Thakur Educational Trust's (Regd.)
THAKUR COLLEGE OF SCIENCE & COMMERCE
AUTONOMOUS COLLEGE PERMANENTLY AFFILIATED TO UNIVERSITY OF MUMBAI
NAAC Accredited Grade 'A' (3rd Cycle) & ISO 9001: 2015 (Certified)

A PROJECT REPORT ON

Design of Embedded Security Door Lock System

SUBMITTED BY

Prajwal Poojary (22751)

Bhavik Bhanushali (22764)

Shikha Karia(22766)

MARCH – 2023

UNDER THE GUIDANCE OF ASST.

PROF. NEENU JOHNSON

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR QUALIFYING

B.SC.-(I.T.), SEMESTER - VI EXAMINATION

Thakur College of Science and Commerce,
Kandivali, Mumbai

2022-2023

Thakur College of Science & Commerce Project Certificate

This is to certify that the project entitled **Design of Embedded Security Door Lock System** is undertaken at the Thakur College of Science and Commerce by Prajwal Poojary (Roll No. 22751),Bhavik Bhanushali(Roll No.22764) and Shikha Karia(Roll no.22766) in partial fulfilment of BSc (IT) degree, Semester 6 Examination has not been submittedfor any other examination and does not form part of any other course undergone by the candidates.

_____	_____
Signature	Signature
External Examiner	Internal Examiner
_____	_____
Signature	Signature
Project Guide	HOD/In-charge/Co-ordinator

Table of Contents:

Introduction

Introduction:

The biometric door lock system using a fingerprint sensor and Arduino Uno board is a security system that allows access to a locked door only to authorized personnel whose fingerprints have been enrolled in the system. This system uses a fingerprint sensor to capture the fingerprint of the user, which is then compared to the stored fingerprints in the system's database. If there is a match, the system unlocks the door, and the user can enter. If there is no match, the system denies access to the user.

The Arduino Uno board is a popular microcontroller board that is easy to program and widely available. It is an ideal choice for this project as it can interface with the fingerprint sensor and control the locking mechanism of the door. The fingerprint sensor can be connected to the board via serial communication, and the code can be written in Arduino's programming language.

The system consists of a fingerprint sensor, an Arduino Uno board, and a locking mechanism. The microcontroller board interfaces with the fingerprint sensor to capture and compare fingerprints and controls the locking mechanism to unlock the door when there is a match. The locking mechanism can be a custom-designed mechanism or an existing one modified to work with the system.

There have been many advancements in biometric technology over the years, with improvements in accuracy and speed of recognition. There have also been concerns about privacy and security, particularly with the storage and use of biometric data.

There have been many projects and research efforts focused on biometric door locking systems, including the development of new hardware and software solutions, as well as studies on the effectiveness and usability of these systems.

Objectives:

- Provide a secure and convenient access control system: The primary objective of the project is to develop a secure and convenient access control system using biometric technology that ensures only authorized individuals can gain access to a restricted area.
- Use fingerprint recognition technology: The project aims to use fingerprint recognition technology to authenticate and verify the identity of the user. This technology is reliable, accurate, and difficult to spoof, making it an ideal choice for security systems.
- Develop an affordable and easy-to-implement system: The project aims to develop a system that is affordable, easy to implement, and can be customized to meet specific needs. The use of the Arduino Uno board provides a cost-effective and flexible platform for developing such a system.
- Develop a user-friendly system: The system should be easy to use and require minimal user input. This objective is achieved by using a fingerprint sensor that eliminates the need for users to carry access cards or remember passwords.
- Ensure system reliability: The project aims to develop a reliable system that can operate continuously without failure or downtime. The use of high-quality components and proper system design will ensure the system's reliability.

Purpose, Scope and Applicability:

Purpose:

The purpose of a biometric door locking system is to provide secure and convenient access control to a space using a person's unique physical characteristics, such as fingerprints. By implementing such a system, the owner of the space can limit access to authorized personnel, reduce the risk of unauthorized entry, and improve overall security.

The significance of a biometric door locking system lies in its potential to improve security and convenience in various settings, such as homes, offices, and public buildings. By reducing the risk of unauthorized entry, these systems can help to protect people and property, while also providing a more convenient and efficient means of access control.

The theoretical framework for a biometric door locking system could draw on various fields, such as computer science and electrical engineering. The hardware components could be designed using principles of electronics and materials science

Scope:

The methodology for a biometric door locking system project would typically involve several stages, including research, design, development, testing, and deployment. During the research stage, the team would gather information on existing technologies, standards, and best practices. In the design stage, the team would create a detailed plan for the system, including the hardware, software, and user interface. During the development stage, the team would build and test the system components, including the sensors, microcontroller, and locking mechanism. After testing, the system would be deployed in the target environment, and ongoing support and maintenance would be provided.

The success of a biometric door locking system project depends on several assumptions, such as the availability of suitable hardware and software components, the accuracy and reliability of the biometric data, and the acceptance and trust of the users.The project team would need to assume that the hardware and software components can be integrated effectively, and that the system can accurately capture and process biometric data. Additionally, the team would need to assume that users would be willing to enroll and use the system, and that they would trust the security and privacy of their biometric data.

There are several limitations to consider when designing and implementing a biometric door locking system. First, the accuracy of biometric data can be affected by environmental factors, such as lighting and temperature, as well as physical factors, such as injuries or changes to the user's appearance. Additionally, there are concerns about the security and privacy of biometric data, which can be vulnerable to hacking or misuse. Finally, there may be legal and regulatory considerations to navigate, such as data protection and privacy laws, as well as standards and certifications for biometric technologies.

Applicability:

- Improved security: Biometric door locking systems provide a higher level of security compared to traditional key-based or card-based systems. This can help to protect people and property from theft, burglary, and other security threats.
- Convenience: Biometric door locking systems offer a more convenient means of access control, as users don't need to carry keys or cards with them. This can save time and reduce the risk of lost or stolen keys.
- Innovation: Biometric door locking systems represent an innovative and exciting technology that can improve the user experience and provide new opportunities for research and development.
- Data collection and analysis: A biometric door locking system connected to a website can provide valuable data on how the system is used in practice, which can inform further research and development in this area.
- Potential for integration: A biometric door locking system can potentially be integrated with other systems, such as home automation or security systems, to provide a more comprehensive and convenient solution for users.

Problem definition:

The problem that the project aims to address is the need for a secure and reliable door locking system that can provide access control based on biometric data. Traditional locking systems that rely on keys or passwords can be vulnerable to security breaches, as keys can be lost or stolen, and passwords can be guessed or hacked. Biometric authentication offers a more secure and convenient alternative by using unique physical characteristics such as fingerprints, facial features, or iris patterns to verify the identity of the user. The project seeks to develop a biometric door locking system that can accurately and efficiently recognize authorized users and grant access while preventing unauthorized access. Additionally, the project aims to provide a system that can collect and store data on user access for monitoring and management purposes.

Surveys of technology:

Awareness and understanding of Available Technologies: Awareness and understanding of available technologies related to biometric door locking systems are essential for anyone involved in designing or implementing such systems.

Related technologies: There are several available technologies related to biometric door locking systems. Some of the key technologies include:

- Facial recognition technology: Facial recognition technology uses algorithms to identify and authenticate individuals based on their facial features. This technology is increasingly being used in biometric door locking systems.
- Iris recognition technology: Iris recognition technology uses the unique patterns in a person's iris to identify and authenticate individuals. This technology is highly accurate and is commonly used in high-security applications.
- Voice recognition technology: Voice recognition technology can be used to identify and authenticate individuals based on their unique voice patterns. This technology is becoming more sophisticated and accurate, but may still have limitations in noisy or crowded environments.
- Smart locks: Smart locks use a variety of technologies, including Bluetooth, Wi-Fi, and Zigbee, to enable remote control and monitoring of door access. Some smart locks also offer biometric authentication features.

- Microcontrollers: Microcontrollers are small, programmable computers that can be used to control the operation of the door locking system. These devices can be programmed to handle data acquisition, storage, and processing, as well as controlling the locking mechanism.
- Cloud computing: Cloud computing can be used to store and manage the biometric data and other information associated with the door locking system. This technology enables remote access and management of the system, as well as providing a scalable and flexible platform for data storage and processing.

Here's a comparative study of the available technologies related to biometric door locking systems:

Facial recognition technology:

- Pros: Contactless, does not require physical contact with the sensor, high accuracy, and can work in low light conditions.
- Cons: Can be affected by changes in facial features due to aging or injuries, and may not work well for people wearing masks or with certain skin conditions.

Iris recognition technology:

- Pros: Very high accuracy, contactless, and can work in low light conditions.
- Cons: Expensive, requires high-quality cameras, and may not work well for people wearing glasses or with certain eye conditions.

Voice recognition technology:

- Pros: Non-contact, easy to use, and can work in noisy environments.

- Cons: May not work well for people with certain accents or speech impairments, and can be affected by background noise.

Smart locks:

- Pros: Can provide remote access and monitoring, can be integrated with other smart home devices, and can offer a range of authentication methods.
- Cons: Can be expensive, may require additional hardware or software, and can be vulnerable to hacking or other cybersecurity threats.

Microcontrollers:

- Pros: Can be easily programmed and customized, can be low-cost and energy-efficient, and can provide real-time data processing and control.

- Cons: Require programming skills and technical knowledge, and may not be suitable for larger-scale systems.

Cloud computing:

- Pros: Can provide scalable and flexible data storage and processing, can enable remote access and management, and can offer high levels of security and reliability.
- Cons: Can be expensive, may require additional hardware or software, and can be vulnerable to hacking or other cybersecurity threats.

The fingerprint sensor is considered to be a reliable and accurate biometric technology for authentication purposes. Here are some reasons why we chose fingerprint sensor for the biometric door locking system project instead of the other available technologies :

1. High accuracy: Fingerprint recognition has been shown to be highly accurate, with a very low false acceptance rate and a very low false rejection rate, which is crucial for ensuring that only authorised users are granted access to the door.
2. Convenience: Fingerprint recognition is a convenient biometric technology because it does not require any special equipment or prior training. Users can simply place their finger on the sensor to gain access, which is easy and fast.
3. Non-invasive: Unlike some other biometric technologies that require contact with the eyes or face, fingerprint recognition is non-invasive and does not pose any health risks.
4. Uniqueness: Each person's fingerprint is unique and unchangeable, making it a reliable and secure means of authentication. This is important in ensuring that only authorised users are granted access to the door.
5. Cost-effective: Fingerprint sensors are relatively inexpensive compared to some other biometric technologies, making them a cost-effective solution for the biometric door locking system project.

While other biometric technologies such as facial recognition or iris scanning may have their own advantages, the fingerprint sensor is a well-established and widely used technology that is highly accurate, convenient, and cost-effective for the biometric door locking system.

Theoretical Background:

The biometric door locking system using R307 sensor is a project that involves the use of biometric authentication technology to secure access to a door or room. Here are some theoretical background concepts that are relevant to this project:

1. Biometric authentication: Biometric authentication is a technology that uses unique physiological or behavioral characteristics to verify the identity of an individual. In the case of the R307 sensor, fingerprints are used as the biometric identifier.
2. Sensor technology: The R307 sensor is a capacitive fingerprint sensor that works by measuring the electrical properties of the skin. It captures a high-resolution image of the fingerprint and uses algorithms to identify unique features that can be used for authentication.
3. Microcontroller: The microcontroller is the brain of the system that controls the sensor and the locking mechanism. It receives signals from the sensor and determines whether to unlock the door or not.
4. Communication protocols: Communication protocols are used to establish a connection between the web application and the microcontroller. The MQTT or HTTP protocol can be used to send data between the web application and the microcontroller.

5. Security: Security is a critical consideration for any biometric authentication system. The R307 sensor uses advanced algorithms and encryption techniques to protect against spoofing and other attacks.

Software Requirement Specification (SRS): -

A software requirements specification (SRS) is a document that describes what the software will do and how it will be expected to perform. It also describes the functionality the product needs to fulfil all stakeholders (business, users) needs.

There are 2 types of user requirements: -

1. Functional
2. Non-functional

Functional requirements: -

Functional requirements are product features or functions that developers must implement to enable users to accomplish their tasks. So, it's important to make them clear both for the development team and the stakeholders. Generally, functional requirements describe system behaviour under specific conditions.

- The system shall provide biometric authentication using fingerprint data.
- The system shall be able to store fingerprint data for multiple users.
- The system shall grant access to authorized users and deny access to unauthorized users.

Non-functional requirements: -

Non-functional Requirements (NFRs) define system attributes such as security, reliability, performance, maintainability, scalability, and usability. They serve as constraints or restrictions on the design of the system across the different backlogs.

- **Extensibility:** - Home automation system for disabled person using voice tag is a system which has an excellent future scope . It will be needed/used by all the houses or any infrastructure that has to control the appliances present over there.
- **Maintainability**: - The scale of the given project may exponentially increase in the coming future. It is much required for the project to be maintained and keep constant updates and addition of new features in the future
- **Reliability**: - This project is reliable to all the users who are seeing to control the appliances without moving from one place to another. It will help them to control the appliances from any place whenever require.
- **Usability**: - It is very user friendly and easy to operate for the users.

  As it is meant for physically disabled individual, they need to have easy and comfortable interaction with the system.
- **Scalability**: - This system is much scalable as it has a high demand in the market in coming future.

Details of Hardware and software Used: -

Hardware Used:

1. Connecting wires
2. Breadboard
3. Single channel relay
4. Arduino-UNO
5. Solenoid Lock
6. R307 Fingerprint Sensor

Software Used:

1. ARDUINO IDE

Coding Language:

1. C

Feasibility study:

A feasibility study is a detailed analysis that considers all of the critical aspects of a proposed project in order to determine the likelihood of it succeeding.

Success in business may be defined primarily by return on investment, meaning that the project will generate enough profit to justify the investment. However, many other important factors may be identified on the plus or minus side, such as community reaction and environmental impact.

A feasibility study assesses the potential for success of the proposed plan or project by defining its expected costs and projected benefits in detail. It's a good idea to have a contingency plan on hand in case the original project is found to be infeasible. A feasibility study is an assessment of the practicality of a proposed plan or project. A feasibility study analyses the viability of a project to determine whether the project or venture is likely to succeed. The study is also designed to identify potential issues and problems that could arise while pursuing the project. Hence it is necessary to conduct a feasibility study before starting a project.

Technical Feasibility:

A technical feasibility study assesses the details of how a project intends to deliver a product or service to customers. It takes into account the various technical aspects like modules, software, algorithms etc. and the hardware requirements the project utilizes. It's the logistical or tactical plan of how the project will produce, store, deliver, and track its products or services. It is assessed based on the Prepared Outline of the project, the labour and the material requirements.

This system is developed in a flexible form, which covers all operation services with the help of optimized code logic to bridge the hardware and software along with C++, for logic. The Project is deemed Technically Feasible.

- The technology required for the project, such as fingerprint scanners, microcontrollers and relay modules, is readily available and affordable.
- The necessary hardware components can be integrated using compatible protocols and interfaces.
- However, there may be technical challenges such as ensuring the accuracy and reliability of the biometric data, managing network connectivity and data transfer, and protecting against potential security vulnerabilities.

Economic Feasibility:

Once the technical feasibility and market studies are complete, it is time to determine Business Feasibility. The first purpose of this effort is to financially model the venture opportunity and achieve a break-even analysis. In other words, based upon the costs of goods sold, capital costs, and management and administration, how much revenue generated from units sold is required to breakeven and over what period of time. The simple objective is to determine what level of revenue is required to satisfy the return on investment demanded by the founder and/or the investors.

Economic feasibility elements include, but are not limited to: Increased agency revenue, decreased agency revenue, increased agency costs, decreased agency costs, increased revenue to other agencies and/or the general public, decreased revenue to other agencies and/or the general public, Increased costs to other agencies and/or the general public, Decreased costs to other agencies and/or the general public, Other public benefits.

In essence economic feasibility study is done to understand if a project will incur a profit or loss to an organization and its extent and thus the execution of the project is dependent on the ROI (Return on Investment) estimated.

This project aims at automating the task of attendance marking for organizations such as schools, universities, Companies, etc. The scope and requirement of the project are estimated and aimed to serve a huge market. The Materials required for hardware are readily available and cheap at mass and requires minimal maintenance. For a business model the software services can be sold in subscription models customized to the client and priced with respect to the cost of running servers and providing profit to the organization.

Resource: -

Resources that are required for the Design of Embedded Security Door Lock System include:

Programming device (Laptop)

Hardware (readily available, Bulk manufactured)

Programming tools (freely available)

Programming individuals

So, it's clear that the project has the required resource feasibility.

- The project cost is within the allocated budget.
- There are no alternative solutions that are significantly more cost-effective than a biometric door locking system.

Operational Feasibility:

Operational feasibility is the measure of how well a proposed system solves the problems, and takes advantage of the opportunities identified during scope definition and how it satisfies the requirements identified in the requirements analysis phase of system development. its success is dependent on how well the humans/ users interact with it, If the software for a new system is too difficult to use, employees may make too many errors and avoid using it. Thus, it would fail to show operational feasibility.

The proposed system will be deemed operationally feasible if users can

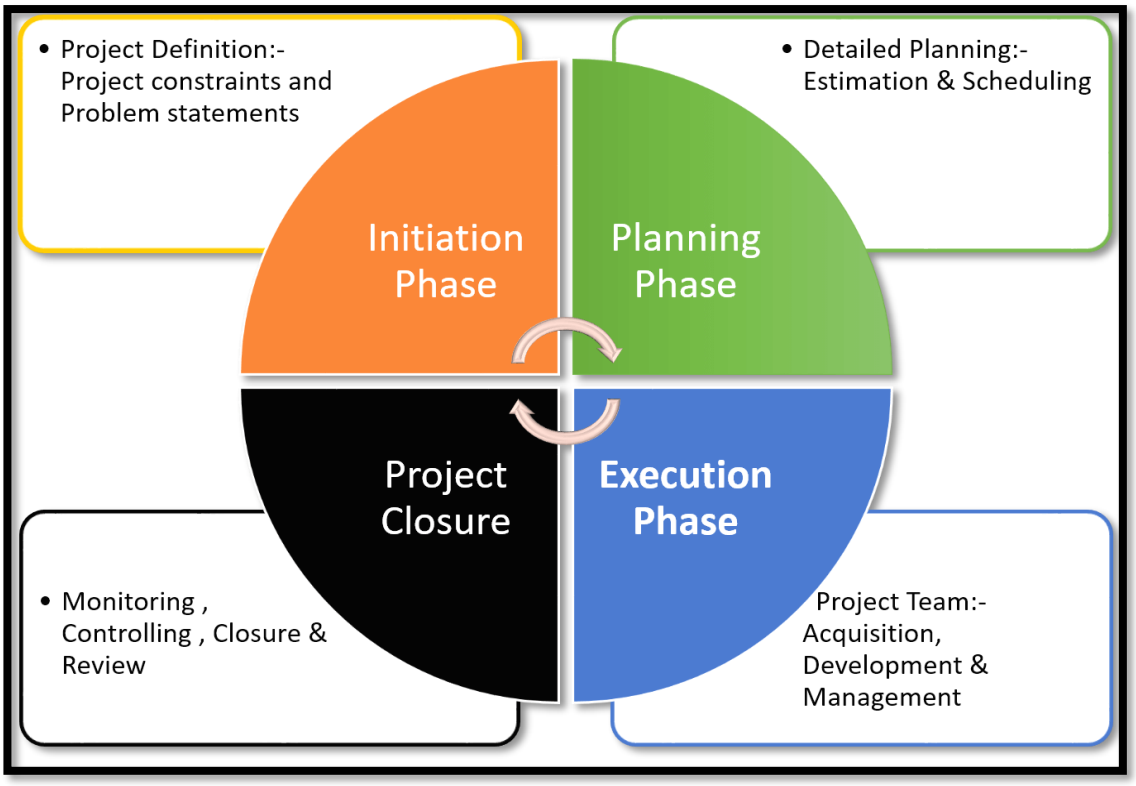
use our site with ease. There are many ways of achieving this including but not limited to user training, Designing user friendly/ intuitive UI, etc. This Design of Embedded Security Door Lock System was designed while keeping it's operationality and user interaction at heart, making sure that the UI is easy to navigate by users of every level ensuring excellent functionality and use of the system by the client on their end

Thus, the Design of Embedded Security Door Lock System in conclusion satisfies all the necessary feasibility requirements and can be deemed feasible

- The system is practical and easy to use for intended users, such as residents or employees who need access to a specific building or room.
- Appropriate training and support can be provided for users and administrators to ensure proper operation and maintenance of the system.
- However, there may be potential operational risks or issues if the system is not properly maintained or if users experience technical difficulties with the system.

System Analysis and Designing

Project Management Life Cycle: -



A Project Development Life Cycle consists of the following 4 stages –

Stage 1 – Project Initiation

Project Initiation is the first step of the Project Development Life Cycle. In this stage, we take a feasibility study of the project, identify the scope of the project and find out the project effect, cost and benefit. Finally working on all the findings.

Stage 2 – Project Planning

In this stage of project Development Life Cycle firstly we plan about the work break

down structure of the work and set a fix an end time of the project. Also finding all the risks related with the project and getting ready to face those issues. All the functionalities are majorly divided into following major parts: -

A. Documentation
B. Designing

Stage 3 – Project Execution

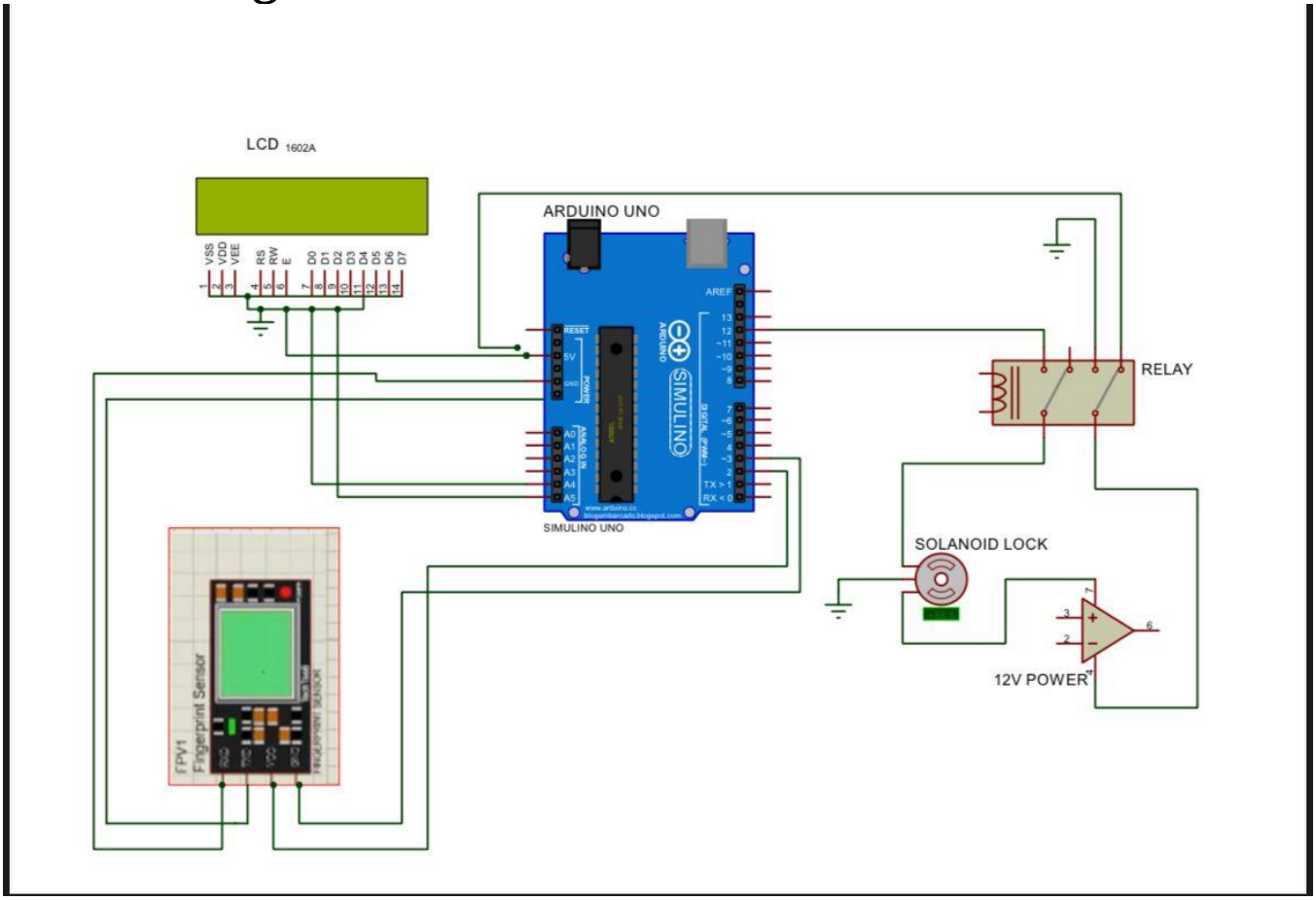
In this phase the plans turned into the action. We allocated our work equally and started our first phase of the project according to the plan.it basically does the following things: -

A. Coding
B. Testing
C. Deployment

Stage 4 –Project Closure

In this phase of the project development life Cycle finally after completion of the project and successful deployment finally the project officially declared closed.
It goes for maintenance only if the user requires it.

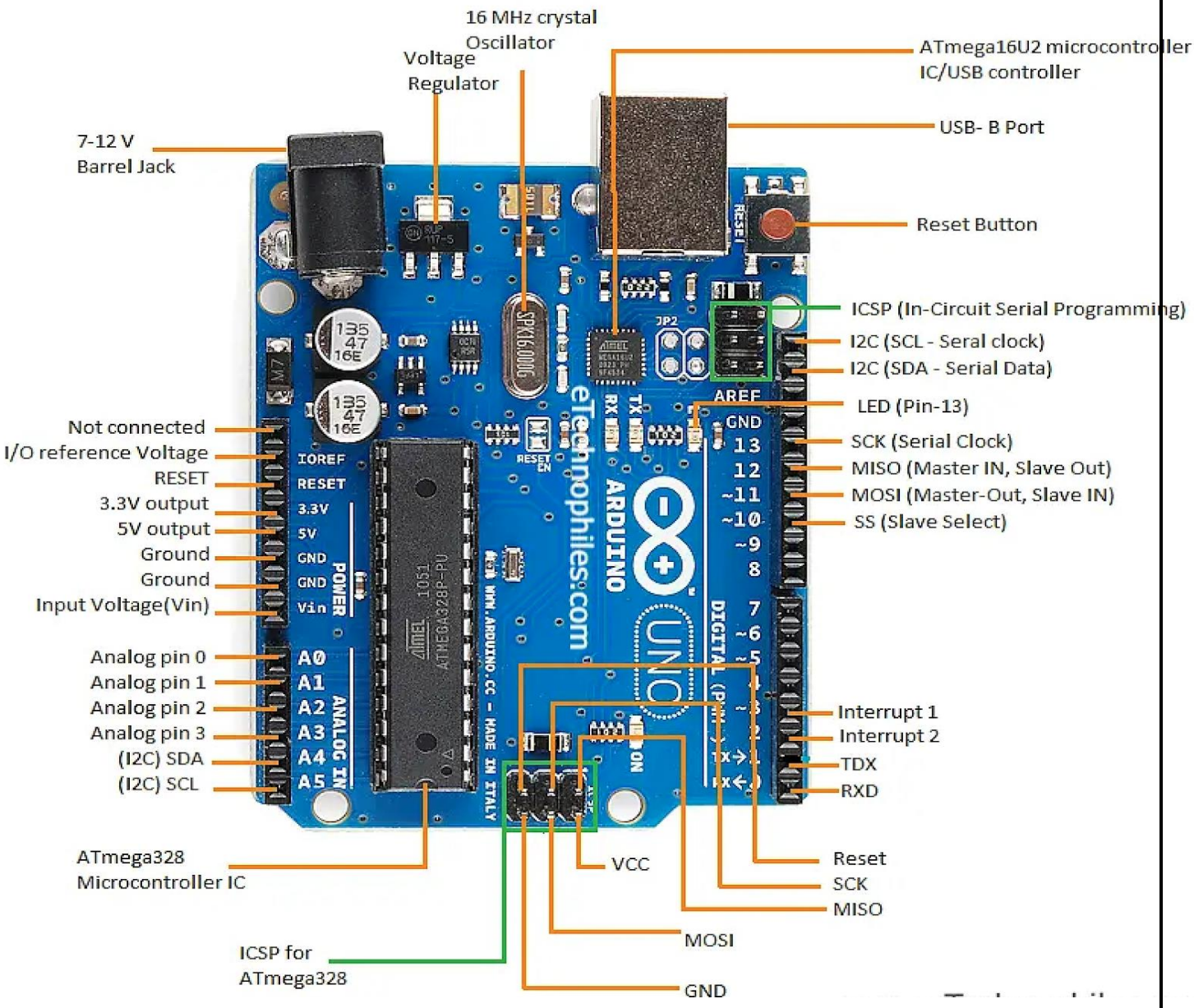
Circuit Diagram:



A circuit diagram (wiring diagram, electrical diagram, elementary diagram, electronic schematic) is a graphical representation of an electrical circuit. A pictorial circuit diagram uses simple images of components, while a schematic diagram shows the components and interconnections of the circuit using standardized symbolic representations. The presentation of the interconnections between circuit components in the schematic diagram does not necessarily correspond to the physical arrangements in the finished device.

Component level Description and Specification:

Arduino Uno:



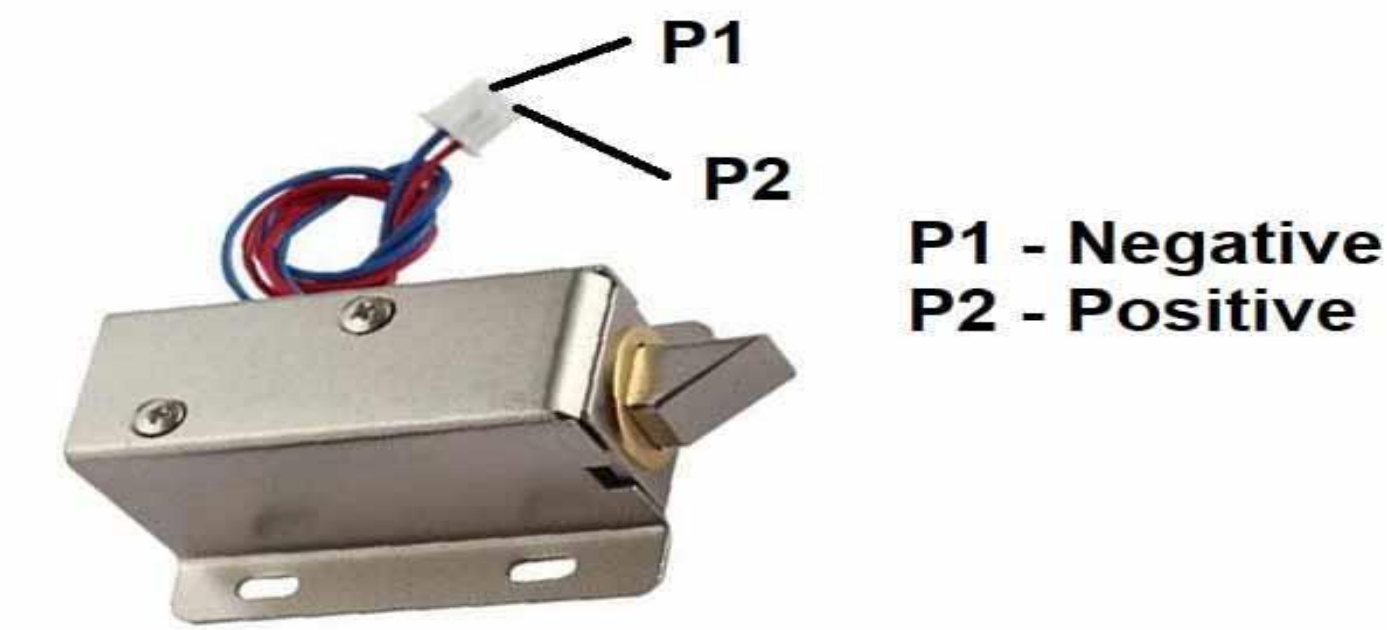
Arduino Uno is a popular open-source microcontroller board that is widely used for prototyping and DIY electronics projects. It is based on the Atmega328P microcontroller chip and comes with a range of input/output pins that can be used to interface with various sensors, actuators, and other electronic components.

The Arduino Uno board is designed to be easy to use and program, even for beginners with no prior experience in electronics or programming. It can be programmed using the Arduino Integrated Development Environment (IDE), a simple and user-friendly software tool that provides a range of libraries and examples for programming the board.

The Arduino Uno board comes with a range of features and specifications, including 14 digital input/output pins, 6 analog input pins, a 16 MHz quartz crystal oscillator, a USB interface, and a power jack. It can be powered using a USB cable or an external power supply, and can communicate with other devices using serial communication protocols such as UART, SPI, and I2C.

Arduino Uno is widely used for a range of electronics projects, including home automation, robotics, environmental monitoring, and wearable technology. It has a large and active community of developers and enthusiasts who contribute to its development and support, and there are a wide range of resources available online for learning and using the board.

Solenoid lock:



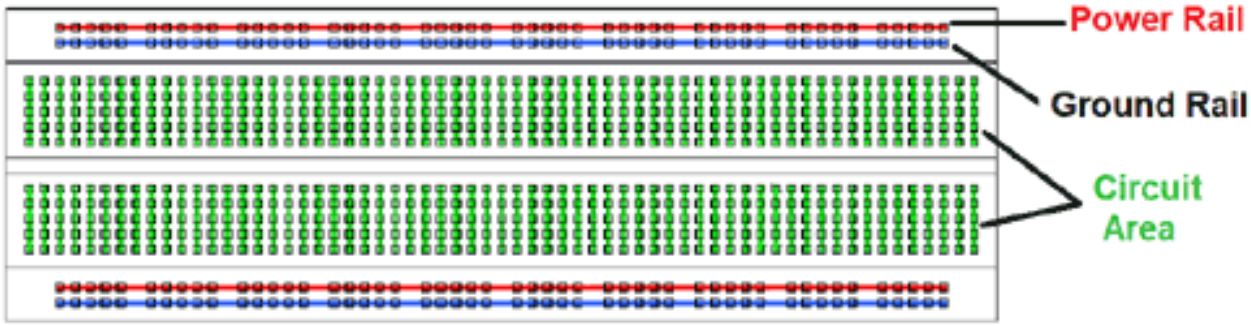
A solenoid lock is an electronic lock that uses a solenoid to control the locking mechanism. A solenoid is an electrical coil that produces a magnetic field when an electric current is passed through it. In a solenoid lock, the magnetic field produced by the solenoid is used to move a locking bolt or latch, which secures the door or gate.

When a solenoid lock is activated, an electric current is sent to the solenoid, causing it to create a magnetic field. The magnetic field then moves a metal plunger, which is connected to the locking bolt or latch, and retracts it from the lock plate, allowing the door or gate to be opened. When the lock is deactivated, the spring-loaded locking bolt or latch returns to its locked position.

Solenoid locks are often used in electronic access control systems and can be operated using a variety of methods, including keypad entry, RFID card readers, or biometric scanners. They offer several advantages over traditional mechanical locks, including faster access, increased security, and the ability to integrate with other security systems, such as alarms and cameras.

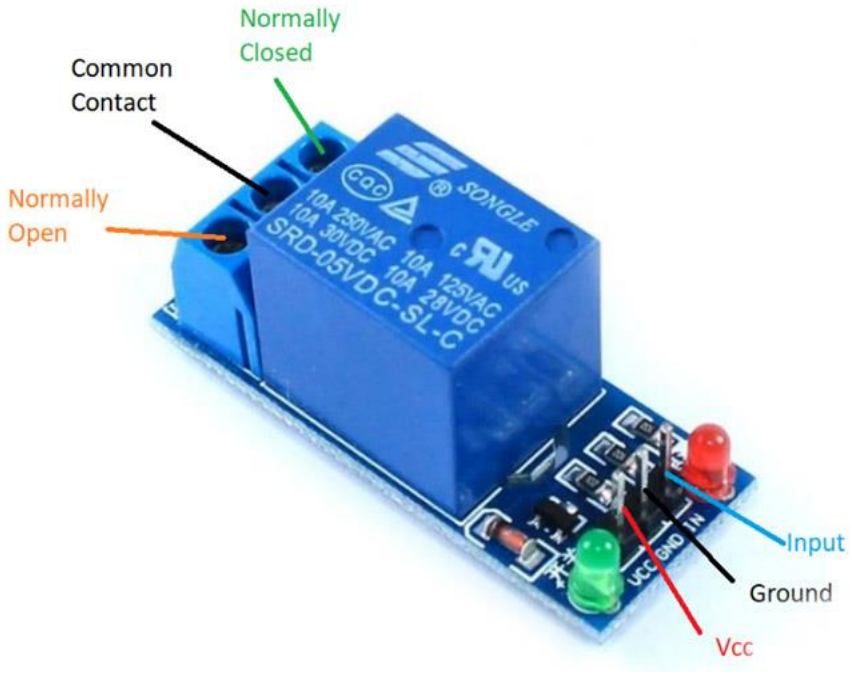
However, solenoid locks also have some limitations. They require a source of electricity to operate, which can be a drawback in the event of a power failure. They can also be vulnerable to hacking and other forms of electronic tampering, which can compromise their security.

Breadboard:



A breadboard is a reusable device used to build and prototype electronic circuits without the need for soldering. It consists of a plastic board with a grid of holes, which are interconnected by metal strips running underneath the board. The holes are designed to accept electronic components, such as resistors, capacitors, LEDs, and integrated circuits, and the metal strips provide a way to connect these components together to form a circuit. The design of the breadboard allows for quick and easy prototyping of electronic circuits, as components can be inserted and removed without the need for special tools or equipment. The holes on the breadboard are arranged in rows and columns, with each row connected horizontally and each column connected vertically. This allows for easy organization of components and connections, and reduces the likelihood of errors or mistakes during the prototyping process.

Single-channel relay:

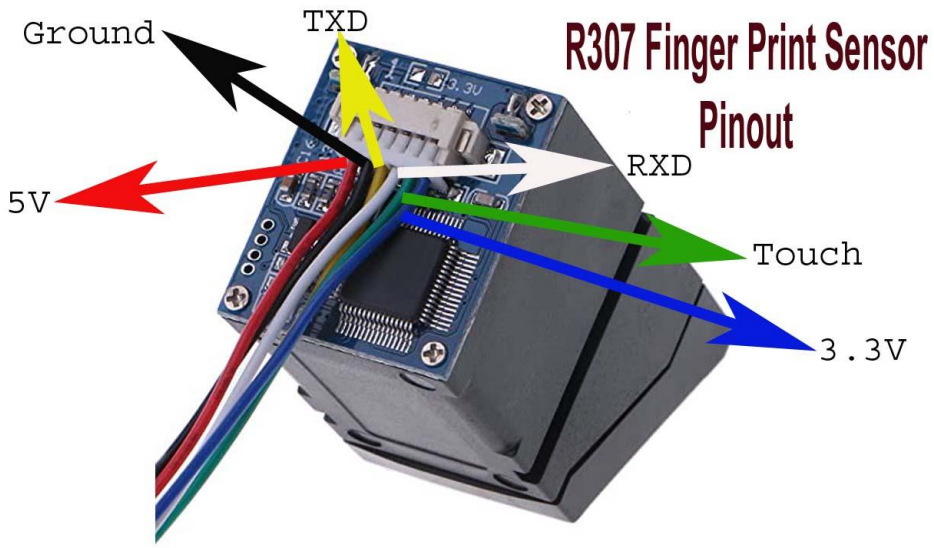


A single-channel relay is an electronic switch that is used to control the on/off state of a single circuit. It consists of a coil that, when energized, creates a magnetic field that activates a switch mechanism, allowing current to flow through the relay contacts and control the operation of the connected circuit.

Single-channel relays are commonly used in electronic circuits to control the operation of motors, lights, and other electrical devices. They are often used in applications where a high level of reliability and safety is required, such as in industrial automation or automotive systems.

Single-channel relays are available in a range of sizes and designs, with different voltage and current ratings to suit different applications. They can be controlled using a variety of signals, including digital signals from microcontrollers or other electronic devices, and analog signals from sensors or other inputs.Overall, single-channel relays are a simple and effective way to control the operation of electronic circuits, and are widely used in a variety of applications in industry, automotive, and other fields.

R307 sensor:



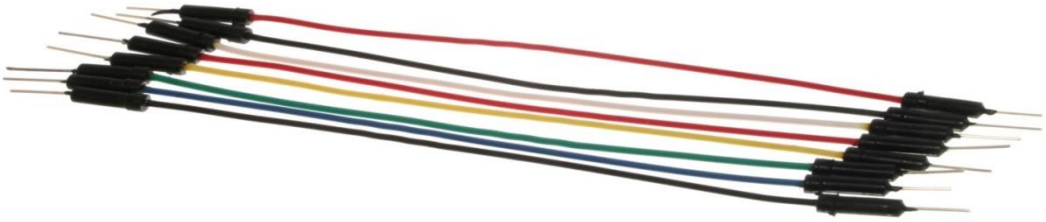
The R307 fingerprint sensor is an electronic device used to capture and recognize fingerprints for authentication purposes. It is a compact and affordable sensor that can be easily integrated into electronic devices such as door locks, safes, and attendance systems.

The R307 sensor uses optical technology to capture a high-resolution image of the fingerprint, which is then processed by an algorithm to extract unique features and create a fingerprint template. This template is then compared to a database of stored templates to determine if the fingerprint is a match.

The R307 sensor has a high level of accuracy and can recognize fingerprints in less than a second. It can store up to 1,000 templates in its memory and has a USB interface for easy communication with other electronic devices.

The R307 sensor is commonly used in applications where security is important, such as in access control systems or attendance systems. It is also used in personal devices such as smartphones and tablets for biometric authentication.Overall, the R307 fingerprint sensor is a reliable and affordable solution for fingerprint recognition and authentication, and is widely used in a range of electronic applications.

Jumper wires:



Jumper wires are an essential electronic component used to create electrical connections between components on a breadboard or other prototyping platform. They consist of a length of wire with pins or connectors at each end, which can be easily inserted into the holes on a breadboard or other circuit board.

Jumper wires come in a range of sizes, colors, and designs, and are available in both male-to-male, female-to-female, and male-to-female configurations. Male-to-male jumper wires are used to connect components that are placed side by side on a breadboard, while female-to-female and male-to-female wires are used to connect components that are not directly adjacent to each other.

Jumper wires are used to create electrical connections between components such as resistors, capacitors, LEDs, and microcontrollers. They are also used to connect sensors, motors, and other electronic devices to a circuit, and to create connections between different circuits or subsystems.

Jumper wires are an essential tool for anyone working with electronic circuits, as they allow for quick and easy prototyping of circuits without the need for soldering or other specialized equipment. They are widely available and affordable, and are an essential part of any electronic hobbyist or engineer's toolkit.

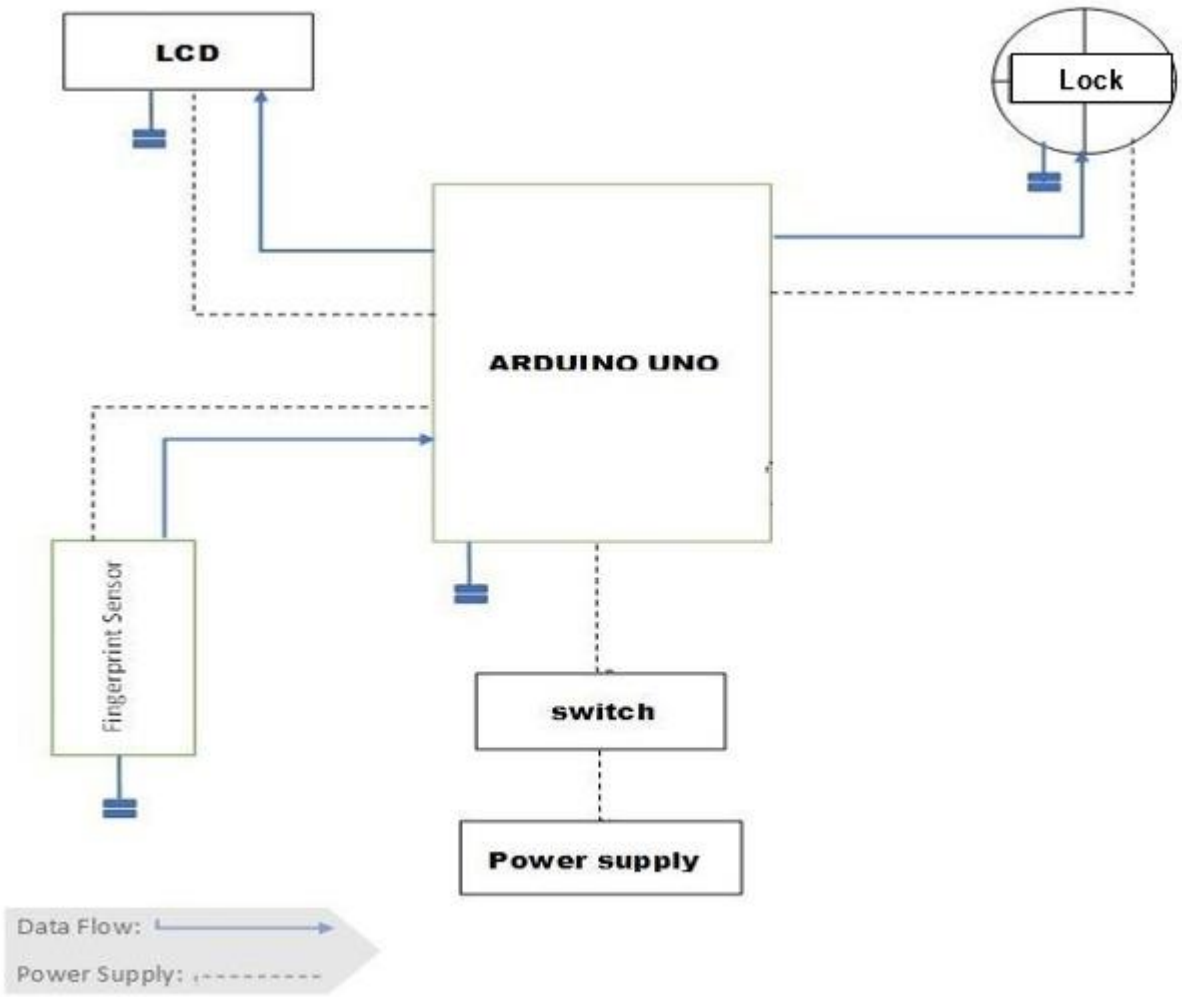
Arduino IDE :

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

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

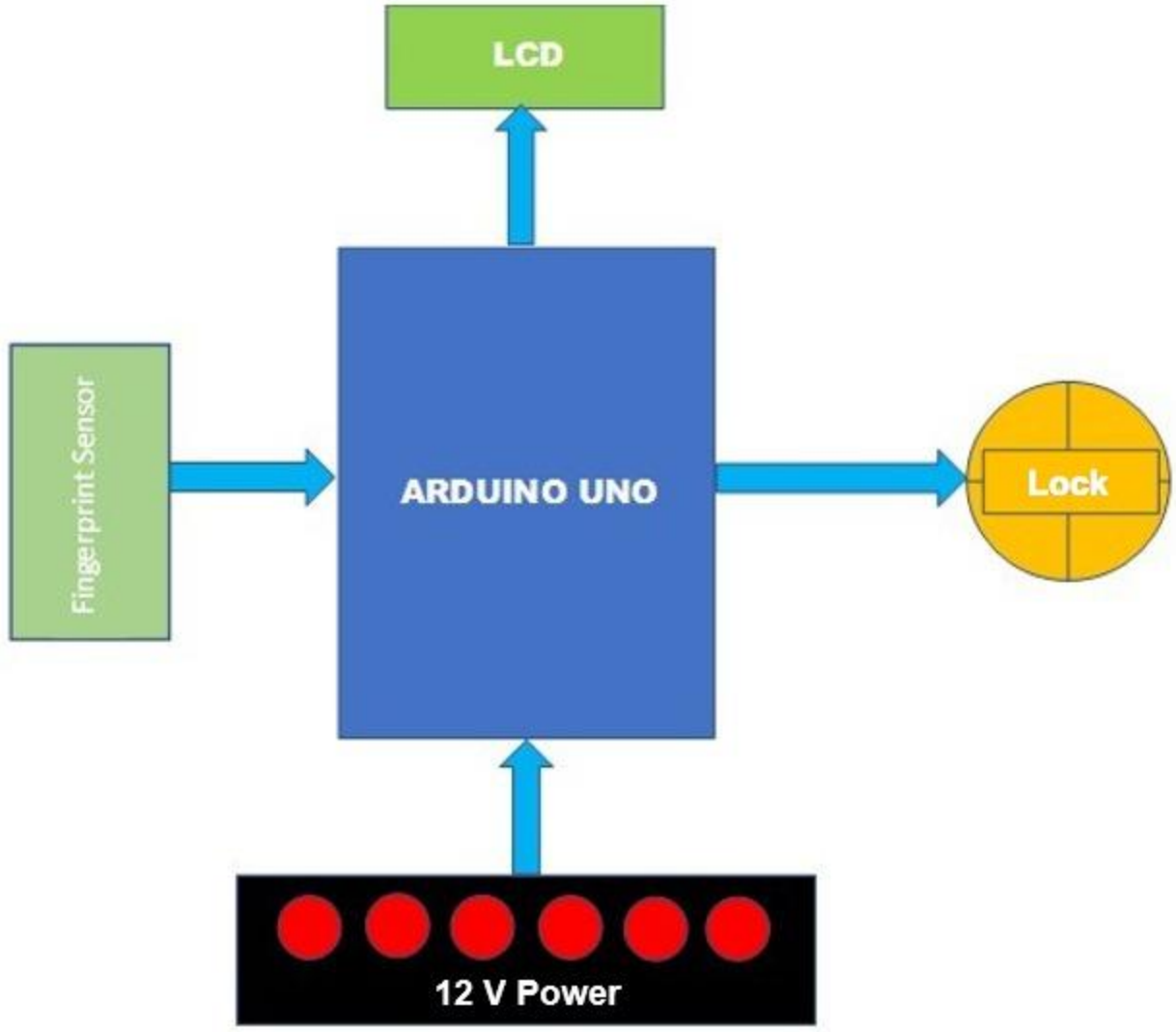
Architecture Design:

The hardware needs the architectural design to represents the design of hardware. Architecture design is defined as “the process of defining a collection of hardware and software components and their interfaces to establish the framework for the development of a computer system.” The software that is built for computer-based systems can exhibit one of these many architectural styles.



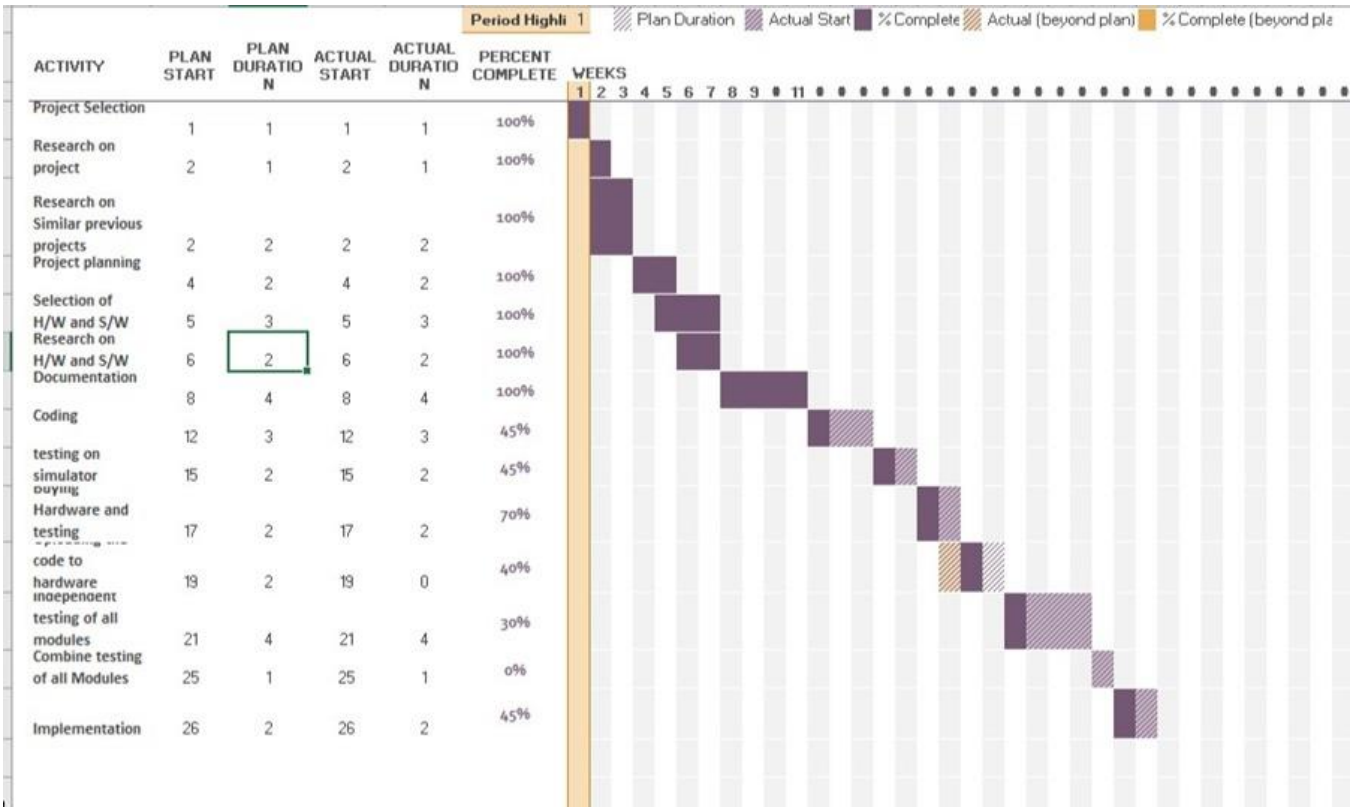
Block Diagram:

A block diagram is a visual representation of a system that uses simple, labeled blocks that represent single or multiple items, entities or concepts, connected by lines to show relationships between them.



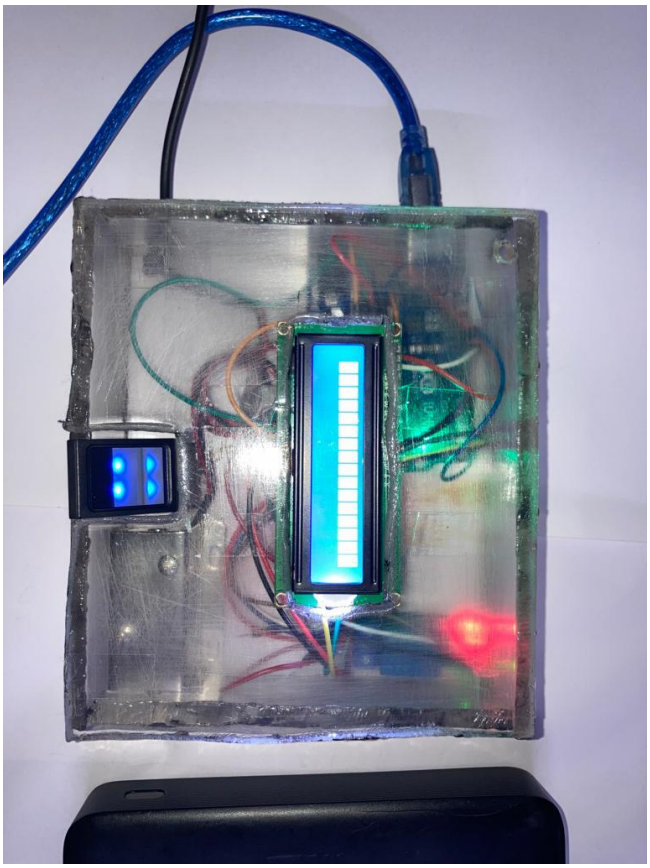
Gantt chart:

Gantt chart is type of chart in which series of horizontal lines are present that show the amount of work done or production completed in given period of time in relation to amount planned for those projects. It is horizontal bar chart developed by Henry L. Gantt (American engineer and social scientist) in 1917 as production control tool. It is simply used for graphical representation of schedule that helps to plan in an efficient way, coordinate, and track some particular tasks in project.



System Implementation:

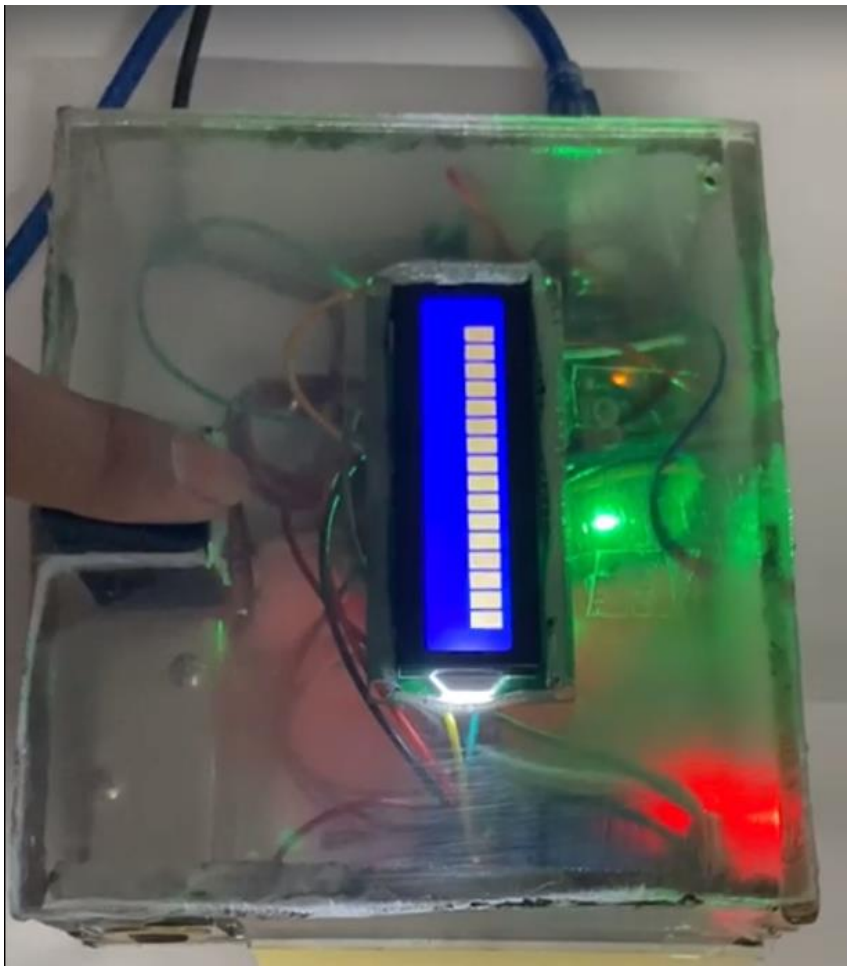
The biometric door lock system using a fingerprint sensor and Arduino Uno board works by capturing the fingerprint of the user and comparing it to the stored fingerprints in the system's database. If there is a match, the system unlocks the door, and the user can enter. If there is no match, the system denies access to the user.



Here are the general steps involved in how the project works:

Enroll the authorized users: The first step is to enroll the fingerprints of the authorized users into the system's database. The fingerprint sensor is used to capture the fingerprints of each user, and the Arduino Uno board stores the fingerprints in its memory.

User authentication: When a user wants to enter the secured area, they will place their finger on the fingerprint sensor. The sensor captures the user's fingerprint and sends it to the Arduino board.



Fingerprint comparison: The Arduino board compares the captured fingerprint with the stored fingerprints in its memory to determine if there is a match.

Lock control: If the fingerprint matches with one of the authorized users, the Arduino board sends a signal to the solenoid lock to unlock the door. The user can then enter the secured area. If the fingerprint does not match, the Arduino board will not send a signal to the lock, and the user will be denied access.

Cost and Benefits Analysis:

As defined, “Cost Estimation is a statement that gives the value of the cost incurred in the manufacturing of finished goods. Cost estimation helps in fixing the selling price of the final product after charging appropriate overheads and allowing a certain margin for profits.”

There are 5 Functional units used to calculate Function Point (FP):

1. Internal Logic Files (**ILF**):

   To control the information or logically related data that is present within the system.

2. External Interface Files (**EIF**):

   The control data referenced by the system but present in another system.

3. External Inputs (**EI**):

   Data/ control info that comes from outside our system.

4. External Outputs (**EO**):

   Data that goes out of the system after generation.

5. External Inquires (**EQ**):

   Combination of input-output resulting data retrieval.

To Compute FP:

We'll use,

FP = UFP * CAF

Where, **UFP** = Unadjusted Function Point

CAF = Complexity Adjustment Factor

Step 1: Calculate **UFP**

To find **UFP** we need to sum all the Complexities of all the **EI**, **EO**, **EQ**, **ILF** and **EIF**.

Function Unit	**Weighting Factors**					
	Count		Low	Average	High	
External Inputs (EI)	4	*	3	4	6	16
External Outputs (EO)	7	*	4	5	7	35
External Inquires (EQ)	1	*	3	4	6	4
Internal Logic Files (ILF)	0	*	7	10	15	0
External Interface Files (EIF)	0	*	5	7	10	0
Total Count	55					

Step 2: Calculating **CAF**:

Formula: **CAF** = 0.65 + (0.01 * **DI**)

Where, **DI** = Value adjustment factors based on responses to the following 14 questions

1	**Data Communication**	**5**
2	Distributed Data Processing	3
3	Performance Criteria	4
4	Heavily Utilized Hardware	5
5	Online Data Entry	0
6	High Transaction Rate	0
7	Online Updating	2
8	End-user Efficiency	5
9	Complex Computations	4
10	Reusability	5
11	Ease of Installation	3
12	Ease of Operation	4
13	Portability	2
14	Maintainability	4
Degree of Influence (DI)		46

Step 3: Calculating **Function Point**

Function Point (FP) = UFP*(0.65+0.01*DI)

Function Point (FP) = 55*(0.65+0.01*46)

Function Point (FP) = 55*1.11

Function Point (FP) = 61.05

That Means, Function Point is **61.05**

Total cost of the hardware used= 5000

Test Cases:

Sr. No	Task	Expected Output	Observed Output	Result
1.	Check Arduino Uno	Board should show up on IDE	Board showing up successfully	Pass
2.	Keypad Integration with Uno Board	Output from the keypad should be visible on the serial monitor	Only few button's output are visible on the serial monitor	Fail
3.	LCD Screen	LCD should able to display messages on screen	Messages are displayed successfully	Pass
4.	R307 Sensor	Sensor should take fingerprint images, convert and store them with proper IDs	Fingerprints are taken and stored successfully	Pass
5.	Solenoid Lock	Lock should be opened and closed at given command	At given command lock is opened and closed successfully	Pass

Codes:

Enrollment Code

```
uint8_t getFingerprintEnroll() {

 int p = -1;
 Serial.print("Waiting for valid finger to enroll as #"); Serial.println(id);
 while (p != FINGERPRINT_OK) {
  p = finger.getImage();
  switch (p) {
  case FINGERPRINT_OK:
   Serial.println("Image taken");
   break;
  case FINGERPRINT_NOFINGER:
   Serial.println(".");
   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(1);
switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Image converted");
    break;
  case FINGERPRINT_IMAGEMESS:
    Serial.println("Image too messy");
    return p;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    return p;
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Could not find fingerprint features");
    return p;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Could not find fingerprint features");
    return p;
  default:
    Serial.println("Unknown error");
    return p;
}
```

```
Serial.println("Remove finger");
delay(2000);
p = 0;
while (p != FINGERPRINT_NOFINGER) {
  p = finger.getImage();
}
Serial.print("ID "); Serial.println(id);
p = -1;
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(2);
switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Image converted");
    break;
  case FINGERPRINT_IMAGEMESS:
    Serial.println("Image too messy");
    return p;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    return p;
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Could not find fingerprint features");
    return p;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Could not find fingerprint features");
    return p;
  default:
    Serial.println("Unknown error");
    return p;
```

```
}

// OK converted!
Serial.print("Creating model for #");  Serial.println(id);

p = finger.createModel();
if (p == FINGERPRINT_OK) {
  Serial.println("Prints matched!");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
  Serial.println("Communication error");
  return p;
} else if (p == FINGERPRINT_ENROLLMISMATCH) {
  Serial.println("Fingerprints did not match");
  return p;
} else {
  Serial.println("Unknown error");
  return p;
}

Serial.print("ID "); Serial.println(id);
p = finger.storeModel(id);
if (p == FINGERPRINT_OK) {
  Serial.println("Stored!");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
  Serial.println("Communication error");
  return p;
```

```
  } else if (p == FINGERPRINT_BADLOCATION) {
    Serial.println("Could not store in that location");
    return p;
  } else if (p == FINGERPRINT_FLASHERR) {
    Serial.println("Error writing to flash");
    return p;
  } else {
    Serial.println("Unknown error");
    return p;
  }
}
```

Find Sensor:

```
finger.begin(57600);
  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Did not find fingerprint sensor :(");
    while (1) {
      delay(1);
    }
  }
  finger.getTemplateCount();
  Serial.print("Sensor contains "); Serial.print(finger.templateCount); Serial.println(" templates");
  Serial.println("Waiting for valid finger...");
}
```

Fingerprint Confidence:

```
int getFingerprintIDez() {
  uint8_t p = finger.getImage();
  if (p != FINGERPRINT_OK)  return -1;

  p = finger.image2Tz();
  if (p != FINGERPRINT_OK)  return -1;

  p = finger.fingerFastSearch();
  if (p != FINGERPRINT_OK)  return -1;


  // found a match!

  {
    digitalWrite(12, HIGH);
    delay(3000);
    digitalWrite(12, LOW);
    Serial.print("Found ID #"); Serial.print(finger.fingerID);
    Serial.print(" with confidence of "); Serial.println(finger.confidence);

  }
}
```

Maintenance and evaluation:

Maintenance:

- Regularly test the system to ensure that it is functioning properly.
- Check for any wear and tear on the hardware components and replace them as needed.
- Update the software as necessary to address any security vulnerabilities or bugs.
- Regularly clean the R307 sensor to ensure that it can properly read fingerprints.
-

Evaluation:

- Define clear evaluation criteria, such as security, convenience, user satisfaction, and cost.
- Collect feedback from users to determine how well the system is meeting their needs and expectations.
- Monitor any security incidents to determine if the system is adequately protecting the locked area.
- Evaluate the cost of maintaining and operating the system against the benefits it provides.
- Consider conducting a cost-benefit analysis periodically to determine if the system is still viable

Limitations of the biometric door locking system:

False rejection rate: Biometric systems like fingerprint recognition can have false rejection rates, which means that authorized users may be denied access due to errors in the recognition system. This can be caused by various factors, such as dirty or wet fingers, scars, or changes in the fingerprints due to aging.

False acceptance rate: Conversely, biometric systems can also have false acceptance rates, which means that unauthorized users may gain access due to errors in the recognition system. This can be caused by various factors, such as fake fingerprints or malfunctions in the sensor.

Cost: Biometric systems can be expensive, especially if they require high-quality sensors and sophisticated software to operate effectively. This can make the technology inaccessible to individuals or organizations with limited budgets.

Power consumption: Biometric systems can consume a significant amount of power, especially if they require continuous operation. This can make the system less energy-efficient and increase the operating costs.

Security: Although biometric systems can provide a high level of security, they are not foolproof. Hackers or intruders may be able to bypass the system using various methods, such as stealing or replicating fingerprints or exploiting vulnerabilities in the system's software or hardware.

Maintenance: Biometric systems can require frequent maintenance to ensure that they are operating effectively. This can involve cleaning the sensors, updating the software, and replacing components as needed. The maintenance requirements can add to the overall cost and complexity of the system.

Future Scope and Conclusion:

Future Scope:

Developments in the biometric door locking system project could prompt investigations into several new areas of research and development, including:

- Integration with other technologies: In the future, the project could be connected to a website to get records of users and information about the logs.

The integration of biometric technology with other emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT) could be explored. This could lead to the development of more sophisticated systems that are capable of learning and adapting to user behavior.

- Enhanced security: The biometric door locking system project could lead to investigations into the development of more advanced security systems that can protect against various types of attacks, including cyber attacks and physical attacks.

- Accessibility and usability: The project could prompt investigations into how biometric technology can be made more accessible and user-friendly. This could include research into how biometric technology can be integrated into everyday devices and how it can be used by people with disabilities.

- Ethical and legal considerations: The use of biometric technology raises ethical and legal considerations that need to be addressed. The biometric door locking system project could prompt investigations into these issues, including privacy concerns and the legal implications of using biometric data.

Overall, the biometric door locking system project has the potential to lead to new areas of investigation and development that could have significant implications for the security and accessibility of various systems and technologies.

Conclusion:

The biometric door lock system using a fingerprint sensor and Arduino Uno board is an innovative and useful project that provides a secure and convenient way of controlling access to a secured area. By using a fingerprint sensor to capture and compare fingerprints, and a solenoid lock to control access, the system provides a high level of security to authorized personnel and prevents unauthorized access.

The project is relatively easy to implement, and it is a great opportunity for beginners to learn about microcontrollers, sensors, and security systems. It also has the potential for customization and expansion, such as adding more features like a user interface, voice commands, and remote access control.

Overall, the biometric door lock system using a fingerprint sensor and Arduino Uno board is a valuable project for anyone interested in learning about electronics, programming, and security systems. It provides a practical solution to access control challenges and can be used in various settings, including homes, offices, and commercial buildings.

References:

- Design and Implementation of Fingerprint-Based Security by M.A. Rahman, M.T. Islam, and M.H. Rashid

- Development of a Fingerprint-Based Security System for Smart Homes by C. G. Attamah and V. S. Eze

- Biometric Door Lock System using Fingerprint Recognition by R. K. Meena and R. K. Jain

- Design and Implementation of Biometric Fingerprint-Based Security System for Banks by M. S. Oyediran and A. A. Atayero

- Arduino-Based Smart Door Lock System using Fingerprint Sensor by H. N. Abu-Salih and A. M. Abu-Alhaj