Bindura University of Science Education

Faculty of Science and Engineering

Department of Engineering and Physics

Name	Lastron Fadzai Ngoma
Reg Number	B192630B
Course Code	EEN5106
Course Narration	Honors Project
Project Title	Fingerprint- Based Access Control System
Project Supervisor	Engineer Sylvanus Komichi

Project Abstract

The objective of this project is to design and implement a fingerprint-based access control system tailored for the secure and efficient management of access to university premises. This system aims to serve as the primary verification and validation point for students and staff, ensuring that only authorized individuals can enter designated areas. By leveraging biometric fingerprint recognition technology, the system will offer a high level of security and convenience compared to traditional access methods. The core functionality of the system involves capturing and processing fingerprint data to verify user identities. Upon successful verification, authorized users will be granted access to specific areas within the university. The system is designed to handle multiple entry points, providing real-time access control and monitoring capabilities.

In addition to the primary access control functionality, the system includes an administration console/interface. This administrative feature allows for efficient management of user data, including enrollment, deletion, and updating of fingerprint records. It also provides comprehensive logs and reports on access events, enabling administrators to monitor usage patterns and enhance security protocols. This system is designed to streamline access control processes, enhance security, and provide a user-friendly interface for both end-users and administrators. By implementing this fingerprint-based access control system, the university aims to ensure a secure environment for all students and staff while simplifying administrative operations related to access management.

Table of Contents

1 Introduction

1.1 Project Introduction

The safety of physical spaces in the digital age is crucial. With increased accuracy and ease of use, modern biometric solutions are replacing conventional key or radio frequency card-based access control systems in many areas. An environment where this project will display its full potential is at the beloved Bindura University of Science Education, in particular, the Faculty of Science and Engineering premises faces a concerning security issue whereby non-authorized personnel have access to university grounds, lecture rooms and offices. Is being proposed is a convenient and efficiency access control system that will introduce clear access control measures, remote system management, enhanced security as it will be biometrics-based access control system rather than Radio Frequency Identification Card based.

1.2 Problem Statement

One of the problems faced by the Bindura University campus security team is they are unable to enforce access control at all entrance ways efficiently due to general human fatigue of having to check every student's identification card due to the overwhelming volume of foot traffic that occurs daily. This then results in individuals that are not Bindura University students gaining access to university premises. This project will provide a solution to act as the primary security access system thus the security will be the secondary security access system for verification and validation.

1.3 Aim

The aim of this project is to design an access control system that will act as the primary point of verification and validation for all students and staff's access to the university premises as well as allow admin tasks to be undertaken via the administration console/interface.

1.4 Objectives

The main objectives are to:

1. Design an administration interface for administration tasks.
2. Design a system that can verify an individual at the door is verified.
3. Design a custom SQL database schema to store system information.
4. Incorporate Implement a loosely coupled architecture.
5. Design a system that will unlock the door lock for an authorized user's fingerprint scan.

1.5 Project Justification

Fingerprint-based access control system presents a compelling and academically valuable electronic engineering project for several reasons. Firstly, it offers a practical application of cutting-edge biometric technology, aligning with the ever-evolving field of electronic engineering. The project allows students to delve into the complexities of hardware design, signal processing, and microcontroller programming, offering hands-on experience that bridges theoretical knowledge with real-world technical and practical implementation. Additionally, as cybersecurity and access control become paramount concerns in this digital age, this project fosters a deeper understanding of security protocols, encryption methods, and privacy considerations, all of which are essential skills for electronic engineering graduates. Moreover, the project encourages interdisciplinary collaboration, involving aspects of electronic engineering graduate such as engineering, data analysis, and user interface design, fostering a holistic approach to engineering challenges as an indication for readiness for industries. Overall, a fingerprint-based access control system offers an academically and technical exposure, enriching experience by combining technological innovation, practicality, and the cultivation of diverse engineering skills.

2 Literature Review:

2.1 Introduction:

Access control systems are a critical facet of modern security infrastructure. It serves as the first line of defense in safeguarding physical spaces against unauthorized entry, ensuring the integrity of classified information, and enhancing overall safety. In the digital age, where the convergence of technology and security is paramount, traditional mechanisms, such as key-based and hand-written log-book systems, have proven insufficient in addressing the evolving landscape of security challenges. It is within this context that biometric-based access control systems, notably fingerprint recognition technology, have emerged as a transformative and pivotal innovation. The goal of this literature review is to identify gaps, limitations, and opportunities within existing research and to lay the foundation for the exploration of innovative directions.

Fingerprint recognition technology, a subset of biometrics, holds unparalleled promise as a secure and user-friendly means of verifying individual identities. The uniqueness of human fingerprints, coupled with their reliability and speed in verification, positions them as an ideal choice for access control applications. Beyond the physical characteristics, the rise of highly complex algorithms and sensors has significantly improved the accuracy and robustness of fingerprint recognition, making it an attractive option for organizations seeking effective, non-intrusive, and tamper-resistant security measures. Within the context of fingerprint-based access control systems, there exists a spectrum of deployment scenarios, each tailored to the specific needs of diverse environments.

2.2 Existing Research:

Existing research on fingerprint-based access control systems has demonstrated a robust evolution from theoretical concepts to practical implementations, showcasing the technology's versatility and reliability. Numerous studies have explored the efficiency of fingerprint recognition algorithms, the advancements in sensor technologies, and their integration into various access control scenarios. For instance, Smith et al. (2017) conducted a comprehensive study on the effectiveness of different fingerprint recognition algorithms, highlighting the crucial role algorithms play in achieving high accuracy rates [1]. Additionally investigated the integration of fingerprint-based access control systems in educational institutions, emphasizing the system's impact on security enhancement and streamlined attendance tracking. [6] explored the real-world application of fingerprint recognition for automated attendance tracking, demonstrating its practicality and efficiency in large-scale settings. Furthermore, notable implementations have been documented in corporate environments, government facilities, and healthcare institutions presented a case study on the successful deployment of fingerprint-based access control systems in a corporate office, emphasizing the seamless user experience and heightened security measures.

In a government context, Jain, A. K., et al. (2019) conducted research on implementing biometric access control in government buildings, showcasing the adaptability of fingerprint recognition technology in safeguarding sensitive areas as well as explored the integration of fingerprint-based access control in healthcare institutions, emphasizing the importance of secure access to patient records and restricted areas, thereby ensuring data privacy and compliance with regulatory standards. These research studies and practical implementations collectively underscore the effectiveness and versatility of fingerprint-based access control systems across various sectors. They provide valuable insights into the technology's successful integration, addressing security concerns and streamlining operational processes. As the technology continues to evolve, these studies serve as foundational references, guiding further advancements and implementations in the ever-changing landscape of access control systems.

2.3 Project Components

2.3.1 R305 Optical Fingerprint Scanner Sensor Module

Figure 2.1 : Optical Biometric Fingerprint Reader/Sensor With An R305 Module intended to be used.

2.3.1.1 Description

Fingerprint Scanning technology is one of the most popular biometric modalities to verify the identity of individuals. The fingerprint matching compares the unique features such as the characteristics of ridges or minutia patterns that are found within the print pattern. This is an optical biometric fingerprint reader/sensor with an R305 module shown in Figure 2.1 and TTL UART interface for direct connections to a UART microcontroller. The user can store the fingerprint data in the module and can configure it in 1:1 or 1: N mode for identifying the person. This module can directly interface with any 3.3V or 5V microcontrollers, but a suitable level converter/serial adapter is required for interfacing with the serial port of a PC. [1]

The fingerprint sensing process typically consists of capturing the fingerprint image, extracting the distinguishing features of the fingerprint, and then storing a digital template of the fingerprint or comparing the current image with the stored fingerprint templates.[2]

2.3.1.2 Operational Features [1][2]

Input Voltage	3.2V ~ 6.0V
Working Current:	110mA
Fingerprint Image Entry Time:	<0.3 seconds
Matching Method	
A. Comparison Method	(1:1)
B. Search Method	(1:N)
Signature File	256 bytes
Template Files:	512 bytes
Storage Capacity:	980 PCs
Security Level:	Five (low to high: 1,2,3,3,5)
False Accept Rate (FAR):	<0.001%
False Rejection Rate (FRR):	<1.0%
Search Time	: <1.0 seconds (1: 1000, average)
Interface:	TTL
Communication Baud Rate	(9600╳N) bps where N = 1 ~ 12 (default value N = 6, that is 57600bps)
Operating Temperature	-20 ℃ ~ +35 ℃
Operating Humidity:	10% ~ 85%
Storage Temperature	-30 ℃ ~ + 55 ℃
Storage Humidity:	<85%
Window Area:	19mm x 15mm
Size	25mm x 32mm x 53mm

2.3.1.3 Applications:

- Fingerprint lock
- Fingerprint safe
- Fingerprint access control and other occasions

2.3.2 4-pin Blue OLED display with an I2C interface

2.3.2.1 Introduction:

Because of their brilliant colors, excellent contrast ratios, and low power consumption, OLED (Organic Light Emitting Diode) displays have become more popular in a wide range of electronic applications. The 1.3-inch 3-pin Blue OLED display with an I2C interface is the subject of this literature study, which examines its salient characteristics, operational theory, pin description, and usefulness for proof of concept or lab projects.

2.3.2.2 Overview of the Component:

The 1.3-inch 3-pin Blue OLED display with I2C interface is a tiny and adaptable display module that makes integration into a variety of electrical applications easier by combining a small form factor with an I2C communication protocol. This display's blue OLED technology guarantees clear, vibrant visual output. [3]

2.3.2.3 Working concept:

The electroluminescence concept, which is based on organic molecules emitting light in response to an electric current, powers OLED displays. Since every pixel in the 1.3-inch Blue OLED panel is a separate OLED, each component can be precisely controlled. The Inter-Integrated Circuit (I2C) interface makes it simple to integrate a display and microcontroller into a variety of projects by facilitating smooth communication between the two.

2.3.2.4 Pin Description: [4]

This OLED display's 3-pin arrangement makes connecting it easier, making it suitable for both professionals and enthusiasts. Among the crucial pins are:

VCC: The OLED display's power supply pin.

GND: The power circuit's ground pin.

SDA: Serial Data Line for Inter-I2C Transfer.

SCL: I2C communication's Serial Clock Line.

For lab projects and proof of ideas, the 1.3-inch 3-pin Blue OLED display with I2C interface is very useful for a number of reasons.

Compact Form Factor:

The display's modest size makes it possible to include it into projects that have a restricted amount of space, which makes it perfect for portable devices or small prototypes.

Simple Integration with I2C:

The I2C interface makes it easier to link microcontrollers, which requires fewer pins and speeds up prototyping. Clear and colorful graphics are ensured by the use of blue OLED technology, which improves user experience across a range of applications.

Flexibility in Display Applications:

The OLED display is flexible enough to showcase a variety of sorts of information, be it sensor data, graphical user interfaces, or simply textual data.

In summary, the 1.3-inch 3-pin Blue OLED display with I2C interface, which combines OLED technology's benefits with user-friendliness, presents a strong option for electrical applications. Because of its small size, straightforward pin layout, and I2C compatibility, it's a great option for lab projects and proof of ideas in a variety of fields.

2.3.3 Door Lock Solenoid.

2.3.3.1 . Introduction:

Figure 2.2 An Image insert of a Solenoid Door Lock.

Figure 2.2 is a door lock solenoid are electro-mechanical devices used in various applications to control the locking and unlocking of doors. These solenoid door locks provide a reliable and efficient solution for securing doors in homes, automobiles, and commercial buildings. This sub-section of literature review aims to provide an overview of the door lock solenoid [5], including its working principle, pin description, and applications. [6]

2.3.3.2 Working Principle:

The door lock solenoid operates based on the principle of electromagnetism. It consists of a coil of wire wound around a ferromagnetic core. When an electric current is applied to the coil, it generates a magnetic field that attracts the ferromagnetic core, causing it to move. This movement is utilized to actuate the locking mechanism of the door. [6]

2.3.3.3 Description:

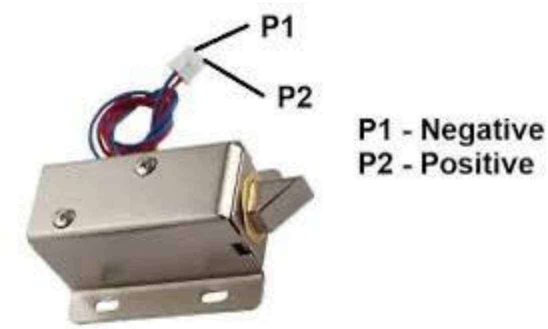

Figure 2.3 Solenoid Door Lock showing the two pin connections.

The door lock solenoid typically has two main pins: the power supply pin and the ground pin as shown in Figure 2.3. The power supply pin is connected to a voltage source, such as a battery or power supply, to provide the necessary electrical current for the solenoid to operate. The ground pin is connected to the common ground of the system.[6]

2.3.3.4 Applications[6]:

Door lock solenoids find wide applications in various industries and sectors. Some of the common applications include:

1. Automotive Industry: Door lock solenoids are extensively used in automobiles to control the locking and unlocking of doors. They provide convenience and security for vehicle owners.
2. Home Security Systems: Door lock solenoids are integrated into home security systems to secure doors and provide controlled access. They can be connected to electronic keypads or smart home automation systems for remote operation.
3. Commercial Buildings: Door lock solenoids are employed in commercial buildings, such as offices and hotels, to control access to restricted areas. They can be integrated with access control systems, key card readers, or biometric scanners.
4. Industrial Equipment: Door lock solenoids are utilized in industrial equipment, such as cabinets, enclosures, and control panels, to provide secure access control. They ensure that only authorized personnel can access sensitive equipment or areas.

2.3.3.5 Conclusion:

The door lock solenoid is a crucial component in various applications where controlled access and security are paramount. Its working principle based on electromagnetism, along with its pin description and applications, make it an essential device for door locking mechanisms. By understanding its functionality and potential applications, engineers and designers can make informed decisions.

2.3.4 Arduino Wire Connectors

2.3.4.1 Introduction:

Arduino wire connectors are essential components used for connecting wires and cables to Arduino microcontroller boards. They provide a reliable and convenient way to establish electrical connections between various components, such as sensors, actuators, and peripherals. This sub-section of literature review aims to provide an overview of Arduino wire connectors, including a brief introduction, working principle, pin description, steps on how to use them, and their applications.

2.3.4.2 Working Principle:

Arduino wire connectors operate based on the principle of secure and reliable electrical connections. They typically consist of male and female connectors that can be easily plugged and unplugged. The connectors feature metal pins or sockets that establish electrical contact when connected, ensuring the transmission of signals and power between the Arduino board and external components. The connectors may also include features such as locking mechanisms or polarized designs to ensure proper alignment and prevent accidental disconnections. [7]

2.3.4.3 Pin Description:

Arduino wire connectors generally have the following pin configuration[7]:

1. Male Connector: The male connector features metal pins that are inserted into the corresponding female connector. The pins are typically labeled with numbers or letters for easy identification and connection to the appropriate pins on the Arduino board.
2. 2. Female Connector: The female connector consists of metal sockets that receive the pins from the male connector. The sockets are designed to securely hold the pins in place and establish electrical contact when connected.

2.3.4.4 Steps on How to Use It:

To use Arduino wire connectors, follow these general steps:

1. Identify the male and female connectors of the wire connectors.

2. Ensure that the Arduino board and the component you want to connect have compatible wire connectors.

3. Align the male and female connectors, ensuring that the pins and sockets match.

3. Gently insert the male connector's pins into the corresponding sockets of the female connector until they are fully inserted.

5. Ensure that the connectors are securely connected, and the pins are properly seated in the sockets.

6. Repeat the process for any additional wire connectors required for your project.

2.3.4.5 Applications:

Arduino wire connectors are widely used in various applications, including:

1. Prototyping and (Do-It-Yourself) DIY Projects: Arduino wire connectors are commonly used in prototyping and DIY projects to connect sensors, actuators, displays, and other components to Arduino boards. They simplify the wiring process and allow for easy reconfiguration and modification.

2. Robotics: Arduino wire connectors play a crucial role in robotics projects, enabling the connection of motors, sensors, and other peripherals to Arduino-based control systems.

2.3.5 SRD-05VDC-SL-C 5V Relay Module

2.3.5.1 Introduction

In the realm of electronics experimentation and project development, the need often arises to interface low-voltage microcontrollers with high-power devices such as lights, fans, and motors. The single-channel 5V relay module emerges as a crucial intermediary in this scenario, facilitating the controlled operation of high-voltage equipment through the manipulation of low-voltage signals. [8]

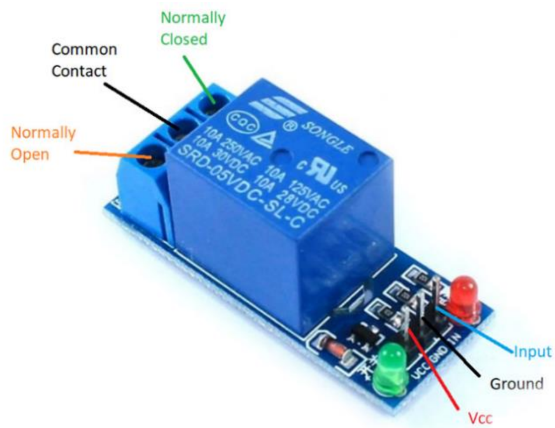

Figure 2.4 SRD-05VDC-SL-C Relay Module

2.3.5.2 Working Principle:

At its core, the functionality of the Figure 2.5.5.1 hinges upon a relatively straight-forward principle. Acting akin to a switchboard operator, the module responds to signals emanating from a microcontroller by energizing an internal electromagnet. This, in turn, prompts the actuation of a switch mechanism within the module, thereby enabling the passage of higher voltage currents through the relay's contacts. Essentially, the module functions as a remote-control mechanism for various appliances and devices, allowing for seamless integration into diverse electronic systems.[9]

2.3.5.3 Pin Description:

Figure 2.5 SRD-05VDC-SL-C Relay Module Pin Layout

Central to the functionality of the single channel 5V relay module are its constituent pins[9]:

Pin Description for Figure 2.5.:

- VCC (Positive Voltage Input):
  This pin is used to supply power to the relay module. It typically requires a 5V DC input voltage to activate the relay and control its switching mechanism.
- GND (Ground):
  The GND pin serves as the reference point for the electrical circuit and completes the power supply connection by providing the ground connection for the module.
- IN (Control Input):
  The IN pin is the control input for the relay module. It accepts signals from a microcontroller or other control devices to trigger the switching action of the relay, allowing for the activation or deactivation of the relay's contacts.
- NO (Normally Open):
  This pin is one of the output terminals of the relay. In its default state (when the relay is not energized), the NO pin is not connected to any other pin. When the relay is activated, the NO pin becomes connected to the COM pin, completing the circuit for the connected load.
- NC (Normally Closed):

The NC pin is the other output terminal of the relay. In its default state, the NC pin is connected to the COM pin, completing the circuit for the connected load. When the relay is activated, the connection between the NC and COM pins is broken.

- COM (Common):

  The COM pin is the common connection point for both the NO and NC pins. It serves as the interface for the load that the relay is controlling. Depending on the relay's state (energized or de-energized), the Common (COM) pin establishes the electrical connection with either the NO or NC pin.

2.3.5.4 Steps on How to Use A SRD-05VDC-SL-C Relay Module[8][9]:

The utilization of a single channel 5V relay module follows a systematic procedure:

- Power Connection:

  Establish the requisite power supply by connecting the VCC and GND pins to the appropriate power source.

- Signal Integration:

  Interface the IN pin with an output pin of the microcontroller, enabling the transmission of control signals to the relay module.

- Load Connection

  Attach the device intended for control to the COM and NO (normally open) terminals of the relay module.

- Programming:

  Develop a software program tailored to the specific requirements of the project, dictating the sequence of signals sent to the relay module.

- Testing and Optimization:

  Execute comprehensive testing procedures to validate the functionality of the relay module within the context of the project, refining the operational parameters as necessary.

2.3.5.5 Significance in the Project:

The single-channel 5V relay module assumes paramount significance within projects necessitating the controlled manipulation of high-voltage equipment. Consider, for instance, the implementation of an automated home garden system, where the module facilitates the orchestrated operation of watering mechanisms, illumination systems, and environmental control devices based on real-time sensor data. By providing a safe and efficient means of interfacing high-power devices with microcontroller-based systems, the relay module emerges as an indispensable component in the realization of sophisticated electronic applications.

In summary, the single channel 5V relay module, despite its unassuming stature, embodies a pivotal element in the landscape of electronic prototyping and project development. Its intuitive functionality, coupled with its versatility and reliability, renders it an indispensable asset for enthusiasts and professionals alike seeking to realize innovative electronic designs.

2.3.6 ESP32 For IOT .

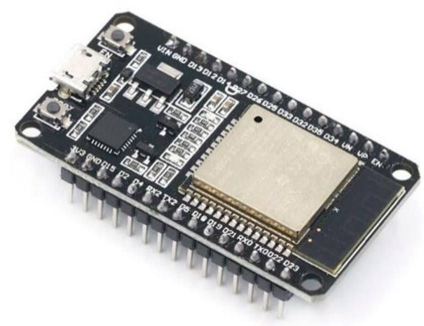

Figure 2.6: ESP 32 Micro controller

2.3.6.1 Introduction:

Figure 2.5.5.1 shows a powerful microcontroller developed by Espressif Systems, renowned for its versatility and capabilities in Internet of Things (IoT) applications. Launched as a successor to the ESP8266, the ESP32 offers enhanced processing power, built-in Wi-Fi and Bluetooth connectivity, and a rich set of peripherals, making it an ideal choice for a wide range of IoT projects, including access control systems.[10]

2.3.6.2 Working Principle and Features on An ESP 32:

At the heart of the ESP32 is a dual-core Tensilica Xtensa LX6 microprocessor, which operates at up to 230 MHz clock frequency. This dual-core architecture enables multitasking and efficient handling of complex tasks, ensuring smooth operation of IoT applications. Furthermore, the ESP32 integrates Wi-Fi 802.11 b/g/n and Bluetooth 3.2/BLE connectivity, providing seamless communication with other devices and networks.[11]

One of the standout features of the ESP32 is its rich set of peripherals, including GPIO pins, SPI, I2C, UART, and ADC interfaces, which facilitate interfacing with various sensors, actuators, and external devices. Additionally, the ESP32 supports low-power modes, enabling energy-efficient operation for battery-powered IoT devices.[11]

2.3.6.3 ESP32 Pin Description:

The ESP32 WROOM module is a powerful microcontroller with numerous pins that serve various functions. Here is a detailed pin description for the ESP32 WROOM module[12]:

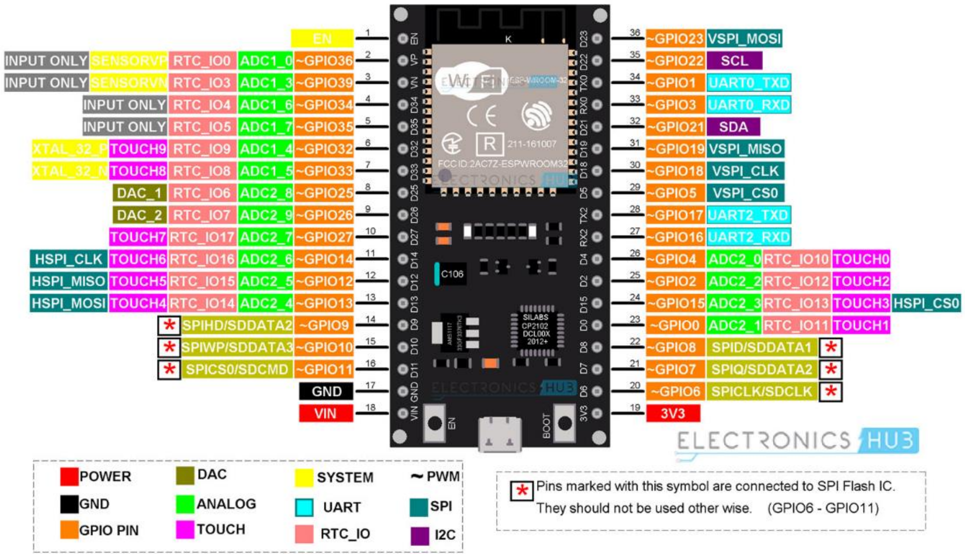

Figure 2.7: ESP 32 Pin Description

1. Power Supply Pins [12]:

- VCC (3.3V): This pin provides the operating voltage for the ESP32 WROOM module. It should be connected to a stable 3.3V power source.
- GND (Ground): These pins are connected to the ground of the power supply.

2. GPIO Pins (General Purpose Input/Output):

- The ESP32 WROOM module features multiple GPIO pins that can be conFigured as digital input or output.
- These pins are used for interfacing with sensors, actuators, and other external devices.
- Each GPIO pin can be individually controlled and conFigured using software.

3. Analog Pins:

- The ESP32 WROOM module includes several analog input pins that support analog-to-digital conversion (ADC).

- These pins are used for reading analog signals from sensors such as temperature sensors, light sensors, and potentiometers.

3. UART Pins:

- UART (Universal Asynchronous Receiver/Transmitter) pins are used for serial communication.
- The ESP32 WROOM module features multiple UART interfaces for communicating with other microcontrollers, computers, or peripherals.

5. SPI Pins:

- SPI (Serial Peripheral Interface) pins facilitate high-speed serial communication between the ESP32 and external devices such as displays, SD cards, and other microcontrollers.
- The ESP32 WROOM module supports multiple SPI interfaces with configurable clock rates and data formats.

6. I2C Pins:

- I2C (Inter-Integrated Circuit) pins enable communication with devices using the I2C protocol.
- The ESP32 WROOM module supports both I2C master and slave modes, allowing it to interface with a wide range of I2C-compatible sensors, displays, and peripherals.

7. PWM Pins (Pulse-Width Modulation):

- PWM pins allow the generation of analog-like signals with varying duty cycles.
- These pins are commonly used for controlling the brightness of LEDs, the speed of motors, and other applications requiring analog voltage control.

8. Bootstrapping Pins:

- Bootstrapping pins are used during the boot process to conFigure various boot modes and settings of the ESP32 WROOM module.
- These pins are typically pulled high or low using external resistors to select different boot configurations.

9. External Interrupt Pins:

- External interrupt pins allow the ESP32 WROOM module to respond to external events or signals with minimal latency.
- These pins can trigger interrupt service routines (ISRs) in response to changes in signal levels, allowing for real-time event handling.

Understanding the pinout and functionality of the ESP32 WROOM module is essential for designing and implementing various IoT projects and applications just as it is crucial in this . By utilizing the diverse set of pins and interfaces provided by the ESP32 WROOM module, developers can create sophisticated and versatile IoT solutions with ease.

2.3.6.4 Significance in IoT Access Control Systems:

In (internet of things) IoT access control systems, the ESP32 offers several key advantages. Firstly, its integrated Wi-Fi capability enables seamless connectivity to local networks and the internet, allowing for remote monitoring and control of access points. Secondly, the ESP32's robust processing power and multitasking capabilities enable the implementation of sophisticated access control algorithms and user authentication mechanisms. Furthermore, its support for low-power modes ensures efficient operation, extending the battery life of wireless access control devices. Moreover, the GPIO (general purpose input/out pins) pins and communication interfaces of the ESP32 facilitate integration with various sensors, Radio Frequency Identification (RFID) readers, biometric scanners, and actuators commonly used in access control systems. This flexibility enables the implementation of diverse access control mechanisms, including card-based, biometric, and smartphone-based authentication methods.[10][12]

In summary, the ESP32 serves as a versatile and feature-rich platform for developing IoT access control systems, offering a combination of processing power, connectivity, and peripheral interfaces that are well-suited to the demands of modern access control applications. The ESP32 represents a pivotal tool in the development of IoT access control systems, providing the necessary features, connectivity, and processing power to implement sophisticated access control mechanisms effectively. Its significance lies in its ability to enable seamless communication, efficient operation, and flexible integration with peripheral devices, thereby empowering developers to create secure and scalable access control solutions for various environments and applications.

3 Design

3.1 Overall Access Control System Architecture

The system architecture diagram of an access control system project shown in Figure 3.1 is a comprehensive visual representation that elucidates the structural framework, interconnections, and functionalities of the system components. It serves as a pivotal tool for understanding how various modules, devices, and services collaborate harmoniously to achieve the overarching goals of the system. The introductory statement for this diagram provides a contextual overview by outlining the purpose, scope, and key aspects of the architecture.

In this context, the introductory statement begins by delineating the overarching purpose of the access control system and the specific scope covered within the architecture diagram. It emphasizes the diagram's role in illustrating the holistic structure of the system, spotlighting critical components such as access controllers, user interfaces, databases, sensors, and communication protocols. Each component's role and contribution to the system's functionality are succinctly described, offering a clear understanding of their interdependencies.

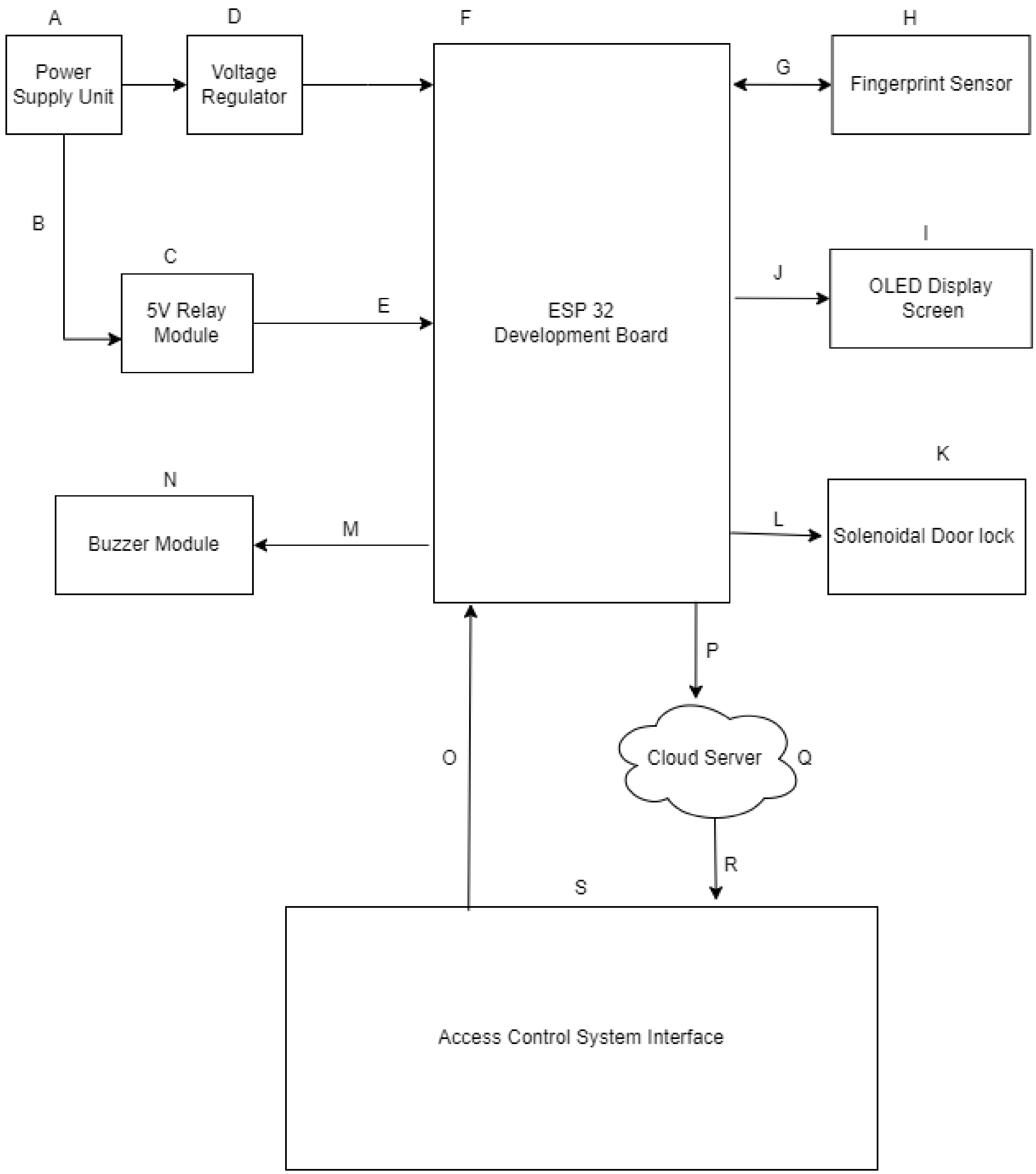

Figure 3.1 : This is the overall Access Control System architecture.

j

Figure 3.1 shows the complete system architecture of the access control system, the elements of this system is explained below:

A. Power Unit Supply – this module will be a 12V power supply that will be the primary source of power to the circuit.
B. Uni-directional connection to a 5V Relay module represents the interface between the micro-controller and the 5V Relay Module serving as the 12V COM connection.
C. 5V Relay 1 Channel Module : This will be used as a switch to momentarily provide power to the solenoidal door lock to unlock.
D. LM7805 Voltage Regulator : This component will ensure that a stable 5V is maintained in case the input power from the power supply fluctuates.
E. Uni-directional connection to micro-controller which acts as the path required by the ESP32 development board needs to send a pulse to an external module such as the buzzer or solenoid door lock.
F. ESP 32 Development Board- this module will act as the processing hub for the access control system.
G. Bi-directional interface between the processing unit and the fingerprint sensor.
H. Fingerprint Sensor – this is the fingerprint module that will store fingerprints as well as performing the verification.
I. OLED Display Screen – this is be used to display readable text to the user.
J. Uni-directional connectors to the OLED display screen from the esp32.
K. Solenoidal Door Lock – this is the module that will allow a authorized user to physically open the access way.
L. Uni-directional connection from the ESP32 Development Board to the solenoidal door look, a electrical pulse is sent along this connection and the mechanism will enable to the lock to unlock.
M. Uni directional Connection to Buzzer Module where a signal is sent along component M to the Buzzer module.
N. Buzzer Module – this will the module that will emit a single beep if a fingerprint is verified and a long beep if the fingerprint is not authorized.
O. This is uni-directional connection from the Access Control Admin interface to the ESP32 Development board in the event that a fingerprint needs to be removed.

P. Access Control System Interface where all the data in the system can be visualized in Cloud Server that will store all access entries verified by the fingerprint sensor and the result of the logic function that is triggered by the successful verification of a fingerprint scan. This interface is going to be created in JavaFX (a combination of java for the logical code and FXML for the visual creations) and operated by the system administrator.

3.2 Proposed Design And Code Flows

3.2.1 Student Option Process Flow

The CRUD (Create, Read, Update, Delete) actions carried out on a Java object that represents a guest are depicted in this flow diagram. In order for the reader to acquire a clearer picture of how data modification happens in the context of student management, each operation is illustrated in Figure 3.2. The basic procedures for maintaining student records are depicted in the diagram, including adding new students, getting student information, updating current student information, and removing student records.

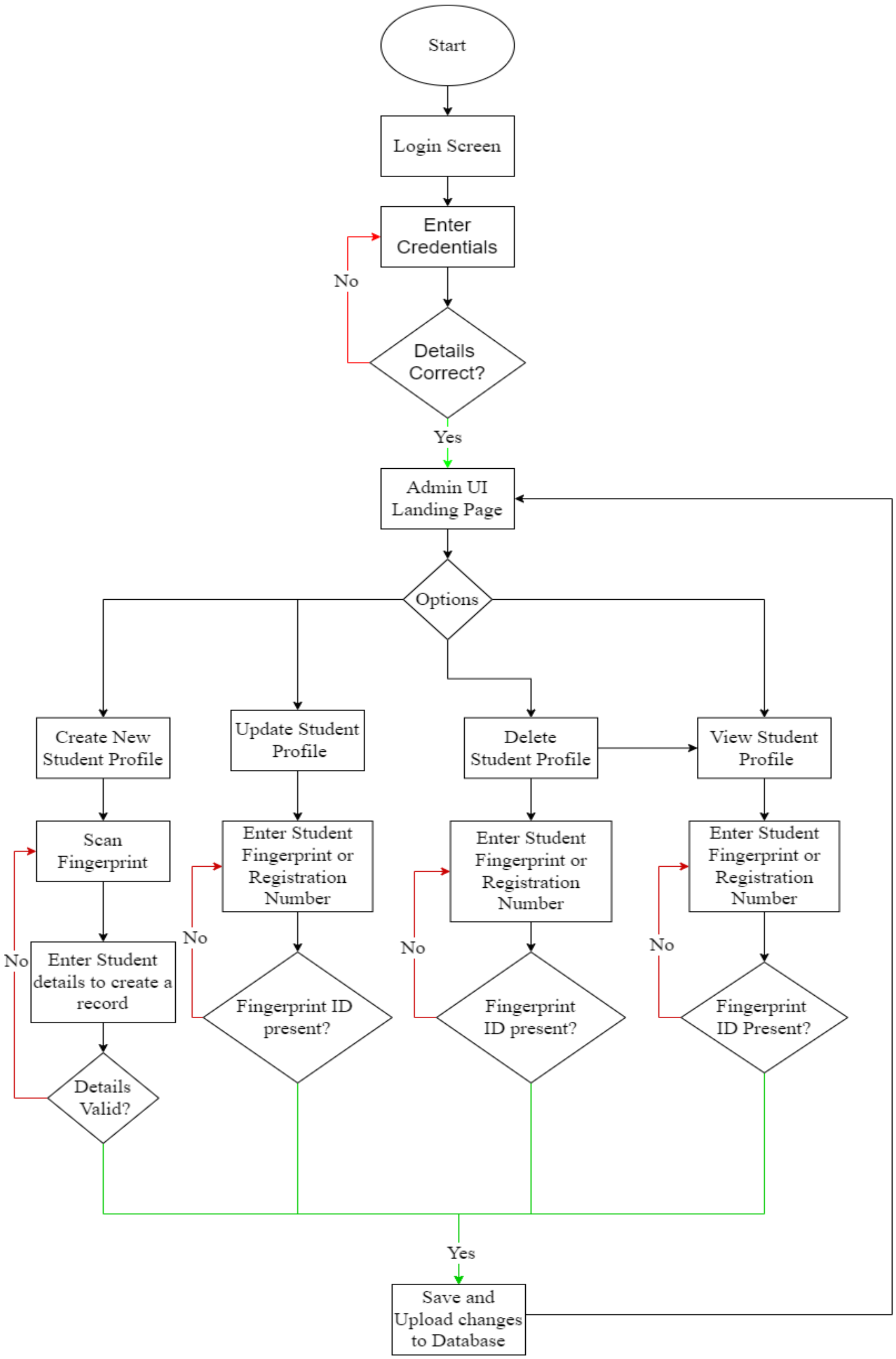

Figure 3.2: Flow chart illustration the Student Process Flow.

.

Figure 3.2 illustrates how the process workflows that the administrator can undertake if they are performing CRUD actions related to students in the system. The illustration clearly shows that the administrator will login into the administration interface the login view, where they proceed if the login credentials are correct. In relation to the workflow, there will be four actions that can be undertaken.

- Create New Student Profile:
  This requires the student to place their finger on the fingerprint sensor so that the sensor can take an initial scan, they will then remove the finger and place it on the sensor again so that the sensor can take another scan. The fingerprint uses the two scans to create a template. Upon successful enrollment, the fingerprint returns an integer value depicting the page ID the fingerprint template has been saved under in the sensor storage, then the admin can head to the next screen to associate the fingerprint ID with the user profile then saving those details into the system.

The admin is led to the All Authorized Users screen where all system users are displayed, by searching and selecting the user's record. The admin is given three options:

- View Student Profile:
  This allows the admin to have the user's profile information displayed in a read-only state.
- Update Student Profile:
  This allows the admin to have the user's profile information displayed in a editable manner to which the alterations can be saved to the database.
- Delete Student Profile:
  This allows the admin to have the user's profile information displayed in a read-only state and by clicking in _Remove Record_ the selected record is deleted.

3.2.2 Guest Process Flow

The CRUD (Create, Read, Update, Delete) actions carried out on a Java object that represents a guest are depicted in this flow diagram. To give a clear picture of how data modification happens in the context of guest management, each operation is illustrated. The basic procedures for maintaining visitor records are depicted in the diagram, including adding new guests, getting guest information, updating current guest information, and removing guest records.

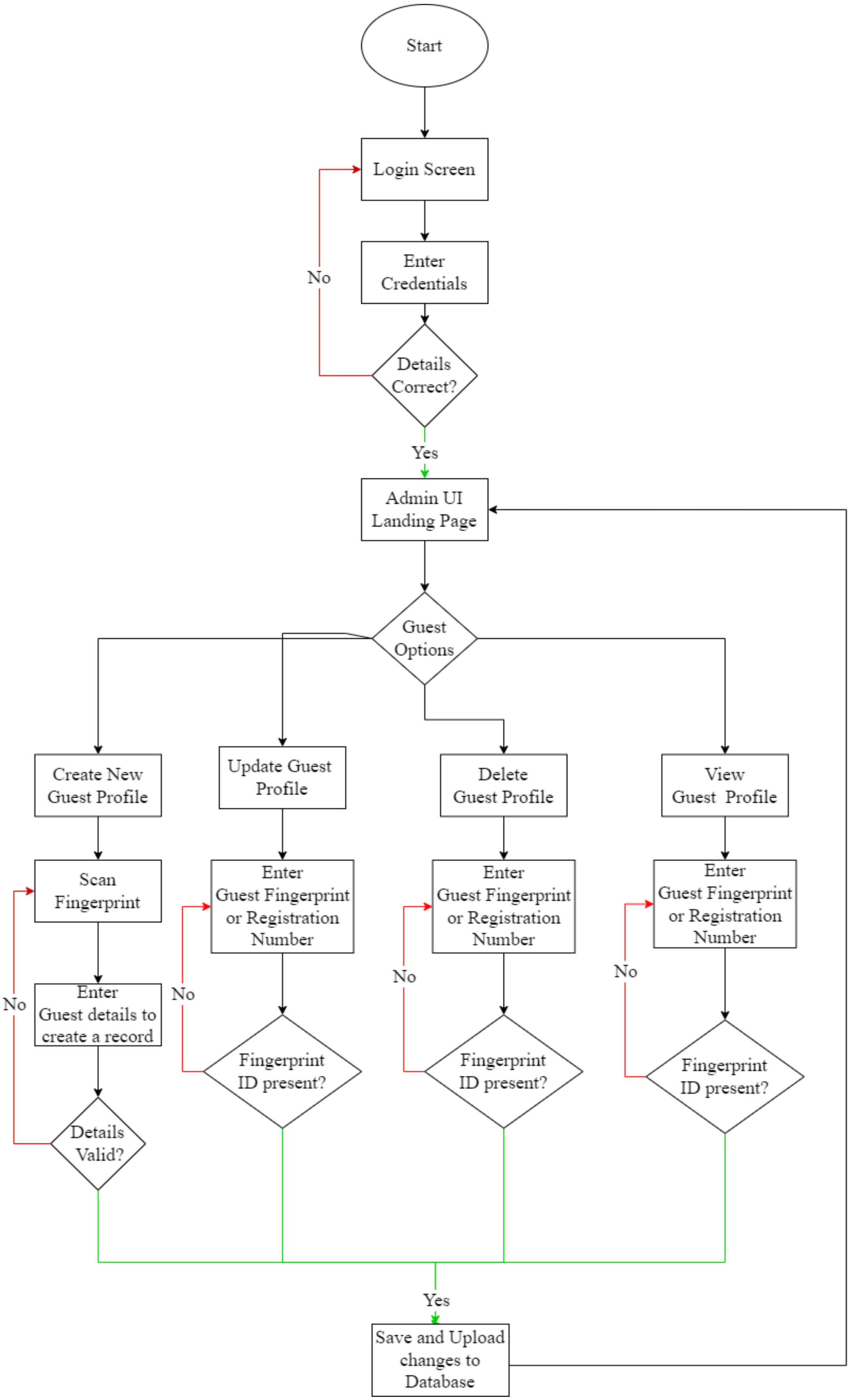

Figure 3.3: Flow chart showing the Guest System Process Flow.

Figure 3.3 illustrates how the guest process workflows that the admin can undertake if they are performing actions related to guests in the system. The illustration clearly shows that the admin will login into the admin interface the login view, where they proceed if the login credentials are correct. In relation to the workflow, there will be four actions that can be undertaken.

Create New Guest Profile:

This requires the student to place their finger on the fingerprint sensor so that the sensor can take an initial scan, they will then remove the finger and place it on the sensor again so that the sensor can take another scan. The fingerprint uses the two scans to create a template. Upon successful enrollment, the fingerprint returns an integer value depicting the page ID the fingerprint template has been saved under in the sensor storage, then the admin can head to the next screen to associate the fingerprint ID with the user profile then saving those details into the system.

The admin is led to the **All-Authorized Users** screen where all system users are displayed, by searching and selecting the user's record. The admin is given three options:

View Guest Profile:

This allows the admin to have the selected user's profile information displayed in a read-only state.

Update Guest Profile:

This allows the admin to have the selected user's profile information displayed in a editable manner to which the alterations can be saved to the database.

Delete Guest Profile:

This allows the admin to have the selected user's profile information displayed in a read-only state and by clicking in *Remove Record* the selected record is deleted.

3.2.3 Admin Process Workflows

The CRUD (Create, Read, Update, Delete) actions on a Java object that represents a user categorized as an admin are displayed in this flow diagram. The admin user related actions related to the management of admin-related data by looking at this Figure 3.4, which shows how new admin profiles can be created, admin information can be retrieved, admin details can be updated, and admin records can be deleted. The present graphic offers a thorough synopsis of all the fundamental functions associated with managing and preserving admin-related information in a Java program.

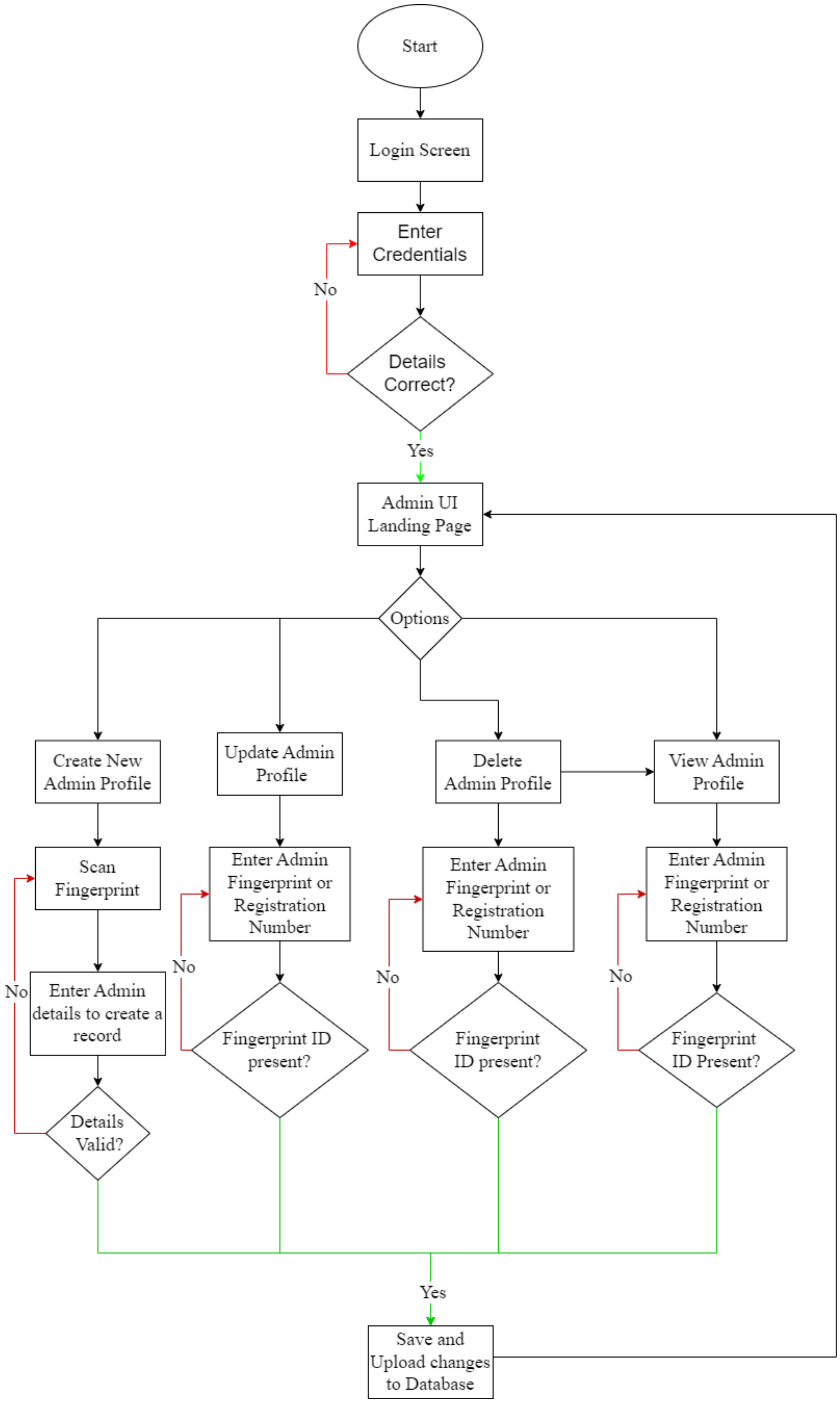

Figure 3.4: Flow chart showing the Admin system process flow

Figure 3.3 illustrates how the process workflows:

that the admin can undertake if they are performing actions related to students in the system. This illustration clearly shows that the admin will login into the admin interface the login view, where they proceed if the login credentials are correct. In relation to the workflow, there will be four actions that can be undertaken.

- Create New Admin Profile:
  This requires the new Admin to place their finger on the fingerprint sensor so that the sensor can take an initial scan, they will then remove the finger and place it on the sensor again so that the sensor can take another scan. The fingerprint uses the two scans to create a template. Upon successful enrollment, the fingerprint returns an integer value depicting the page ID the fingerprint template has been saved under in the sensor storage, then the admin can head to the next screen to associate the fingerprint ID with the user profile then saving those details into the system.

The admin is led to the **All-Authorized Users** screen where all system users are displayed, by searching and selecting the user's record. The admin is given three options:

- View Admin Profile:
  This allows the admin to have the selected user's profile information displayed in a read-only state.
- Update Admin Profile:
  This allows the admin to have the selected user's profile information displayed in a editable manner to which the alterations can be saved to the database.
- Delete Admin Profile:
  This allows the admin to have the selected user's profile information displayed in a read-only state and by clicking in _Remove Record_ the selected record is deleted.

3.3 Low Fidelity Wire Frame Descriptions.

Low-fidelity wireframes are fundamental designs for digital interfaces that provide a condensed visual depiction of the organization and design of the Admin interface software program. Functionality takes precedence over aesthetics in these wireframes, which concentrate on crucial components including interactive features, navigation flow, and content placement. These help in the early phases of design by outlining important features and user interactions in a clear and organized manner for the user interface. Low-fidelity wireframes play a crucial role in promoting cooperation among designers, developers, and stakeholders, steering the development process in the direction of producing digital experiences that are simple and easy to use.

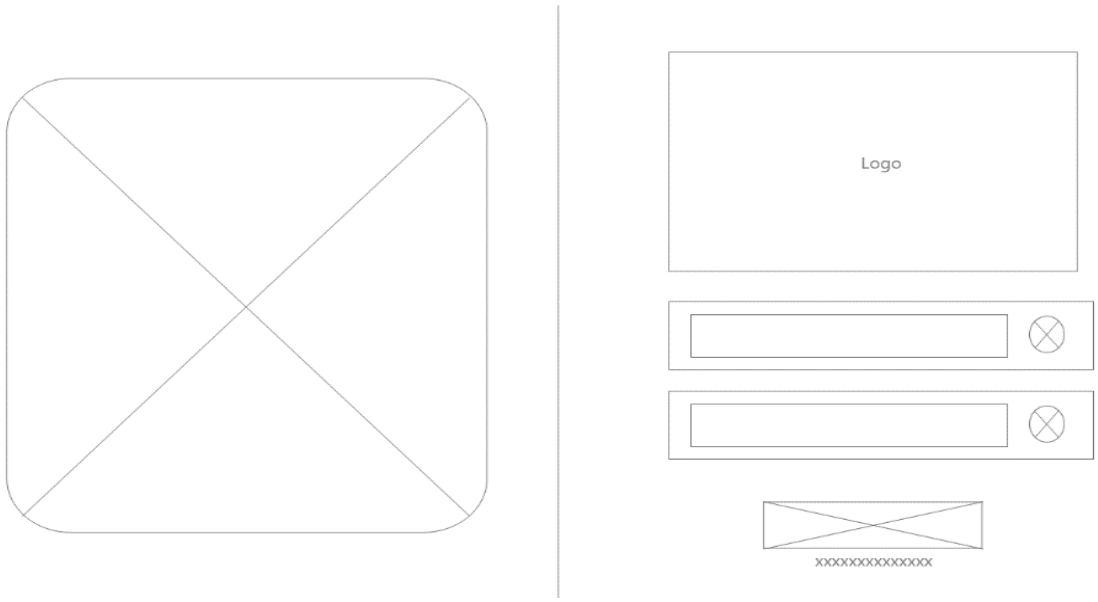

Figure 3.5: Low fidelity wire frame for the login user screen

Figure 3.5 show the low fidelity wire frameor the login user screen, it shows that there is going to be an image insert on the left and the rest of the screen elements are going to be on the right. On the right it starts with the system logo followed by the username input field with an icon logo and the same repeated for the password input field and its corresponding icon that will be used to display the error icon. The last two elements are buttons and some text to be displayed underneath the button.

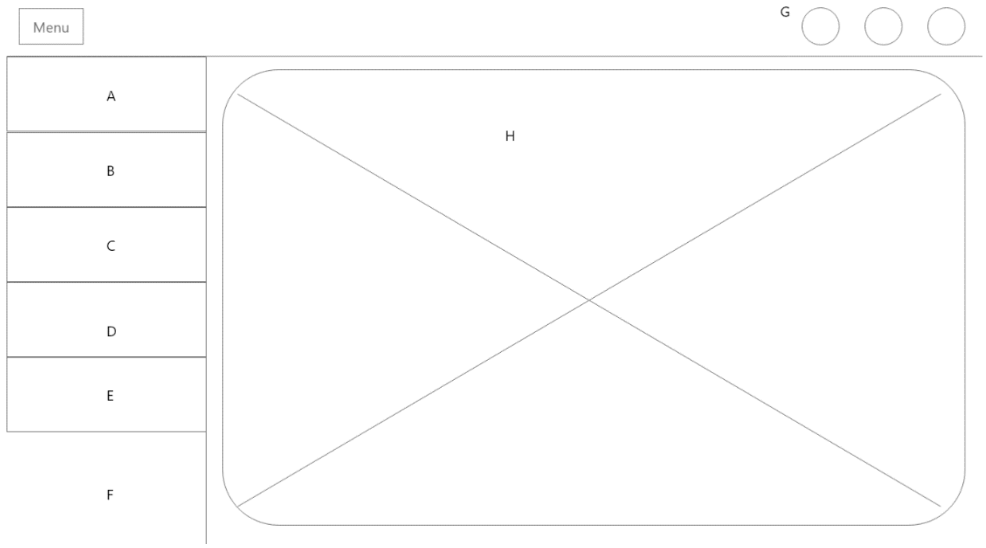

Figure 3.6: the low fidelity wire frame for the dashboard user screen,

Figure 3.6 show the low fidelity wire frame for the dashboard user screen, it shows that there is going to be an options pane on the left and in the header-area will be used to display the access entries.

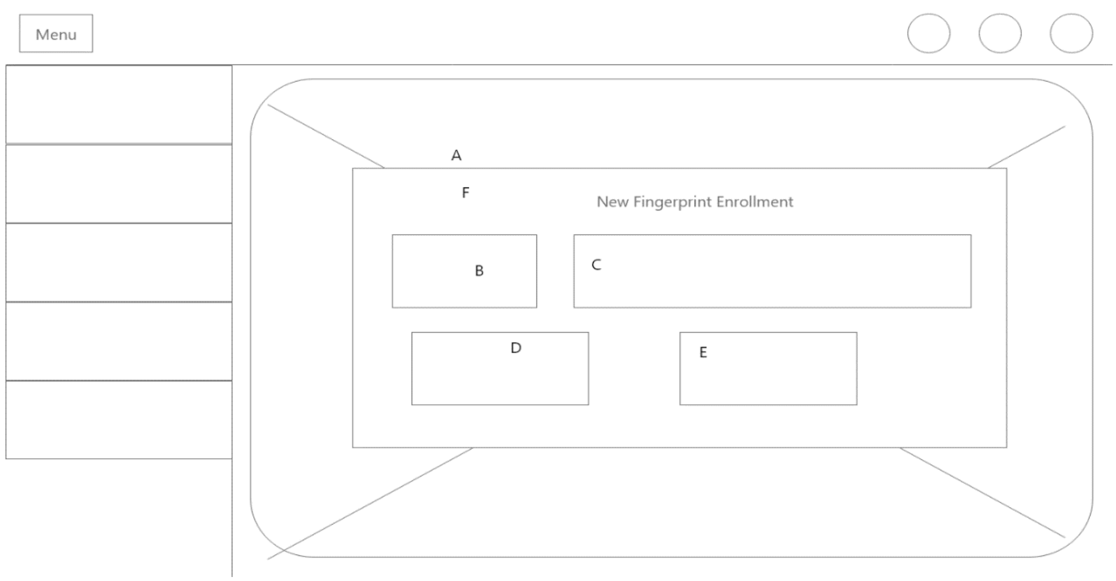

Figure 3.7: Low fidelity wire frame for the add new fingerprint screen,

Figure 3.7 show the low fidelity wire frame for the add new fingerprint screen, it shows that there is going to be a screen pop up that will inflate when the admin wishes to add a new fingerprint. Items B, C, are input fields which will automatically filled with read-only data. B is the fingerprint ID and C is the fingerprint owner's System ID (registration number for students, employment number for admins and national ID for guests).

Item D and E will be buttons, D will the cancel button to dismiss the pop-up window and E will be the confirm button to proceed.

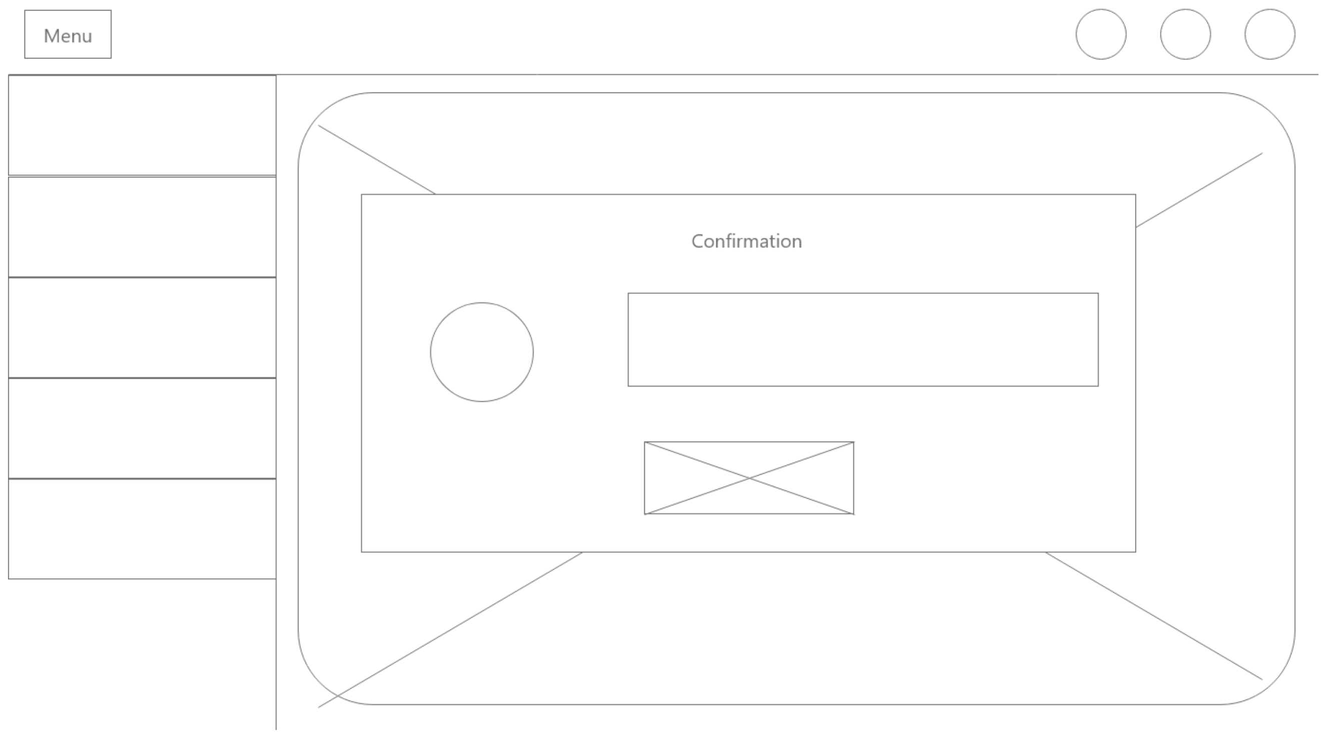

Figure 3.8 : low fidelity wireframe shows the confirmation pop up

Figure 3.8 shows the low fidelity wireframe shows the confirmation pop up where the admin will receive a confirmation screen that the task that was being undertaken is successful. The icon will gave a title, with an icon next to some content block with a button underneath. That is how this wireframe is to be interpreted.

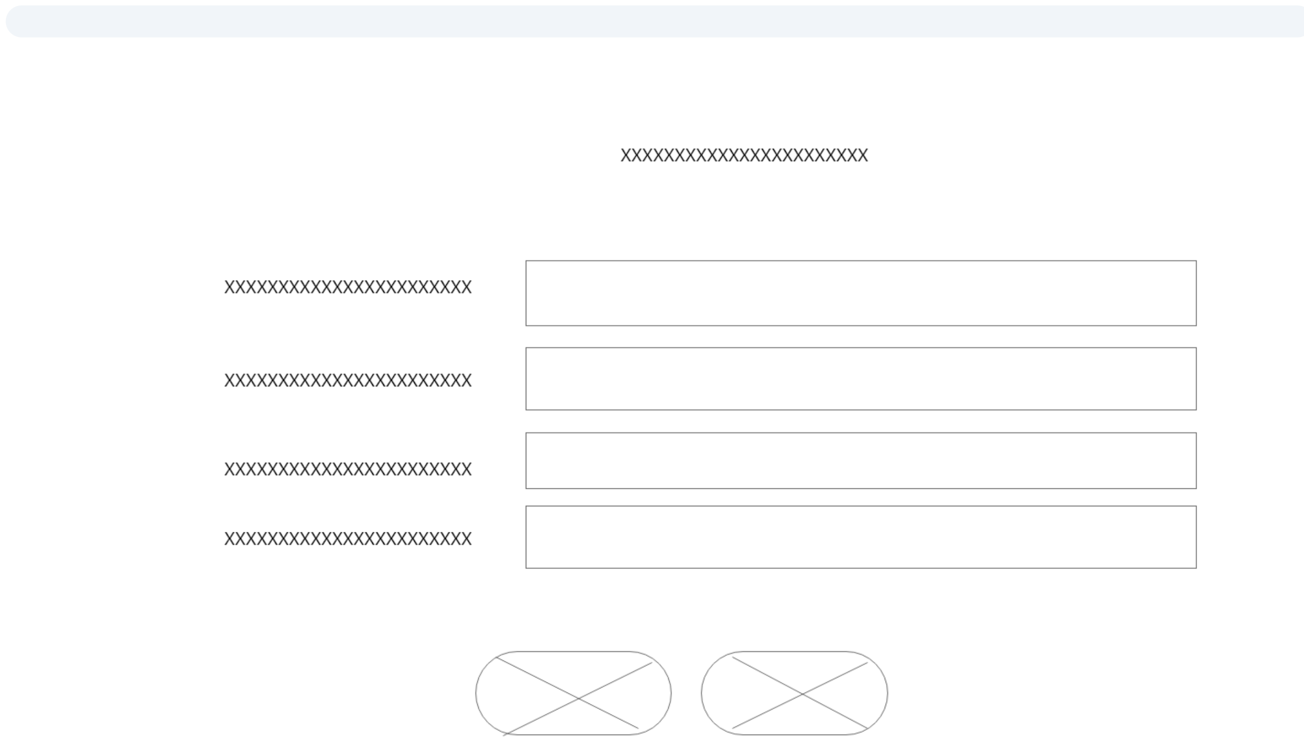

Figure 3.9 : The wireframe layout will be used for the fingerprint association, update, delete and view authorized user details.

Figure 3.9 shows the wireframe layout will be used f to design the form that will be utilized for fingerprint association, update, delete and view authorized user details. Each rectangle resembles an input field and the dummy text represented by X's will be descriptive text of what the content of the input field.

3.3.1 The Proposed High Fidelity Admin Interface Designs

Compared to low-fidelity wireframes, high-fidelity wireframes are a more polished and visually correct representation of the final product, representing a more iterated and comprehensive version of digital interface concepts. To accurately mimic the real user interface experience, these wireframes include design elements including color schemes, typography, images, and interactive components. They give stakeholders and designers a thorough understanding of the structure, features, and visual appeal of a website or software program, enabling them to assess and improve the design prior to implementation. High-fidelity wireframes are essential for conveying design ideas, validating usability, and ensuring that design choices meet user needs. All of these processes lead to the development of captivating and user-focused digital experiences.

3.4 Admin Interface Login Screen High Fidelity Frame.

Figure 3.10 :Admin interface Login Screen High Fidelity Frame.

Figure 3.10 is the high-fidelity wireframe design for the login page has a simple, user-friendly interface with security and convenience in mind. Prominent components in the layout include an input form for the username, a field for the password, and a login button. The password and username fields are placed thoughtfully, and the labels clearly indicate what data should be entered.

The unusual design of the login button makes it stand out and indicates that it is the primary step for starting the login process. The whole layout places a high value on usability and functionality, making it possible for users to safely and easily visit the login page and validate their credentials.

3.4.1 High Fidelity Wire Frame – Dashboard.

Figure 3.11: High Fidelity Wire Frame – Dashboard

Figure 3.11 show the high fidelity wire frame for the dashboard user screen, it shows that there is an options pane on the left and in the header area is used to display the access entries as mentioned in the description for Figure 3.6.

3.4.2 High Fidelity Wire Frame – Add New Fingerprint Pop Up.

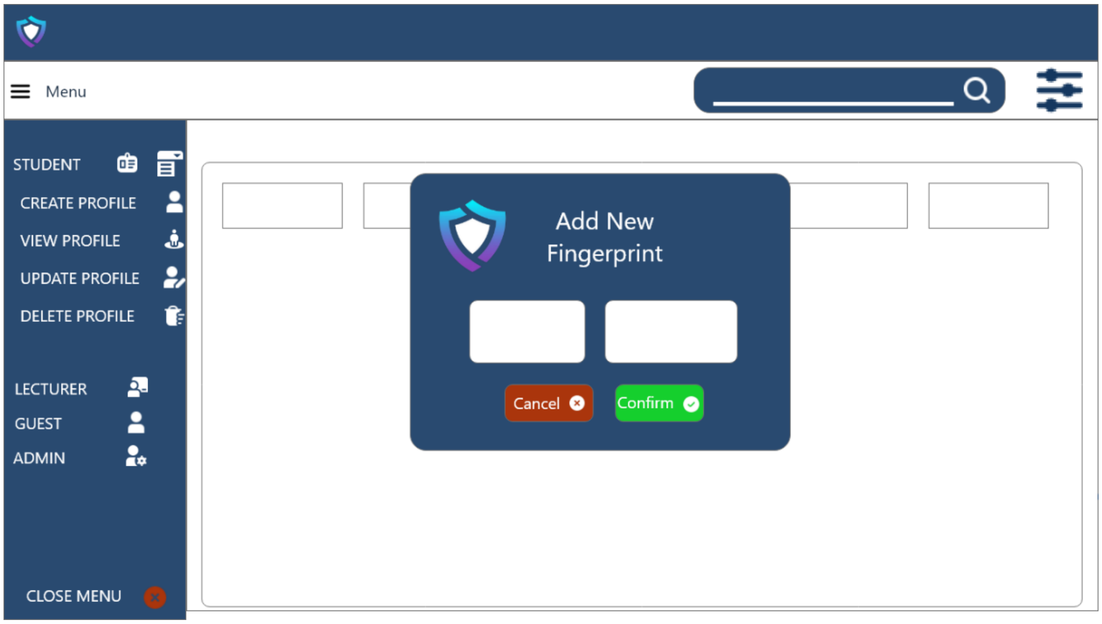

Figure 3.12 High Fidelity Wire Frame – Add New Fingerprint Pop Up

Figure 3.12 is the *Add New Fingerprint* screen view that was references from the low fidelity that was then converted to a high-fidelity (high quality).

3.4.3 High Fidelity Wire Frame – Add New Fingerprint Confirmation Pop

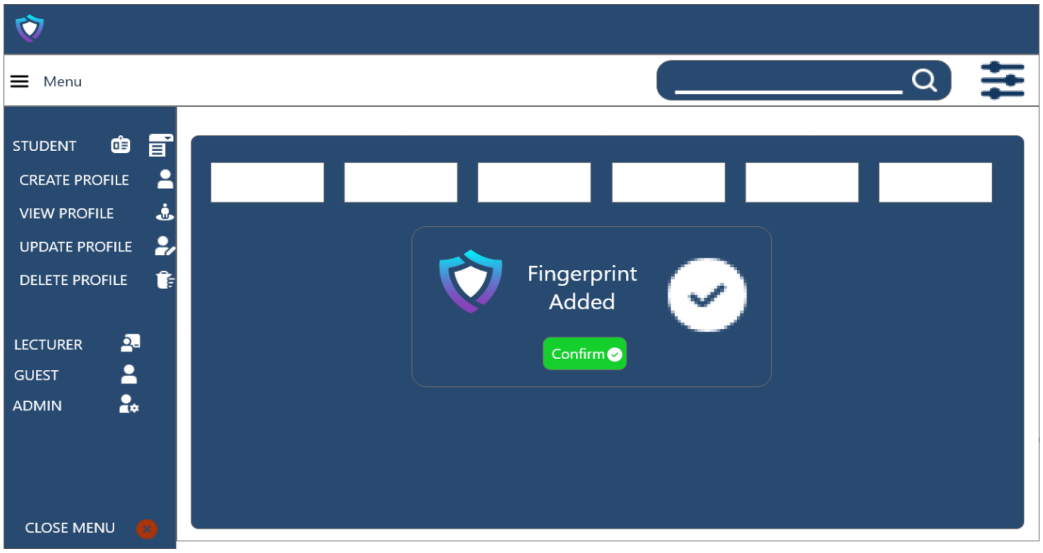

Figure 3.13 :High Fidelity Wire Frame – Add New Fingerprint Confirmation Pop Up

Up.

Figure 3.13 shows the high-fidelity wireframe shows the confirmation pop up where the admin will receive a confirmation screen that the ***Add fingerprint*** task that was being undertaken is successful. The pop will be given a title, with a tick icon next to some content block with a confirm button underneath. That is how this wireframe is to be interpreted as mentioned in Figure 3.8.

3.4.4 High Fidelity Wire Frame – Associate Fingerprint with User Profile

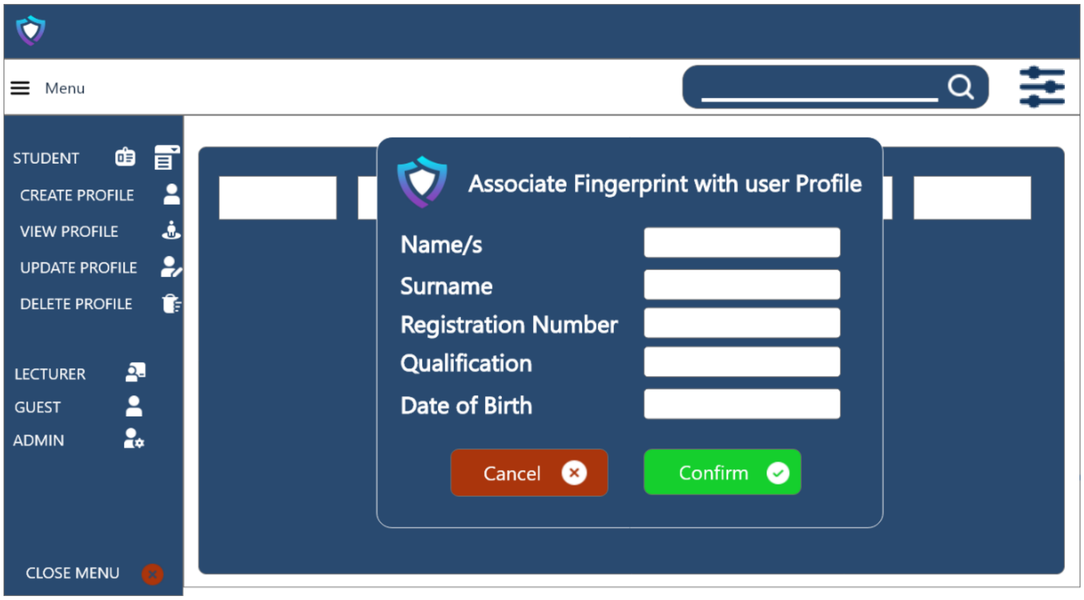

Figure 3.14 High Fidelity Wire Frame - Associate Fingerprint with User Profile

Figure 3.11 shows the high-fidelity wireframe layout will be used for the fingerprint association, update, delete and view authorized user details. input fields and the supporting instructional text are shown which hints on the required content of the input field as initially mentioned in Figure 3.9.

3.4.5 High Fidelity Wire Frame – User Successfully Association

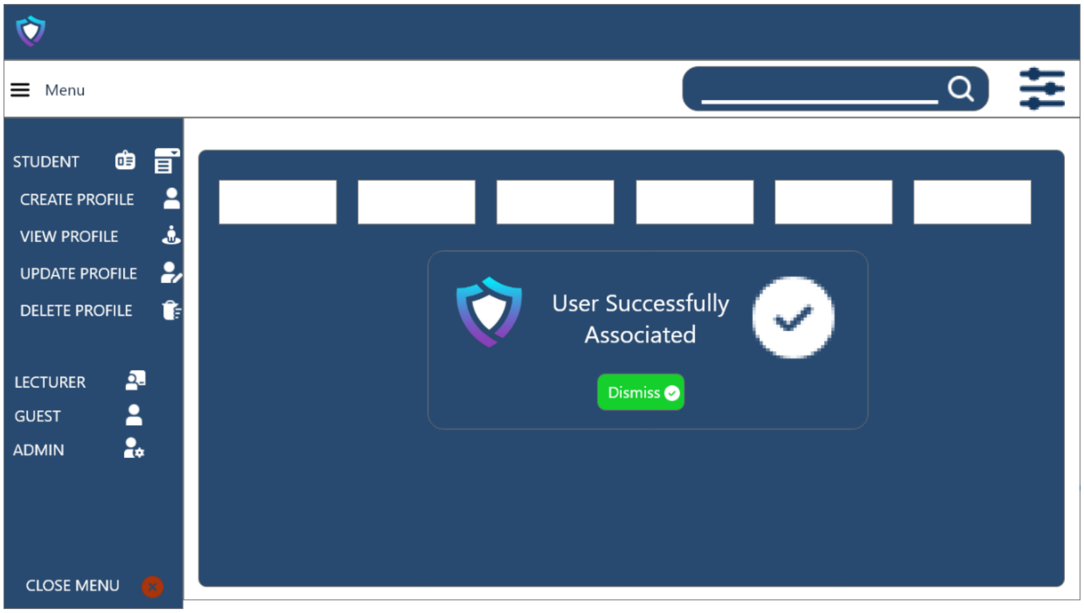

Figure 3.15 High Fidelity Wire Frame - User Successfully Association

Figure 3.15 shows the low fidelity wireframe shows the confirmation pop up where the admin will receive a confirmation screen that the user has been successfully linked to the fingerprint ID. The icon will have a title, with an icon next to some content block with a confirmation button underneath. That is how the high fidelity wireframe is to be interpreted.

3.5 Circuit Hardware Design

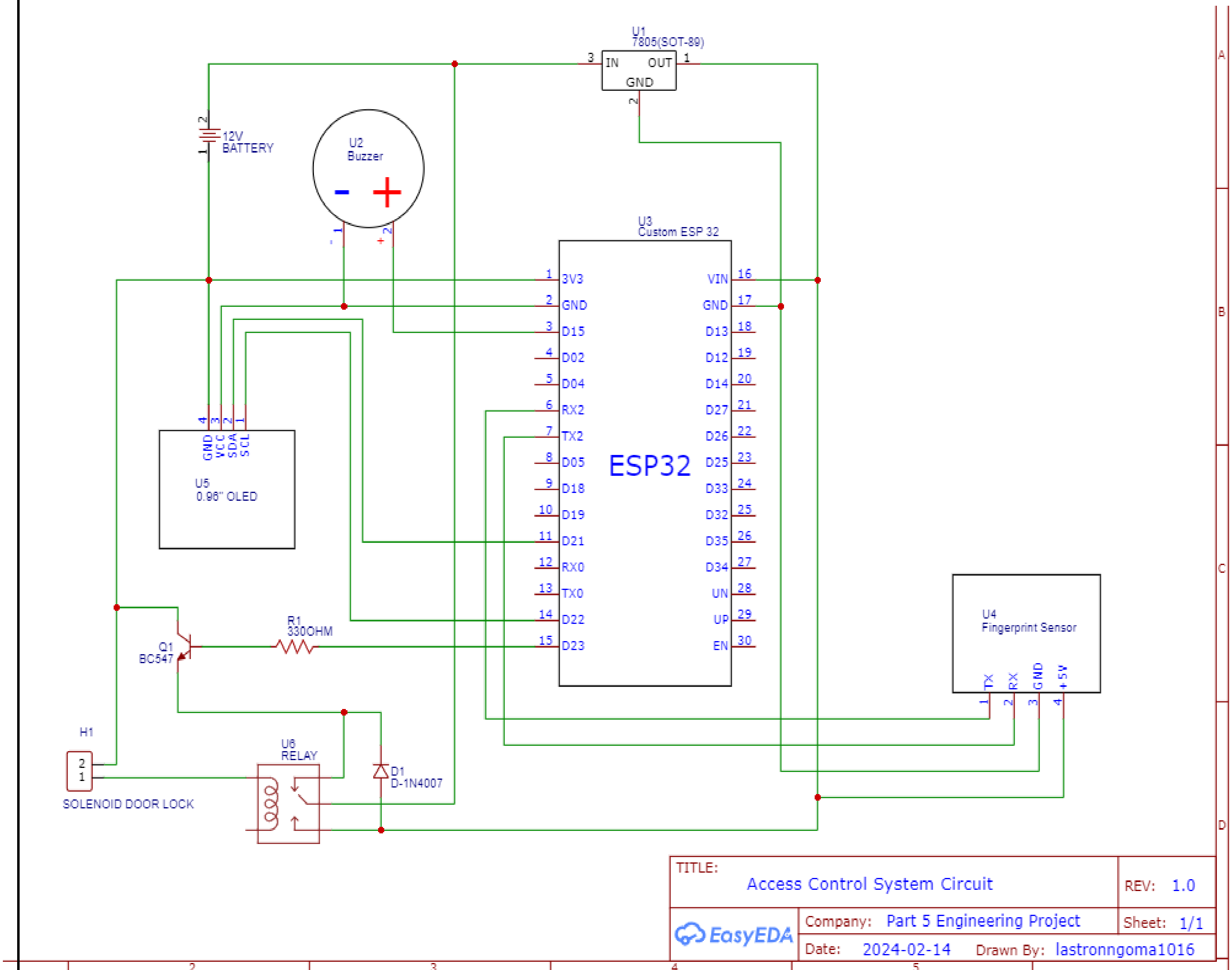

Figure 3.16: The image insert shows the schematic circuit diagram for the access control system

Figure 3.16 shows the schematic circuit diagram for the access control system hardware unit, this circuit was created using an online editor called EasyEDA. The circuit shown in Figure 3.16 serves as the electronic circuit implementation of the hardware architecture design shown in Figure 3.1. The 12V battery will act as the source of power that feeds the LM7805 regulator, its purpose is to provide a stable 5V power supply to the ESP 32 Micro-controller, the fingerprint sensor, 5V relay module and the OLED display. Thus with the varying loads, the LM7805 ensures that a 5V is maintained. The ESP32 controller is the heart of the system as it contains the logical code base that determines how the statuses, input, output from the peripherals devices (Fingerprint sensor, OLED display, solenoid door lock. buzzer) attached to the controller. Transistor Q1 is the BC547 is a transistor that was incorporated in the design since the ESP32 uses a logical voltage of 3.3V. This is because of the SRD-05VDC-SL-C relay requires a minimum switching voltage of 5V, hence the Q1 will act as a switch, the enabling signal from D23 is sent to the base, will enable transistor Q1 allowing the 12V to be supplied to the relay's IN pin (input signal pin) thus switching the relay on which in turn retracts the solenoid door lock. Diode (D1) is the current overload relay, the solenoidal door lock is a very current heavy device, so it will draw a lot of current when energizing the solenoid that when a current overload occurs during the switching off action of the relay, hence to protect the relay and the ESP32, the excess current is conducted to ground. This ensures that the 3.3V logic high voltage from the ESP32 pin is sufficient to operate the relay.

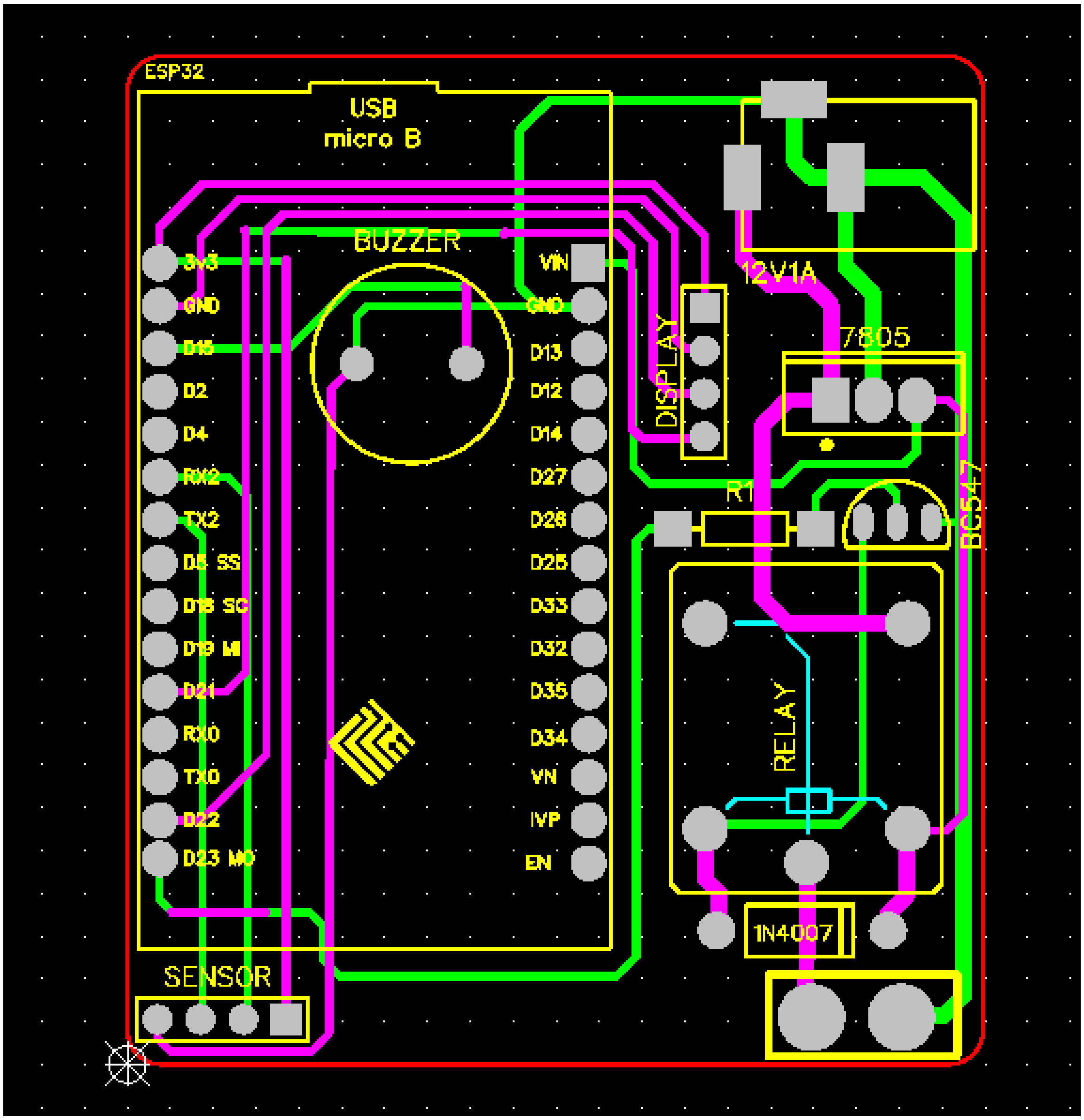

Figure 3.17: Image Insert Of Most Optimized Circuit Print Circuit Board (PCB) Layout

Figure 3.17 is the project author's most optimized circuit print circuit board (PCB) layout that was designed and developed given the level of knowledge of this report's author at that point in time. This circuit passed all the quality control tests when compared against the industry standards (strict regulations like no 90-degree wire bends.) that must be abided by. The purple lines represent the top conducting layer hence the purple lines are the circuit lines for the top layer and the green layer represents the bottom conducting layer meaning that this is a double conducting layer printed circuit board diagram.

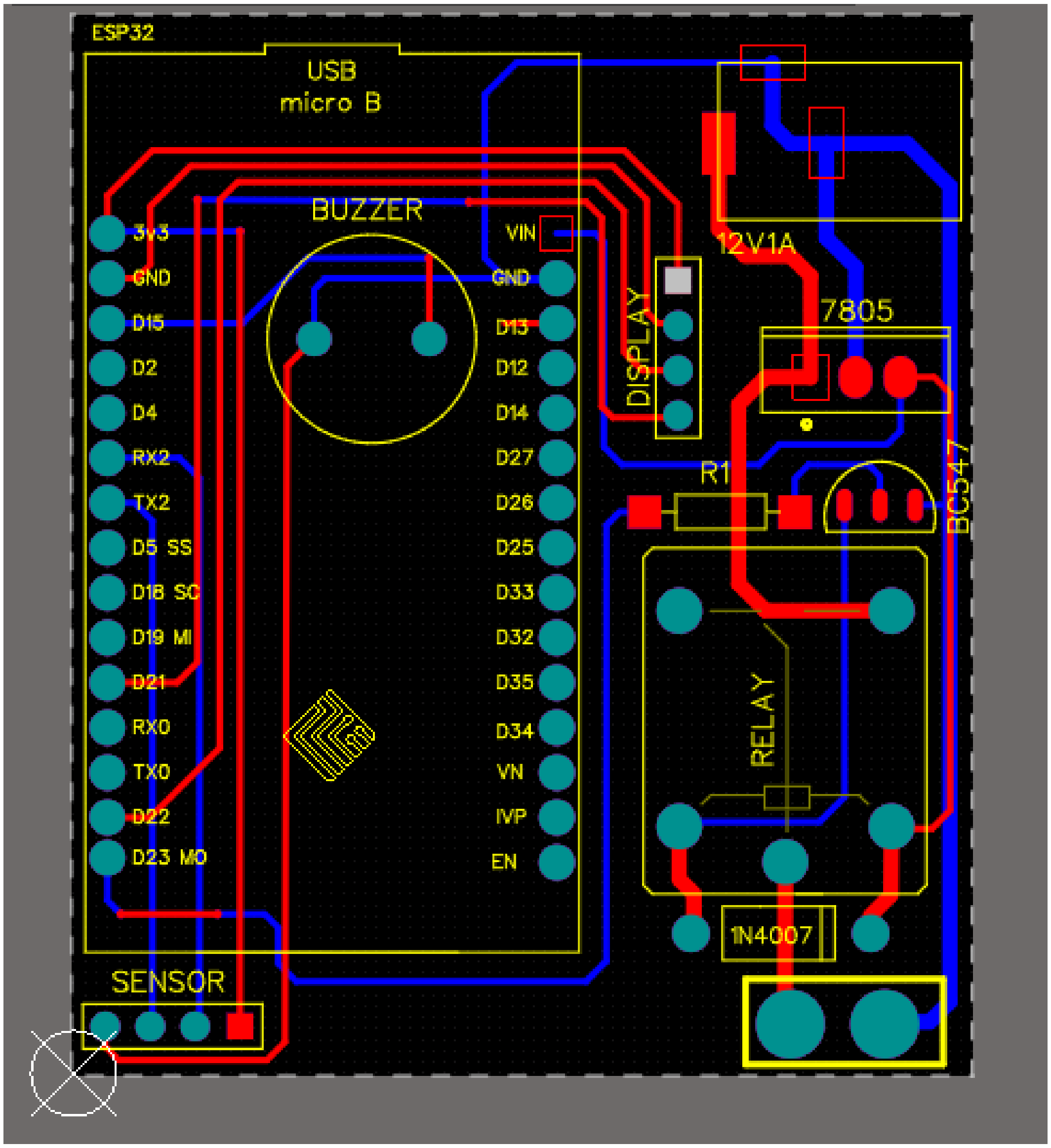

Figure 3.18: The image shows simply is the PCB circuit inserted as a png image insert in the report.

Figure 3.18 shows simply is the PCB circuit developed and designed as per the project's custom inserted as a PNG image insert in the report. It is the same image; the only difference is that Figure 3.18 is a the raw circuit design where as Figure 3.17 is the circuit design exported from the PCB Designer called Altium. This PCB design considers a number of factors in order to guarantee efficiency, usefulness, and compactness. The ESP32 module, the piezo buzzer, and other required components are among the first few steps in the process that must be clearly understood in order to meet the project's needs. Digital drafts or sketches are utilized to see how the layout will look.

The components are carefully chosen, with special attention paid to the piezo buzzer, whose dimensions are such that it fits snugly beneath the ESP32 module without sticking out over the top of the module. This stage entails looking over physical measurements and datasheets.

Custom footprints, which precisely define pad widths, pin positions, and component outlines, are made for every component according to its specifications using Altium. In particular, the ESP32 footprint must match the pin layout of the module. When moving from schematic to PCB layout, component placement is optimized for compactness and effective routing. The placement of the piezo buzzer beneath the ESP32 module was thoughtfully designed to maximize available space.

Avoiding 90-degree wire turns can be difficult since they can cause problems with signal integrity and complicate manufacturing. Sharp turns are avoided in wire routing by using angled traces, vias, and component positioning techniques.

In order to improve the PCB's functionality and make room for more conducting tracks, a twin-layer PCB design is chosen. This allows for the creation of a ground plane and gives plenty of room for routing traces on both the top and bottom layers. To make sure the design complies with industry standards, reduces electromagnetic interference, and supports dependable operation, extensive signal integrity checks and design rules verification are carried out after the layout is finished.

A prototype is then created for testing and validation, which involves assembling the components onto the PCB, testing connectivity, functionality, and making sure the piezo buzzer performs as intended.

3.6 Adafruit Subscription

Firstly, a subscription to Adafruit must be created, this requires signing up with Adafruit and once there set of credentials has been created, signing in is show in the steps below.

3.6.1 Create And Link an Adafruit IO Access Control Feed

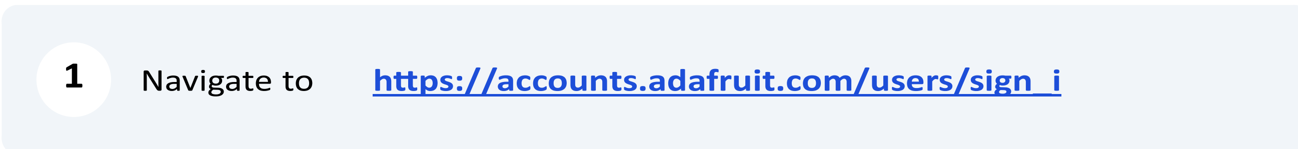

Figure 3.3.19: Adafruit signin interactive link

Figure 3.19 shows the sign in interactive link for Aida fruit IO clicking on this link will directs the user to the sign in Page for adafruit IO.

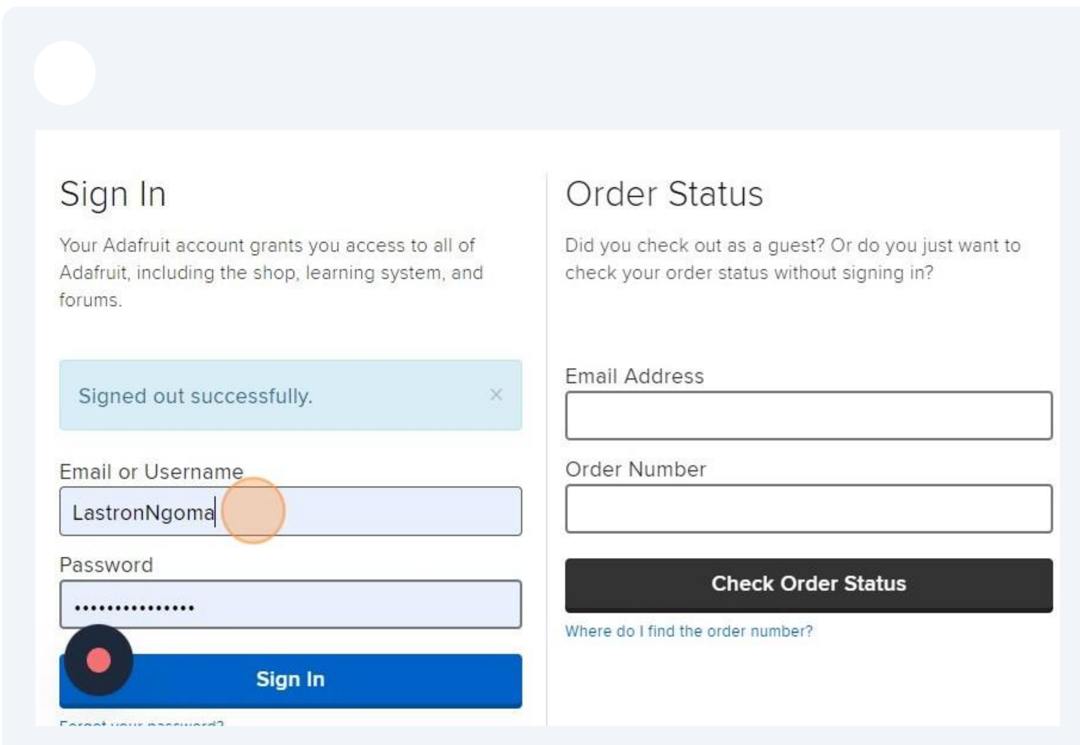

Figure 3.3.20 Sign in page for Adafruit IO

Figure 3.20 shows two input fields that are needed in order to sign in to the aid of fruit IO account entering the username and password. Clicking the sign in button with the correct the ADAFRUIT IO account credentials will then lead to the dashboard being displayed as shown in the Figure 3.3 below.

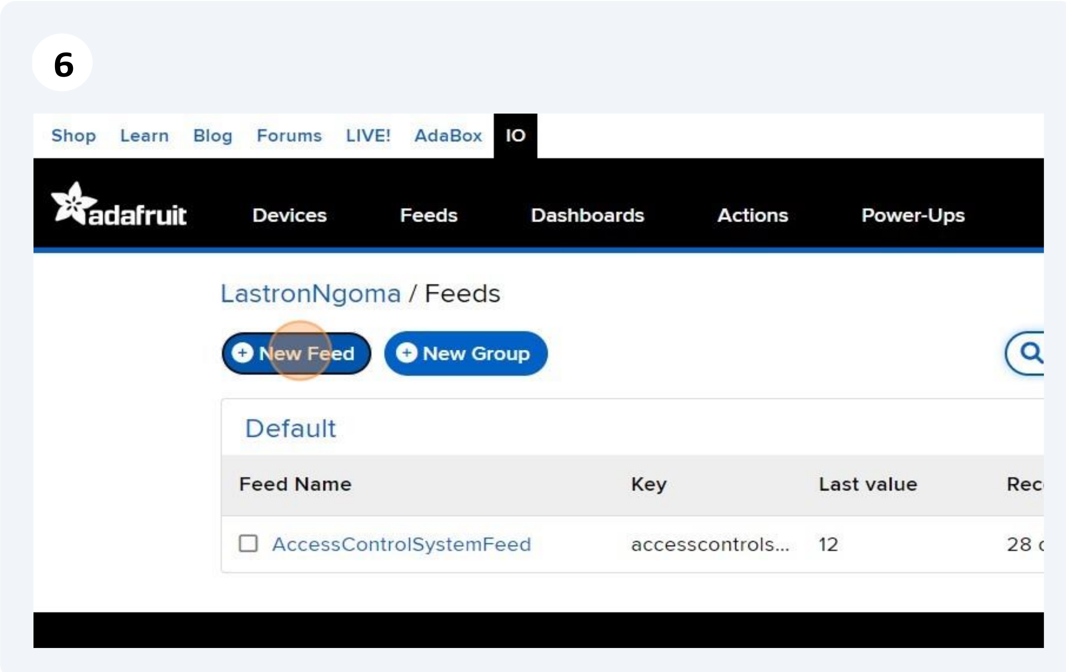

Figure 3.3.21: Snapshot of Adafruit IO dashboard.

Figure 3.21 shows a snapshot of the Adafruit IO dashboard. Navigating to the IO header option following by clicking feeds would lead to the account username slash feeds page this is where a new feed needs to be created clicking on new feed will bring up the feed details input fields that's shown in Figure 3.3 below.

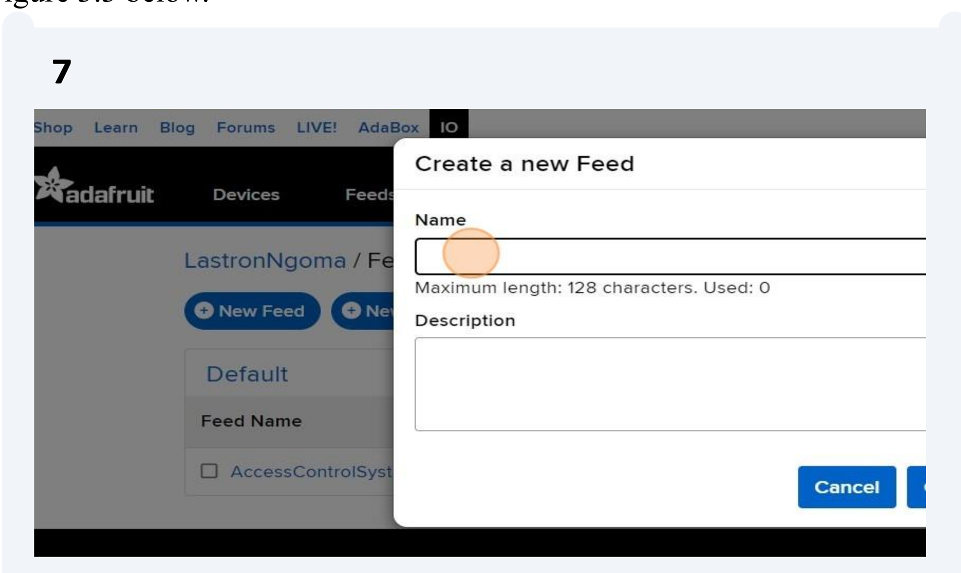

Figure 3.22: Snapshot of Adafruit IO feed creation form.

Figure 3.22 is a snapshot of the Adafruit IO feed creation form. This is where the feed name needs to be named as well as a brief description of the feed functionality. Essentially a feed is going to be the end point where the published data of the Internet of Things project is going to be stored for later access it also provides a free dashboard where the account owner is able to see the timestamps as well as upload data. Upon successful feed creation the new feed will be visible as shown in Figure 3.5 below in this instance access control feed is the newly created feed.

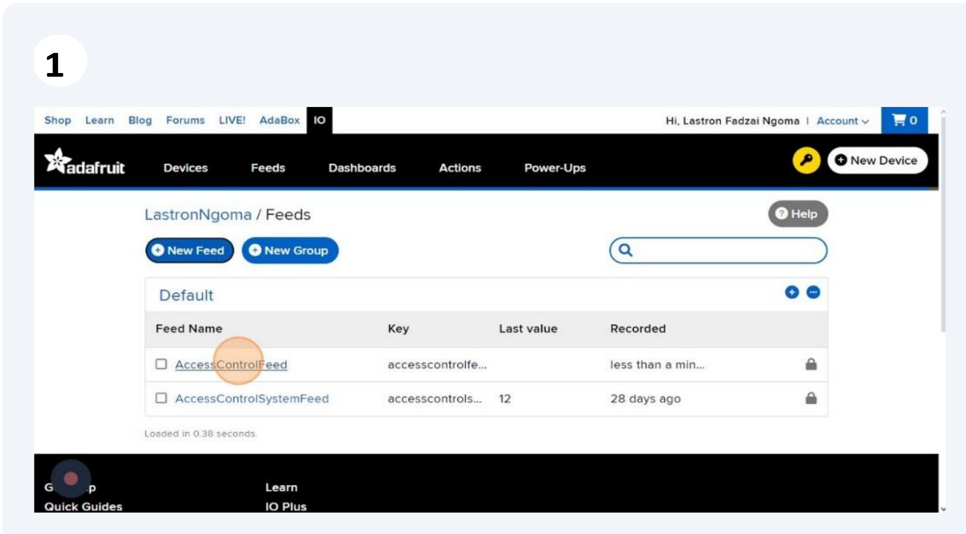

Figure 3.23: Adafruit IO feed dashboard.

Figure 3.23 shows the Adafruit IO collection view, where all account feeds can be viewed and accessed. In this project's context, the AccessControlFeed is desired feed to be accessed, clicking

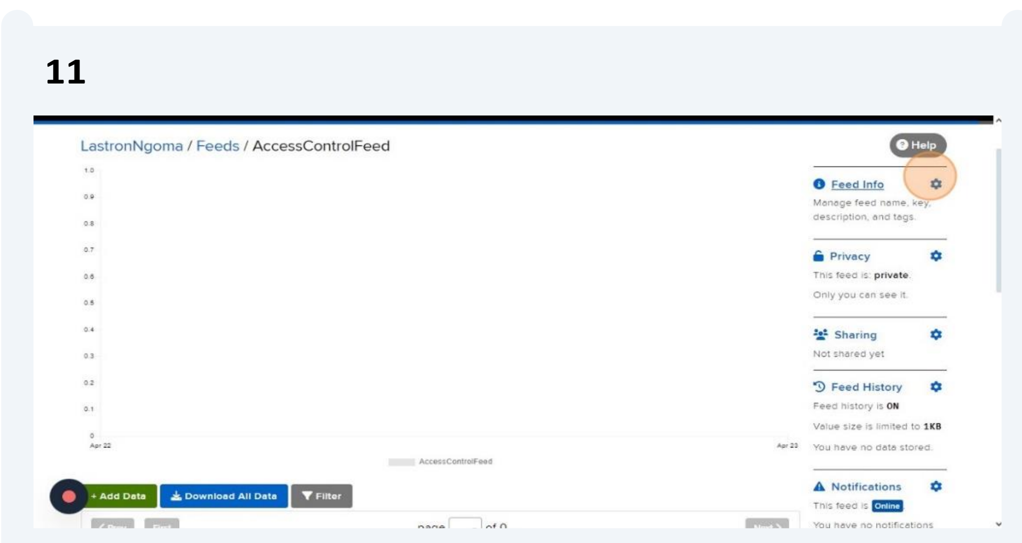

Figure 3.24: Created feed dashboard with dashboard information.

on the feed will open the feed dashboard where all feed details are displayed as shown below in Figure 3.25.

In Figure 3.25 is the feed dashboard where further information about the feed can be acquired. Whats important is under the feed information option where the way the feed needs to be accessed as shown in Figure 3.25.

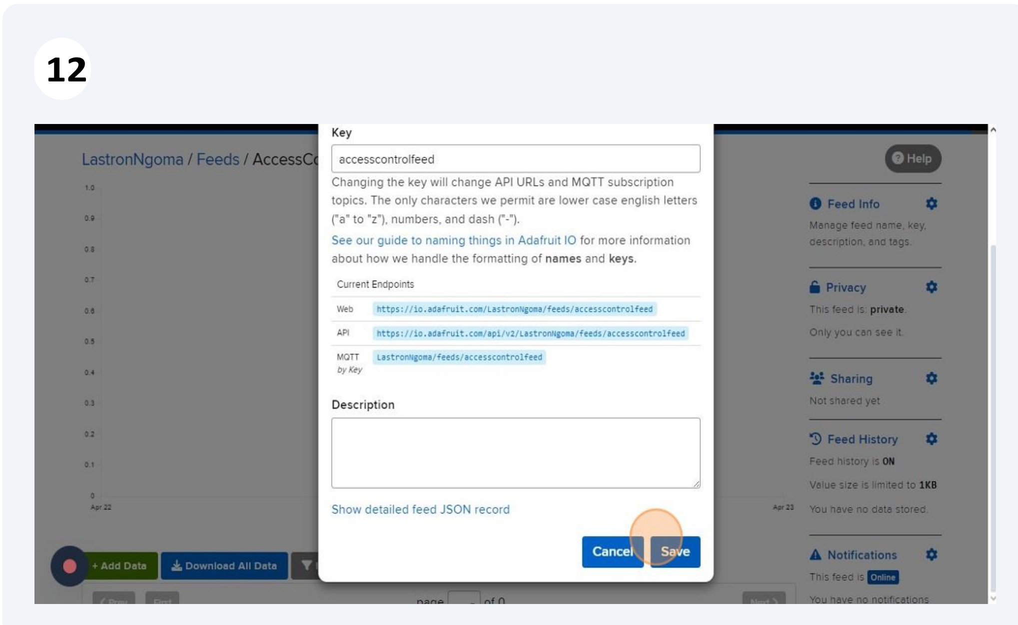

Figure 3.25: Snapshot of the created feed info.

Figure 3.7 shows the feed info and how it can be used in the code base to make a connection to the Adafruit IO platform. For the purposes of this project, the MQTT (Message Queuing Telemetry Transport) by key will be the current endpoints used. This will be used in the ESP 32 code. MQTT stands for Message Queuing Telemetry Transport. It is a lightweight messaging protocol for use in cases where clients need a small code footprint and are connected to unreliable networks or networks with limited bandwidth resources.

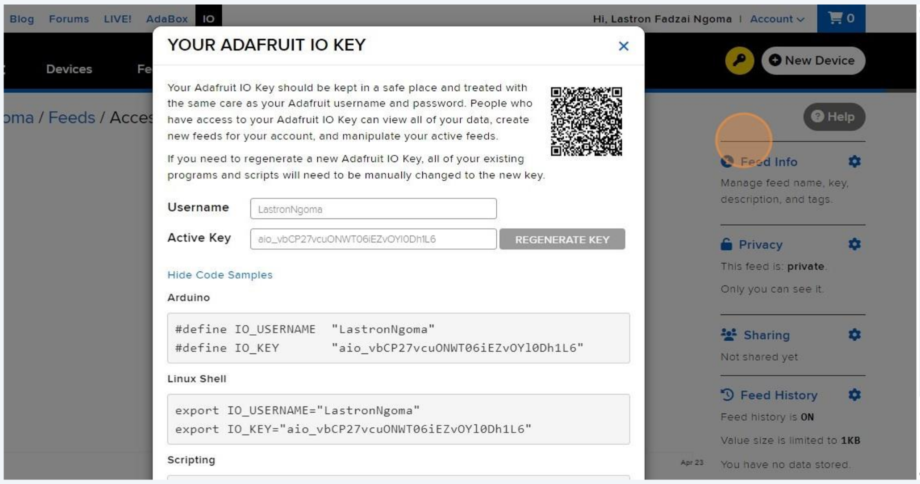

Figure 3.26: This Is The Feed Info Display.

Figure 3.26 shows the code samples that will be used to initiate to the Adafruit IO feed connection, the connection relies on the username and API key as credentials.

3.7 Creating Firebase Project

Once this has been completed, create a firebase project that will act as a bridge or buffer in the loosely coupled architecture that is created in the main system architecture Figure 3.1.

3.7.1 Create Access Control Project on Firebase

Click on the interactive link to head to the google firebase portal:
https://console.firebase.google.com/u/0

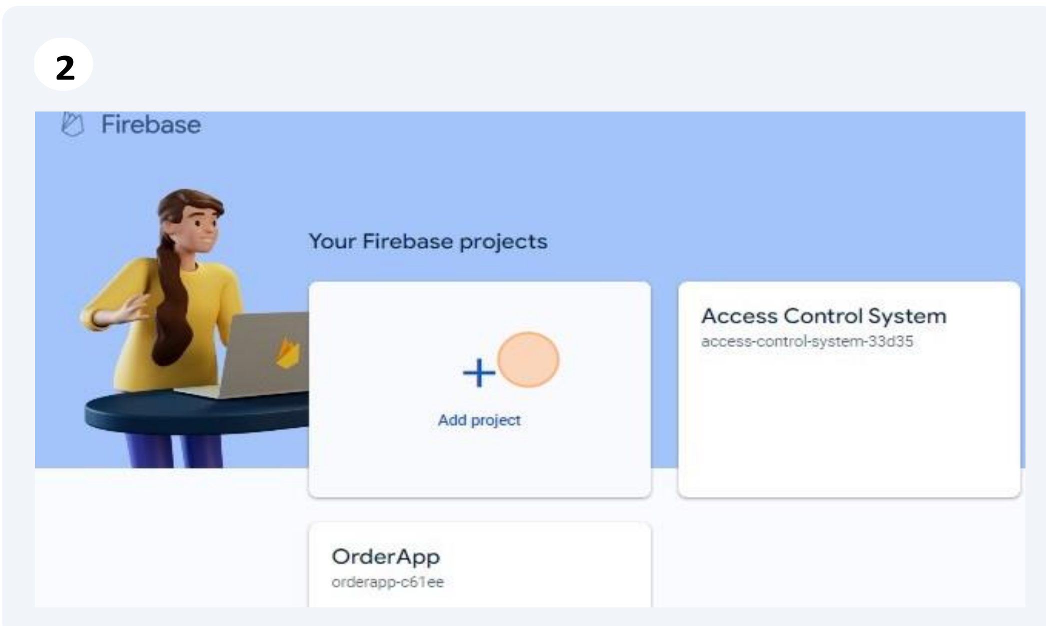

Figure 3.27: Snapshot Of A Firebase Projects On The Firebase Dashboard.

After successfully logging into the google firebase portal as shown in Figure 3.27, a project needs to be created and be assigned a name, after that accept the default project settings and click *Continue* until the permissions page is reached.

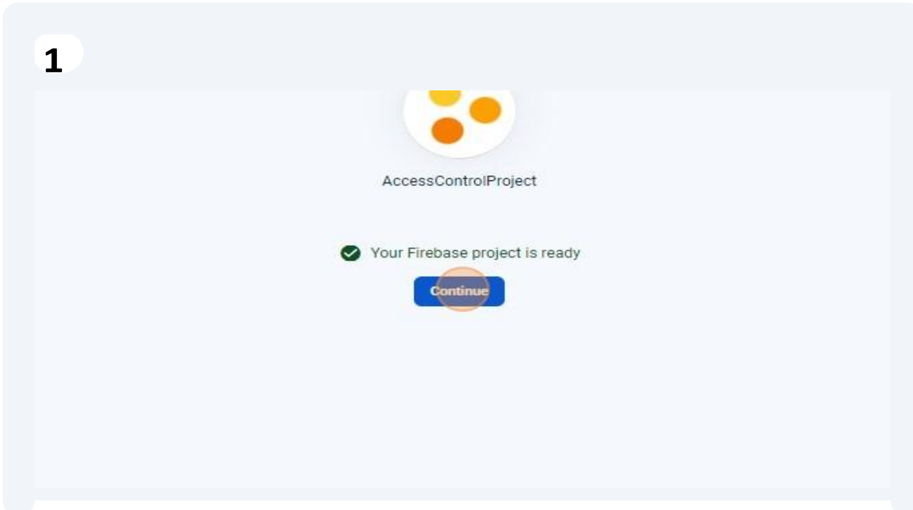

Figure 3.28: Project creation confirmation page.

Figure 3.28 shows the project creation confirmation page that will be displayed upon successfully creating a firebase project.

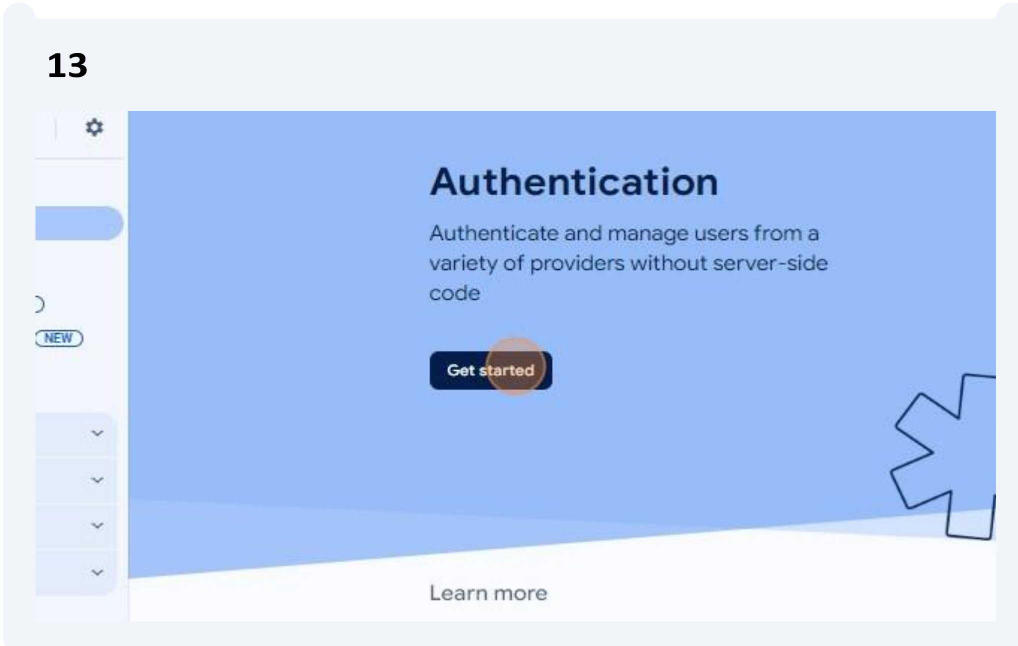

Figure 3.29: Firebase Authentication

Figure 3.29 is the get started page for firebase authentication once clicking on get started the list of authentication providers are displayed for the purpose of this project anonymous authentication is going to be used hence relating that option opens the anonymous authentication subpage and enable anonymous authentication and save those settings as displayed in the Figure 3.30 below.

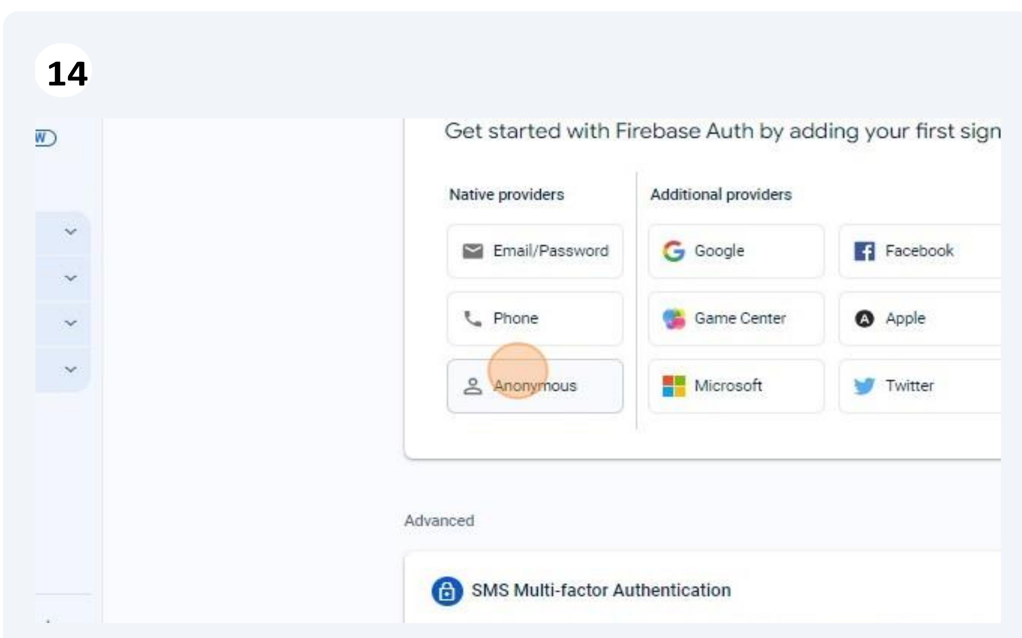

Figure 3.30: Firebase Authentication Services.

Figure 3.30 shows the sum of the firebase authentication services between native providers as well as additional providers as mentioned anonymous firebase authentication is going to be used this removes the need for e-mail and password-based authentication, each time the ESP 32 microcontroller initiates a connection to the firebase project and new anonymous identity sign in is created with its own unique identifier.

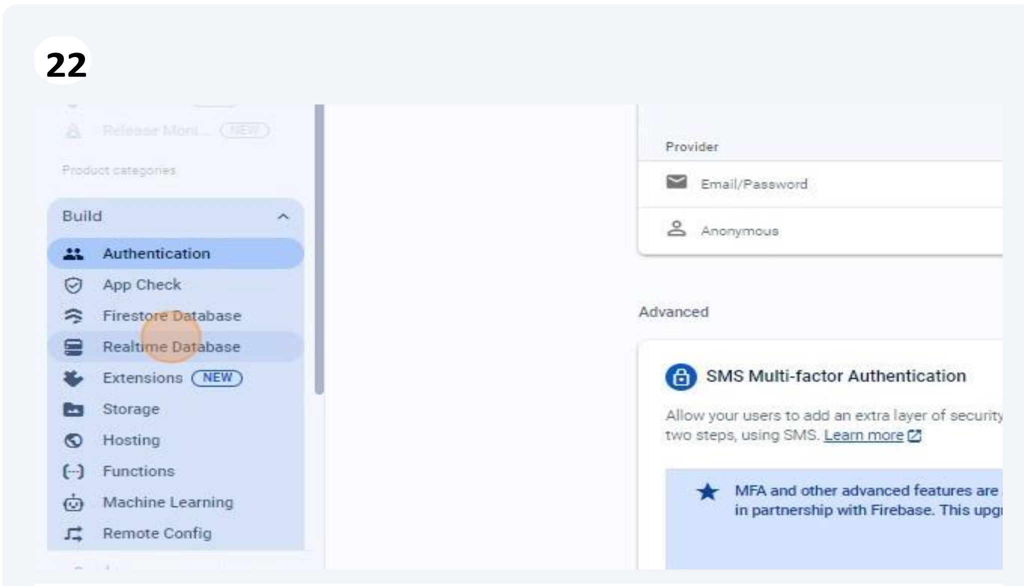

Figure 3.31: Image Insert Showing The Next Build Service To Be Added To The Project.

Once authentication has been set up there is then a need to create a real time database as shown in Figure 3.31 this is where the data is going to be stored for the purpose of this project it's going to store the total number of fingerprints it's also going to be used to read the fingerprint state whether it's in enrollment or verification mode and lastly it's going to be used to store all the fingerprint ID profiles that are created in the fingerprint sensor but are not associated with an individual in the admin interface

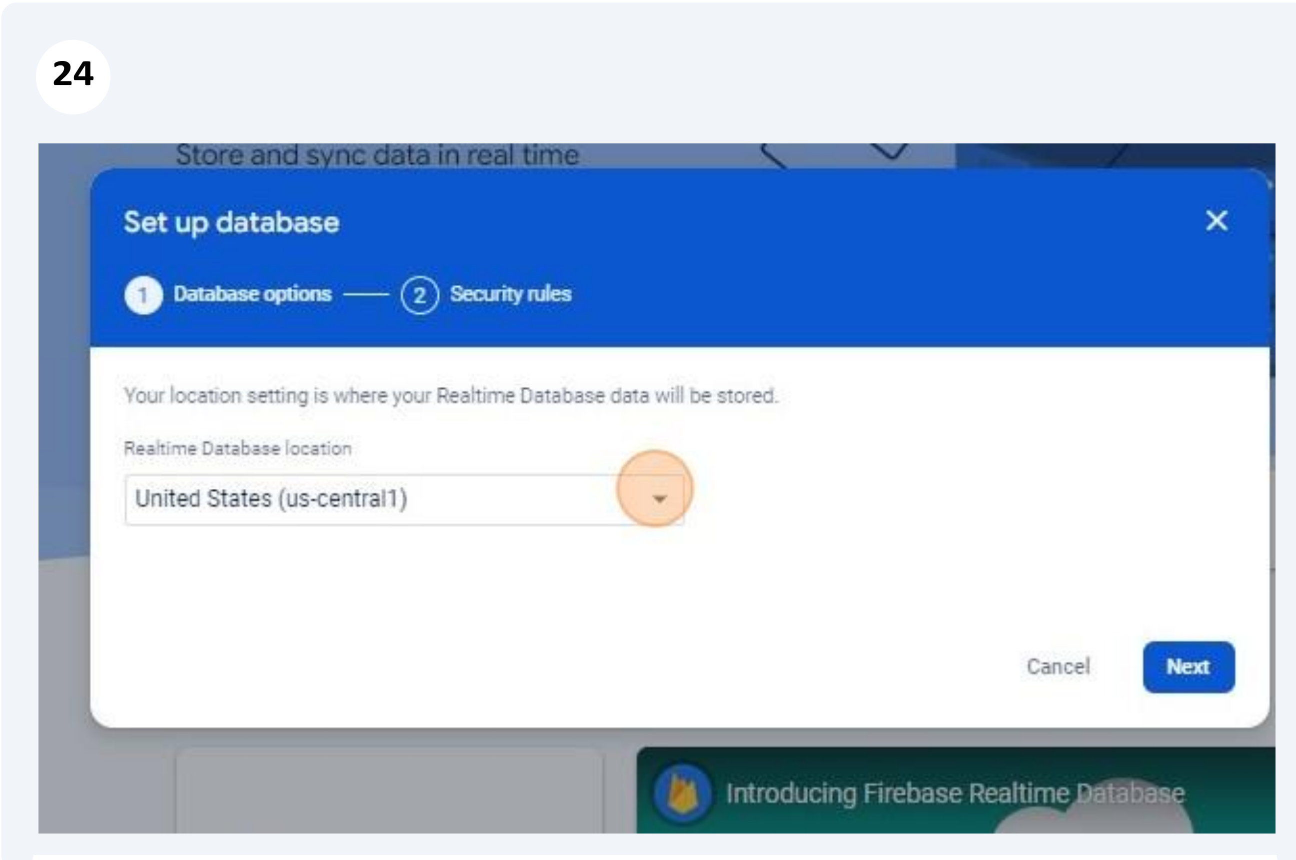

Figure 3.32: Image Snippet Of Firebase Realtime Database Setup Location.

Once the real time database service is selected and the get started button is clicked the setup database popup will display as shown in Figure 3.32 the initial step is to select the real time database location it is advised to accept the default location and click next.

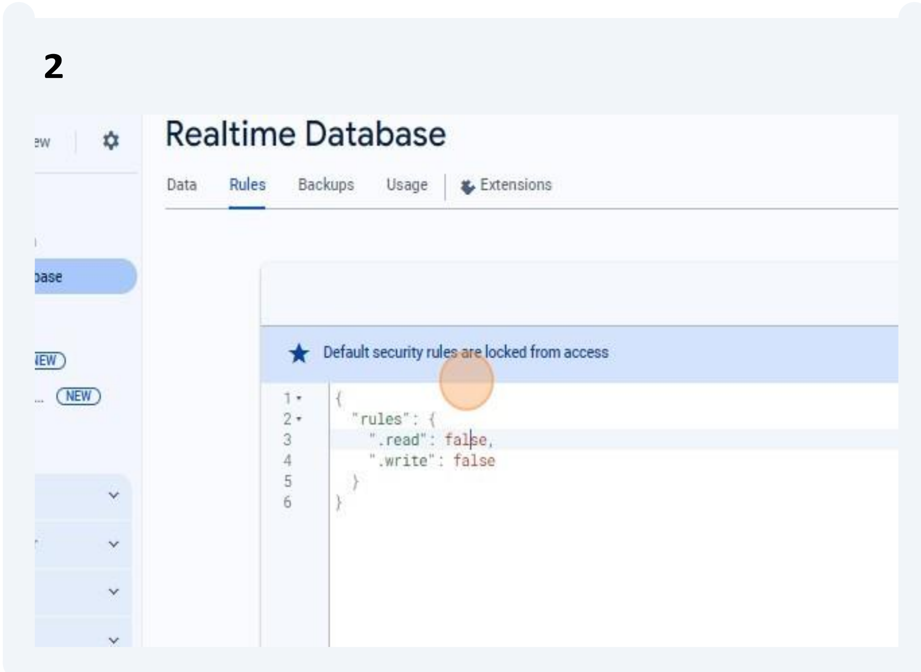

Figure 3.33: Image Snippet Showing The Created Realtime Database Security Rules With Read And Write Access Set To False.

Once the real time database instance has been successfully created , click on the rules option under the return database title this will open the default security roles for the database instance the default settings are read is false and write is false this means that the read and write permissions are false and the database instance is in locked mode those brilliant values need to be changed to true.

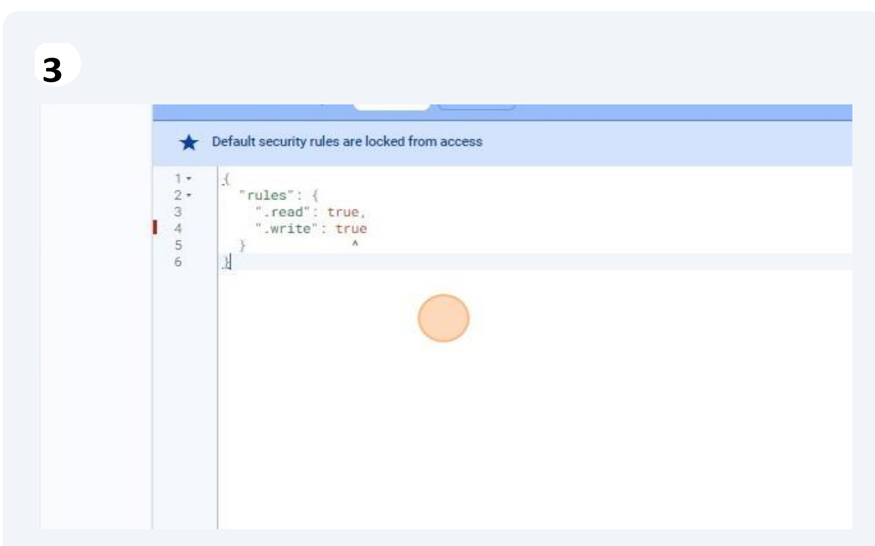

Figure 3.34: Image Snippet Showing The Created Realtime Database Security Rules With Read And Write Access Set To True.

Figure 3.34 shows the database instance now in unlocked mode as the read and write permissions have been set to true now *http get* and *push* requests can now be made to this database instance In order for these new rules to take into effect click on publish which is right: *the default security rules are locked from access message.*

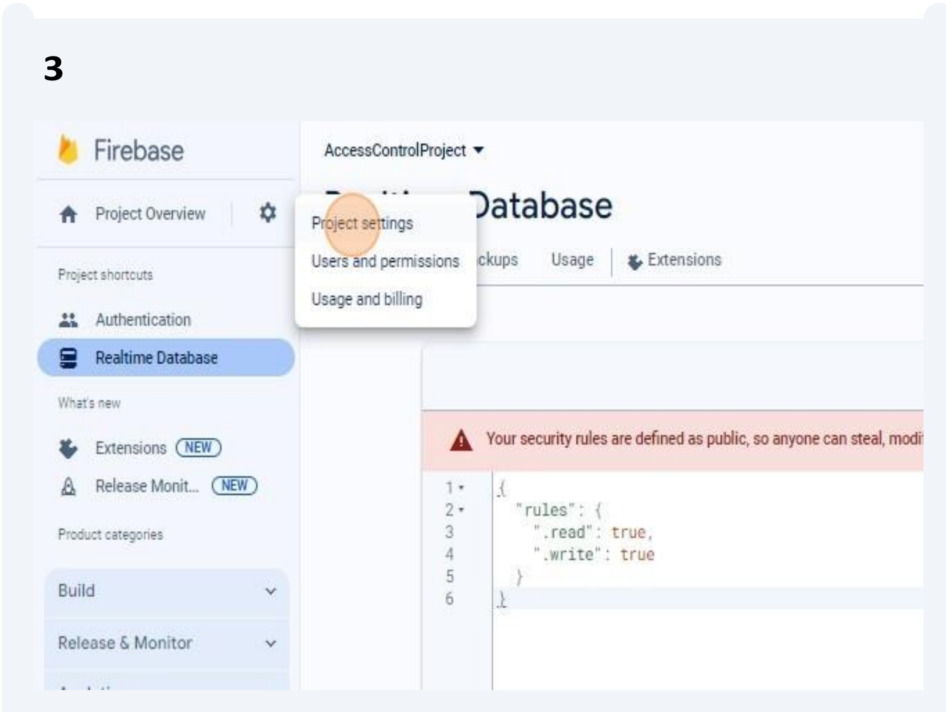

Figure 3.35: Image Snippet Showing The Project Overview With The Project Settings Option Shown.

Once the database rule instance rules have been successfully published as shown in Figure 3.35, on the right of the project overview option is in gear icon tracking on that gear icon review some projects overview options clicking on project settings or display or open a page that has some key project information as shown in Figure 3.35 below.

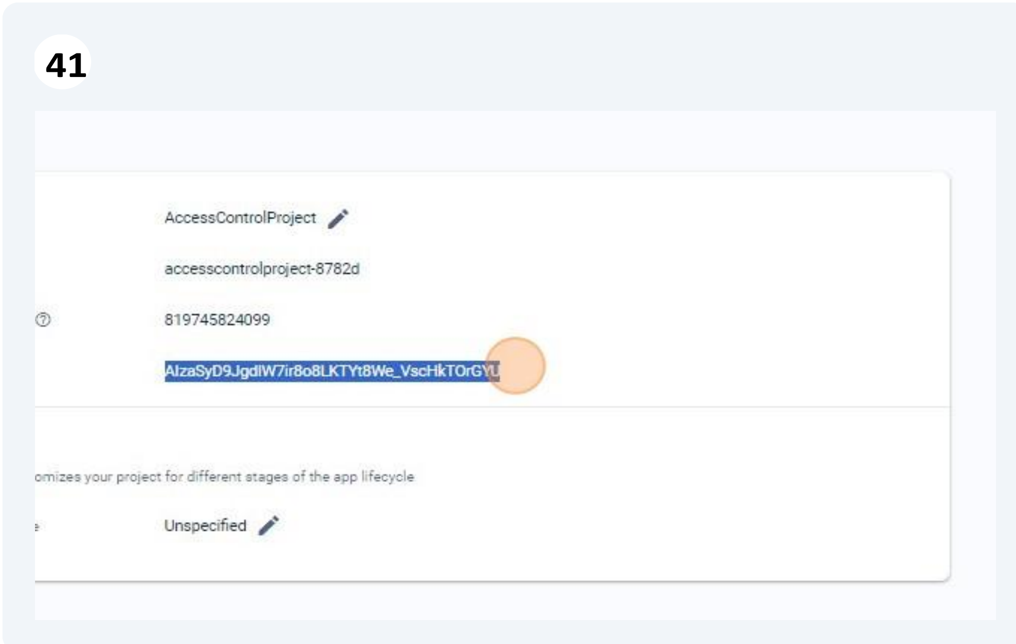

Figure 3.36 Shows the Project Settings and Details.

What is important at this point is the highlighted text as that is the project web API key. This allows information to be to make requests http fetch and post requests to the real time database securely this API key will be integrated in the code both in the ESP 32 microcontroller and the admin dashboard hence it must be copied and pasted in the code base for use.

4 Implementation

4.1 Introduction

This access control system project's implementation chapter offers a thorough rundown of the actual actions done to put the system's design into practice. This chapter explores the in-depth procedures and techniques utilized to convert theoretical ideas and architectural blueprints into a working, functional system. It includes configuring software modules, setting up hardware components, integrating different subsystems, and carrying out testing procedures to guarantee security and dependability. The chapter also outlines the difficulties that arose during implementation and the strategies used to overcome them. The chapter seeks to give a clear and organized narrative of the development, deployment, and validation of the access control system in an actual setting through this in-depth report.

4.1.1 Adafruit Io Implementation

4.1.1.1 Introduction

In this project, Adafruit IO is implemented using the MQTT protocol for data exchange. Real-time data interchange between the ESP32 microcontroller and the Adafruit IO platform is made possible by the MQTT code setup. The code takes care of configuring the MQTT parameters, such as the feed names, key, and username for Adafruit IO. On Adafruit IO, information is published to the appropriate feeds, including sensor readings and system states. The Adafruit IO dashboard then shows this data graphically, giving users an easy-to-understand and interactive way to view the outcomes. The dashboard's easy-to-use interface makes data monitoring and analysis possible, guaranteeing effective surveillance of system conditions and performance.

4.1.1.2 Initialization

```
21 #define MQTT_SERV "io.adafruit.com"
22 #define MQTT_PORT 1883
23 #define MQTT_NAME "LastronNgoma"
24 #define MQTT_PASS "aio_vbCP27vcuONWT06iEZvOYl0DhlL6"
25 #define PIEZO_BUZZER_PIN 4 // Use GPIO 2 or D4 on ESP32
26 // adafruit
27 Adafruit_MQTT_Client mqtt(&client, MQTT_SERV, MQTT_PORT, MQTT_NAME, MQTT_PASS);
28 //Set up the feed you'r publishing to
29 Adafruit_MQTT_Publish FingerprintFeed = Adafruit_MQTT_Publish(&mqtt, MQTT_NAME "/f/AccessControlSystemFeed");
30 //-----------------------------------------------------------------
```

Figure 4.1: ESP 32 Adafruit code snippet

Figure 4.1 shows code snippets of the declarations of Adafruit IO API. These are pre-requisite configurations:

Lines 21-25 define the credentials and connection parameters for the Adafruit IO MQTT server. Specifically:

- MQTT_SERV defines the Adafruit IO server address.
- MQTT_PORT specifies the port used for MQTT communication.
- MQTT_NAME sets the username for Adafruit IO.
- MQTT_PASS sets the Adafruit IO key for authentication.

Line 27 initializes an ***Adafruit_MQTT_Client*** object named ***mqtt***. This object handles the MQTT client setup, including the server address, port, username, and password. The &client parameter refers to a previously defined network client, which manages the network connection.

Line 29 initializes an ***Adafruit_MQTT_Publish*** object named ***FingerprintFeed.*** This object sets up the MQTT feed to which the ESP32 will publish data. The feed name is constructed using the MQTT_NAME and the specific feed path ***"/f/AccessControlSystemFeed***". The ***&mqtt*** parameter links this feed to the previously initialized ***mqtt*** client, enabling data publication to Adafruit IO.

```
        if (FingerprintFeed.publish(ID)) {
          Serial.println("Printed to Adafruit: " + ID );
          Serial.println("Current ID ==========: " + ID);
        }
```

Figure 4.2: Adafruit Feed publish code snippet

Figure 4.2 code segment checks if publishing a fingerprint ID to the Adafruit IO feed is successful and then prints relevant information to the Serial Monitor:

Line 237: This line attempts to publish the value of `ID` to the Adafruit IO feed associated with the `***FingerprintFeed***` object.`***FingerprintFeed***` is an `***Adafruit_MQTT_Publish***` object, which handles the publishing of data to a specified feed on Adafruit IO. The `publish(ID)` method returns `***true***` if the data is successfully published to Adafruit IO, allowing the code inside the `if` statement to execute. If is it true, then success text is displayed in the IDE console for the engineer to view.

4.1.2 Firebase Realtime Database

4.1.2.1 Introduction

This implementation chapter describes how the system performs CRUD (Create, Read, Update, Delete) operations on user access credentials and event logging data using Firebase Realtime Database. The methods used to handle data transactions, the architecture of the database nodes, and the setup and configuration of Firebase will all be covered. This chapter will also cover the advantages of utilizing Firebase Realtime Database, including scalability, ease of interaction with our ESP32-based hardware components, and real-time data synchronization.

4.1.2.2 Initialization

```
16
17 // Firebase configuration
18 #define DATABASE_URL "https://access-control-system-33d35-default-rtdb.firebaseio.com/"
19 #define API_KEY "AIzaSyBMbj3j7lpJAmz-2f5PhyoxNtsDP3lzO5E"
20 FirebaseData firebaseData;
21 FirebaseAuth auth;
22 FirebaseConfig config;
23 // Initialize Firebase object
24 FirebaseData fbdo;
25 FirebaseJson json;
26 //================================
```

Figure 4.3: ESP 32 Conde Snippet of Firebase Realtime Database initialization.

Lines 18-19: Define constants for the database URL and API key.

Lines 20-26: Create instances of Firebase-related classes for handling data communication (FirebaseData), authentication (FirebaseAuth), and configuration (FirebaseConfig). A comment indicating that the subsequent code is related to Firebase initialization.Create additional FirebaseData and FirebaseJson objects for managing Firebase operations and JSON data respectively.

```
void UploadJSON(int ID) {
  String UUID = getRandomString();
  String path = "/EnrollmentNode/Enrollments/EnrolledIDs/" + UUID + "/";

  // Add data to the JSON object
  json.set("uniqueID", UUID);
  json.set("fingerprintID", ID);
  // Upload JSON string to Firebase RTDB node
  if (Firebase.RTDB.setJSON(&firebaseData, path.c_str(), &json)) {
    Serial.println("JSON data uploaded successfully");
  } else {
    Serial.println("Failed to upload JSON data");
    Serial.println("Reason: " + firebaseData.errorReason());
  }
}
```

Figure 4.4: Example ESP 32 Firebase Realtime Database code interaction.

Figure 4.4 shows the ESP32 Code function ***UploadJSON*** generates a random unique ID using another function called ***getRandomString***() and constructs a Firebase Realtime Database (RTDB) path based on this ID. It then populates a JSON object (json) with two key-value pairs: "***uniqueID***" with the generated Universal Unique Identifier (UUID) and "***fingerprintID***" with the provided ID. The function attempts to upload this JSON data to the specified Firebase RTDB node using ***Firebase.RTDB.setJSON().*** If the upload is successful, it prints a success message; otherwise, it prints an error message along with the reason for the failure obtained from **firebaseData.errorReason().**

Chapter 4.2 and 4.3 are action points that are being incorporated in order to achieve objective number 4 which is incorporate a loosely coupled architecture.

4.2 Circuit Implementation

4.2.1 Power Supply Module Implementation

Figure 4.5: Image insert showing power supply implementation.

Figure 4.5 shows two pictures illustrating power supply testing. The first image features an XL6009 DC-DC buck-boost converter, which is adjusted to deliver a 12V output using a 3.7V 18650 battery as the input source. The positive terminal of the voltmeter is not connected to the output terminal of DC-DC buck boost convertor. The second image showcases a voltmeter connected to the output terminals of the converter, displaying a voltage reading of 12.08V. This demonstrates the effectiveness and accuracy of the converter in boosting the battery voltage to the required 12V output.

Components	Expected Voltage	Practical Voltage	Possible Reason for Deviation
Battery	3.7	3.4	Internal resistance
Buck Boost Convertor XL6009	12.0	12.08	Operator's due diligence to use this voltage, the sensitive nature of the potentiometer makes it difficult to precisely get 12V
LM7805 Regulator	5.0	5.0	

4.2.2 OLED Display and Fingerprint Sensor Integration

The access control system's integration is essential since it enables real-time feedback and sensor connectivity verification. When the AS609 fingerprint sensor is correctly integrating with the system's microprocessor, the OLED display acts as an instant visual indicator. This configuration guarantees that the user is aware of the sensor's status at a look in addition to showcasing the sensor's functionality.

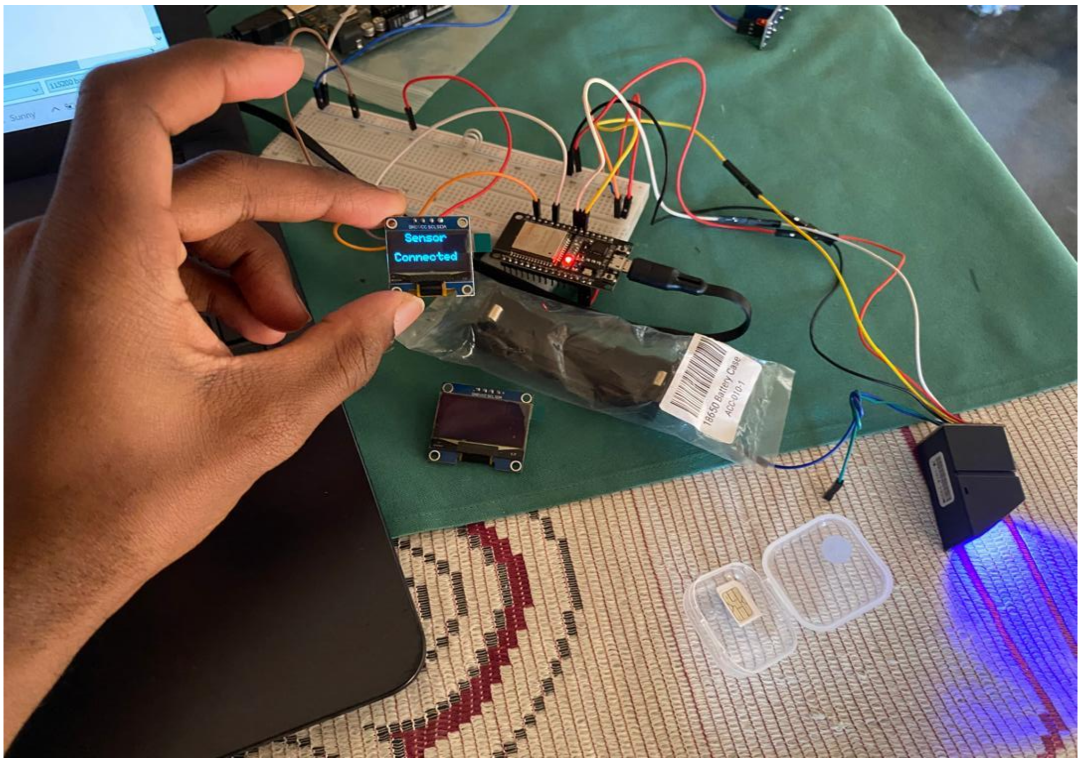

Figure 4.6: Image insert showing the display and fingerprint sensor testing.

Figure 4.6 shows the integration of the fingerprint sensor and the OLED display is linked to the fingerprint sensor and controls the data flow between the sensor and the OLED display. The connection message's successful display is evidence of the system's efficient power distribution and communication. Reliability and efficiency are guaranteed at this degree of integration, which are essential to the access control system's overall efficacy. In the ESP32 code base, logic was placed so that the ESP32 initially checks the connected to the fingerprint sensor correctly. This is achieved by communicating through the ESP 32's TX (transmit in) and RX (receive pins) in the fingerprint sensor as well as the RX pin of the ESP 32 and the TX pin of the fingerprint sensor. Upon successfully completing the handshake (a term used to define a successful connection between two handware devices), the ***Sensor Connected*** message is displayed on the Oled Display screen.

Components	Expected Voltage	Practical Voltage	Possible Reason for Deviation
Battery	3.7	3.4	Internal resistance
Buck Boost Convertor XL6009	12.0	12.08	Operator's due diligence to use this voltage, the sensitive nature of the potentiometer makes it difficult to precisely get 12V
LM7805 Regulator	5.0	5.0	

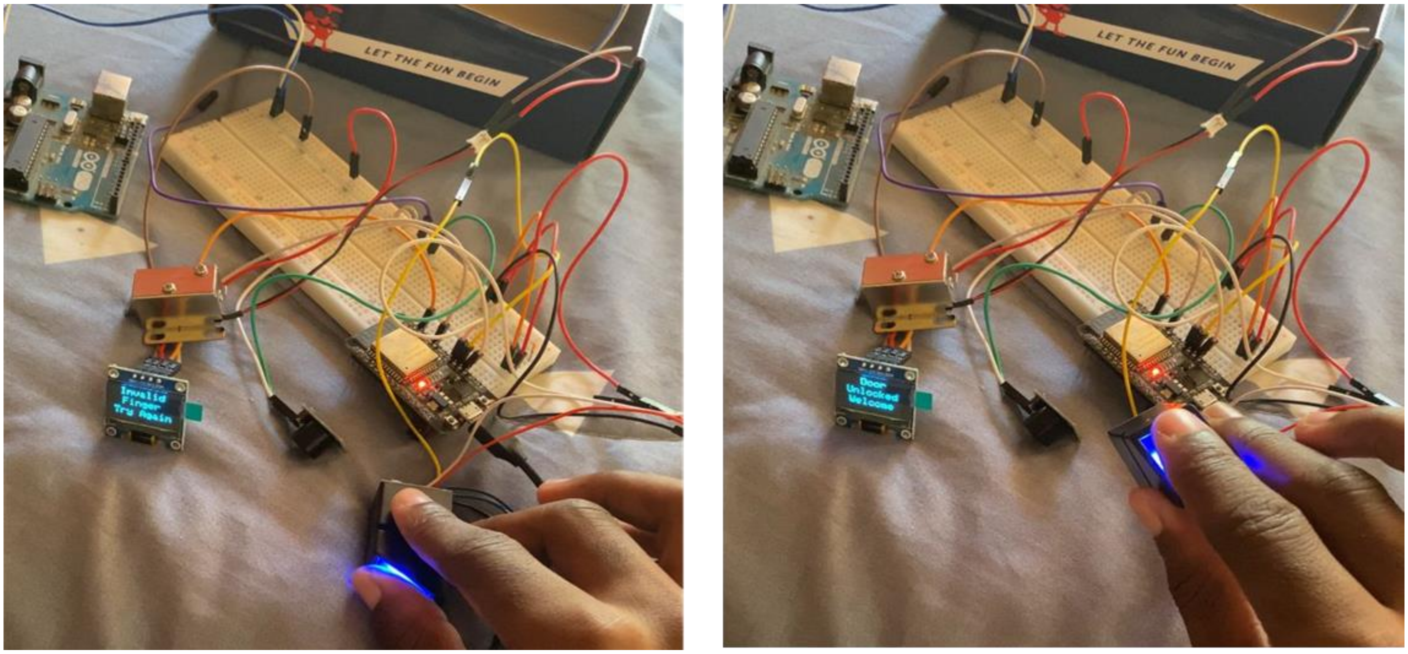

Figure 4.7: Fingerprint Sensor and Display Modules Implementation Phase

Figure 4.7 shows when the two image inserts are placed side by side, it can be seen how the access control system in its implementation phase reacting to various fingerprint inputs. The fingerprint that is provided on the sensor in the image on the left is not recognized by the system, at the time of module testing, the right thumb was not enrolled into the fingerprint sensor hence it resembles an unknown person attempting to gain access. The unauthorized access will be denied as indicated by the "Invalid Fingerprint" warning that is displayed on the OLED display.

The blue backlight of the fingerprint sensor illuminates, indicating that the sensor is in a constant state of polling which is scenario when a sensor is in a constant state of actively searching for input. On the other hand, the image on the right illustrates how the system recognizes a registered fingerprint and displays a "Success" message on the OLED screen to indicate a match. The right had pointing finger was the enrolled finger thus upon placing in the fingerprint sensor, it was recognized resembling what will occur is an authorized user where to attempt to gain access.

4.2.3 Solenoid Door Lock And Relay Module.

The integration of a relay module and a solenoid door lock is examined in this subchapter, enabling automatic and safe door locking systems. By serving as a middleman and using signals from a microprocessor to regulate the high-power solenoid lock, the relay module guarantees accurate and dependable performance.

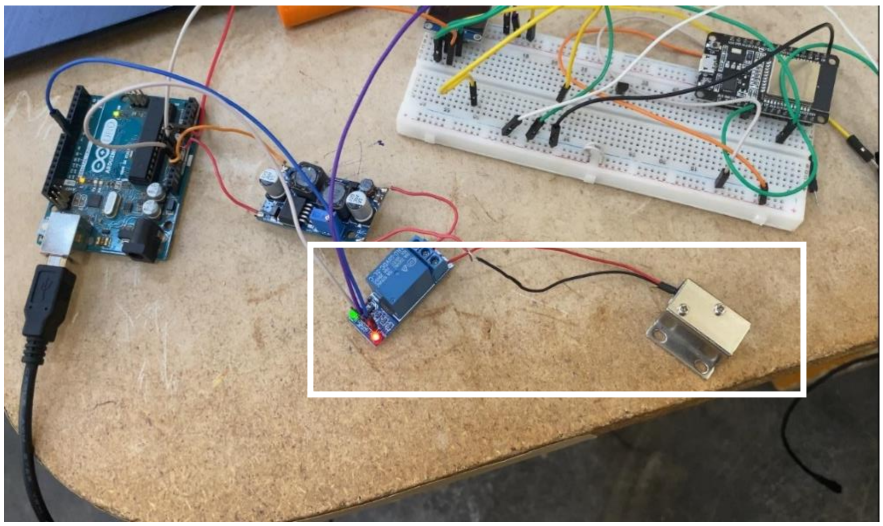

Figure 4.8: Activated 5V Relay and 9-12V Solenoid Door Lock.

Figure 4.8 shows the integration testing of the locking and unlocking module which consist of the SRD-05VDC-SL-C relay and solenoidal door lock. As highlighted in the image, the green switch status indicator light on in the image indicates that the SRD-05VDC-SL-C relay is in its operational mode. The solenoid door lock retracts in this position, demonstrating that the locking mechanism has been successfully activated. This arrangement precisely satisfies the requirements for the system design, proving that the relay module can effectively regulate the solenoid door lock and guarantee accurate and dependable door operation. The connections interface between the relay and the door lock are explained in chapter 2.1.5.4.

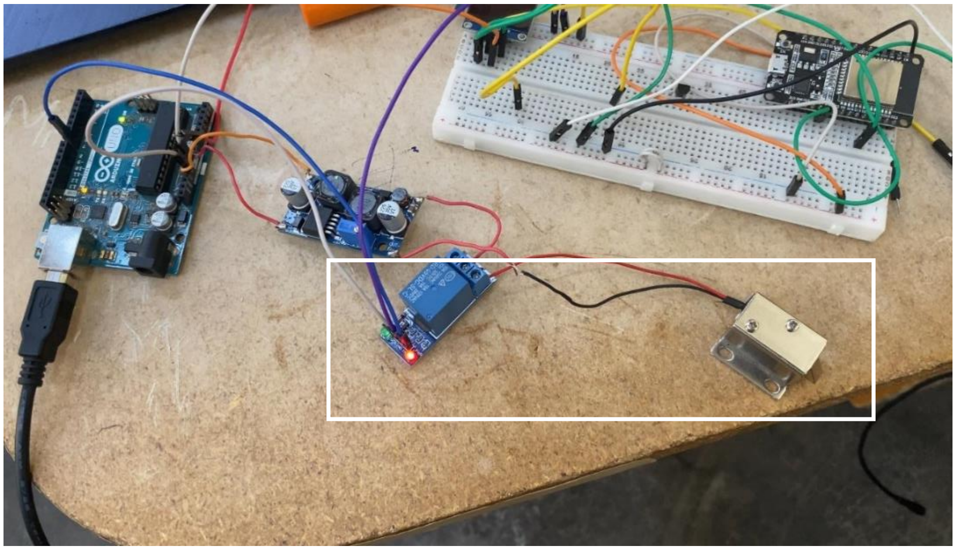

Figure 4.9: Deactivated 5V Relay and Solenoidal Door Lock

Figure 4.9 shows an SRD-05VDC-SL-C relay is depicted in the picture in its deactivated state, with the green switch status indicator light turned off. At this point, the door is locked since the solenoid door lock is sticking out. This setup demonstrates how to effectively deactivate a solenoid door lock via the relay module, guaranteeing secure door locking even when the lock is not in use. It also precisely complies with the system design specifications.

4.2.4 Complete Access Control System Circuit Integration

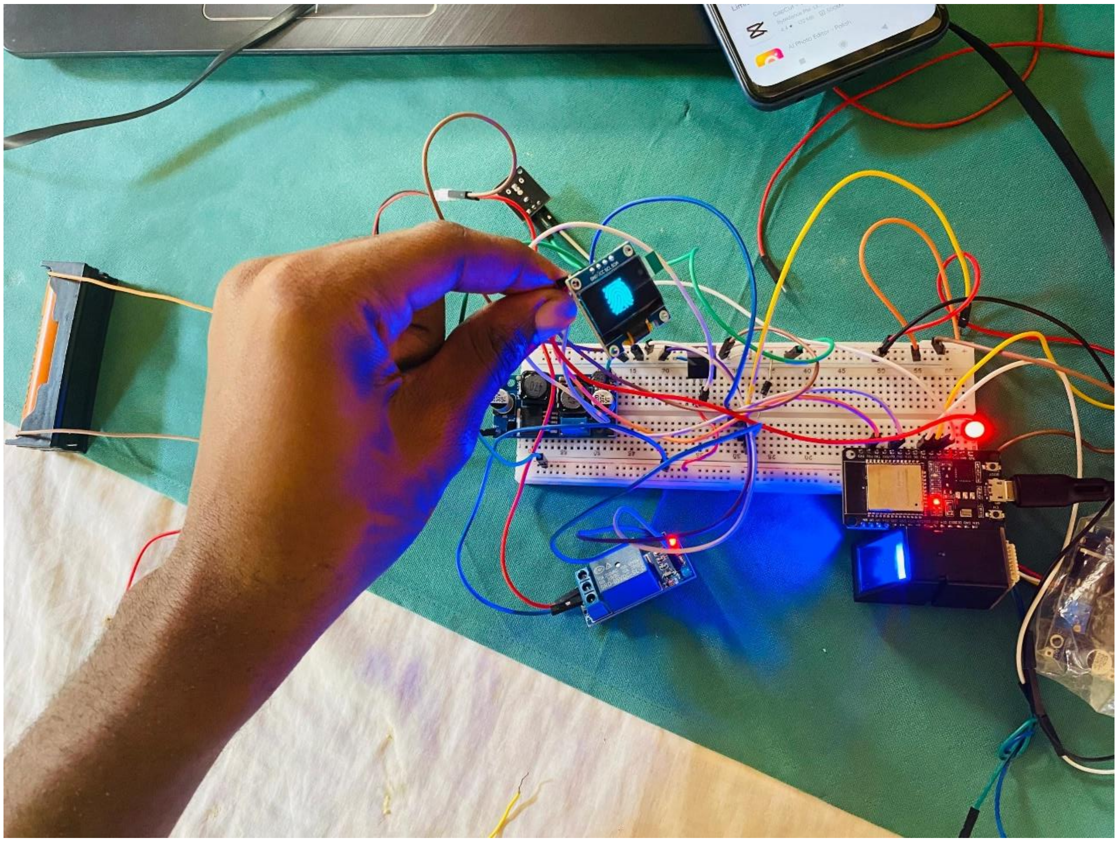

Figure 4.4.10: Fully Assembled Access Control System Circuit.

Figure 4.8 shows the ready condition of the access control system. The fingerprint indicator on the OLED display indicates that the system is ready to accept a fingerprint as input. This indicates that the OLED display module is showing positive result as it working as desired which is desired. The blue lighting on the fingerprint sensor indicates that it is actively scanning and prepared to receive a fingerprint. This is classified as a positive result from the fingerprint sensor module.

It is also possible to see the power supply module, which consists of an XL6009 DC-DC buck booster converter connected to an 18650 3.7V cell. A steady 12V output has been achieved by adjusting the potentiometer of the converter which acts as the input voltage to the LM7805 regulator. Its 5V output is the input voltage (Vin) is the supply voltage to the ESP32 controller In this image, it can be clearly seen ESP32 in-built Power status light is on and the external red LED (Light Emitting Diode) is also ON. The picture also shows the solenoidal door lock, which will retract upon a successful fingerprint scan which will allow the individual requesting access to open the door illustrating how the access control system is configured in its whole. This configuration demonstrates how a strong power management system is integrated with a vital locking mechanism to provide dependable and secure operation.

4.2.5 Implementation Conclusion.

In the project's implementation phase, the access control system's effective assembly and integration represent a major accomplishment. The ESP32 microcontroller, AS609 fingerprint sensor, OLED display, relay module, power supply, and other components of the circuit were carefully built and tested. The seamless integration of the system's components ensures dependable functionality and communication. Extensive testing was done at this phase to confirm that every component (especially the fingerprint sensor and its interface with the OLED display) was operating as intended. Real-time message displays, like "*Sensor connected,", "invalid finger", "Opening door"* gave users quick status updates on the system and verified that the power distribution and settings were accurate. The ESP32's control over the activation and deactivation of the relay module showed how the system might control external devices via fingerprint authentication. The overwhelming evidence of the system's response to enrolled fingers proves that the objective of determining if an individual who places their finger on the sensor is authorized or not authorized successfully proves that this system is able to act as a primary point of verification and validation for all staff and students' access to university. The system's administrator's ability to enroll new authorized users supports the project's aim of allowing the administrator to perform administrative tasks such as deleting users or updating users on the custom administration user interface that was a custom creation, design and development for this access control system's unique requirements. This project also satisfies the technical skills, experience, problem-solving skills needed in electronic hardware, tools as well as the supporting software knowledge of the electronic engineering industry. And it is evident that those skills, experience and exposure were tested and prevailed.

The fully constructed circuit's correct operation has created a strong basis for more research and assessment. This accomplishment flows naturally into Chapter 6, the Results Chapter, which looks in-depth at the functionality and efficiency of the access control system. The system's dependability, responsiveness, and overall performance in achieving the project's goals will be highlighted through detailed findings from a variety of tests and operating scenarios that will be presented.

5 Results

5.1 Introduction

The access control system project report's Results chapter summarizes the findings from the testing and implementation stages. This chapter gives a thorough explanation of how the system functions in different situations, evaluating its overall efficacy, dependability, and efficiency in limiting access. The results arise from extensive testing of the system's modular parts, such as the relay module, fingerprint sensor, and interaction with Adafruit IO and Firebase Realtime Database. The information gathered during the testing procedure, including fingerprint recognition success rates, access denial reaction times, and data synchronization accuracy with cloud platforms, will be presented in this section. Performance metrics and any problems found during the tests will be explained with the use of visual aids like tables and screenshots. This chapter's mission is to present a fair and impartial assessment of the access control system. stressing both its advantages and disadvantages.

5.2 Tables Of Results

5.2.1 Power Supply Results Table.

Components	Expected Voltage	Practical Voltage	Possible Reason for Deviation
Battery	3.7	3.4	Internal resistance
Buck Boost Convertor XL6009	12.0	12.08	Operator's due diligence to use this voltage, the sensitive nature of the potentiometer makes it difficult to precisely get 12V
LM7805 Regulator	5.0	5.0	

Figure 5.1: Table of Power Supply Results

Figure 5.1 is a table featuring four headers: **Components Name, Expected Voltage, Practical Voltage, and Possible Reason for Deviation**. It is designed to document and compare the theoretical and actual voltages of various components in a circuit that was analyzed during system testing. The Components Name column lists each component, the Expected Voltage column states the ideal voltage values, the Practical Voltage column records the measured voltages during testing, and the Possible Reason for Deviation column provides potential explanations for any discrepancies between expected and practical values. This table helps in diagnosing and understanding variations in the circuit's performance.

5.2.2 Fingerprint Sensor Results Table.

Scanned Finger	Registered? (Yes/No)	Proposed Scan Duration (Seconds)	Practical Successful Scan Duration	Reason for deviation	Fingerprint ID	Value Uploaded to Adafruit API
Thumb	No	1	5		N/A	N/A
Index	Yes	1	2	Incorrect testing fingerprint position.	2	2
Middle	Yes	1	3	Incorrect testing fingerprint position.	3	5
Ring	Yes	1	5	Incorrect testing fingerprint position.	8	8
Pinkie	No	1	2		N/A	

Figure 5.2: Table of results for fingerprint and Cloud API Testing

Figure 5.2 is a table of results including the following headers: Scanned Finger, Registered? (Yes/No), Proposed Scan Duration, Practical Scan Duration, Reason for Deviation, Fingerprint ID, and Value Uploaded to Adafruit API. This table is intended to log the details of fingerprint scans during a project.

- **Scanned Finger:** Lists each finger that was scanned.
- **Registered? (Yes/No):** Indicates whether the scanned fingerprint is already registered in the system.

- **Proposed Scan Duration**: Specifies the anticipated time for the scanning process.
- **Practical Scan Duration**: Records the actual time taken for the scan.
- **Reason for Deviation:** Provides explanations for any differences between the proposed and practical scan durations.
- **Fingerprint ID**: The unique identifier assigned to each scanned fingerprint.
- **Value Uploaded to Adafruit API**: Shows the data sent to the Adafruit API for each scan.

This table aids in monitoring the scanning process, identifying inefficiencies, and ensuring accurate registration and data logging during the access control system testing. This is quite evident as the practical scan duration is significantly higher than the proposed scan duration due the additional delays stated in the code base to allow for further processing of the enrolled fingerprint. This further processing includes uploading the enrolled fingerprint's ID to Adafruit Access Control System's Feed.

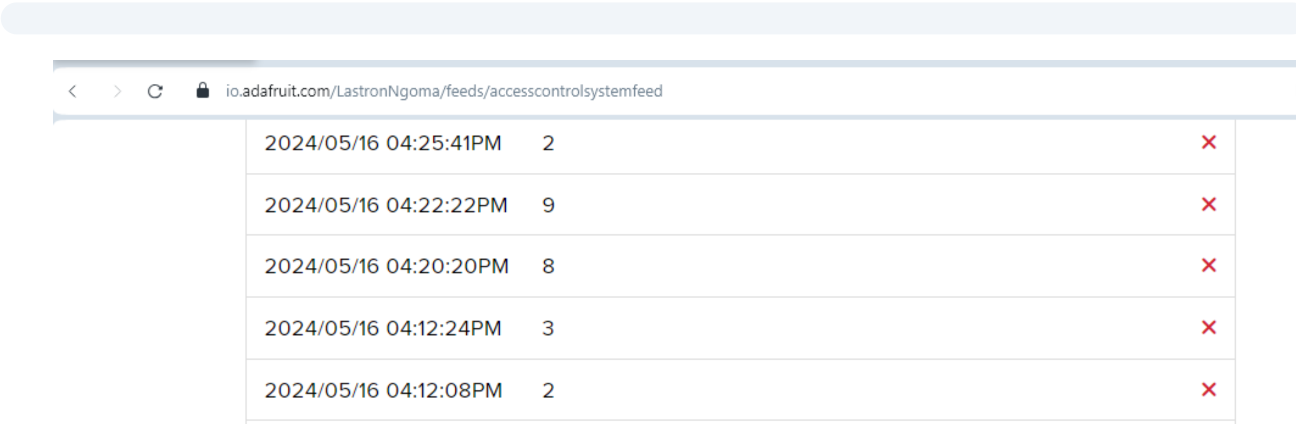

Figure 5.3: Adafruit Feed IO Uploaded Values

Figure 5.4 shows the uploaded fingerprint ID values to an Adafruit IO feed. These values represent different test fingers scanned during the system's operation. Specifically, the values 2, 3, 8, and 9 correspond to test fingers from the project author's right hand.

Each time a fingerprint is scanned and identified by the system, the corresponding fingerprint ID is sent to the Adafruit IO platform, where it is logged for monitoring and analysis purposes. This data helps in verifying the correct functioning of the fingerprint recognition system and ensures that the enrolled fingerprints are being correctly identified.

- **Value 2**: Represents the index finger of the right hand.
- **Value 3**: Represents the middle finger of the right hand.
- **Value 8**: Represents the ring finger of the right hand.

By observing these values in the Adafruit IO dashboard, one can track which fingers have been used for authentication and ensure that the system responds accurately to different fingerprint inputs. This information is crucial for debugging and improving the accuracy and reliability of the access control system.

5.3 Successful Scan Full Circuit Result.

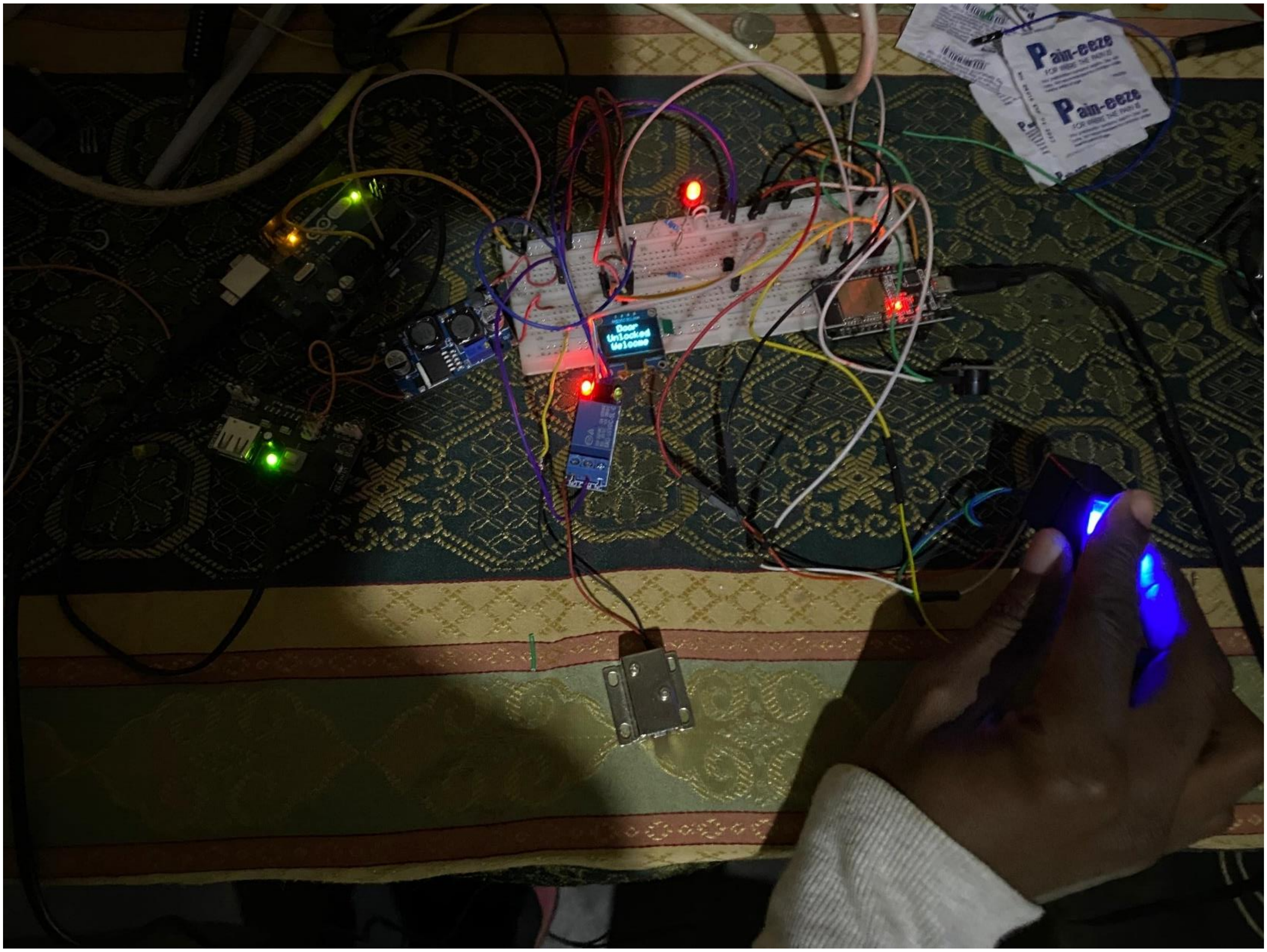

Figure 5.4: Authorized User System Response.

Figure 5.4 shows displays the completely constructed door access control system hardware that uses fingerprints. The fingerprint sensor, where a hand has been placed by an authorized user, is the system's focal point. The mechanism activates upon successful fingerprint identification. First, the word "*Door Unlocked, Welcome"* is displayed clearly on the OLED display, signifying that the user has been recognized and given admission. This message improves the user experience by verifying the successful authentication and by sending a warm greeting.

The relay module, designated by its model number SRD-05VDC-SL-C, activates simultaneously. The relay's green switch status indicator light turning on verifies this visually. Relay activation is an essential part of the process since it directly regulates the power going to the solenoid door lock. The solenoid door lock mechanism receives an electrical signal from the relay when it engages. Retraction of the locking pin is the solenoid's response; it is made to run on 5V DC. The image makes it evident that the solenoid pin has retracted, signifying that the door has been effectively unlocked. The door opens due to this mechanical motion, giving the authorized individual physical access.

The fingerprint sensor, OLED display, relay module, and solenoid door lock all work together seamlessly, which is evidence of the system's meticulous design and integration. Every component works together harmoniously to complete the task at hand. The solenoid lock guarantees safe and dependable door operation, the relay precisely regulates the power flow, and the OLED display gives instant visual feedback. This thorough illustration of the system in operation attests to the fact that it operates exactly as intended and that it strictly complies with the requirements. Reliability and efficiency are demonstrated by the system's prompt and accurate response to an approved fingerprint. Figure 5.4 offers a safe, user-friendly access control solution and acts as a visual evidence of the system's efficacy, guaranteeing that all functional and design requirements are satisfied.

5.4 Unsuccessful Scan Full Circuit Result.

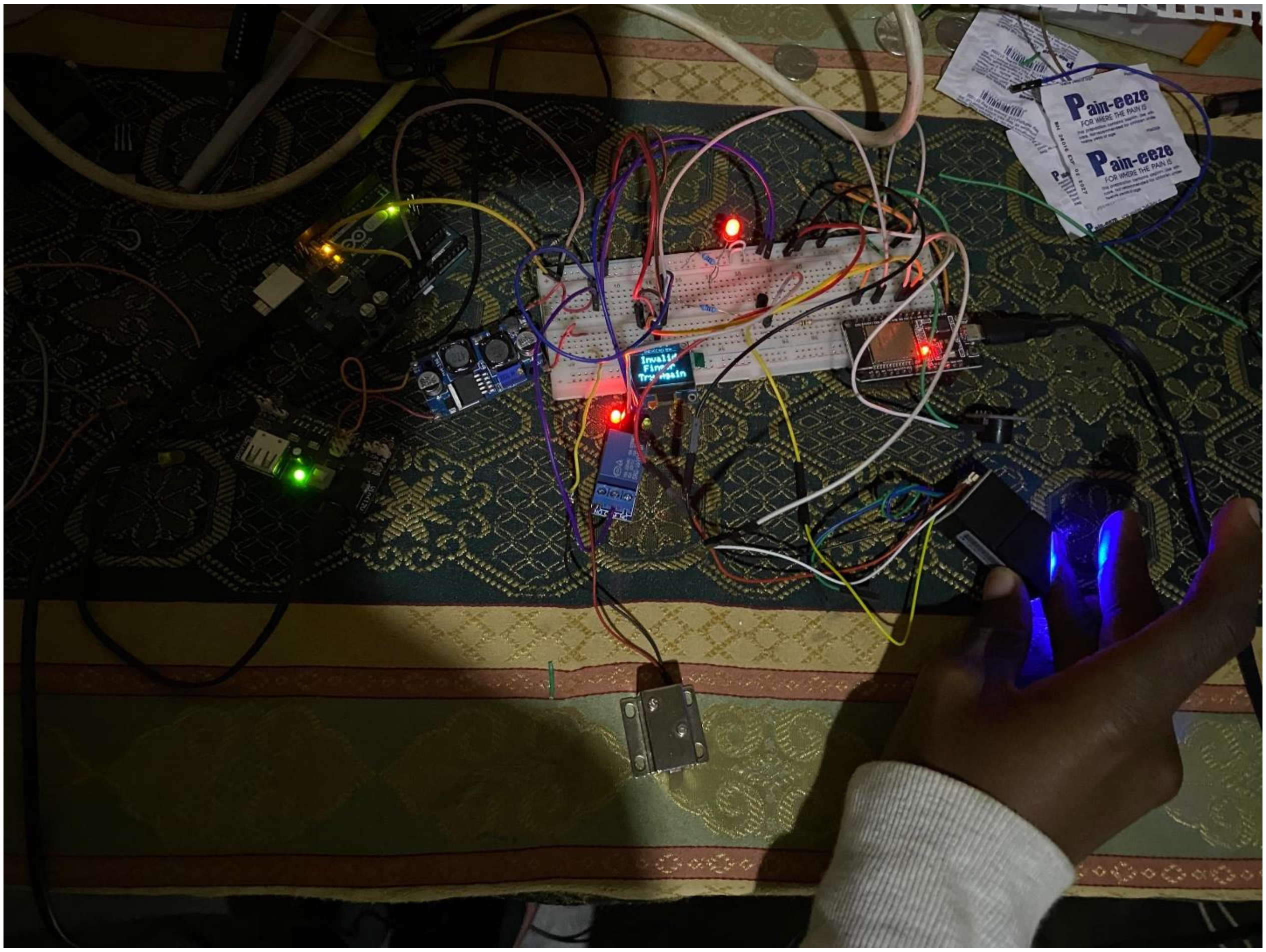

Figure 5.5: Unauthorized User Scan Result

Figure 5.5 shows the completely constructed hardware circuit of a fingerprint-based door access control system reacting to an attempt to enter by an unauthorized person. The fingerprint sensor, where the unauthorized user's finger was placed, is the focal point of the picture. As soon as the fingerprint is scanned, the system analyzes the information and finds that the fingerprint does not match any enrolled fingerprints. The outcome is that the message *"Invalid Finger, Try Again"* appears on the OLED display right away. This message not only informs the user that access is blocked because the credentials are not recognized, but it also asks them to try again in case the fingerprint was placed incorrectly.

Along with the statement on the OLED display, the relay module is not active. The relay's green switch status indicator light being off serves as an indicator of this. A key component of the system's security response is the relay's inactivity, which keeps it from closing the circuit that would otherwise power the solenoid door lock. As a result, the door lock with solenoid remains locked. The locking pin of the solenoid is clearly visible in the picture, indicating that the door is still firmly locked. The mechanical state guarantees that the restricted area cannot be physically accessed by an unauthorized person.

The system's strong security measures are highlighted by the way the fingerprint sensor, OLED display, relay module, and solenoid door lock interact. The solenoid lock physically enacts the access control choice, the OLED display gives immediate and obvious feedback, and the relay's condition validates the electrical control. This detailed figure 5.5 demonstrates that the system functions as intended, essentially excluding unauthorized individuals from access. Every module works as conceptualized, designed, and created to guarantee that security is maintained. The provided evidence and precise reaction of the system to an unidentified fingerprint serves as a positive indication that the system does act as a primary point of access control. This picture highlights the system's capability to keep people out of restricted locations, proving its effectiveness and resilience in practical situations.

6 References

[1] R305 Optical Fingerprint Scanner Sensor Module," electropeak.com. https://electropeak.com/optical-fingerprint-module-r305 (accessed Jun. 08, 2024).

[2] "How to use USB interface of R305 Fingerprint Module instead of UART," Stack Overflow. https://stackoverflow.com/questions/53677575/how-to-use-usb-interface-of-r305-fingerprint-module-instead-of-uart (accessed Jun. 08, 2024).

[3] tonygo2, "Arduino and the SSD1306 OLED I2C 128x64 Display," Instructables. https://www.instructables.com/Arduino-and-the-SSD1306-OLED-I2C-128x64-Display/

[4] A. Industries, "Monochrome 0.96" 128x64 OLED graphic display," www.adafruit.com. https://www.adafruit.com/product/326

[5] "Mini Electric Door Lock (12V DC Solenoid)," Future Electronics Egypt. https://store.fut-electronics.com/products/mini-electric-door-lock-12v-dc-solenoid (accessed Jun. 08, 2024).

[6] "12v Electromagnetic/solenoid door lock," HUB360. http://hub360.com.ng/product/12v-electromagnetic-solenoid-door-lock/ (accessed Jun. 08, 2024).

[7] "Cables & Wires," Arduino Official Store. https://store.arduino.cc/collections/cables-wires

[8] Tarantula3Youtube, "Driving a Relay With an Arduino," Instructables. https://www.instructables.com/Driving-a-Relay-With-an-Arduino/

[9] S. C. | Arduino | 68, "How to Set Up a 5V Relay on the Arduino," Circuit Basics, Nov. 28, 2015. https://www.circuitbasics.com/setting-up-a-5v-relay-on-the-arduino/

[10] "The ESP32 Chip explained: Advantages and Applications," Sep. 25, 2023. https://www.deepseadev.com/en/blog/esp32-chip-explained-and-advantages/#:~:text=IoT%20devices%3A%20The%20ESP32%20is

[11] "ESP32 for IoT Tutorial," www.tutorialspoint.com. https://www.tutorialspoint.com/esp32_for_iot/index.htm (accessed Jun. 08, 2024).

[12] Espressif, "ESP32 Overview | Espressif Systems," www.espressif.com, 2023. https://www.espressif.com/en/products/socs/esp32