present and write a thesis	Remember(L1)

PROJECT MEMBERS

M.NAVYAKA 22KP5A0411
P.VANAJA 21KP1A0488
A.SANJAY 22KP5A0417
P.KAVITHA 21KP1A04A0

NRI INSTITUTE OF TECHNOLOGY

DEPARTMENT OF ELECTRONICS &COMMUNICATION ENGINEERING

CO-PO MAPPING

Class: IV B. Tech, ECE-B Academic Year:2024–25

PROJECT TILE: SMART SECURITY SYSTEM BASED ON BIOMETRIC

1. Student Name:
    1. M.NAVYAKA
    2. P.VANAJA
    3. A.SANJAY
    4. P.KAVITHA.
2. Name Of Guide: Ms.E.V.SANTHI

Page	Activity description	CO mapped	PO mapped
1	Student an abstract for: SMART SECURITY SYSTEMBASED ON BIOMETRIC	C426.2	PO1,PO2, PO 4
2-16	Introduction of the project	C426.6	PO3,P05
17-26	. Literature Survey	C426.1	PO1,PO2
27-31	Existing System	C426.6	PO4
. 32-38	Proposed System	C426.5	PO5
39-49	Software and Hardware Requirements	C426.4	PO3,PO5
50-54	Results	C426.3	PO3,PO4,PO6
55-57	Future Scope	C426.6	PO7,PO3,PO6
58-65	Refer and collect information from latest journals	C426.5	PO3PO6,

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
Project	3	3	3	3	3	3	2	2	3	3	3	3	3	3	2

SIGNATURE OF STUDENT SIGNATURE OF GUIDE

SMART SECURITY SYSTEM BASED ON BIOMETRIC

[1]E.V. Santhi, [2]Dr. K. Sri Hari Rao, [3]M. Navyaka, [4]P.Vanaja, [5]A. Sanjay [6]P. Kavitha
[1]Assistant Professor, Department of ECENRI Institute of Technology, Visadala ,Guntur, Andhra Pradesh
[2]Professor and HoD, Department of ECE, NRI Institute of Technology, Visadala,Guntur, Andhra Pradesh
[3,4,5,6]B.Tech Scholars, Department of ECE, NRI Institute of Technology, Visadala ,Guntur, Andhra Pradesh

Abstract: A biometric door locking system is an advanced security solution designed to improve access control by utilizing unique biological characteristics such as fingerprints, facial recognition, or iris scans. Unlike traditional locks that depend on keys or passwords, which can be lost, stolen, or duplicated, biometric authentication provides a significantly higher level of security. Since biometric data is unique to each individual and difficult to forge, this technology ensures that only authorized users can gain access, thereby reducing the risks associated with unauthorized entry and enhancing overall safety. The system functions by capturing and securely storing the biometric information of authorized individuals. When an access attempt is made, the system scans the provided biometric data and compares it with the stored records. If a match is detected, the door unlocks; otherwise, access is denied. Modern biometric door locking systems are designed to integrate with smart technology, enabling features such as remote monitoring, real-time access tracking, and seamless compatibility with home automation or corporate security infrastructures. To enhance reliability, these systems often include backup power supplies, multi-factor authentication, and emergency access options. These systems are widely adopted in residential, commercial, and institutional environments where security is a top priority. They offer greater convenience by eliminating the need for physical keys or memorizing passwords. Additionally, continuous advancements in biometric technology have improved the accuracy, speed, and affordability of these systems, making them more accessible to a wider range of users. However, certain challenges remain, including concerns over data privacy, the risk of spoofing attempts, and the impact of environmental factors on biometric recognition. Despite these challenges, biometric door locking systems continue to advance, providing a highly efficient and secure solution for modern access control needs.

Keywords: Biometric Door Locking System, Advanced Security, Remote Monitoring, Real-Time, Accuracy, Speed, Data Privacy.

I. INTRODUCTION

Security is a fundamental concern in both residential and commercial settings, leading to the development of advanced access control systems. One such innovation is the biometric door locking system, which enhances security by using unique biological traits such as fingerprints, facial recognition, or iris scans. Unlike traditional locks that rely on physical keys or passwords, which can be lost, stolen or duplicated, biometric systems offer a more secure and convenient alternative. This technology ensures that only authorized individuals can gain entry, significantly reducing the risk of unauthorized access.

Biometric door locking systems operate by capturing and storing the biometric data of registered users. When a person requests access, the system scans the provided biometric input and compares it to the stored database. If a match is found, the door unlocks; otherwise, access is denied. These systems are designed to provide a seamless and efficient authentication process, reducing the reliance on physical keys or codes that can be compromised. With advancements in biometric recognition, these systems now offer high accuracy, speed and reliability.

One of the major benefits of biometric door locks is their integration with smart technology. Many modern systems support remote access, real-time monitoring and automated security logs, allowing users to track entry and exit records effortlessly. Additionally, these systems can be incorporated into broader security frameworks, such as home automation systems or corporate security networks. To enhance reliability, biometric locks often include backup power supplies, multi-factor authentication, and emergency override options, ensuring functionality even in critical situations.

The growing adoption of biometric door locking systems is driven by their ability to provide both security and convenience. They are widely used in residential buildings, corporate offices, government institutions, and high-security facilities. These systems eliminate the need for physical keys and password memorization, making them user-friendly while maintaining a high level of protection. As biometric technology continues to advance, these systems are becoming more accessible and affordable, further encouraging their widespread use.

Despite their many advantages, biometric door locking systems do come with challenges. Concerns about data privacy, potential spoofing attempts, and environmental factors affecting biometric recognition must be addressed to ensure their effectiveness. However, ongoing research and technological advancements are continuously improving the security and reliability of these systems. As a result, biometric door locks remain a cutting-edge solution for modern access control, providing an efficient, secure, and convenient way to protect homes, businesses, and institutions.

II. LITERATURE SURVEY

R. Bhardwaj, R. Kothiyal and S. Sharma et al. Security is a process; it's an ongoing endeavor to keep one step ahead of threats and safeguard what matters most. Security is not a product. Everybody can find shelter in a home, which offers a sense of security and stability. Its security is crucial for defending belongings against potential dangers including break-ins and burglaries, which may increase the risk of theft, burglary, and property damage, resulting in financial and emotional suffering. In this study, we analyze these issues, pinpoint potential remedies, and offer predictions about the development of smart home security. In order to improve the safety and security of houses more effectively than some of the current accessible alternatives, an effective home security system technology is a crucial first step. This investigation assesses the

current state of IoT security, identifies the issues encountered, and proposes workable solutions in order to increase the security of IoT systems and devices. A person is found using a PIR motion sensor. The YOLO method is used to identify the images that are captured by the camera module. Depending on the circumstance, electromagnetism is opened using a Raspberry Pi. The user is received the last notification regarding cloud-based door opening [1].

M. A. Khan et al. Biometric-based digital door locking system plays a significant role in providing authentication, reducing the workforce in smart homes, and building automation scenarios. This paper proposes a prototype model of an IoT-based Smart Door Locking System (SDLS) with reliable double-access authentication. The IoT and biometric technology authentication mechanism is adopted to make SDLS more secure and reachable with the alert mechanism on unauthorized access. The SDLS contains a biometric scanner, and a thumb impression is made either from a mobile or a biometric-mounted device on the door and both are connected to the centralized cloud-hosted real-time database. The proposed system was tested in real-time and has shown competitive results compared to other Radio-Frequency Identification (RFID) and password-based door locks. Hence, the overall performance efficiency of SDLS is satisfactory and provides biometric-based remote access to control and monitor door locks with the alert system on unauthorized access [2].

T. H. L. Nguyen and T. T. H. Nguyen et al. In traditional Public Key Infrastructure (PKI) system, Private Key could be stored in central database or store distributed in smart-card and delivered to the users. The Private Key is usually protected by passwords that are easily guessed or stolen and thus lead to the collapse of the whole system. Current trend for PKI system is based on physiological and behavioral characteristics of persons, known as biometrics. This approach can increase the security of Private Key because in theory, the biometric features could not be guessed or forged. However, this approach still reveals a gap that is the vulnerability of storage device of Private Key and biometrics data. Malefactors can attack directly to these storage devices and steal user identification information. In this paper, we propose a solution that uses Biometric Encryption Key (BEK) to encrypt Private Key and protect Private Key in a secure way for both of two these kind of information. We also present the BEK generation algorithm and the BioPKI system to support this solution and then we illustrate the experimental results [3].

D. B, N. K. Mathala, S. A and I. K et al. As smart home technology becomes more and more common, there is an increasing demand for user identification techniques that are both secure and energy-efficient. This study highlights the energy economy while introducing a novel automatic fingerprint security system for smart home applications. To increase security, the suggested solution uses a fingerprint scanner. Users may control various appliances and gadgets via a website or

mobile app. By activating smart appliances based on user identification, the system actively helps energy saving and offers sophisticated security features, such as room-specific access and emphasizing user-centricity. The project includes both software and hardware elements, including a MongoDB database, Raspberry Pi microcontroller, fingerprint reader, and web based React JS control interface. Thorough testing and assessment confirm the system's ability to detect reliably [4].

A. Saroha, A. Gupta, A. Bhargava, A. K. Mandpura and H. Singh et al. The trend towards smart cities that use devices based on IOT has been rapidly adopted across the globe. The devices in the smart cities are connected to database and key features include convenience, economical, and most importantly secure. In this paper a biometric authentication based automated secure and smart IOT door lock is developed. The access to authorized user is accomplished by face recognition. Further a provision for passcode based authentication and access has also been incorporated. The proposed door lock takes care of the user comfort by eliminating the need of carrying keys or RFID cards. An email and app based notification system is also incorporated that collects the data and also informs and alerts the end user [5].

R. J. Prarthana, A. M. Dhanzil, N. I. Mahesh and S. Raghul et al. Internet of Things (IoT) have revolutionized the entire way in which the industry operates. The authenticity and entry access to certain places of the industry plays a crucial role in maintaining the secrecy of the operations. Therefore providing limited access to such confidential places proves to be seemingly vital. The proposed work provides a dual security mechanism against unauthorized entry and hence enhances the integrity of the system. This system thus eradicates the common security threats such as Spoofing, Repudiation and trafficking from evaders especially in the current scenario of industry 4.0. This system uses two techniques for the controlled access. One via a fingerprint access that utilizes the raspberry pi3 and a biometric database system for control. This method is a thorough hardware based solution and could be utilized when there is a physical presence of a person. In case if the authenticator is not available in the arena, the alternate mechanism would be followed to provide a secured access authenticity through Virtual Point Network (VPN) & IoT. The utility of VPN facilitates the personnel to prove his / her credentials from any remote location. Thus this dual mode system provides a highly credential entry / exit system in an industrial arena [6].

R. Bakhteri and M. K. Hani et al. This paper discusses a biometric encryption system using fuzzy vault scheme implemented on FPGA development board. Cryptographic algorithms are very secure overall but have a weak point in terms of the storage of the crypto keys. Biometric authentication systems have many exploitable weak points that can be used to compromise the system. Biometric encryption is a security scheme that combines strong cryptographic algorithms with biometric authentication to provide better security. This paper discusses a simple implementation of a biometric encryption system as a stand-alone

embedded device. Fuzzy vault scheme is used as the method to bind the crypto key and biometrics. The system processes were implemented as software blocks run on the firmware [7].

III. METHODOLOGY

The implementation of a biometric door locking system follows a structured methodology to ensure security, efficiency, and reliability. This process involves multiple stages, including data acquisition, storage, authentication, system integration, and security measures. By leveraging advanced biometric recognition techniques, the system provides a robust and seamless access control solution. The methodology focuses on accuracy, speed, and ease of use while ensuring the protection of biometric data against unauthorized access.

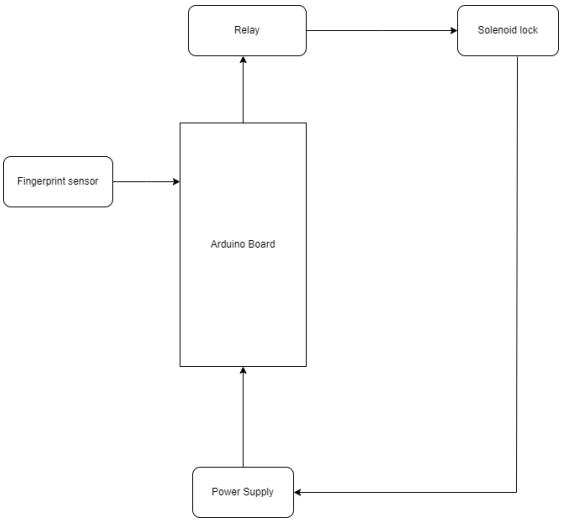


Fig. 1: Block Diagram

The biometric data acquisition, where the system captures unique biological traits such as fingerprints, facial features, or iris patterns from authorized users. Specialized biometric sensors, including fingerprint scanners, cameras, or infrared sensors, are used to collect high-quality data. This data is then processed and converted into a digital template, ensuring that only distinctive and identifiable features are stored for authentication purposes.

Once the biometric data is captured, it is securely stored and encrypted within the system's database. Encryption techniques, such as hashing or tokenization, are applied to protect stored templates from unauthorized access or duplication. Cloud-based or local storage solutions can be used depending on security requirements. Additionally, data compression and optimization techniques help improve storage efficiency while maintaining accuracy. The system also implements strict data access controls to prevent potential security breaches.

The authentication process involves biometric verification and access control mechanisms. When a user attempts to unlock the door, the system scans the provided biometric input and compares it with the stored templates. Advanced matching algorithms analyze the biometric data, verifying whether it belongs to an authorized user. If a match is found, access is granted, and the door unlocks. If authentication fails, the system denies entry and may trigger security alerts. To enhance accuracy, multi-factor authentication (MFA) can be implemented, combining biometrics with PIN for added security.

To ensure system reliability and security, biometric door locking systems incorporate additional safeguards such as backup power supplies, fail-safe mechanisms, and

emergency access options. In case of power failure or sensor malfunctions, alternative authentication methods, such as mechanical keys or administrator overrides, can be used. Additionally, the system is regularly updated with improved algorithms and security patches to prevent vulnerabilities. By following this methodology, biometric door locking systems provide a high level of security, convenience, and efficiency for modern access control applications.

IV. RESULTS

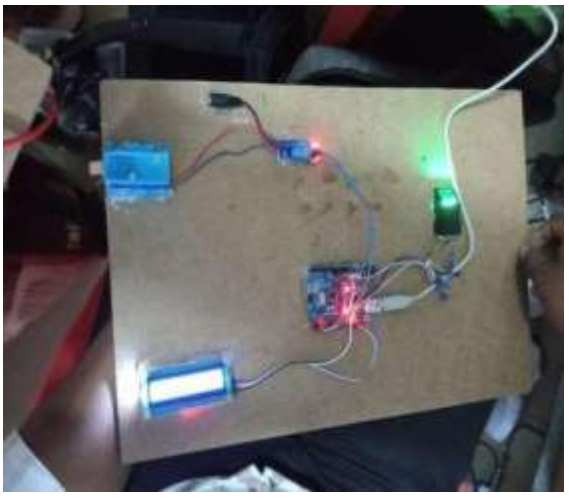


Fig. 2: Hardware Implementation

Fig. 3: Output Display's

V. CONCLUSION

Biometric door locking systems offer a highly secure and convenient solution for modern access control by utilizing unique biological traits for authentication. Their integration with smart technology, along with features like remote monitoring and multi-factor authentication, enhances their reliability and effectiveness. While challenges such as data privacy concerns and environmental factors affecting biometric recognition persist, continuous advancements in biometric technology are improving accuracy, security, and affordability. As these systems continue to evolve, they are becoming an essential component of residential, commercial, and institutional security, providing a robust and efficient means of safeguarding access.

VI. REFERENCES

[1] R. Bhardwaj, R. Kothiyal and S. Sharma, "Automated Smart Home Security System Using Biometric Solution," 2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA), Pune, India, 2023, pp. 1-6, doi: 10.1109/ICCUBEA58933.2023.10392199.

[2] M. A. Khan et al., "Prototype Model of an IoT-based Digital and Smart Door Locking System with Enhanced Security," 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2022, pp. 1-7, doi: 10.1109/MACS56771.2022.10023385.

[3] T. H. L. Nguyen and T. T. H. Nguyen, "An approach to protect Private Key using

fingerprint Biometric Encryption Key in BioPKI based security system," 2008 10th International Conference on Control, Automation, Robotics and Vision, Hanoi, Vietnam, 2008, pp. 1595-1599, doi: 10.1109/ICARCV.2008.4795763.

[4] D. B, N. K. Mathala, S. A and I. K, "Secure and Energy-Efficient Smart Home Automation: A User-Based Fingerprint Security System," 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), Krishnankoil, Virudhunagar district, Tamil Nadu, India, 2024, pp. 1-6, doi: 10.1109/INCOS59338.2024.10527495.

[5] A. Saroha, A. Gupta, A. Bhargava, A. K. Mandpura and H. Singh, "Biometric Authentication Based Automated, Secure, and Smart IOT Door Lock System," 2022 IEEE India Council International Subsections Conference (INDISCON), Bhubaneswar, India, 2022, pp. 1-5, doi: 10.1109/INDISCON54605.2022.9862840.

[6] R. J. Prarthana, A. M. Dhanzil, N. I. Mahesh and S. Raghul, "An Automated Garage Door and Security Management System (A dual control system with VPN IoT & Biometric Database)," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 1468-1472, doi: 10.1109/ICECA.2018. 8474630.

[7] R. Bakhteri and M. K. Hani, "Biometric encryption using fingerprint fuzzy vault for FPGA-based embedded systems," TENCON 2009 - 2009 IEEE Region 10 Conference, Singapore, 2009, pp. 1-5, doi: 10.1109/TENCON.2009.5396047.

[8] Oscar Olazabal, Mikhail Gofman, Yu Bai, Yoonsuk Choi, Noel Sandico, Sinjini Mitra, et al., "Multimodal biometrics for enhanced iot security", 2019 IEEE 9th annual computing and communication workshop and conference (CCWC), pp. 0886-0893, 2019.

9 Billy Indrawan, Deanova Ghivari Alzamora, Muhammad Shiddiq Rahmatullah and Alief Wikarta, "Facial Recognition-Based Automatic Door Security System Integrated with Internet of Things for Smart Home Actualization", Recent Advances in Mechanical Engineering: Select Proceedings of ICOME 2021, pp. 360-368, 2022.

10 M. Chamath Hettiarachchi, WC Dilshan Abeysiriwardhana, AMR Eshandi Aththanayaka, L. Dinithi Panangala, Chandimal Jayawardena and Isuri Udara, "A Secure and Intelligent Smart Home Controlling System", 2022 3rd International Informatics and Software Engineering Conference (IISEC), pp. 1-6, 2022.

[11] Al Rakib, Md Abdullah, Md Moklesur Rahman, Salah Uddin, Md Shamsul Alam Anik, ABM Hasan Talukder, et al., "Fingerprint Based Smart Home Automation and Security System", European Journal of Engineering and Technology Research, vol. 7, no. 2, pp. 140-145, 2022.

[12] Olutosin Taiwo, Absalom E. Ezugwu, Olaide N. Oyelade and Mubarak S. Almutairi, "Enhanced intelligent smart home control and security system based on deep learning model", Wireless communications

and mobile computing, no. 2022, pp. 1-22, 2022.

[13] Nicolae-Gabriel Vasilescu, Paul Pocatilu and Mihai Doinea, "Io'T Security Challenges for Smart Homes", Education Research and Business Technologies: Proceedings of 21 st International Conference on Informatics in Economy (lE 2022), pp. 41-49, 2023.

[14] Vijender Singh and Chander Kant, "Biometric-Based Authentication in Internet of Things (loT): A Review", Advances in Information Communication Technology and Computing: Proceedings of AICTC 2021, pp. 309-317, 2022.

[15] Shagun Singh Dasawat and Sachin Sharma, "Cyber Security Integration with Smart New Age Sustainable Startup Business Risk Management Automation and Scaling System for Entrepreneurs: An Artificial Intelligence Approach", 2023 7th International Conference on Intelligent Computing and Control Systems (lCICCS), pp. 1357-1363, 2023.

[16] Shreya Aggarwal and Sachin Sharma, "Voice Based Deep Learning Enabled User Interface Design For Smart Home Application System", 2021 2nd International Conference on Communication Computing and Industry 4. 0 (C2I4), pp. 1-6, 2021.

[17] Sachin Sharma, Abhinav Sharma, Tanya Goel, Rohan Deoli and Seshadri Mohan, "Smart Home Gardening Management System: A Cloud-Based Internet-of-Things (loT) Application in VANET", 2020 11 th International Conference on Computing Communication and Networking Technologies (lCCCNT), pp. 1-5, 2020.

[18] A. S Falohun, E.O. Omidiora, O.A. Fakolujo, O, A. Afolabi, A.O. Oke and F.A. Ajala, "Development of a biometrically-controlled door system (using iris) with power backup", American Journal of Scientific and Industrial Research, vol. 3, no. 4, pp. 203-207, 2012.

Ms. E. V. SANTHI has 11 years of teaching experience. Obtained B.Tech degree and M.Tech degree from JNTU Hyderabad. she is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering, NRI Institute of Technology, Visadala, Guntur District. She has taught courses for UG students and guided several projects. She has published 1 Book and 6 papers in National / International Conferences, Journals. She is a Life Member in IFERP, IAENG. Mail ID: vsanthi10@gmail.com

K. Srihari Rao completed B. Tech at V.R Sidhartha Engineering College Vijayawada, M. Tech from P.S.G college of Technology, Coimbatore and Ph.D from Andhra University. He has 35 years of Teaching experience and working as professor and HOD at NRI Institute of Technology, Visadala, Guntur, AP. He has published 3 papers in international journals and 40 papers in national and international conferences. He has 2 patents. Mail Id: ksrihariraoece@gmail.com

M. Navyaka is currently pursuing B. Tech final year in the department of ECE at NRI Institute of Technology, Visadala, Guntur, Andhra Pradesh.

P. Vanaja is currently pursuing B. Tech final year in the department of ECE at NRI Institute of Technology, Visadala, Guntur, Andhra Pradesh.

A. Sanjay is currently pursuing B. Tech final year in the department of ECE at NRI Institute of Technology, Visadala, Guntur, Andhra Pradesh.

P. Kavitha is currently pursuing B. Tech final year in the department of ECE at NRI Institute of Technology, Visadala, Guntur, Andhra Pradesh.

Journal of Interdisciplinary Cycle Research
An UGC-CARE Approved Group - A Journal
An ISO : 7021 - 2008 Certified Journal
ISSN NO: 0022-1945 / web : http://jicrjournal.com / e-mail: submitjicrjournal@gmail.com

Certificate of Publication

This is to certify that the paper entitled

SMART SECURITY SYSTEM BASED ON BIOMETRIC

Authored By

E.V. Santhi

From

Assistant Professor, Department of ECENRI Institute of Technology, Visadala ,Guntur, Andhra Pradesh

Has Been Published in

JICR JOURNAL, Volume XVII, Issue 04, April/2025

Dr. R. Rezwana Begum, Ph.D Editor-In-Chief
JICR JOURNAL

6.2 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008

Journal of Interdisciplinary Cycle Research
An UGC-CARE Approved Group - A Journal
An ISO : 7021 - 2008 Certified Journal
ISSN NO: 0022-1945 / web : http://jicrjournal.com / e-mail: submitjicrjournal@gmail.com

Certificate of Publication

This is to certify that the paper entitled

SMART SECURITY SYSTEM BASED ON BIOMETRIC

Authored By

Dr. K. Sri Hari Rao

From

Professor and HoD, Department of ECE, NRI Institute of Technology, Visadala,Guntur, Andhra Pradesh

Has Been Published in

JICR JOURNAL, Volume XVII, Issue 04, April/2025

Dr. R. Rezwana Begum, Ph.D Editor-In-Chief
JICR JOURNAL

6.2 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008

Journal of Interdisciplinary Cycle Research
An UGC-CARE Approved Group - A Journal
An ISO : 7021 - 2008 Certified Journal
ISSN NO: 0022-1945 / web : http://jicrjournal.com / e-mail: submitjicrjournal@gmail.com

Certificate of Publication

This is to certify that the paper entitled

SMART SECURITY SYSTEM BASED ON BIOMETRIC

Authored By

M. Navyaka

From

B.Tech Scholars, Department of ECE, NRI Institute of Technology, Visadala ,Guntur, Andhra Pradesh

Has Been Published in

JICR JOURNAL, Volume XVII, Issue 04, April/2025

Dr. R. Rezwana Begum, Ph.D Editor-In-Chief
JICR JOURNAL

6.2 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008

Journal of Interdisciplinary Cycle Research
An UGC-CARE Approved Group - A Journal
An ISO : 7021 - 2008 Certified Journal
ISSN NO: 0022-1945 / web : http://jicrjournal.com / e-mail: submitjicrjournal@gmail.com

Certificate of Publication

This is to certify that the paper entitled

SMART SECURITY SYSTEM BASED ON BIOMETRIC

Authored By

P. Vanaja

From

B.Tech Scholars, Department of ECE, NRI Institute of Technology, Visadala ,Guntur, Andhra Pradesh

Has Been Published in

JICR JOURNAL, Volume XVII, Issue 04, April/2025

Dr. R. Rezwana Begum, Ph.D Editor-In-Chief
JICR JOURNAL

6.2 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008

Journal of Interdisciplinary Cycle Research
An UGC-CARE Approved Group - A Journal
An ISO : 7021 - 2008 Certified Journal
ISSN NO: 0022-1945 / web : http://jicrjournal.com / e-mail: submitjicrjournal@gmail.com

Certificate of Publication

This is to certify that the paper entitled

SMART SECURITY SYSTEM BASED ON BIOMETRIC

Authored By

A. Sanjay

From

B.Tech Scholars, Department of ECE, NRI Institute of Technology, Visadala ,Guntur, Andhra Pradesh

Has Been Published in

JICR JOURNAL, Volume XVII, Issue 04, April/2025

Dr. R. Rezwana Begum, Ph.D Editor-In-Chief
JICR JOURNAL

6.2 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008

Journal of Interdisciplinary Cycle Research
An UGC-CARE Approved Group - A Journal
An ISO : 7021 - 2008 Certified Journal
ISSN NO: 0022-1945 / web : http://jicrjournal.com / e-mail: submitjicrjournal@gmail.com

Certificate of Publication

This is to certify that the paper entitled

SMART SECURITY SYSTEM BASED ON BIOMETRIC

Authored By

P. Kavitha

From

B.Tech Scholars, Department of ECE, NRI Institute of Technology, Visadala ,Guntur, Andhra Pradesh

Has Been Published in

JICR JOURNAL, Volume XVII, Issue 04, April/2025

Dr. R. Rezwana Begum, Ph.D Editor-In-Chief
JICR JOURNAL

6.2 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008