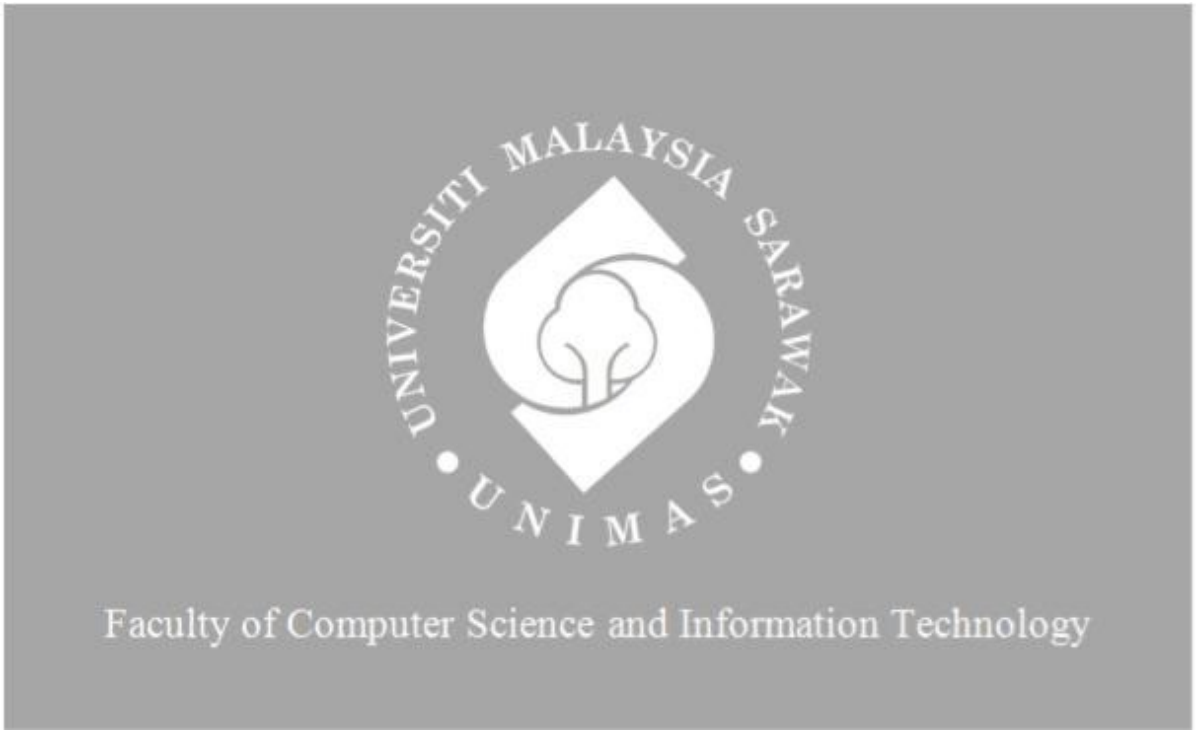


# *SMART ACCESS HOTEL SYSTEM USING FINGERPRINT TECHNOLOGY*

Mohamad Arief Haqiem Bin Adnan

(78160)

Bachelor of Computer Science with Honours (Network Computing)

2025

# SMART ACCESS HOTEL SYSTEM USING FINGERPRINT TECHNOLOGY

MOHAMAD ARIEF HAQIEM BIN ADNAN

This project is submitted in partial fulfilment of the

requirements for the degree of Bachelor of

Computer Science with Honors

Faculty of Computer Science and Information Technology

UNIVERSITI MALAYSIA SARAWAK 2025

# SMART ACCESS HOTEL SYSTEM USING FINGERPRINT TECHNOLOGY

MOHAMAD ARIEF HAQIEM BIN ADNAN

Projek ini merupakan salah satu keperluan untuk

Ijazah Sarjana Muda Sains Komputer dan Terknologi Maklumat

Fakulti Sains Komputer dan Teknologi Maklumat

UNIVERSITI MALAYSIA SARAWAK 2025

**ACKNOWLEDGEMENT**

I would like to take this opportunity to show how grateful I was to all the people who always help and guide me to do my Final Year Project.

Firstly, Alhamdulilah and thank you to Allah s.w.t for making my journey to complete and finishing my final year project in ease and smooth way. A greatest thank you to my supervisor, Associate Professor Dr. Kartinah Bt Zen, for always guiding my way, correcting my faults and showing the right things that I need to do during my final year project. Because of her unstoppable support, my confidence level has increased and I made some improvements while doing this project. Besides that, I would like to thanks Associate Professor Dr. Noor Alamshah B. Bolhassan and Associate Professor Dr. Cheah Wai Shiang for teaching and guiding me about how to make a good final year project. An important appreciation goes to my unreplaceable people in my life which are my parents who always giving me the moral supports and the motivations for me to complete my project

Thank you.

# TABLE OF CONTENTS

Contents

## LIST OF TABLES

## TABLE OF FIGURES

## ABSTRACT

The goal of this project is to develop a Smart Access Hotel System that enhances security, convenience, and operational efficiency by utilizing fingerprint authentication and Internet of Things (IoT) technology. Traditional hotel access systems, which rely on physical keys or magnetic key cards, are prone to security risks such as loss, theft, and unauthorized duplication. These issues not only compromise guest safety but also increase the administrative burden on hotel staff. This project proposes a modern solution by integrating a smart door lock, utilizing the Arduino Nano 33 IoT microcontroller, a fingerprint sensor, a keypad, and a buzzer, along with a mobile application. Guests can conveniently book a room via the mobile app, complete a self-check-in process and securely access their rooms without needing physical keys. At the same time, hotel staff can remotely manage access, monitor logs, and receive real-time alerts through the same mobile app. By addressing the shortcomings of traditional systems, the proposed solution provides a more reliable and user-friendly method for managing hotel room access, ultimately enhancing the overall guest experience and improving hotel operations.

## ABSTRAK

Matlamat projek ini adalah untuk membangunkan Sistem Akses Pintar Hotel yang meningkatkan keselamatan, kemudahan, dan kecekapan operasi dengan menggunakan teknologi pengesahan cap jari dan Internet of Things (IoT). Sistem akses hotel tradisional yang bergantung kepada kunci fizikal atau kad kunci magnetik terdedah kepada pelbagai risiko keselamatan seperti kehilangan, kecurian, dan penduaan tanpa kebenaran. Masalah ini bukan sahaja menjejaskan keselamatan tetamu, malah menambah beban kerja pentadbiran kepada kakitangan hotel. Projek ini mencadangkan satu penyelesaian moden dengan mengintegrasikan kunci pintu pintar yang menggunakan mikropengawal Arduino Nano 33 IoT, penderia cap jari, papan kekunci, buzzer, serta aplikasi mudah alih. Tetamu boleh menempah bilik dengan mudah melalui aplikasi, melengkapkan proses daftar masuk kendiri, dan mengakses bilik mereka dengan selamat tanpa memerlukan kunci fizikal. Pada masa yang sama, kakitangan hotel boleh mengurus akses, memantau log, dan menerima makluman masa nyata secara jarak jauh melalui aplikasi yang sama. Dengan menangani kekurangan sistem tradisional, sistem yang dicadangkan ini menyediakan kaedah yang lebih dipercayai dan mesra pengguna untuk mengurus akses bilik hotel, sekaligus meningkatkan pengalaman tetamu dan memperbaiki operasi hotel secara menyeluruh.

# CHAPTER 1: INTRODUCTION

## 1.0 Project Title

Smart Access Hotel System Using Fingerprint Technology

## 1.2 Introduction

A smart access door system combines technology such as biometric identification, RFID, or mobile-enabled access into a technology that enables secure, keyless entry into buildings and rooms and an advanced alternative to old-fashioned lock and key solutions which use unique identifiers, including fingerprints or facial recognition. Leveraging IoT, smart access doors frequently sync with remote monitoring and control so that administrators or property managers can manage entry points in real-time and alter access permissions if necessary. This provides a combination of security and remote access, which makes smart access doors increasingly used in residential, commercial and hospitality settings to meet the requirement for safer and more flexible access (Hassan et al., 2023).

Although the demand for advanced security solutions across industries is increasing and growing, especially in the hospitality sector, where guest's convenience and safety are critical, many hotels still use traditional access methods to secure their room. These traditional hotel access methods, including physical keys and key cards have many drawbacks, as physical keys can be lost, duplicated or stolen (Alnabhi et al., 2020). On the other hand, key cards that damage or deactivate challenges are security and operationally problematic. Thus, the secure and user-friendly aspects of biometric technology, especially fingerprint recognition, provide a promising alternative for hotel access control systems (Balaji et al., 2023).

As a solution to these challenges, this project suggests a Smart Access Hotel System Using Fingerprint Technology, as a solution for hotels to these security and operational challenges. The system provides an efficient, streamlined solution to hotel access control, by integrating IoT with secure fingerprint recognition. Using the mobile app, guests can book the room and then have an access code to their room. After entering the access code, which the guest gets from the mobile app to the smart lock, the client can set their own PIN and register their fingerprint. Through the IoT based network, the guest fingerprint data and the room to which it links will be stored and managed in a real time. There is also a dashboard for hotel

staff to remotely monitor and manage guest access and improve security and operational efficiency at the same time.

This biometric IoT solution not only has added greater security but also makes things easier for the hotel to operate and provides guests with a hassle-free experience. The system, positioned to minimize key loss risk and operational inefficiencies, promotes the entire guest experience by setting an entirely new standard for access control within the hospitality

### 1.3 Problem Statement

Securing room access to avoid loss in the hospitality industry is crucial for guest satisfaction and operational efficiency. The traditional access control methods used by almost hotel such as magnetic key cards still pose a problem to the hotel staff and guests. Loss or duplication of the physical keys like magnetic key cards can lead to security vulnerability and the guest safety can be compromised. Beside that, the hotel staff also needs to continually issue and replace these keys, increasing their workload and reducing the overall efficiency of the staff. Although magnetic key cards are more modern, they also have their own limitation, such as demagnetization, misplacement, and card failure that result in guests being unable to access their rooms. It causes inconvenience and intervention of staff is required, resulting in delays and frustration. Since guest turnover is frequent in a busy hotel these inefficiencies can lead to long check-in times and higher demand for front desk services, which in turn will affect the overall guest experience (Mustafa et al., 2023).

These access challenges beyond inconvenience also comprise serious security risks, a misplaced or duplicated key card can provide access to guest rooms to unauthorized persons, subject to person and property security (Alnabhi et al. 2020). As an example, based on Yeap (2023) report the Singapore family report that an intruder entered their room in KSL Hotel and Resort at 3 am over the Deepavali holiday weekend during their stay. Moreover, the constant requirement to settle access related issues diverts hotel staff away from other vital service related jobs leading to a drop in overall service quality and guest satisfaction. With these limitations, it is critical that there is a more advanced, secure and efficient access control system that meets the expectations of the modern traveler. A biometric-based access system using the fingerprint technology provides a possible solution that eliminates the risk of losing or having stolen access credentials with improved security and convenience. Integration of technologies to IoT enabled smart access solutions to hotels can facilitate a smooth running of such hotels

as it improves guest experience, leads to improved security, and enhances safety in a hotel environment (Wang et al., 2021).

### 1.4 Scope

The scope of the Smart Access Hotel System is designed to use Fingerprint Technology, a biometric-based access control system tailored for hotels. This system will allow guests to register their fingerprints upon check-in and use them to access their rooms at the same time eliminating the need for traditional keys or key cards. It includes the development of an intuitive mobile app for guests and hotel staff and integration with the hotel's management system for room assignment and access control. The project will enhance guest convenience and hotel security through biometric authentication technology.

### 1.5 Aims and Objective

a) To design and develop finger recognition system for a hotel.
b) To evaluate the proposed system using usability testing.

### 1.6 Brief Methodology

The methodology that is chosen for this project is Agile methodology.


Figure 1.1: Agile Methodology Cycles (Aguayo Publicidad, n.d.)

Agile methodology was chosen as the methodology for this project instead of Waterfall and Rapid Application Development (RAD) methods. Agile is marked by a strong emphasis on flexibility, quick adaptation, and, most importantly, continuous improvement. One of the important things Agile supports is the shorter development cycle called a sprint which makes products or features released faster (Devharsh, 2021). Agile, which is unlike the Waterfall model, is more adaptable to future changes and is faster, deploying prototyping as its key

strategy. The rapid, iterative development and regular testing and reviews that it takes to identify and solve problems early in the process result in a better outcome (Waja et al., 2021).

### 1.6.1 Phases in Agile Methodology

#### 1.6.1.1 Planning Phase

The first stage of each cycle defines the scope of the project in terms of requirements, product features and functionality. Furthermore, necessary hardware and software components are also identified and documented.

#### 1.6.1.2 Design Phase

This is the critical phase where the design plans for the system, from design to architecture and user interface. In other words, it describes the system architecture by explaining what hardware and software components to use such as sensor selection, communication protocol, and data processing platform. It also entails the IoT sensor system integration planning and sensor data communication protocols and data formats for data transmission.

#### 1.6.1.3 Develop Phase

The system is developed incrementally and iteratively during the development phase, creating the software and hardware of the system. The design of various components that constitute the software, such as a graphical user interface, database and other data processing functions and fingerprint identification system, is done to work together in this phase. The hardware components, such as fingerprint sensor, sensors and communication modules, are assembled and examined for correct functional operation of components. During this phase, the design mainly focuses on verifying if all the components form a coherent system and, if so, all components meet the specified security and operational standards of the hotel access control system.

#### 1.6.1.4 Test Phase

In Agile methodology, testing is a continuous and essential part of the development process. Unlike traditional Waterfall methods, where testing typically happens in a separate phase after development concludes, Agile integrates testing throughout the entire development cycle. Testing occurs alongside development to verify that the product consistently meets quality and functionality standards.

#### 1.6.1.5 Deploy Phase

In Agile methodology, the deployment phase is when the product or system is released to users or customers. This is the concluding step in the Agile development process, focused on ensuring the product is successfully delivered, installed, and fully operational.

#### 1.6.1.6 Review Phase

Agile practices promote ongoing review and feedback throughout the software development process

### 1.7 Significance of Project

The importance of the Smart Access Hotel System using Fingerprint Technology is that it can change the way how guests access the property and improve the whole security in the hospitality industry. The project provides a solution to the main challenges of traditional key-based access systems, including security vulnerabilities, inconvenience of lost keys, and operational inefficiencies by the implementation of a biometric solution. Using this system would enhance the guest experience because it automates the process of check in and reduces the need for physical contact when operating it, and it will reduce hotel administrative burden with a dashboard that can monitor the room status. The project is also a strategic improvement in hotel management practices and it conforms to the trends in technology and customer service expectations.

### 1.8 Project Schedule

This final year project 1 starts on 10 October 2024 and is expected to be completed on 19 February 2025, which will take approximately 3 months. The project details are described in the table below and represented in the Gantt Chart.

Table 1.1: Project Schedule for FYP 1 and FYP2

| Task Name | Start | End |
|---|---|---|
| Final Year Project 1 (FYP1) | 10 Oct 2024 | 19 Feb 2025 |
| Project Preparation | 10 Oct 2024 | 14 Nov 2024 |
| Project Briefing | 10 Oct 2024 | 10 Oct 2024 |
| Prepare Brief Proposal | 11 Oct 2024 | 19 Oct 2024 |

| | | |
|---|---|---|
| Approved Brief Proposal Submission | 20 Oct 2024 | 20 Oct 2024 |
| Feedback from Supervisor and Examiner | 20 Oct 2024 | 27 Oct 2024 |
| Prepare full Proposal | 28 Oct 2024 | 13 Nov 2024 |
| Full Proposal Submission | 14 Nov 2024 | 14 Nov 2024 |
| Chapter 1: Introduction | 14 Nov 2024 | 20 Nov 2024 |
| Finalize Project Introduction | 14 Nov 2024 | 20 Nov 2024 |
| Chapter 1 Submission | 20 Nov 2024 | 20 Nov 2024 |
| Chapter 2: Background | 21 Nov 2024 | 13 Dec 2024 |
| Finalize Project Background and Reference | 21 Nov 2024 | 13 Dec 2024 |
| Chapter 2 Submission | 13 Dec 2024 | 13 Dec 2024 |
| Chapter 3: Methodology | 14 Dec 2024 | 05 Jan 2024 |
| Finalize Project Methodology and Phases | 14 Dec 2024 | 05 Jan 2024 |
| Chapter 3 Submission | 05 Jan 2024 | 05 Jan 2024 |
| Final Report | 06 Jan 2025 | 19 Feb 2025 |
| Finalize FYP1 Final Report | 06 Jan 2025 | 17 Jan 2025 |
| Final Report Amendment | 17 Jan 2025 | 19 Feb 2025 |
| Final Report Submission | 19 Feb 2025 | 19 Feb 2025 |
| Final Year Project 2 (FYP2) | 17 Mar 2025 | 23 Jun 2025 |
| Chapter 4: Implementation and Testing | 17 Mar 2025 | 15 May 2025 |
| Finalize Project Implementation and Testing | 17 Mar 2025 | 14 May 2025 |
| Chapter 4 Submission | 15 May 2025 | 15 May 2025 |
| Chapter 5: Conclusion | 16 May 2025 | 31 May 2025 |
| Finalize Project Conclusion | 16 May 2025 | 30 May 2025 |
| Chapter 5 Submission | 31 May 2025 | 31 May 2025 |
| Final Report | 1 June 2025 | 23 June 2025 |
| Finalize FYP2 Final Report | 1 June 2025 | 10 June 2025 |

| | | |
|---|---|---|
| Final Report Amendment | 10 June 2025 | 22 June 2025 |
| Final Report Submission | 23 June 2025 | 23 June 2025 |

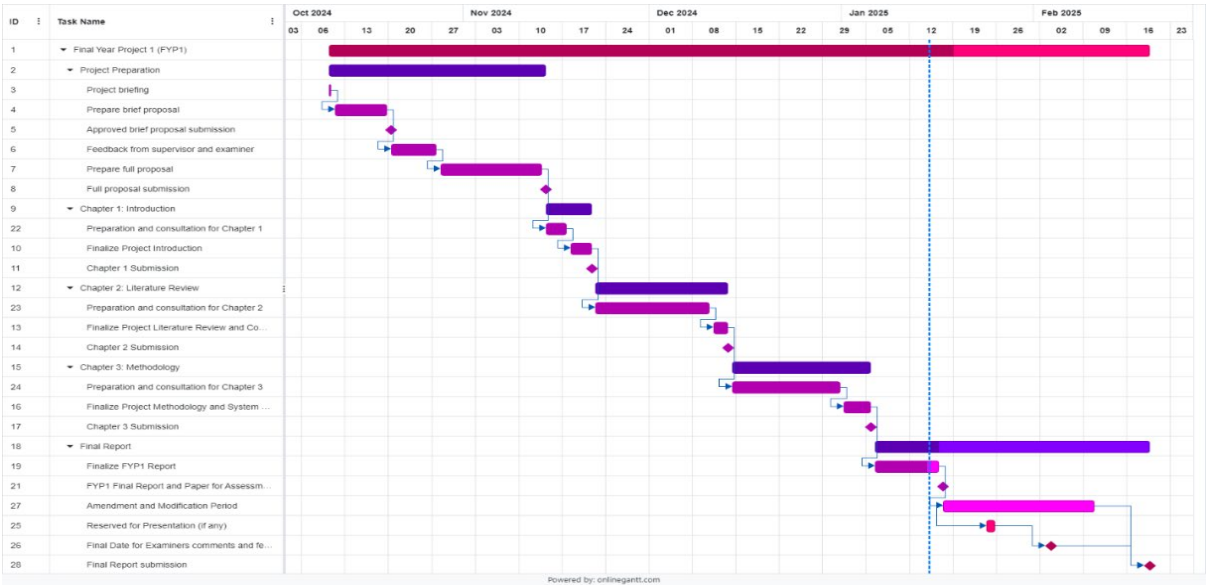


*Figure 1.2:* Schedule for FYP1

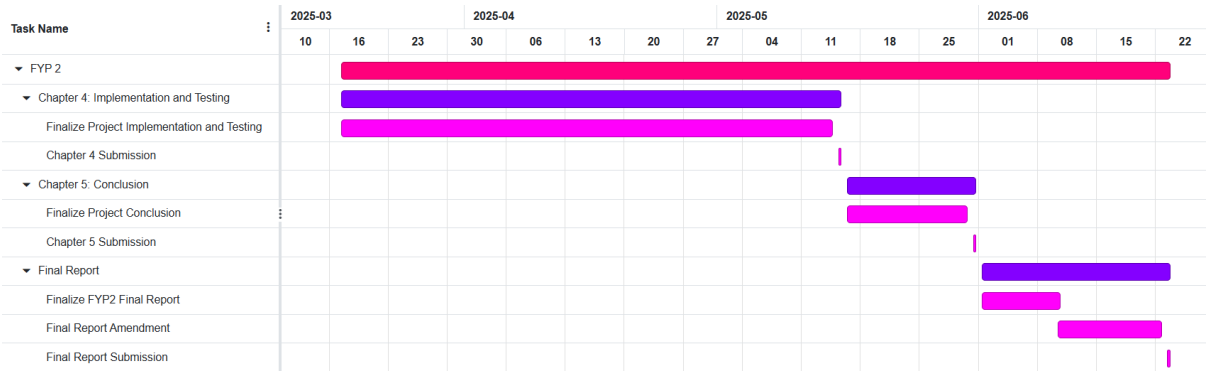


*Figure 1.3*: Schedule for FYP2

## 1.9 Expected Outcome

The Smart Access Hotel System utilizing Fingerprint Technology offers significant benefits for both guests and hotel management.

a) Hotel Room Access System with Fingerprint Recognition:
   The system uses an IoT framework with fingerprint recognition for quick and accurate guest identification. This real-time processing ensures fast access, improving security by restricting entry to authorized individuals only.

b) Seamless Check-In and Access Experience:

The system features an intuitive interface and simplifies check-in and room access. Guests can register their fingerprints via a touch screen, eliminating physical keys and providing a contactless, hassle-free experience.

c) Administrative Management Dashboard:
The management dashboard enables staff to monitor guest access in real-time. It provides insights into room assignments and status, allowing quick responses to issues and optimizing hotel operations for greater efficiency

## 1.10 Project Outline

This project contains five chapters, which are an introduction, literature review, requirement analysis, design, implementation and testing, conclusion, and future work. All the five chapters will be summarised as below:

Chapter 1 is about the general understanding of the project, this chapter will discuss the problem statement of the project, the objective of the project, the methodology to develop the system, the project scope, the significance of the project, and the expected outcome of the project. The project schedule will also be included to track the progress of the project.

Chapter 2 is about reviewing the existing system that is similar to the Smart Access Hotel System Using Fingerprint Technology. It compares each of the existing system features and weaknesses to gain an understanding of how to enhance the proposed system. Moreover, the software and hardware used to develop the proposed system will be briefly introduced in this chapter.

Chapter 3 is about the methodology applied to project development. The methodology chosen for this project is Agile. Through this chapter, Agile will be explained in detail in terms of how to develop the Smart Access Hotel System Using Fingerprint Technology in each phase mentioned in Chapter 1.

Chapter 4 describes the implementation phase and the testing phase of this project. It involves building and testing a prototype of the Smart Access Hotel System Using Fingerprint Technology, and further details on testing the prototype will be explained in this chapter.

Chapter 5 concludes the whole project and comprehends the lesson learned throughout this project as well as the outline for future works.

## 1.11 Summary

In this chapter, a brief overview of the project has been outlined and discussed. The project aims are defined to solve the problems that have been stated. Additionally, the methodology has been identified along with the project schedule to manage the project timeline, which takes three months in order to achieve the project's objectives. Furthermore, the project's significance has been introduced, which is that it can enhance the guest experience by offering a smooth, contactless check-in procedure and lessening the administrative load on hotel employees. In addition, agile methodology has been identified as the approach for project development to achieve the project's expected outcome. Therefore, the next chapter will discuss the project's methodology in detail.

# CHAPTER 2: LITERATURE REVIEW

## 2.0 Introduction

In order to achieve the objectives of the project that have been mentioned in previous chapter, background research of the system need to be done and analyze. This chapter reviewed the others three (3) similar existing systems that are related to this topic and the background study of each of the existing systems will be compared with the proposed project to analyze the requirement of provided from each system. Furthermore, this chapter includes the brief overview of the key features of the proposed system. The comparison of the systems is based on three (3) journal articles which are:

a) Design and implementation of a fingerprint-based biometric access control system (Esekhaigbe & Okoduwa, 2022).
b) Arduino-Powered Fingerprint Authentication for Door Access Control (S et al., 2024).
c) Design and Implementation of a Fingerprint Based Lock System for Shared Access (Baidya et al., 2017).

## 2.1 Reviewed on Existing Systems

### 2.1.1 Fingerprint-based biometric access control system

To improve on the weakness of traditional locking systems, which can be easily copied of left open, this system has been created. A biometric solution using fingerprint is presented by Esekhaigbe and Okoduwa (2022), which guarantees that only authorized people can access restricted areas interwoven with fingerprint recognition technology and Atmega328p microcontroller, which makes it a cost effective and efficient access control solution. The objective of the project is to increase security while offering a user friendly interface for end users and administrators and is applicable to residential, commercial and institutional applications (Esekhaigbe & Okoduwa, 2022).

Esekhaigbe and Okoduwa (2022) proposed this system which has a fingerprint module, Atmega328p microcontroller, H-bridge motor driver, OLED , and other peripheral components like control buttons and LEDs as its main components. The biometric data captured and processed by the fingerprint module consists of detecting and extracting the minutiae points for comparing, while the Atmega328p microcontroller plays the central processing unit role by

controlling all input and output operations. In addition to that, the motorized door lock is controlled by H-bridge motor driver which controls the motorized door lock to appropriately lock and unlock and OLED displays messages like 'Access Granted' or 'Access Denied' and buttons allow administrative functions of adding or removing users (Esekhaigbe & Okoduwa, 2022). The tools integrated into the system are shown in the figure below.

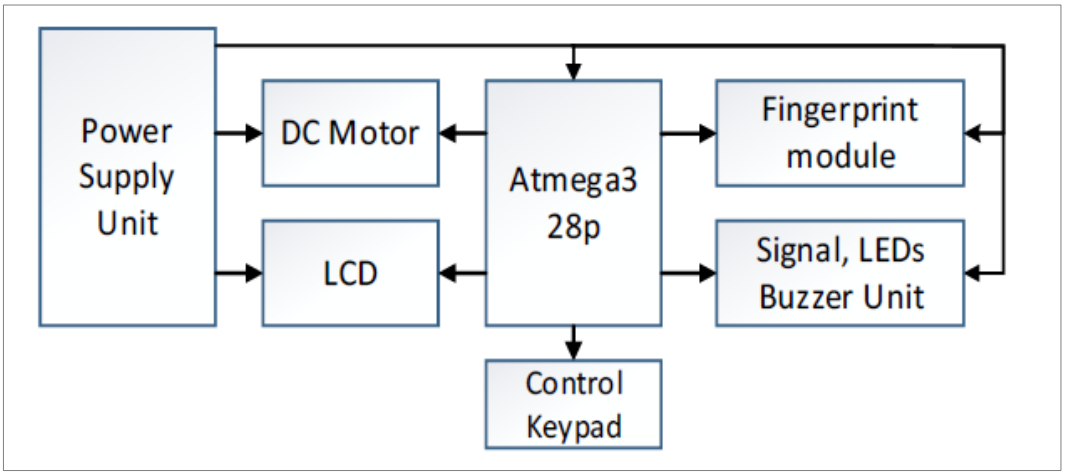


*Figure 2.1.*: The tools integrated into the system (Esekhaigbe & Okoduwa, 2022)

The system proposed by Esekhaigbe and Okoduwa (2022) operates through two primary phases, which is enrolment and authentication. During the enrolment phase, user fingerprints are scanned and stored in the system's database. Then the fingerprint module uses minutiae-based algorithms to extract and record unique features of the fingerprint. During authentication, the module compares a live scan against stored templates and if a match is found, the Atmega328p microcontroller activates the H-bridge motor driver to unlock the door. Additional features include an emergency override system and an administrative mode that allows system reconfiguration, such as adding or deleting fingerprints and the door that automatically relocks after four seconds, preventing unauthorized reentry. The inclusion of emergency and admin buttons enhances usability and flexibility, making the system adaptable to various scenarios.

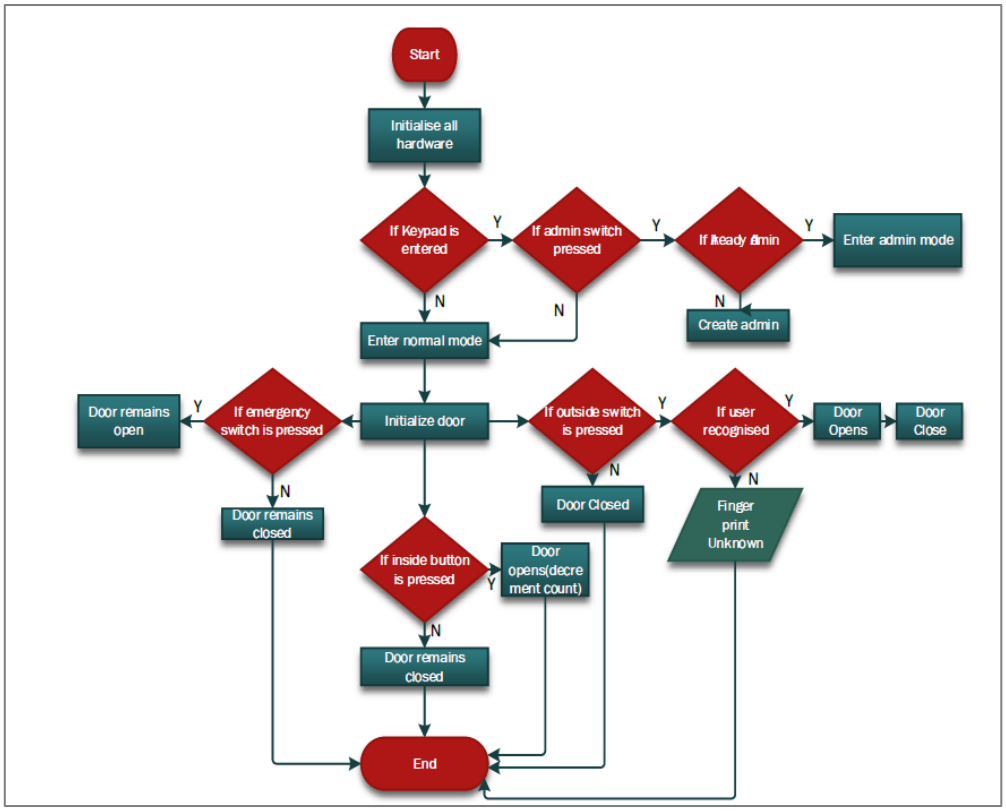


*Figure 2.2* The tools integrated into the system (Esekhaigbe & Okoduwa, 2022)

Using biometric data, this system has several advantages, such as high reliability and ease of use, and also eliminates physical keys which can be lost or duplicated. The security is enhanced with the automatic relocking feature so that the window of vulnerability post access is minimised. Moreover, the modular design of the platform enables it to be scalable and adaptable, and hence, a cost-effective and future-ready solution for different applications.

### 2.1.2 Arduino-Powered Fingerprint Authentication for Door Access Control

Based on this traditional biometric security, this system further integrates GSM technology to achieve remote operability and security from advanced communication capabilities. The system combines fingerprint biometrics with GSM-enabled remote access to overcome the limitations of standalone solutions and fits the current trend for flexible and efficient access control (S et al., 2024). The main objective of the system is to develop a robust, scalable and user-friendly system suited for smart homes, offices and other high-security environments.

S et al. (2024) propose a system that uses an Arduino microcontroller as its central unit to process fingerprint data and communicate with the GSM module. The SIM800L GSM module allows users to communicate remotely in an encrypted manner and manage access permissions via their mobile devices. Next, a fingerprint sensor collects biometric data from the user, and an OLED displays the real-time status to the user. Other components include control buttons for configuring the system and LEDs to show the status of the system. The scalability and compatibility with future technological advancements of the system are enabled by the modular design. The figure below shows how the components in the system are connected to each other.

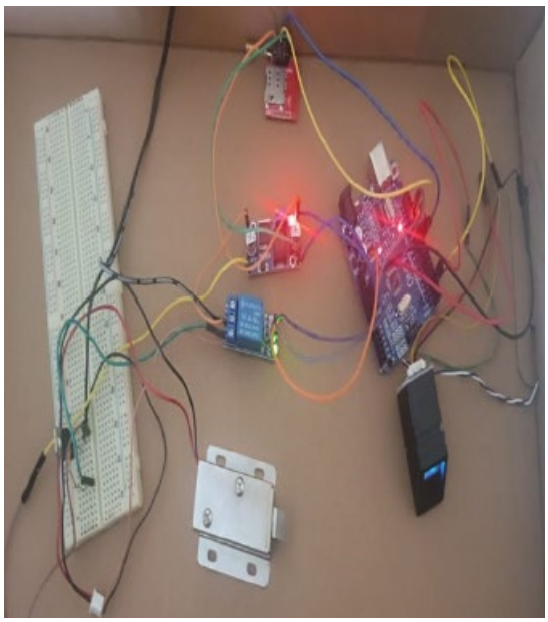

*Figure 2.3:* Circuit connections for the proposed system (S et al., 2024)

The system consists of three main phases, enrolment, authentication and remote management. Fingerprints are scanned and safely kept in the database when a person is enrolled. Then, authentication consists of matching live scans with stored templates to confirm that it is the person. By using the GSM module, the system also provides a functional layer through the transmission of encrypted data to remotely lock and unlock the device. The usefulness of this feature is especially for users who need to access the system remotely very often or for those who need to observe system activity in real-time. In addition ,the GSM module enables the capability to notify and alert the user when there is an intrusion, thereby increasing the system responsiveness and security in general

This system that been introduced by S et al. (2024), stands out for its remote operability and high accuracy. The integration of GSM technology allows users to control access from anywhere, enhancing convenience and flexibility. Its encrypted communication safeguards against data breaches, ensuring secure management of access permissions and its modular design also ensures adaptability to evolving security requirements, making it a versatile and scalable solution for modern access control needs

### 2.1.3 Fingerprint Based Lock System for Shared Access

The fingerprint-based lock system proposed by Baidya et al. (2017) is intended to offer a secure, reliable and user-friendly solution for controlled access environments like homes, offices, universities and shared facilities. The fingerprint system unlocks the door without using physical keys or codes like conventional locks but instead uses the person's unique biometric data to grant or deny the request to access with fingerprint only getting granted for authorized users whose fingerprint is enrolled into the system. The system also includes a secondary method of access via a keypad by which a password can be entered if fingerprint authentication is not available. This dual-layer approach to security greatly reduces the potential for unauthorized access and provides a modern, practical means for shared access environments where security and ease of use are important.

Several key hardware elements are integrated for optimal performance of the system. The microcontroller used for input and output operation is Arduino Uno. After that, high-resolution images are then captured by the FPM10A fingerprint sensor and are matched with previously stored fingerprints that can support up to 126 unique entries (Baidya et al., 2017). Then, the door is secured by using the electronic lock which works through a relay module that switches power between 5V and 12V components. Lastly, password-based backup access is provided through a 4x4 matrix keypad, a buzzer is used to give audio feedback for different system states, and a push-button allows manual unlocking from inside the premises.

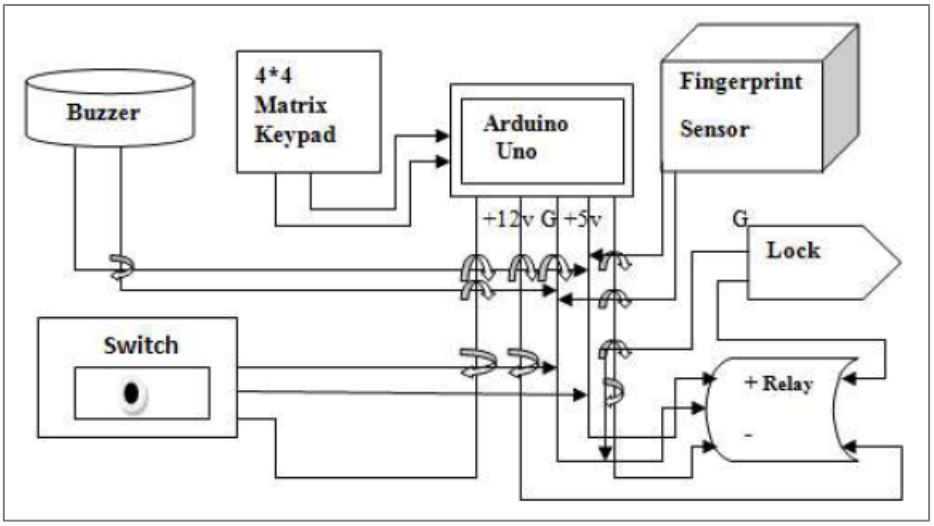


*Figure 2.4:* Block diagram of the whole system (Baidya et al., 2017)

The fingerprint-based lock system combines hardware and software integration, the FPM10A fingerprint sensor connects to the Arduino Uno for fingerprint enrollment and verification, while a relay module controls the electronic lock. Then 4x4 matrix keypad provides backup password access, and a buzzer and push button offer feedback and manual unlocking. The software, developed with the Arduino IDE and the Adafruit Fingerprint Sensor Library, manages fingerprint matching and password verification and if authentication succeeds, the door will unlocks. On the other hand, if the system detects three failed attempts, an alarm triggers that will alert the user (Baidya et al., 2017).

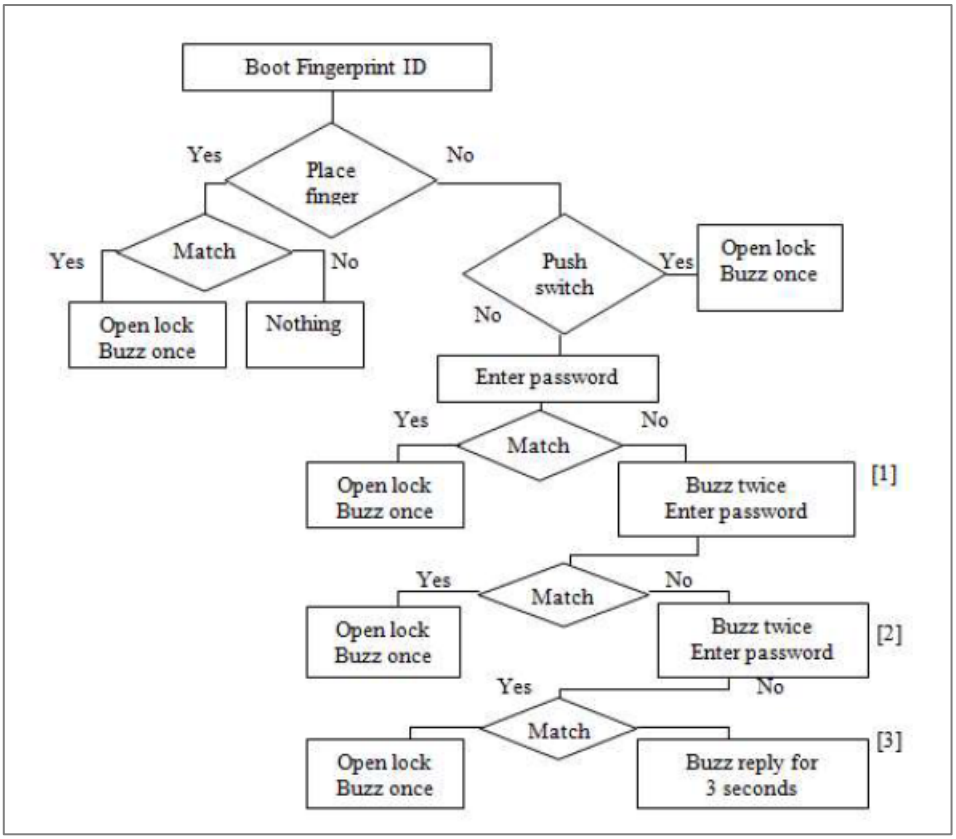


*Figure 2.5:* Flowchart of the entire system (Baidya et al., 2017)

This fingerprint-based lock system offers several advantages over traditional security methods. First, it enhanced security through biometric authentication, which reduces the risk of unauthorized access (Baidya et al., 2017). The system also provides convenience for the user since they do not need to carry keys or remember passwords to open the door. In addition, it is also cost-effective because it is built with affordable components suitable for small and large organizations, and the dual-layer security with a keypad ensures backup access during emergencies. Lastly, auditory feedback that was built into the system enhances user awareness and alerts in case of intrusion attempts happen.

## 2.2 Comparison on Existing Systems and the Proposed System

*Table 2.1:* Comparison of Features Between Existing Systems and Proposed System

| Features | Fingerprint-based biometric access control system | Arduino-Powered Fingerprint Authentication for Door Access Control | Fingerprint Based Lock System for Shared Access | Proposed System |
|---|---|---|---|---|
| **Hardware** | Arduino Atmega328p, OLED , H-bridge motor, buzzer, fingerprint sensor | Arduino microcontroller, SIM800L GSM module, fingerprint sensor | Arduino UNO, optical fingerprint sensor (FPM10A), keypad, buzzer | Arduino Nano 33 Iot, optical fingerprint sensor, keypad, buzzer |
| **Authentication Method** | Fingerprint recognition (minutiae-based) | Fingerprint + GSM remote access | Fingerprint + Keypad (dual authentication) | Fingerprint + Keypad (dual authentication) + Wifi remote access |
| **Intruder Response** | Local alarm for unauthorized access | Remote alerts via GSM to mobile devices | Buzzer alerts and continuous sound after 3 failed attempt | Buzzer alerts and continuous sound after 3 failed attempt + Remote alerts via Wifi to admin |
| **Remote Management** | No remote management | Yes, via GSM module (SIM800L) | No remote management | Yes, via built in Wifi module |
| **System Functionality** | Local verification with limited user management | Remote verification, notifications, and management | Local verification, user management, and alerts | Local verification, notifications, and user management and alerts |
| **User Interface** | Basic OLED display for status updates and alerts | Application to access the door | No Interface | Basic OLED and Mobile app for user registration and admin management |

Based on the Table 3.0, the comparison features of each existing system of fingerprint-based biometric access control systems and the proposed system, Smart Access Hotel System Using Fingerprint Technology, may differ in terms of hardware, authentication method, intruder response, remote management, system functionality, and user interface.

a) The Fingerprint-Based Biometric Access Control System uses an Arduino Atmega328p, an OLED , an H-bridge motor, a buzzer, and a fingerprint sensor. It relies on fingerprint recognition for authentication, providing a basic local alarm in case of unauthorized access. This system has no remote management capabilities and offers local verification with limited user management. The user interface includes a basic OLED display for status updates and alerts, making it suitable for small-scale applications.
b) The Arduino-Powered Fingerprint Authentication for Door Access Control incorporates an Arduino microcontroller and a SIM800L GSM module for remote notifications. Authentication involves fingerprint recognition with GSM remote access, allowing for remote alerts via GSM to mobile devices if unauthorized access is detected. This system supports remote management through GSM, offering remote verification, notifications, and user management. The interface features an application to access the door and comes with GSM-based notifications, making it ideal for scenarios where remote monitoring is necessary.
c) The Fingerprint-Based Lock System for Shared Access uses an Arduino UNO, an optical fingerprint sensor (FPM10A), a keypad, and a buzzer. Authentication involves fingerprint recognition with dual authentication via a keypad. In the event of an intruder, it triggers buzzer alerts and continuous sound after three failed attempts. This system does not support remote management, limiting functionality to local verification, user management, and alerts. The user interface includes no display, but it comes with a keypad for password fallback and buzzer alerts, making it suitable for shared-access environments.

Proposed System

The Smart Access Hotel System Using Fingerprint Technology enhances functionality by using an Arduino Nano 33 IoT with an optical fingerprint sensor, keypad, and buzzer. It offers fingerprint and keypad dual authentication with local access. For intruder response, it

triggers buzzer alerts and continuous sound after three failed attempts, while also sending Wi-Fi-based remote alerts to an admin. The system supports remote management via built-in Wi-Fi, enabling remote verification, user registration, and alert management. The user interface is robust, featuring an interface for registration, alerts, and remote admin management. This makes the proposed system versatile, cost-effective, and suitable for both shared and remote-access control scenarios.

### 2.3 Brief Overview of The Proposed System

Smart Access Hotel System Using Fingerprint Technology is proposed based on the strengths of existing fingerprint-based authentication systems and to address their limitations to provide a more robust, efficient, and versatile solution. The system integrates modern hardware and software components to add security, user experience, and functionality, making it suitable for personal as well as shared access environments.

Compared to existing systems, the proposed solution includes the Arduino Nano 33 IoT, which has built-in Wi-Fi connectivity, an optical fingerprint sensor, a keypad, and a buzzer. This hardware configuration is more compact and more powerful compared to the standalone microcontrollers such as Arduino UNO or Atmega328p used in the previous designs. In addition, the proposed system incorporates a dual layer of authentication through the use of both fingerprint recognition and a keypad. Unlike existing systems, which provide only local verification and GSM-based remote access, the integration of Wi-Fi provides for real-time, remote monitoring and management of access events. It gives the administrators greater flexibility to manage the authentication process from anywhere. The proposed system does not only provide local alarms or GSM notifications but also intruder responses. After three failed attempts, it generates audible buzzer alerts and continuous sounds and sends real-time notifications to administrators through its Wi-Fi-enabled notification system. This leads to faster responses to potential security breaches, and that means less vulnerabilities. In addition, users and administrators will find the mobile app intuitive and easy to use with seamless registration and management compared to the only basic OLED displays or GSM-based notifications offered by other systems, which are a major improvement over this.

### 2.4 Summary

This chapter examines and describes the features and objectives of three similar systems, comparing them with the proposed system. A comparison table is also provided to

summarize the key features of the existing systems alongside the proposed system. Additionally, the advantages of each system are briefly outlined. Furthermore, the chapter presents an overview of the proposed system, highlighting the approaches that distinguish it from the existing systems. This review lays the groundwork for a more detailed specification of the requirements, which will be addressed in Chapter 3.

# CHAPTER 3: REQUIREMENT ANALYSIS AND DESIGN

## 3.1 Introduction

This chapter provides an in-depth discussion of the requirement analysis for the proposed system, covering a range of relevant topics. It also introduces the project methodology, outlining the steps involved in the system's development. Additionally, the chapter offers a detailed description of the system's architecture and flowchart

## 3.2 Project Methodology

Agile methodology is implemented in developing the proposed system for Smart Access Hotel System Using Fingerprint Technology, as stated in Chapter 1. This methodology adapted the sprint, which enables the processes to be divided into lengths of time. Therefore, the time management and process development of the system will be more manageable and allow the minimization of the system's cost.


*Figure 3.1:* Agile Development Model

The Agile methodology is ideal for this project as it enables flexibility and iterative development, making it manageable even when conducted individually (Make Computer Science Great Again, 2024). The project will follow six key phases: Requirement, Designing, Development, Testing, Deployment, and Review, allowing for continuous progress, testing, and improvement.

### Requirement Phase

The requirement phase involves identifying and documenting the system's key functionalities and features. These include fingerprint authentication as the primary access

mechanism, a keypad for secondary verification, Wi-Fi connectivity for remote monitoring and control, and a user-friendly interface for hotel staff and administrators. Requirements will be organized into a prioritized backlog using Agile techniques, ensuring that critical features are addressed first during development. This phase ensures a clear understanding of the project's scope and objectives.

**Designing Phase**

The designing phase focuses on creating a comprehensive blueprint for the system. The software architecture will outline the integration of fingerprint authentication, secondary keypad verification, Wi-Fi-enabled communication, and alert mechanisms. Additionally, user interface design concept will be created to illustrate how administrators will interact with the system, manage access logs, and monitor notifications. The design will be reviewed and refined iteratively to ensure alignment with the defined requirements.

**Development Phase**

The development phase will follow an incremental approach, with features built and tested in successive iterations. Initial iterations will focus on core functionality, such as fingerprint registration and verification, followed by integrating the keypad for dual-layer authentication. Subsequent iterations will implement Wi-Fi connectivity, enabling remote monitoring and management. Each component will be developed modularly to ensure efficient debugging and integration. Continuous integration and testing will maintain the system's stability throughout the development process. The use of tools like version control systems will ensure effective management of code and documentation.

**Testing Phase**

During the testing phase, each component and system feature will undergo rigorous evaluation to ensure functionality, security, and reliability. Unit testing will be performed on individual components, such as the fingerprint sensor and keypad, to validate their performance. Integration testing will ensure seamless communication between hardware and software components. Simulated scenarios, such as repeated failed authentication attempts, will test the system's intruder response mechanisms, including buzzer alerts and real-time notifications. The stability of the Wi-Fi connection and the responsiveness of remote monitoring features will also be tested under various conditions. This phase ensures the system is robust and ready for real-world deployment.

**Deployment Phase**

In the deployment phase, the system will be installed in a controlled environment, such as a prototype door lock, for initial implementation. Performance will be monitored to evaluate the system's reliability, ease of use, and response accuracy. Any inconsistencies or areas for improvement identified during this phase will be addressed before full deployment. The system will also be documented with user manuals and maintenance guidelines to facilitate its use by hotel staff and administrators.

**Review Phase**

During the review phase, user feedback is important in assessing the performance of the user's system and confirming that it is consistent with the first set of requirements of the planning phase. In this phase, any inconsistencies, shortcomings or new requirements that arise out of the user's interaction with the system or reviews are analysed in detail. All collected feedback is prioritized and actions or enhancements are planned in order to deal with those issues successfully. This is an iterative process which ensures that the system is constantly refined and improved to meet user expectations and for operations needs.

To summarize, the project will follow a cyclical process, from planning to each phase until the planning stage where feedback will be collected. This is an iterative approach, where the system can be continually refined to meet those required conditions. Revisiting earlier phases will be part of each cycle, but considering new insights, and as needed. The project will stay flexible and responsive to feedback in order to hit its goals and result in a successful outcome that meets all identified criteria.

## 3.3 Requirement Analysis

### 3.3.1 Identify the User

The Smart Access Hotel System Using Fingerprint Technology operates for **hotel guests** and **hotel staff or administrators** as its primary users. The end-users of the system, which are **hotel guests**, can check in to their rooms seamlessly without needing to go to the reception desk and access their rooms through keyless entry using either fingerprint or PIN authentication for enhanced security. Then, the system real-time access monitoring and room permission management functions will help **hotel staff or administrators** perform their duties to oversee the guest room access log effectively and assist the hotel guests when needed. The

system delivers secure and efficient modern solutions that improve the access control of all stakeholders in the hotel.

### 3.3.2 Hardware Requirement

The prototype of the proposed system will rely on this hardware, including a microcontroller, sensors, and other necessary tools. Table 3.1 provides a detailed list of the hardware requirements for the system

*Table 3.1:* Hardware requirement for the proposed system

| Hardware | Specification |
|---|---|
| Microcontroller | Arduino Nano 33 IoT with headers |
| Sensors | Fingerprint Sensor |
| Other tools | Passive Buzzer |
| | Led |
| | Keypad |
| | I2C Graphic OLED Display 128x64 |

From Table 4.0, Arduino Nano 33 IoT has been chosen as the central microcontroller for this project because of its vast features and ability to be used in IoT-based applications. This microcontroller has a built-in Wi-Fi module so that it can easily be connected to the Internet and communicate in real time with a remote management platform through the access control system. Due to its compact form factor, it is a perfect fit for integration into the physical housing of the access control system that requires constrained space.

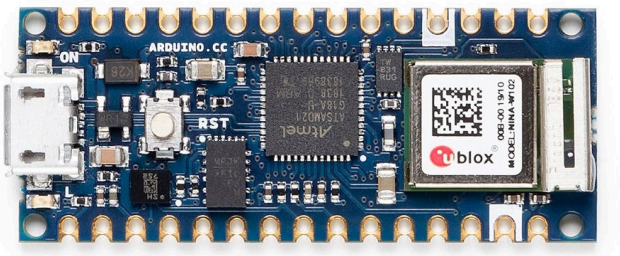


*Figure 3.2:* Arduino Nano 33 loT board with headers (Arduino, nd)

On top of that, Arduino Nano 33 IoT is also compatible with a wide variety of sensors and modules and can support fingerprint sensors, keypads, and other hardware components. The microcontroller's strong processing capability allows it to perform multiple tasks at once, including authenticating fingerprints, processing keypad inputs, and transmitting data. Collectively, these features make the proposed system reliable and efficient to build.

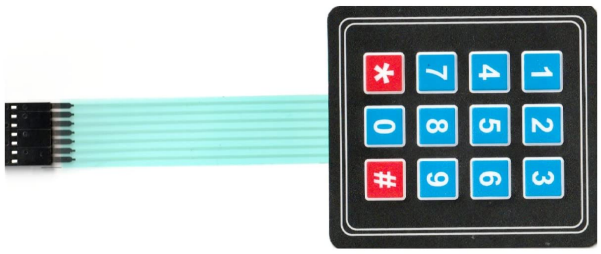


*Figure 3.3:* Keypad 3x4 (Electronation Pakistan, 2024)

A keypad inclusion in the proposed system makes it a secondary authentication mechanism, improving the security and flexibility of the access control system. The fingerprint sensor is the main mode of verification, but the keypad serves as security verification that must be entered with a Personal Identification Number (PIN). This dual authentication approach provides that the system will still be secure even in those cases where biometric authentication would be insufficient by itself. Furthermore, the keypad is adaptable to situations where temporary access has to be granted via PIN codes, for example, maintenance personnel or an emergency situation. It is durable, easy to integrate, and cost effective and, therefore, practical for improving the functionality and reliability of the system.


*Figure 3.4:* I2C Graphic OLED Display 128x64 (0.96 Inch OLED Display 128*64 Pixels Blue - I2C, n.d.)

In the project, the I2C Graphic OLED 128x64 is used to provide a simple and efficient method of displaying system information to the user by giving messages like system status, PIN entry prompts or notifications in the case of successful and failed authentication attempts are shown on screen. This is also compatible with the I2C protocol, which is nice because it cuts down on the number of pins you need to connect this up, which is great for projects where you don't have an abundance of I/O pins like the Arduino Nano 33 IoT. Additionally, the OLED clear and customizable text output helps to improve user interaction to make this system more user friendly such that users can easily understand system prompts or feedback.

*Figure 3.5:* Fingerprint sensor (MYBOTIC, n.d.)

To offer a robust and secure biometric authentication, the fingerprint sensor is incorporated into the project because of the fingerprints strait that are unique and difficult to replicate. So, this sensor will ensure that only the authorised person can access them and also makes the system more secure than typical methods, such as keys, which could get lost or duplicated. The fingerprint sensor is reliable and fast and integrates very well with the Arduino platform, allowing very quick enrolment and verification of fingerprints. In addition to strengthening access control, its incorporation into the system includes an extra layer of convenience to users that obviates the use of physical keys.

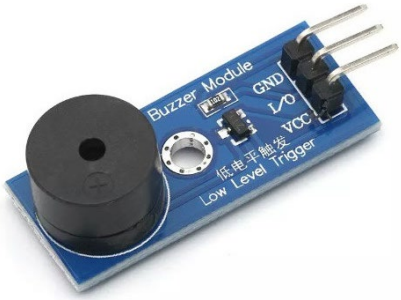


*Figure 3.6:* Passive Buzzer with Module (Module Buzzer Passif Pour Arduino, n.d.)

Lastly, the buzzer is a critical proposed system component, providing immediate auditory feedback to users and administrators. Its primary function is to act as an alert mechanism, producing sound to indicate different system states, such as successful authentication, errors, or security breaches. For instance, the buzzer will emit a continuous sound after multiple failed authentication attempts, alerting users and administrators to potential unauthorized access attempts. The inclusion of this real-time feedback mechanism enhances the usability of the system by ensuring that users are informed of its status at all times. Additionally, the buzzer's simple design, low power consumption, and compatibility with the Arduino Nano 33 IoT make it an effective and economical solution for incorporating sound-based notifications into the access control system.

### 3.3.3 Software Requirement

The successful development and implementation of the proposed system depend heavily on fulfilling the essential software requirements. These requirements play a crucial role in ensuring that the system functions as intended. The specific software needed for building and testing the prototype of the proposed system is outlined in detail in Table 5.0.

*Table 3.2:* Software requirement for the proposed system

| Software | Specification |
|---|---|
| Integrated Development Environment (IDE) | Arduino IDE Software |
| | Visual Code Studio Software |
| | Firebase |
| Operating System | Windows 7,8 and 10. macOS or Linux |
| Programming Language | C/C++ language |

## 3.4 System Design and General Architecture

The system design includes the overall architecture and flowchart of the system, developed based on the requirement analysis. Additionally, this section will present the user interface of the Arduino IoT Remote Mobile Application. The figure below depicts the system architecture of the proposed system.

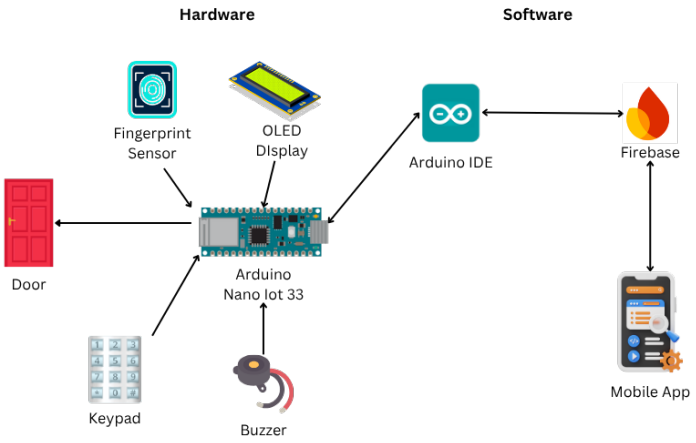


*Figure 3.7:* System Design of the proposed system

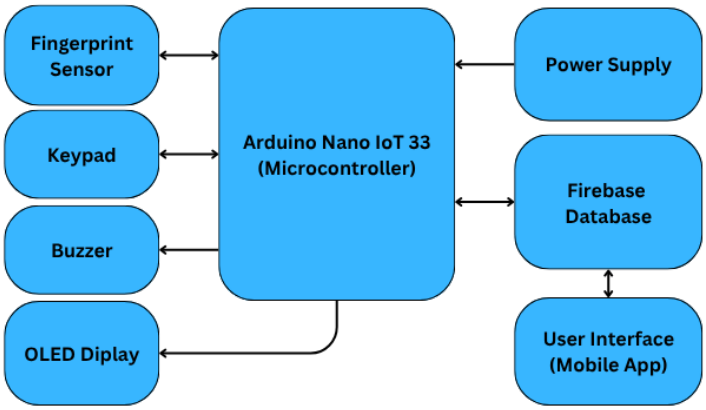


*Figure 3.8:* Simple block diagram for the proposed system

The block diagram of the proposed Smart Access Hotel System shows all the components needed to operate the system as shown in Figure 14.0. The central controller is the Arduino Nano 33 IoT that gathers all the sensors and components and provides them with the reliable 5V power supply. The Arduino is connected to a fingerprint sensor to perform biometric authentication, which will authorise users who have previously been registered. As a secondary authentication method, a keypad is included for application of dual security layer by verifying PIN. Moreover, the buzzer gives immediate auditory feedback and I2C OLED informs users of successful authentication, errors or failed access attempts. The Arduino Nano 33 IoT's Wi-Fi capability allows real time communication with a remote database to manage access log and send alert. The configuration of the system guarantees that all components work together in a secure, efficient and user friendly access control system.

### 3.4.1 System Flow Chart

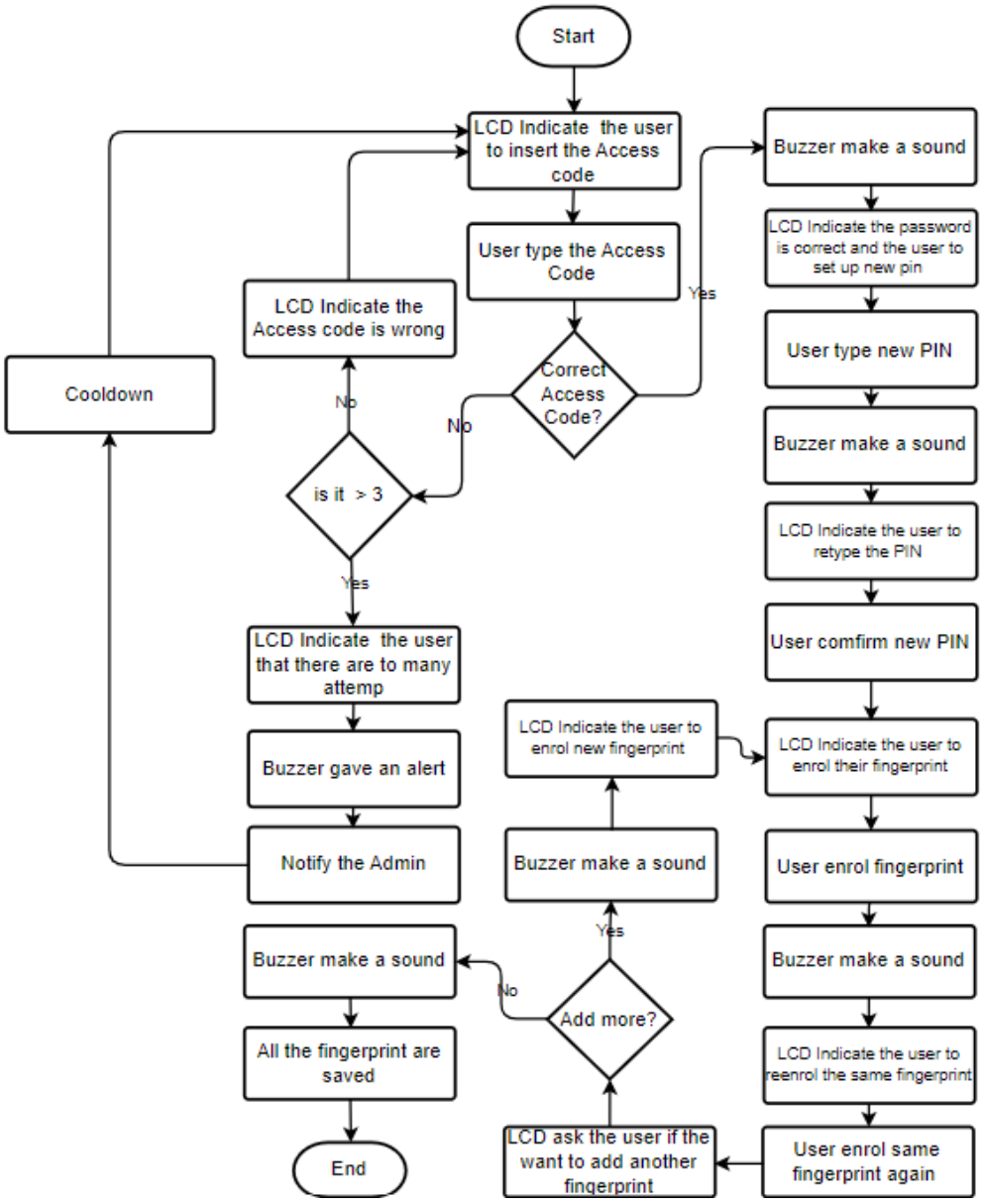


*Figure 3.9:* User first-time registration flowchart

Based on Figure 15.0, the first-time registration process begins with the user entering the access code provided through the mobile application. The system verifies the entered access code to determine its validity. If the PIN is correct, the system triggers the buzzer to produce a sound, prompting the user to create a new PIN. After entering the new PIN, the buzzer sounds again, and the user is asked to confirm the new PIN to complete the registration process. However, if the entered PIN is incorrect, the system checks whether the user has made more than three incorrect attempts. If not, the user is given another opportunity to re-enter the correct PIN. If three incorrect attempts are exceeded, the buzzer issues an alert, and the system notifies

the administrator of a potential security threat. Following this, the system activates a cooldown period, temporarily preventing further PIN entry to safeguard against brute-force attacks. During this period, further PIN entry is temporarily disabled to protect against brute-force attacks and ensure system security. After successfully setting a PIN, the user proceeds to enrol their fingerprint. The system prompts the user to enrol the same fingerprint twice for verification. After each enrolment, the buzzer sounds to confirm the action. Once the fingerprint is verified, the system asks whether the user wants to enrol additional fingerprints. If the user chooses to add more, the process loops back, allowing them to enrol another fingerprint. If no additional fingerprints are needed, the buzzer sounds to indicate the completion of the enrolment process, and all fingerprints are saved in the system. This marks the end of the first-time registration process.

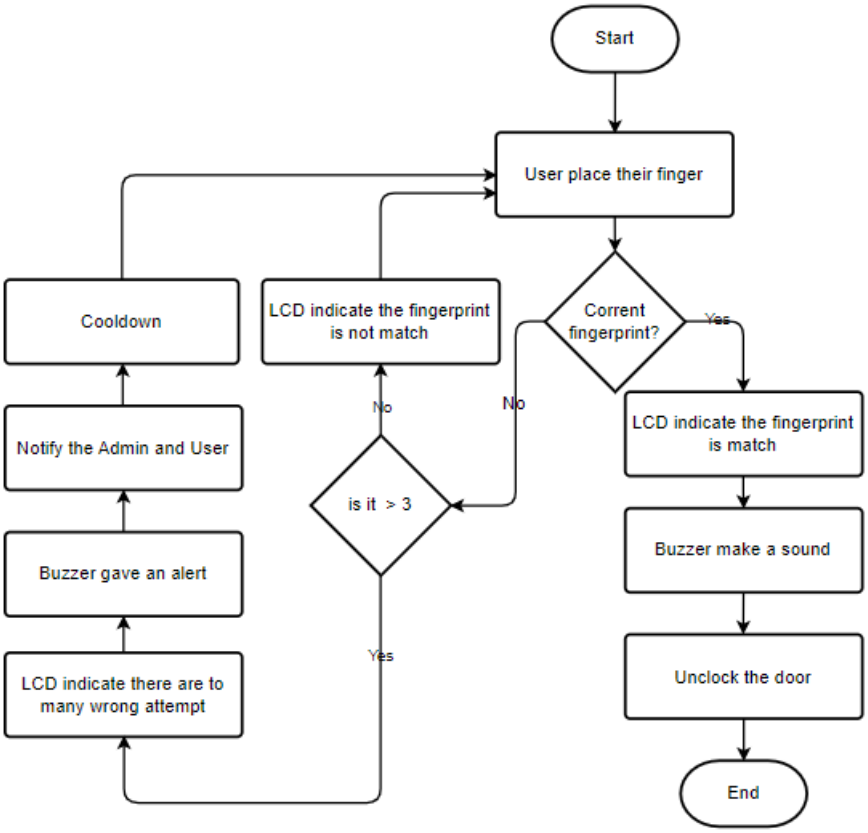


*Figure 3.10:* Fingerprint authentication flowchart

Based on Figure 16.0, the fingerprint authentication flowchart illustrates the process of user verification in the proposed system. Initially, the user enrols their fingerprint for authentication. If the fingerprint matches the stored data, the system triggers the buzzer to make a sound and unlocks the door, allowing access. However, if the fingerprint is incorrect, the

system checks the number of failed attempts. If the failed attempts exceed three, the buzzer generates an alert, and the system notifies the admin and user about the unauthorized access attempt. Afterward, the system enters a cooldown period before allowing further attempts. If the failed attempts are less than three, the system allows the user to try again, repeating the process until the conditions are met.

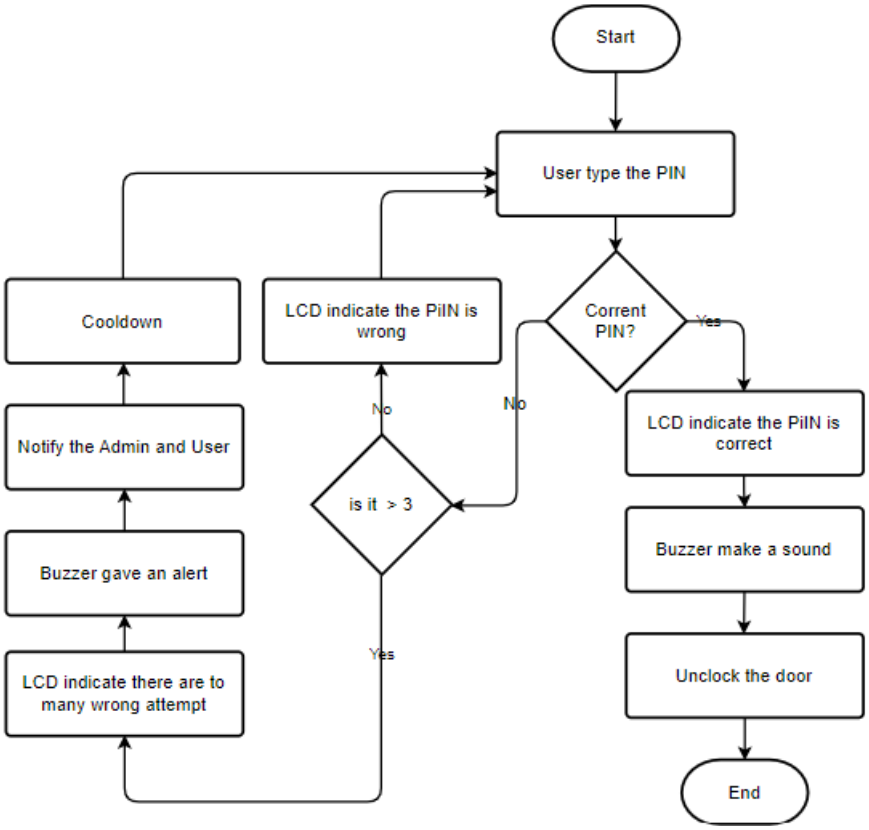


*Figure 3.11:* PIN authentication flowchart

Based on Figure 17.0, the PIN authentication flowchart demonstrates the process of verifying the user's PIN in the proposed system. The process begins with the user entering their PIN. If the entered PIN matches the stored PIN, the system triggers the buzzer to produce a sound and unlocks the door, granting access. If the entered PIN is incorrect, the system checks the number of failed attempts. If the failed attempts exceed three, the buzzer generates an alert, and the system notifies the admin and user of the unauthorized access attempt. The system then enters a cooldown period before allowing further attempts. If the failed attempts are fewer than three, the system allows the user to re-enter the PIN, repeating the process until the correct PIN is entered or the conditions for an alert are met.

### 3.4.2 Entity Relationship Diagram

The Entity Relationship Diagram (ERD) presented in Figure 18.0 outlines the logical structure of the database designed for the proposed system. It visually represents the connections and relationships between the different entities within the system, providing a clear and organized overview of how the data is structured and interrelated.

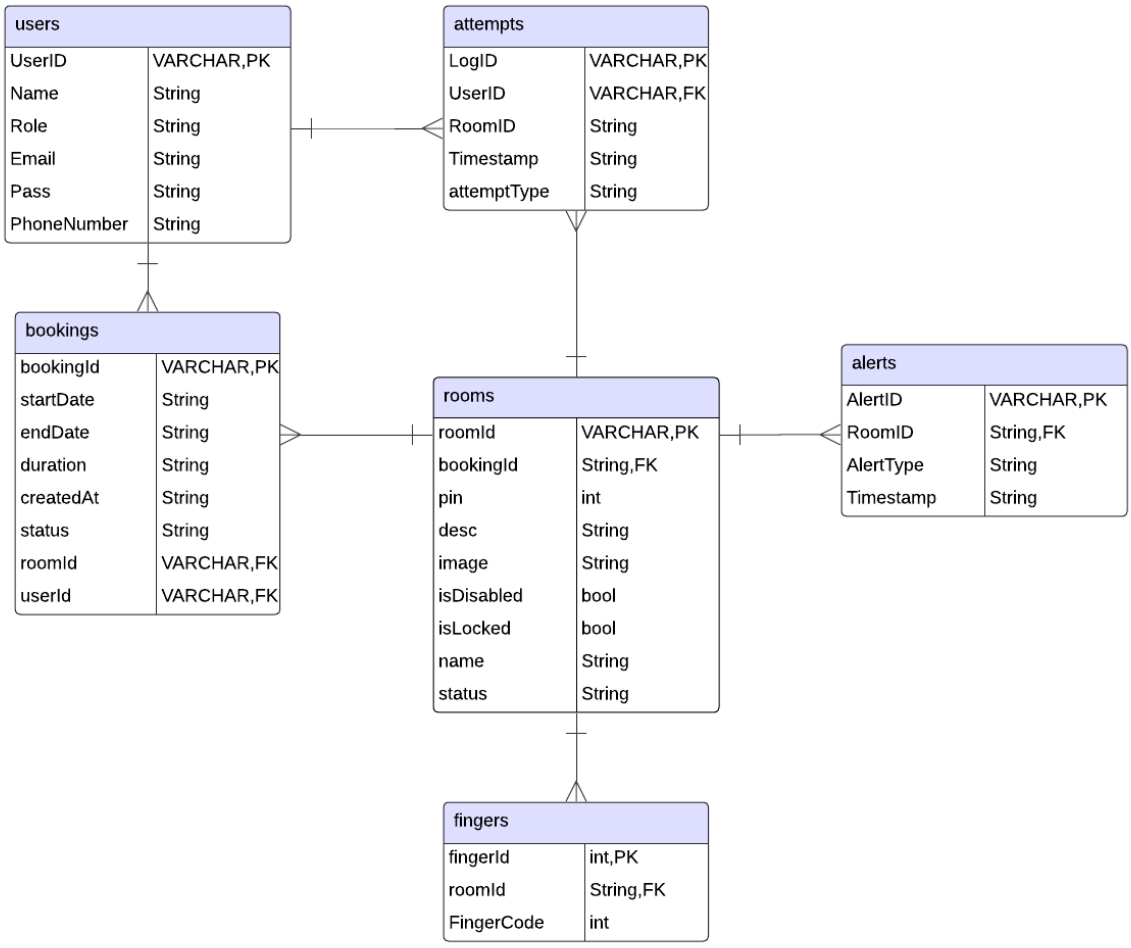


*Figure 3.12:* Entity Relationship Diagram for the Proposed System

### 3.4.3 User Interface Design Concept for the Mobile Application

The main reason for the user interface design of the mobile application is to give users an easy and efficient way to choose the room the client wants to enter and get the code they need to get in. This functionality keeps the system secure for users while being seamless and on top of that, the application has also elaborated features for the admin side of things, including the ability for the admin to monitor detailed room access logs, which in turn allows the admin

to check who has accessed what room and when. Moreover, the application is able to send real time alerts to the admin as unusual activity like repeated failed attempts to enter a PIN or fingerprint. Therefore, the admin can react quickly to these alerts, such as unlocking a door remotely in the case of an emergency or totally disabling the lock if a threat is detected. This multifunctional access system not only provides security and additional functionality to the existing circuitry, but it also grants the admin more control and flexibility with how and when users can access the system or to cover unexpected situations.

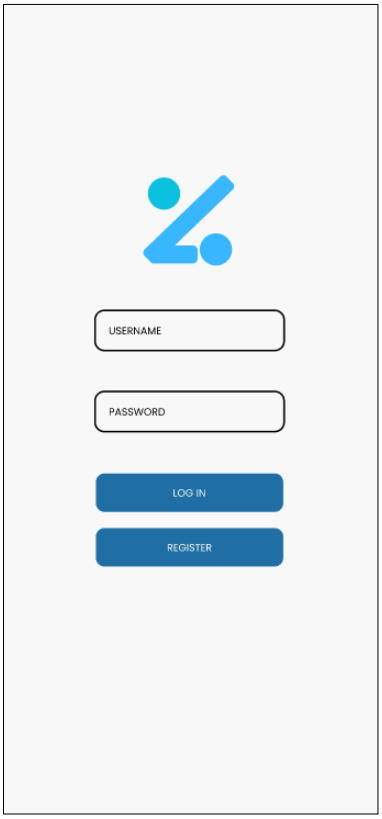


*Figure 3.13:* Log in page concept design

The figure above shows the Login page concept design for the mobile app. Before the user is able to use the app, the user needs to create an account or log in to the app. It is essential to determine whether the account that had logged in is a customer or an administrator.

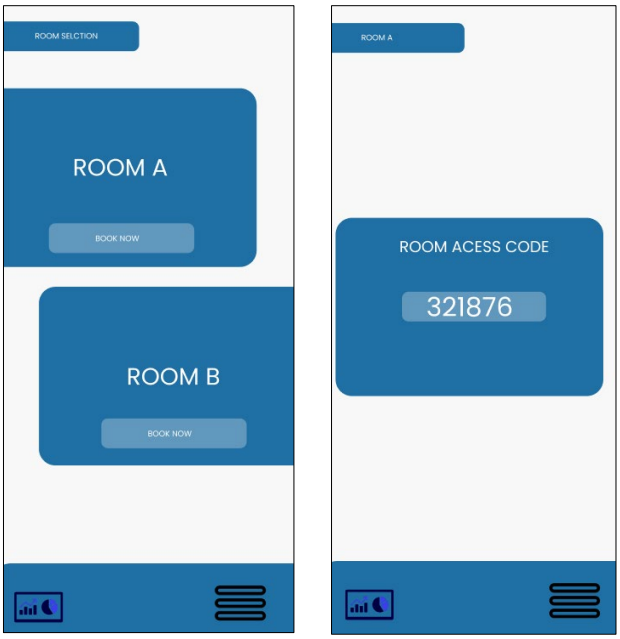


*Figure 3.14:* Room selection page concept design

After logging in, the customer can select the room they wish to book. Once they have chosen the desired room and date, the system generates a code, which the customer will need for the check-in process. This code is provided 10 minutes before the scheduled booking time, as shown in Figure 20.0.

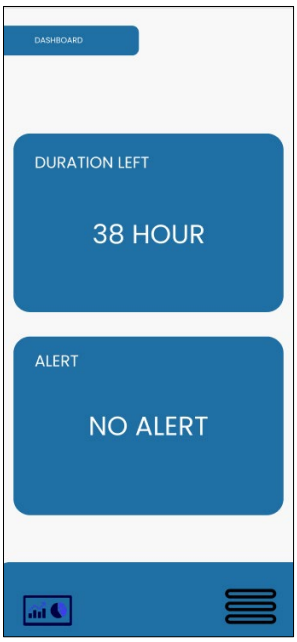


*Figure 3.15:* User dashboard page concept design

Based on Figure 21.0, the user dashboard page concept design provides an intuitive and user-friendly interface for monitoring the system's status. The dashboard consists of two primary sections, which are duration and alert. The duration section displays the total time left before the user needs to check out from the room, allowing the user to track it quickly and able to prepare beforehand. After that, the alert section will notify the user about the presence or absence of security alerts, such as unauthorized access attempts. The clean and minimalistic design ensures ease of navigation, enabling users to quickly access essential information.

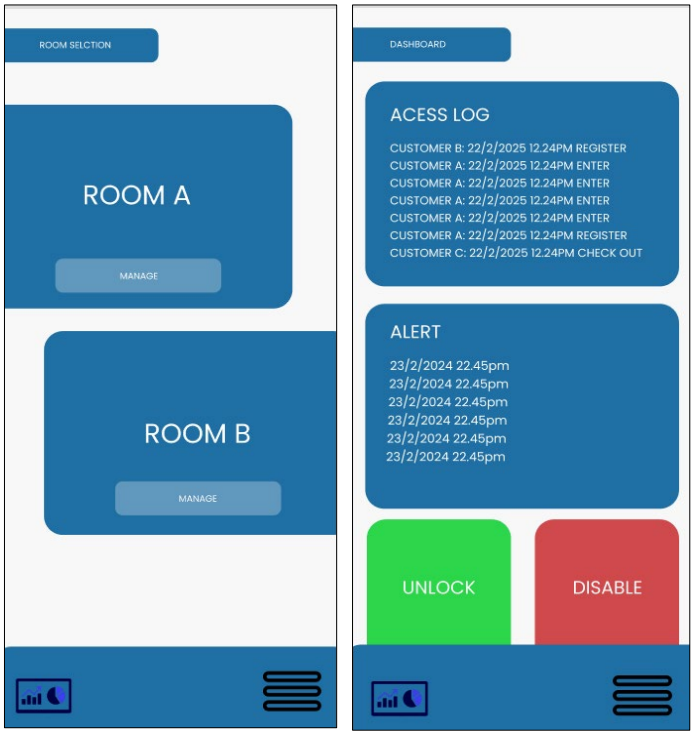


*Figure 3.16:* Admin menu and dashboard page concept design

Figure 22.0 shows the admin menu and dashboard page concept design for the access control system, which is based on a simple, intuitive, and efficient interface. Once the admin has chosen which room to manage, the admin will be able to see the dashboard, which is divided into three main parts, which are the access log, alert, and control buttons, such as unlock and disable. The customer activity access log section displays the customer activities like registrations, check-ins, and check-outs with timestamps. This will give an admin the ability to monitor access history in case of an unexpected event. Next, the alert section will show the timestamps of security notifications or unauthorised access attempts so that the admin is able

to take appropriate action on time. Apart from this, there are also control buttons at the bottom, which facilitate system management as the admin can disable or unlock the system remotely. With the clean layout and well organized structure, it made sure the admin could gain easy access to the critical information and do what was necessary well on time.

### 3.4.4 Use Case Diagram

The use case diagram in Figure 23.0 below shows how guests and staff or administrators interact with the proposed hotel access control system. Hotel guests need to complete three essential tasks, starting with booking rooms, followed by checking in, and then performing fingerprint and PIN registration to finish the check-in registration. Hotel guests who complete registration can use their access to their designated room while receiving security alerts about their hotel stay. Hotel staff or administrators maintain access to supplementary features that let them view room entry and exit records for security purposes. Remote management allows users to activate or deactivate room locks when necessary security issues arise or when guests request it. The design shows how fingerprint authentication joins with PIN entry to provide enhanced safety measures that enable remote monitoring and access management for hotel guests and staff members.

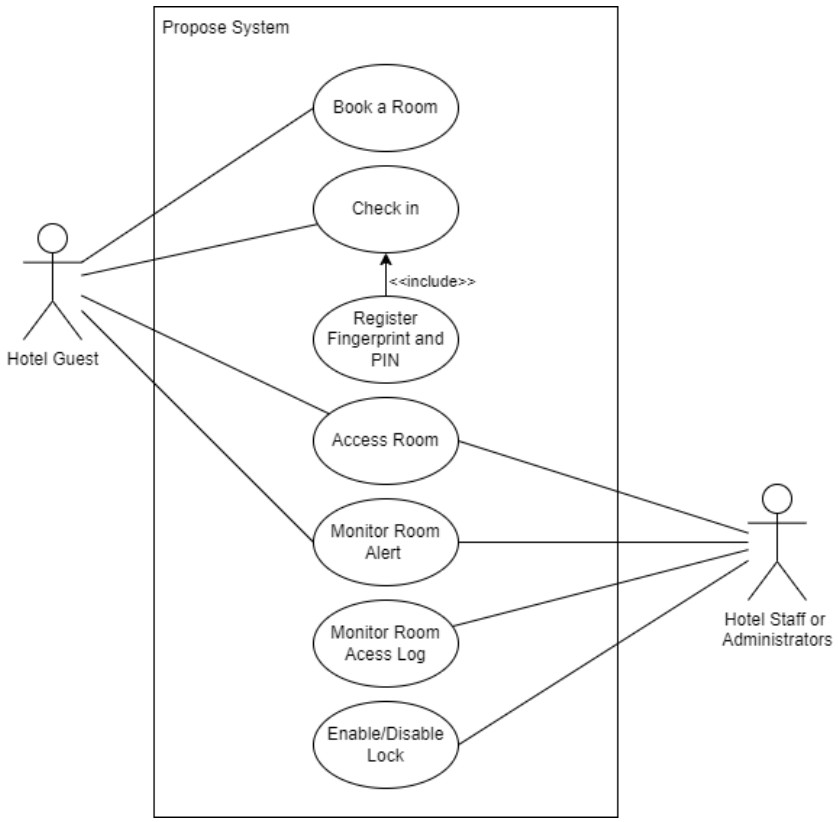


*Figure 3.17:* Propose System Use Case Diagram

### 3.5 Summary

This chapter examines the requirements necessary for the proposed system to achieve the objectives outlined in Chapter 1. It provides a detailed system design and outlines the application's interface. Furthermore, the chapter highlights the methodology adopted for the proposed system, which is based on the Agile approach. This methodology is particularly advantageous due to its focus on efficient time management, cost-effectiveness, and iterative development. Additionally, the system design and application interfaces are presented and elaborated upon with the aid of illustrative figures.

# CHAPTER 4: IMPLEMENTATION AND DEVELOPMENT

## 4.1 Introduction

This chapter outlines the prototype's implementation, which follows the design proposed in Chapter 3. The structure and specifics of the prototype are demonstrated through diagrams and detailed descriptions. The implementation is categorized into hardware and software components. Additionally, this chapter covers functional testing to evaluate whether the prototype meets the project's objectives. Below is a list of the hardware components utilized in developing this project.

a) Arduino Nano 33 IoT with headers
b) Fingerprint Sensor
c) Passive Buzzer
d) Led
e) Keypad
f) I2C Graphic OLED Display 128x64

## 4.2 System Implementation

The implementation of the system requires the installation of the Arduino Integrated Development Environment (IDE) software on the host computer, as the Arduino microcontroller platform serves as the foundational hardware component for this project. There are several steps that must be completed in order for the Arduino to function correctly. For data management and remote access, the system integrates Firebase Realtime Database, which facilitates seamless communication between the hardware components and the Flutter-based mobile application interface. This cloud-based solution enables real-time data synchronization and remote monitoring capabilities. As previously stated in Chapter 3, the following hardware will be explained in more detail.

### 4.2.1 Arduino Nano 33 IoT with headers

The Arduino Nano 33 IoT is a compact microcontroller board equipped with built-in Wi-Fi capabilities, enabling internet connectivity. This feature allows the board to transmit and receive data through Firebase, making it suitable for IoT applications. Designed in the Arduino Nano form factor, it serves as an accessible platform for developing basic IoT and pico-network solutions. To begin working with this microcontroller, users must first install the Arduino IDE software on their computer. This development environment is required to upload and manage

the necessary code (referred to as "sketch" in Arduino terminology) onto the board. The pinout configuration of the Arduino Nano 33 IoT is illustrated in the accompanying figures, which provide a visual reference for its hardware interfaces and connections.

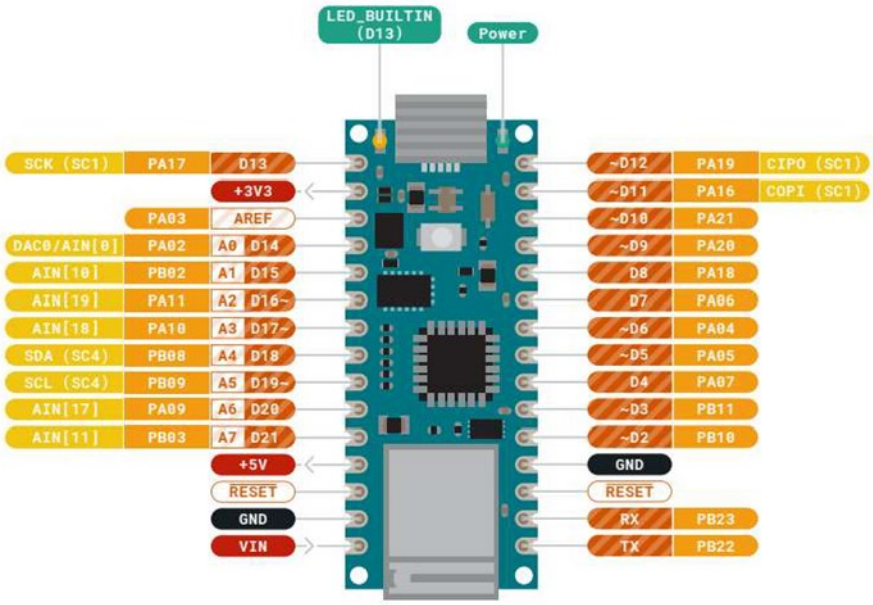


*Figure 4.1*: Pinout for Arduino Nano 33 loT microcontroller (Arduino Nano 33 IoT, n.d.)

### 4.2.2 Fingerprint Sensor

The fingerprint sensor implementation begins with coding the necessary functions through the Arduino IDE before uploading them to the Arduino Nano 33 IoT microcontroller. The sensor operates by first detecting and capturing a fingerprint image when a finger is placed on its scanning surface. Using the Adafruit fingerprint library, the system then processes this image to identify unique biometric patterns such as minutiae points, including ridge endings, where fingerprint ridges terminate and bifurcations, where ridges split. For enhanced security, these extracted patterns are converted into a mathematical template rather than storing the actual image data. This digital template format provides significant security advantages as it cannot be reverse-engineered to reconstruct the original fingerprint. The final processed template is then stored in the sensor's onboard memory for future authentication purposes.


*Figure 4.2:* Fingerprint Image with different identifying points.(Rashid & Zaki, 2014)

### 4.2.3 Passive Buzzer

The passive buzzer was selected for this project due to its ability to generate different tones through programmed frequency control, making it ideal for creating distinct audio alerts. Unlike active buzzers that produce a fixed tone, the passive buzzer allows the system to emit varied sounds to indicate different system states, such as a short beep for successful authentication, a continuous alarm for security breaches and a short tone when the device is active. The implementation of the buzzer requires connecting the buzzer to a digital PWM pin on the Arduino Nano 33 IoT, as this enables precise frequency control through software. For programming, the Arduino's tone() function generates specific frequencies, while noTone() stops the sound. For example, three failed authentication attempts trigger tone(buzzerPin, 1000, 200), producing a 1 kHz alarm for two milliseconds. This implementation provides clear, immediate feedback while maintaining system security through distinct audible warnings.

### 4.2.4 Keypad

The 3×4 matrix keypad serves as a secondary authentication method in the system, working alongside the primary fingerprint sensor to enhance security and flexibility. This dual-layer approach addresses several critical needs, such as providing reliable PIN-based access when biometric authentication fails. The implementation of the keypad involves connecting the keypad's four rows and three columns to digital pins D2-D8 on the Arduino Nano 33 IoT. The Keypad.h library handles button press scanning and decoding, mapping the physical keys to a logical matrix. When a user enters their PIN, the system compares it with the PIN stored in Firebase, and if the PIN matches, the room will be unlocked.

### 4.2.5 I2C Graphic OLED Display 128x64

The I2C 128×64 graphic OLED display was implemented in this project to provide clear visual feedback to the user. The OLED connects to the Arduino Nano 33 IoT via the I2C pins, which are A4 for SDA and A5 for SCL. Using the Adafruit_SSD1306 library, the system displays crucial information, including authentication prompts, success/failure notifications, and system status messages. Unlike traditional LCDs, this OLED module offers sharper text and graphics without backlight bleeding, and its low current draw, typically under 20 mA, helps maintain power efficiency for the system. These characteristics of the OLED display make it an optimal choice for this access control system, providing reliable visual communication to the user.

### 4.2.6 Firebase

Firebase is a cloud-based database service provided by Google that allows real-time data storage and synchronization. In this project, Firebase is used to store and manage all system information, including user details, room access permissions, booking schedules, and authentication logs. The main reason for choosing Firebase is its ability to instantly sync data between the Arduino hardware and the mobile app, ensuring both sides always have up-to-date information. The implementation begins by creating a Firebase project through the Google Firebase console and configuring a real-time database. The Arduino Nano 33 IoT establishes a connection to Firebase via Wi-Fi, transmitting access attempt records and receiving updated user permissions.

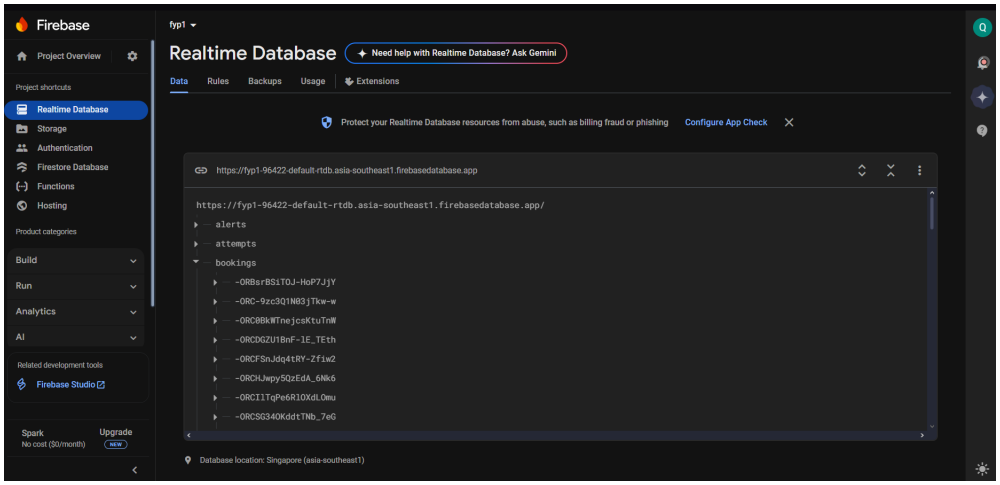


*Figure 4.3:* Proposed System Database

### 4.3 Prototype Development

This project involves three development stages, which are setting up the prototype circuitry, configuring the Firebase database, and developing the Flutter mobile application. The key components implemented in this project include the Arduino Nano 33 IoT, the fingerprint sensor, keypad, passive buzzer, and OLED display.

### 4.4 The Management of Mobile Applications

The objectives of this system are to make a systematic way or design for both admins and guests to do their tasks, and this section will explain the systematic ways in detail. Besides that, each part of the admin and guest module will also be explained in this section. It is to give a clear view of how and what the exact functions are involved in the system, and who is involved with it.

#### 4.4.1 Guest systematic way or design

The interfaces and the flows of this system for the guest section are different from the admin section. In order to the guest book their room, there will be some steps that the user needs to take after the guest logs in to this system.

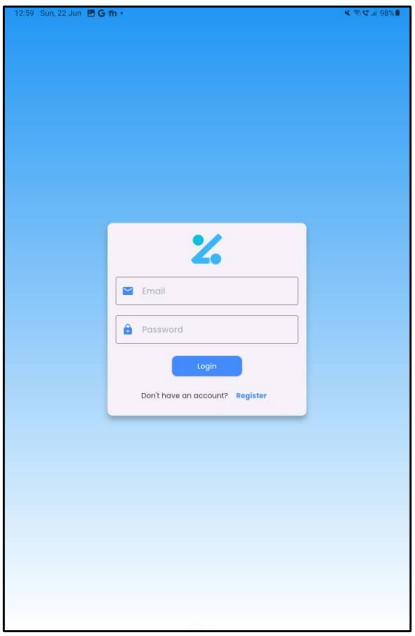


*Figure 4.4*: User Log in Page

When the user opens the app, they will be greeted by the login page of the mobile application. If the user is a new user, they can tap the register now button to go to the registration page and fill in the registration form so they can access the application. On the other hand, if the user is an existing user, the user just needs to enter their existing account email and password on the login page to get access to the application instantly.

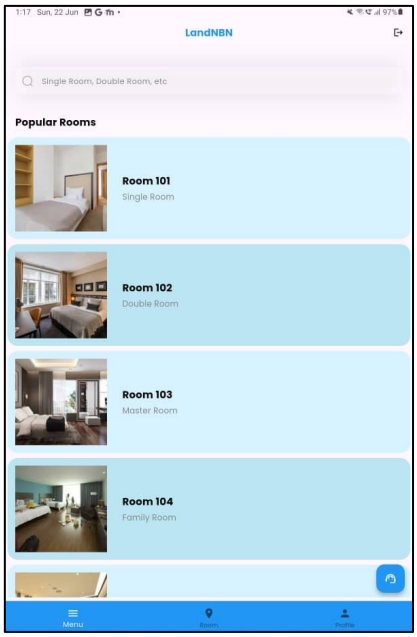


*Figure 4.5:* User Homepage

After the user enters a correct account credential on the login page, they will be redirected to the user homepage. On this page, the user will be presented with all the room options that can be booked. Besides that, the bottom bar will show all the menu options for the user and on the top right corner is the logout button that the user can tap if they want to log out of the app.

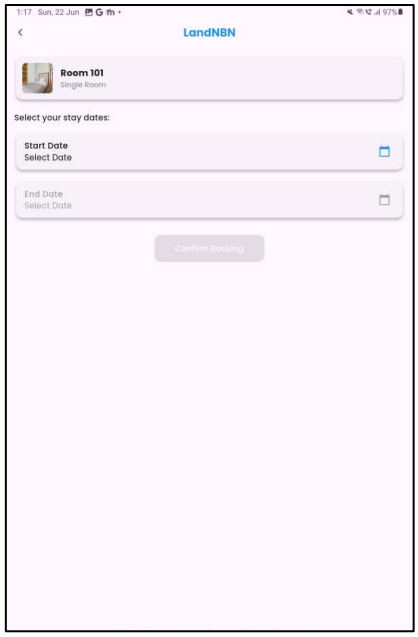


*Figure 4.6*: Room Booking Page

When the user taps the room that they want to book on the homepage, the user will be navigated to the room booking page, where the user can select the duration of their booking. On the room booking page, the user will see the details and a picture of the room they want to book, allowing them to verify if they have selected the correct room.

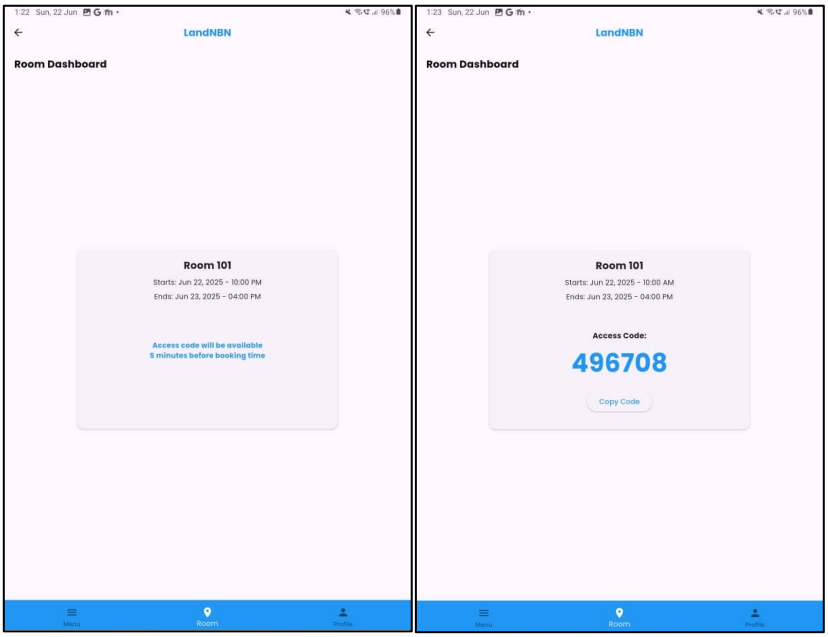


*Figure 4.7:* Room Dashboard Page

After the user has booked a room, they will be redirected to the room dashboard page where they can see the booking details of their ongoing booking. If the current time is more than 5 minutes before the user booking start time there will be no PIN display, but just a text

that tells the user that the PIN will be displayed if the current time is less than 5 minutes before the booking start time. In contrast, if the current time is less than 5 minutes before the booking start time rather than just a text, the PIN for the room will be displayed to the user and the user can insert it into the room door lock to access the room.

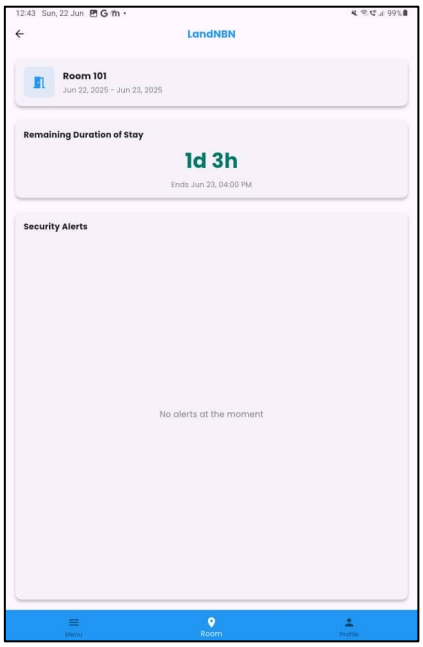


*Figure 4.8:* Room Dashboard after User Check In

Finally, when the user successfully enters a correct PIN that was provided in the application to access the room door, they will be navigated to the room dashboard page. On this page, the user will be shown the details of the booking, such as the countdown of the remaining duration of their stay and the details of the room that they had booked. Moreover, the user can also see any security alert that happens, such as a 3 times incorrect PIN attempt on the room lock.

### 4.4.2 Admin systematic way or design

The interfaces and the flows of this system for the admin section are different from the guest section. In order for the admin to check the room status, there will be some steps that the admin needs to take after the guest logs in to this system.

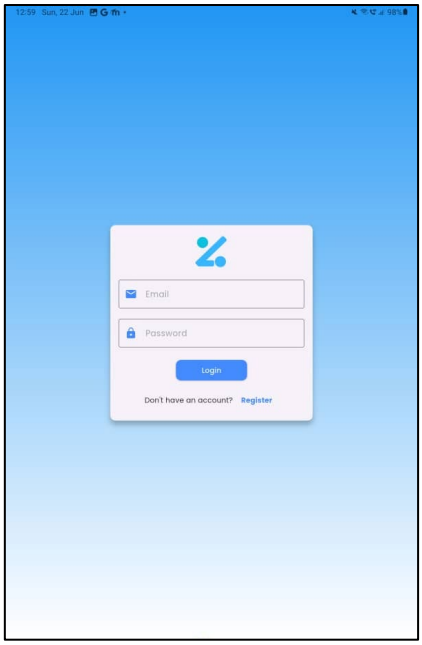


*Figure 4.9:* Login Page

When the admin opens the application, they will be greeted by the same login page as a guest in the mobile application. Unlike the guest, the admin cannot just register an account using the register page. The admin account can only be created by the system administrator using the database management system of the application.

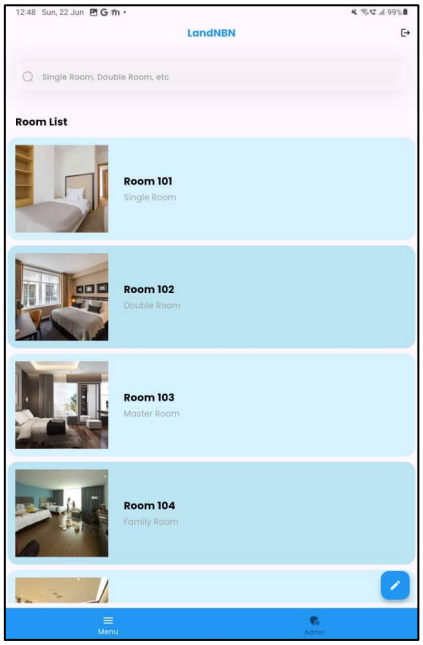


*Figure 4.10:* Admin Homepage

After the admin enters a correct account credential on the login page, they will be redirected to the admin homepage. On this page, the admin will be presented with all the room options that can be checked for their status. Besides that, the bottom bar will show all the menu options for the admin and on the top right corner is the logout button that the admin can tap if they want to log out of the app

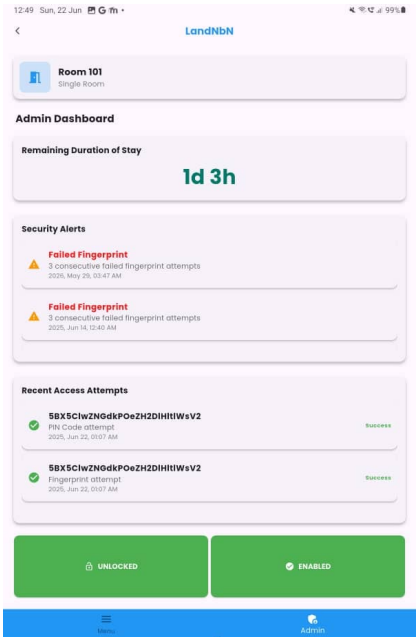


*Figure 4.11:* Admin Room Dashboard

Finally, when the admin has selected the room that they want to view the room status on the homepage, they will be navigated to the room dashboard page. On this page, the admin can view the details of the booking, including the countdown of the remaining duration of the guest's stay and the room details. Moreover, the admin can also view any security alerts that occur, such as multiple incorrect PIN attempts on the room lock and recent access attempts, whether they are successful or unsuccessful. Additionally, there are also an unlock/lock button and an enable/disable button for the admin to use. The unlock/lock button, as the name suggests, is used to lock or unlock the room in case of an emergency, such as when a guest in the room has passed out. On the other hand, the disable/enable feature is used to disable the lock, for example, when cleaners want to enter the room to tidy it.

### 4.4.3 Admin and Guest Module

In the module, all the processes of functions require an action from both the guest and the admin. The process that the users need to take to access the system is logging in to the system. After that, the users can view the Homepage while accessing the system.

#### 4.4.3.1 Login

The purpose for the login function is to authenticate which users is authorized to use the system. As the rule of the authentication, users need to enter their email and password that they already registered. If the users cannot access the system because of the authorization problem, they need to register their information first and then the database for the new user will be created automatically.

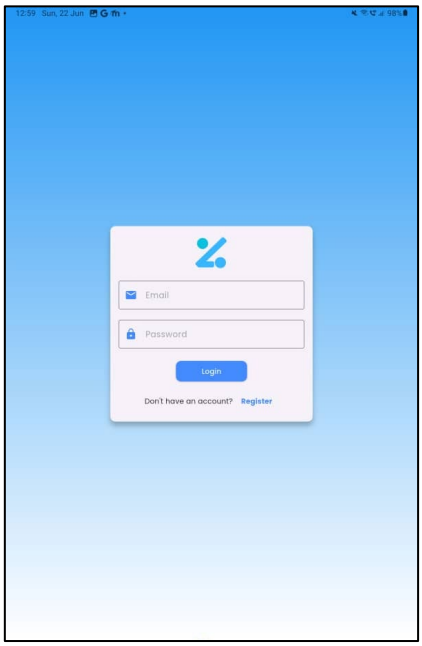


*Figure 4.12:* Login Page for Admin and Guest

The email address for this system is unique, only one email address is allowed to be registered in this system. After the user confirms their login credentials, the system checks the database for the user's role, whether admin or guest and then navigates the user to the corresponding homepage based on their role. This function is included in the admin modules and guest modules.

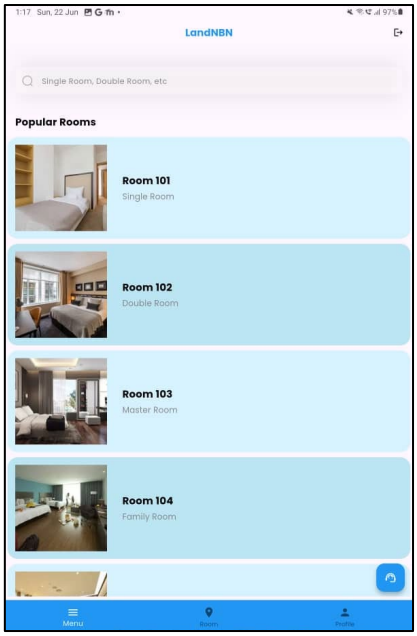


*Figure 4.13:* Homepage if the User is a Guest

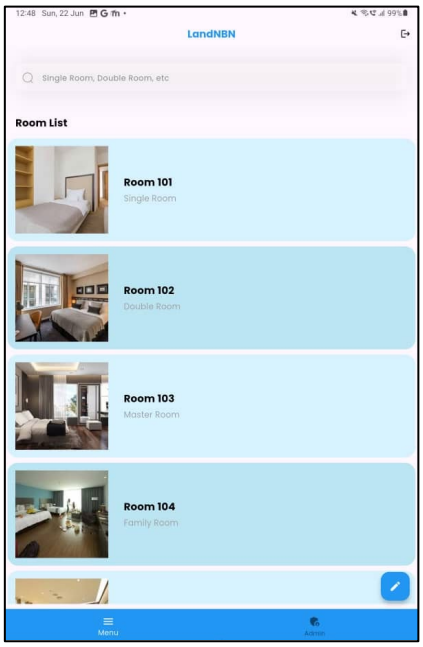


*Figure 4.14:* Homepage if the User is a Admin

The primary difference between the guest and admin homepages is their bottom bar, the floating button, and the functionality of the room list when the user selects it.

### 4.4.4 Admin Module

This module shows the functions that only belong to the admin. Only the admin can have these functions, and it only shows in the admin interface. The function is available when the admin taps the floating button on the admin homepage, as referred to in Figure 40.0.

#### 4.4.4.1 Create New Room

The function is developed for the admin to create a new room to display to the guest without having to add it in the database management system manually. When the admin wants to create a new room, they have to enter the details of the new room in the form shown on the create new room page and upload the photo of the room to the system before the room appears in the room list for the guest to book.

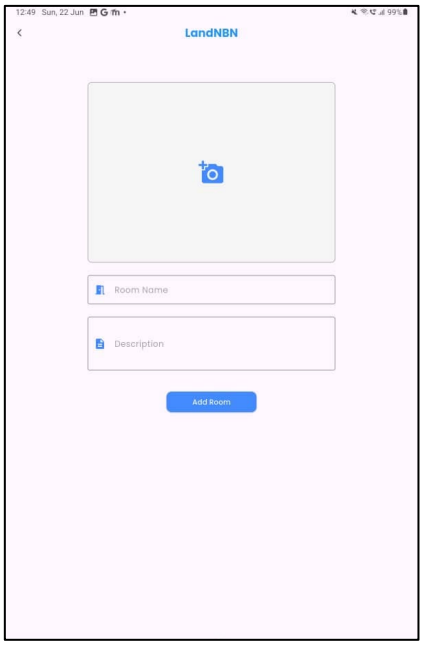


*Figure 4.15:* Create New Room Page

### 4.4.5 Guest Module

This module shows the functions that only belong to guests. Only guests can have these functions and it only shows in the guest interface. The functions are to make a booking for the room, view the ongoing booking details and view the user profile.

#### 4.4.5.1 Make a Booking

This function is designed to enable users to book a room at the hotel without needing to visit the hotel, and at any time they wish to make a booking. To navigate to the room booking page, the user had to select any room that they wanted to book on the guest homepage, as referred to in Figure 39.0. On this page, the user can enter the duration of the time that they want to stay at the hotel and after all the information has been filled in, the user must tap the “Confirm Booking” button to confirm their booking so the application can send it to the database.

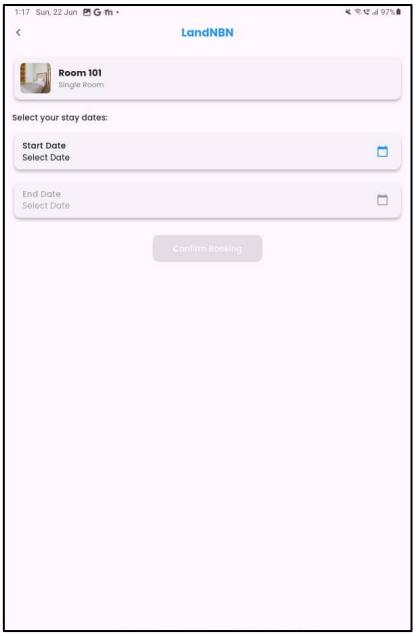


*Figure 4.16:* Guest Room Booking Page

#### 4.4.5.2 View Ongoing Booking

This function is developed to allow the user to view their ongoing booking after they have successfully booked a room using the room booking page, as shown in Figure 42.0. The user can navigate to view ongoing bookings by selecting the room icon on the bottom bar of the application or wait for the application to redirect the user after the user confirms their booking automatically. With this function, the user can view their booking details such as the booked room number, the booking start and end date and the room PIN if the current time is less than five minutes before the start booking time.

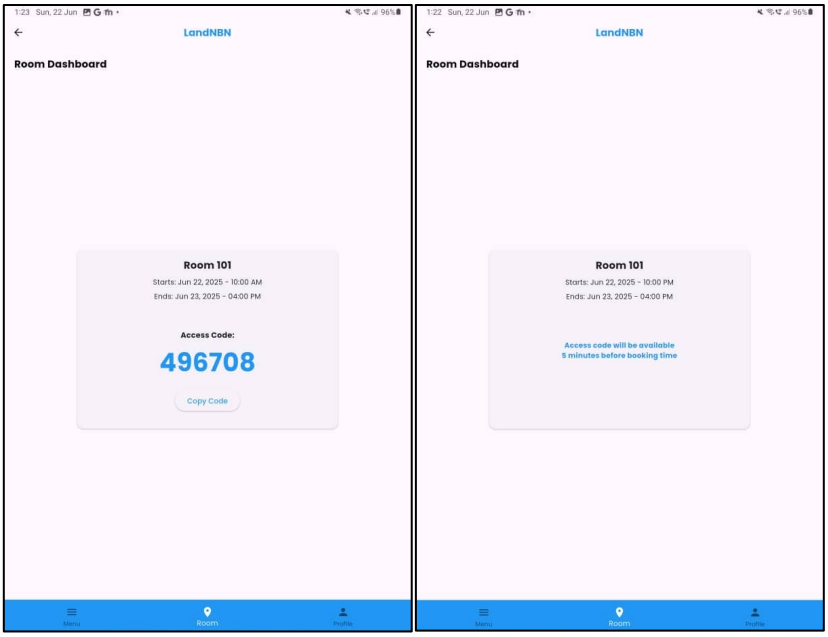


*Figure 4.17:* Guest Room Dashboard Before Check In

### 4.4.5.3 View User Profile

This function is developed to allow the user to view their personal profile information within the application, as shown in Figure 44.0. The user can access the profile page by selecting the profile icon located on the bottom navigation bar. Upon navigating to this page, the user will be able to view their full name, registered email address, and phone number, which are retrieved from their account details. This function serves to ensure that users can conveniently review and confirm their personal information as stored in the system. Additionally, users may update their details by selecting the edit icon located at the top-right corner of the page.

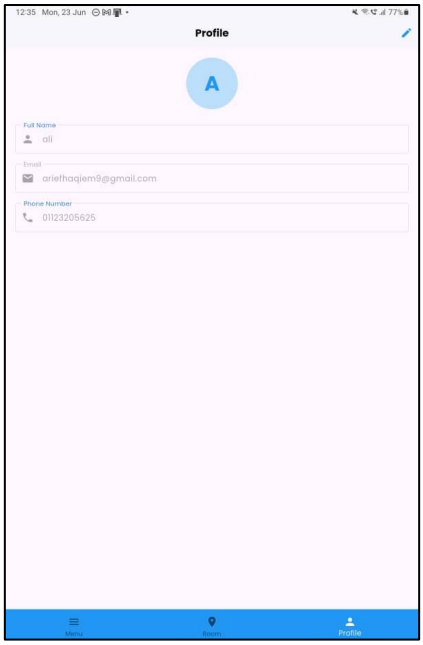


*Figure 4.18:* Guest User Profile

This function is developed to allow the user to view their personal profile information within the application, as shown in Figure 43.0. The user can access the profile page by selecting the profile icon located on the bottom navigation bar. Upon navigating to this page, the user will be able to view their full name, registered email address, and phone number, which are retrieved from their account details. This function serves to ensure that users can conveniently review and confirm their personal information as stored in the system. Additionally, users may update their details by selecting the edit icon located at the top-right corner of the page.

### 4.5 Door Lock System User Interface

The OLED screen that has been used in the project will display a user interface to the user. This user interface will assist and guide the user on how to use the door lock correctly, so the user is able to complete the check-in process without any issues. The reason why the user interface is crucial in the system is that it allows the system to inform the user of the necessary actions to use the system without requiring any human intervention.

#### 4.5.1 Waiting Mode Interface

When there is no booking for the room, the lock will be in the waiting mode, where it will continuously check for a booking that starts at the current time from the Firebase. The lock will compare all the pending bookings that are placed for the door lock room number, for

example, 101 and compare the start time of the booking with the current time, which is fetched by the system from the NTP server.


*Figure 4.19:* Waiting Mode Interface

Besides checking the booking, the system also checks if the admin has disabled the lock remotely from the app by checking the 'isDisabled' Boolean variable in the database. If it is true, the lock will display a disabled dialog on the screen, indicating that the lock has been disabled. As a result, anyone can enter the room without authentication, allowing workers such as cleaning staff to do their work efficiently. Although the admin can easily disable the door lock, posing a security issue to the guest to ensure the guest's safety the system will notify the guest with a security alert in the security alert section on the user dashboard in the mobile app as shown in Figure 4.8, each time the admin disables the room.


*Figure 4.20:* Room Disable Dialog

### 4.5.2 Initialization Mode Interface

Suppose the system finds the booking that starts at the current time in the database. In that case, the system will begin the initialization stage, where the system fetches the required booking information such as the user id of the guest, the booking id of the booking, and the access code that had been generated by the mobile application as shown in Figure 4.17, to authenticate the user. Hence, there is no one besides the legitimate guest who has booked the room who can check in to the room.


*Figure 4.21:* User Welcome Interface

` When the user starts to insert the access code, the OLED screen will display the typing mode where it shows each character that the user has input to the system using the keypad as a star '*' on the screen with the audio feedback produced by the buzzer. Besides the user input, the display also shows the option for the user to select whether to confirm the access code by pressing the '*' key or to retype and correct the mistake by pressing the '#' key using the keypad. If the user presses the confirm key and the access code they have inserted matches the access code generated by the mobile application, the display will show a success dialog. Otherwise, it will show a fail dialog.


*Figure 4.22:* Typing Mode Interface

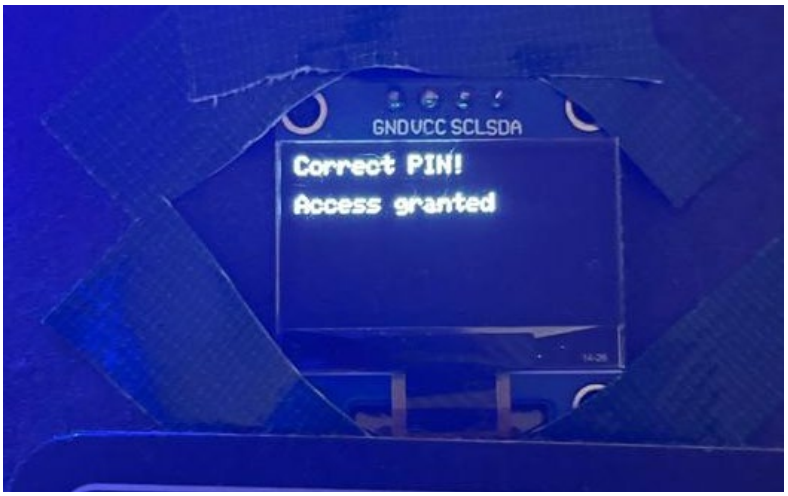


*Figure 4.23:* Success Dialog Interface


*Figure 4.24:* Failure Dialog Interface

On the other hand, if the user presses the retype key, the system will clear all the characters the user has entered and ask the user to re-enter the access code. With this, users can correct any accidental mistakes made while inserting the access code.

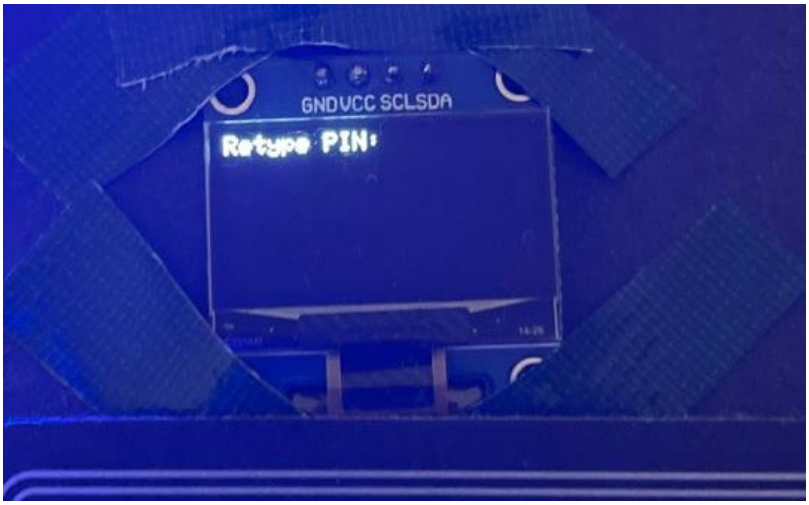


*Figure 4.25:* Retype Interface

### 4.5.3 Check In Mode Interface

After the user enters the correct access code, the system will change to the check-in mode. Since the door lock has a dual access method, which uses PIN or fingerprint, in this mode the user will be required to set up their own PIN and register the fingerprint that they want to be able to access the room. The PIN that has been registered will be stored in the database, while the fingerprint encoding will be stored locally. Each PIN set up and fingerprint registration requires the user to confirm the input by re-entering the PIN for the second time or placing the same finger again. It acts as a safeguard mechanism to prevent mistakes made during the process, such as the user being unable to enter the room later due to an error made during PIN setup or fingerprint registration.


*Figure 4.26:* First PIN Setup Interface

Similar to when the user inserts the access code, the display will show two options and display the user input character as a '*'. While the '#' will display the same user interface as Figure 4.21, the confirm button '*' will now function differently when the user presses it. When the first PIN setup screen is displayed, the system saves it in a variable and then proceeds to the confirmation stage. Once the user is in the confirmation stage, the confirmation key compares the confirmed PIN entered by the user with the previously stored PIN. If they match, the system uploads the new PIN to the database and the system will display a success dialog.


*Figure 4.27:* PIN Confirmation Interface


*Figure 4.28:* PIN Success Dialog

After the user completes the PIN setup process, the system will ask the user to register their fingerprint to the system via the fingerprint sensor. In this process, the user just had to place their finger to the sensor and remove the finger when the system tells the user. The system will automatically encode the guest's fingerprint into the fingerprint template simply by placing their finger on the sensor, without requiring the user to press any key.


*Figure 4.29:* Fingerprint Registration Interface


*Figure 4.30:* The System Prompt the User to Remove Their Finger

Similar to the PIN setup, the user must confirm their fingerprint after placing and removing their finger from the sensor. With this, the system ensures the consistency of the fingerprint template encoding, allowing the user to access the room with the fingerprint without any issues later. After the system confirms fingerprint template consistency, it will store the fingerprint template locally, display a success dialog, and then prompt the user to either continue or register another fingerprint with the system. If the user wants to add another fingerprint, they must repeat the fingerprint registration process, starting with the interface shown in Figure 4.28. Otherwise, the door lock will now be in access mode, allowing users to open the door using any access method they prefer.


*Figure 4.31:* The System Prompt the User to Place The Same Finger

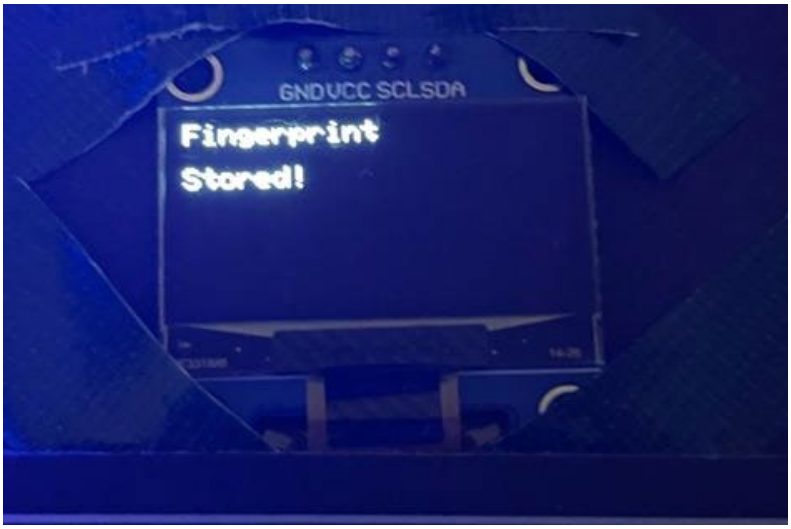


*Figure 4.32:* The Fingerprint Registration Success Dialog

The user can just press any key beside the '*' to register another fingerprint that is able to access the room, or press the '*' key to proceed to the access mode to exit the check-in process and use the lock like other normal smart lock.

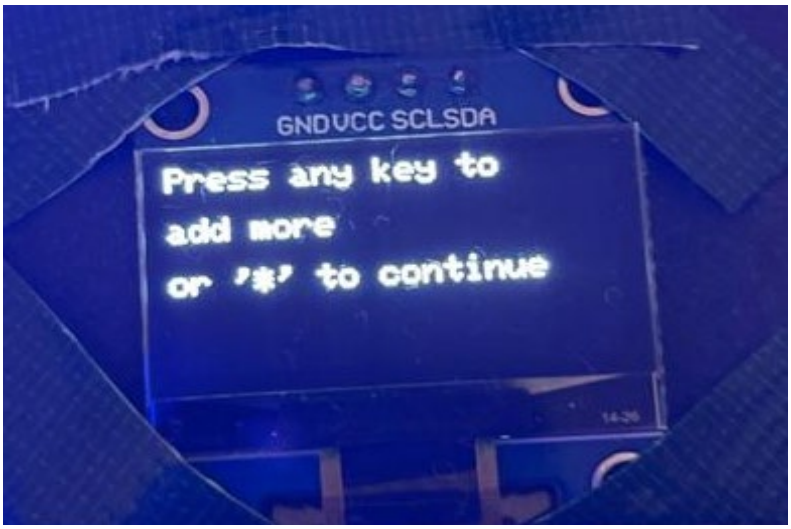


*Figure 4.33:* The System Prompt the User to Choose to Add More Fingerprints or Proceed

### 4.5.4 Access Mode Interface

In this mode, the lock behaves like a standard lock, allowing the user to access the room using the PIN or fingerprint registered during the check-in mode. To use the fingerprint access method, the user just needs to place their finger on the fingerprint sensor, and then the system will encode the fingerprint and compare it with the stored fingerprint template. If the fingerprint matches, the system will display the success dialog and unlock the room but show the failure dialog otherwise.


*Figure 4.34:* Access Mode Intro Interface

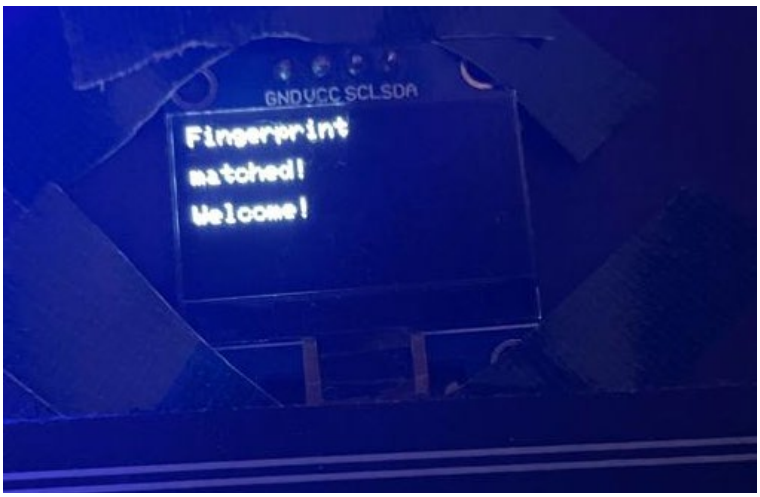


*Figure 4.35:* Fingerprint Access Success Dialog


*Figure 4.36:* Fingerprint Access Failure Dialog

Different from fingerprint access which only requires the user to place their finger to access the room, when the user wants to use PIN they are required ot to press the PIN that has been set up and press '*' using the keypad to confirm the PIN. Then the system will validate the PIN that has been inserted with the store PIN. If it matches, the system will display a success dialog and a failure dialog when it does not match. Similar to other type mode in the system, the user had the option to enter by pressing the '*' key and retype the '#' key on the keypad.


*Figure 4.37:* PIN Entry Mode


*Figure 4.38:* PIN Access Success Dialog


*Figure 4.39:* PIN Access Failure Dialog

During access mode, the system tracks the number of failed entries to the room. If the number exceeds three, regardless of whether the attempt is via PIN or fingerprint, the system displays the ‘too many attempts’ dialog and transitions to the cooldown state. During this state, the user will not be able to make any access attempts until the cooldown time has ended, which will be indicated by the system with the ‘cooldown ended’ dialog. The cooldown time will be twice the original cooldown time if the user fails to access the room three times consecutively.


*Figure 4.40:* Too Many Attempt Dialog


*Figure 4.41:* Cooldown Interface


*Figure 4.42:* Cooldown Ended Dialog

Besides waiting for the user's attempt to access the room, the system will also check if the admin has locked or disabled the room lock through the admin dashboard in the mobile application. If the boolean variable ‘isLocked’ in the database is true, then the system will lock the room and display the room lock interface. During the time the room was locked, no guest was allowed to access the room until the admin had unlocked it. On the other hand, if the admin had disabled the lock, it would allow anyone to enter the room without authentication and display the interface as shown in Figure 4.20.

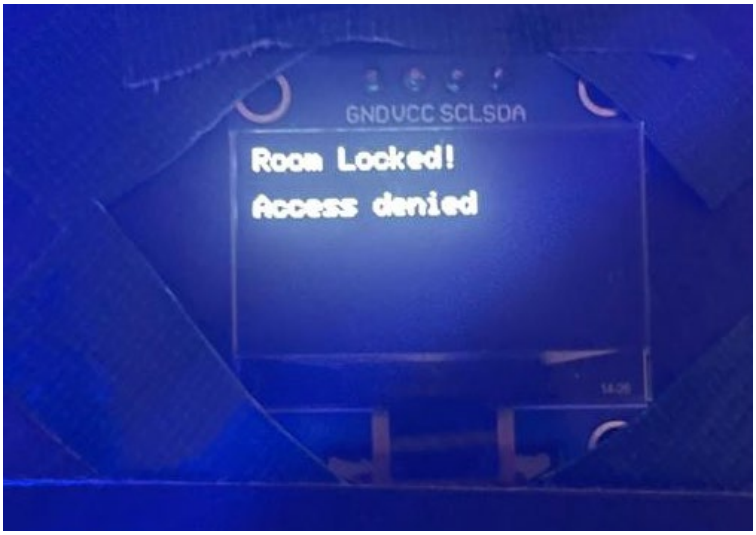


*Figure 4.43:* Room Lock Interface

## 4.6 Conclusion

As the conclusion, the implementation process is being done in this chapter. During the work in this phase, there are a few changes in the design and features that have been made and not followed the plan that was stated before this. Although there are some changes in this system, it is still fulfilling the objective of the system. As a prove and to explain how this system works, some screenshots of the important function interface are being provided in this chapter. The discussion about the system testing will be continued in the next chapter, which is Chapter 5, and it is based on the testing phase that was stated in the previous chapter.

# CHAPTER 5: TESTING

## 5.1 Introduction

In this chapter, the system testing will be explained on how the system works with a real user. This is a very important phase in developing the system because the developer can detect and trace whether the system is working correctly or not. The system must be tested by the developer first before handing it to the real user. It is to check the functionality of the system and to avoid any problems that might happen when users use the system. This system has two objectives that were set when the system was proposed and were stated in the previous chapter. All the objectives are achieved successfully and will discuss more in this chapter. The system uses functionality, usability, and prototype testing as guidelines to assess how well the system works.

## 5.2 Prototype Testing

The testing phase is essential to ensure the prototype meets the objectives outlined in Chapter 1 and to guarantee the system's quality. This project includes two types of testing which are component testing and complete circuit testing

### 5.2.1 Component Testing

These are the test on the circuit components of the prototype which include Arduino, all the sensors and mobile application.

First, to ensure all circuit components run smoothly, the Arduino IDE operating system must be functioning properly. The Arduino IDE needs to be running when the microcontroller is connected to the PC or laptop without any issues. Additionally, it is necessary to ensure that no errors occur during the upload of all program codes into the microcontroller.

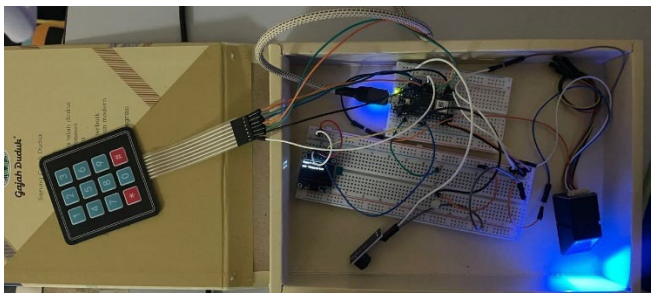

*Figure 5.1:* Testing of the Prototype

#### 5.2.1.1 Arduino

The Arduino IDE is essential for Arduino devices to function properly, as it enables uploading and verifying code using this software. To test the functionalities of this software, the board is connected to the laptop without any errors. From Figure 47.0, the Arduino Nano 33 IoT will turn on the green light to indicate a successful power-on. Besides that, based on Figure 48.0, after verifying and uploading the sketch on the board, the orange light will turn off, indicating the successful sketch upload.

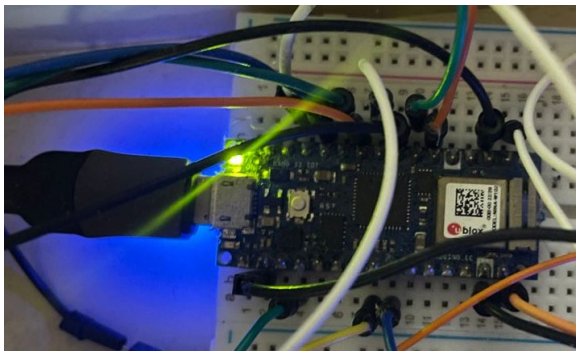

*Figure 5.2:* The Green Light Onboard

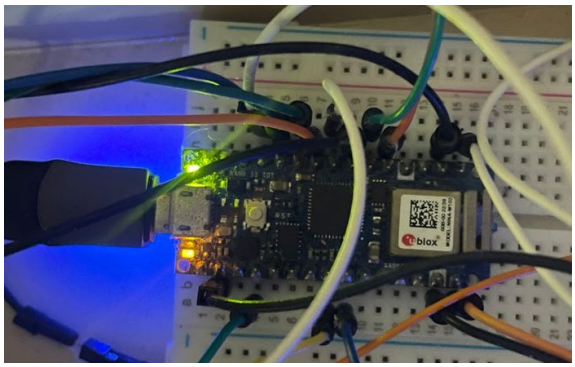

*Figure 5.3:* The Green and Orange Light Onboard

#### 5.2.1.2 Fingerprint Sensor

In this proposed system, the fingerprint serves as the primary verification method for users to access the room, so it is essential to ensure the fingerprint sensor functions correctly as intended. Some tests that can be used to test the fingerprint sensor include writing some validation code that can be viewed in the serial monitor to check if the sensor is detected and working well with the microcontroller, as shown in Figure 48.0. After that, make sure the sensor lights up after powering up the microcontroller to ensure that the sensor is powered on, as shown in Figure 49.0.

```
Found fingerprint sensor!
Connecting to WiFi
Connected to WiFi!
```

*Figure 5.4:* Snapshot of the Serial Monitor

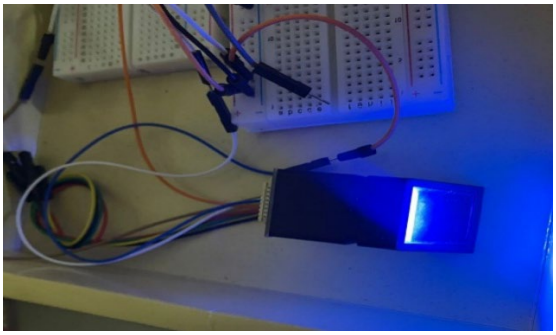

*Figure 5.5:* Light up Fingerprint

#### 5.2.1.3 Keypad

The keypad acts as a secondary way to access the room, to act as a backup if the fingerprint sensor is not working or breaks. To test the keypad, there is code to display the input as '*' that has been programmed into the microcontroller. Therefore, if the keypad is working well, there will be '*' displayed on the OLED screen

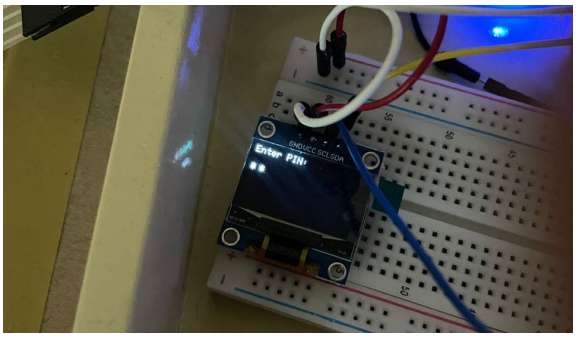


*Figure 5.6:* OLED Display the Keypad Input

#### 5.2.1.4 OLED Display

Finally to test the OLED display that will act as a mediator between the program and the user, it is essential to make sure that the display lights up after the microcontroller is powered up and will display the intended text or graphic to the user as shown in Figure 51.0.


*Figure 5.7:* OLED Display Light Up and Display Text to The User

### 5.2.1 Circuit Testing

For overall prototype testing, all devices, sensors, and the module need to be retested to ensure that the entire component's functionality is functioning properly. A set of test cases will be conducted to ensure the user is satisfied with the prototype.

*Table 5.1:* Test Case for Arduino

| **Test Case Name** | **Arduino** | | |
|---|---|---|---|
| **Test Case Description** | i. To evaluate the Arduino IDE system working completely.<br>ii. To ensure the Arduino Nano 33 IoT fully working. | | |
| **Pre-Condition** | i. Arduino needs to be connected to the power source.<br>ii. To evaluate the Arduino IDE system working completely.<br>iii. To ensure the Arduino Nano 33 IoT fully working. | | |
| **Step** | **Test Description** | **Expected Result** | **Result** |
| 1. | Connect the Arduino Nano 33 IoT to a power source (Laptop or battery) | The Arduino Nano 33 IoT will reboot and the LED on the board will turn on. | Pass |
| 2. | Access into the Arduino IDE to setting the Arduino board based on | The Arduino IDE will show the board settings. | Pass |

| | | | |
|---|---|---|---|
| | its specification. | | |
| 3. | Connect the Arduino board to laptop using USB cable. | The Arduino IDE will list the Arduino Nano 33 IoT under the any available ports. | Pass |

*Table 5.2:* Test Case for Fingerprint Sensor

| **Test Case Name** | **Fingerprint Sensor** | | |
|---|---|---|---|
| **Test Case Description** | i. To evaluate the Fingerprint sensor working completely.<br>ii. To make sure the sensor initializes correctly and communicates with Arduino Nano 33 IoT | | |
| **Pre-Condition** | i. The Arduino Nano 33 IoT must be powered on using a power source from the laptop or battery. | | |
| **Step** | **Test Description** | **Expected Result** | **Result** |
| 1. | Connect the Fingerprint Sensor to the Arduino IoT 33 | The Fingerprint sensor will light up | Pass |
| 2. | Initialize the Fingerprint Sensor | The Fingerprint sensor will initialize without any issue | Pass |
| 3. | Put the Finger on the sensor | The sensor is able to capture the fingerprint to validate or store it | Pass |

*Table 5.3:* Test Case for Keypad

| **Test Case Name** | **Keypad** | | |
|---|---|---|---|
| **Test Case Description** | i. To evaluate the keypad working completely.<br>ii. To make sure the keypad initializes correctly and communicates with Arduino Nano 33 IoT | | |
| **Pre-Condition** | i. The Arduino Nano 33 IoT must be powered on using a power source from the laptop or battery. | | |
| **Step** | **Test Description** | **Expected Result** | **Result** |
| 1. | Connect the keypad to the Arduino IoT 33 | The keypad receive power without any visible damage or overheating. | Pass |
| 2. | Press the any keypad button | The '*' will be display on the display | Pass |

*Table 5.4:* Test Case for OLED Display

| **Test Case Name** | **OLED Display** | | |
|---|---|---|---|
| **Test Case Description** | iii. To evaluate the OLED working completely.<br>iv. To make sure the OLED initializes correctly and communicates with Arduino Nano 33 IoT | | |
| **Pre-Condition** | ii. The Arduino Nano 33 IoT must be powered on using a power source from the laptop or battery.<br>iii. The OLED must be connected to the correct pin on the microcontroller | | |
| **Step** | **Test Description** | **Expected Result** | **Result** |
| 1. | Connect the OLED to the Arduino IoT 33 | The OLED lights up | Pass |

| | | | |
|---|---|---|---|
| 2. | Write a function to display text | The OLED display shows the intended text | Pass |

*Table 5.5:* Test Case for Passive Buzzer

| **Test Case Name** | **Passive Buzzer** | | |
|---|---|---|---|
| **Test Case Description** | v. To evaluate the buzzer working completely.<br>vi. To make sure the buzzer initializes correctly and communicates with Arduino Nano 33 IoT | | |
| **Pre-Condition** | iv. The Arduino Nano 33 IoT must be powered on using a power source from the laptop or battery. | | |
| **Step** | **Test Description** | **Expected Result** | **Result** |
| 1. | Connect the buzzer to the Arduino IoT 33 | The buzzer should receive power without any visible damage or overheating. | Pass |
| 2. | Write a function to make a sound | The buzzer produces the intended sound | Pass |

### 5.3 Functional Testing

Functional testing is a suitable method to confirm whether the system operates as planned. This functionality testing is able to check the functionality of the system and make sure the system is ready to be handed over to the user. This is one of the ways to prevent problems and avoid users' frustration.

#### 5.3.1 Functionality Testing

This testing indicates that all the proposed functions are functioning correctly in the system. It will make sure all the proposed function meets their requirements perfectly according to the

previous chapter. The focus of this testing is primarily on the main functions in the system. The result of this testing is shown in the tables that have been included in **Appendix A**. It is a functionality test result of the proposed system.

### 5.4 Non-Functional Testing

Non-functional testing involves the real user experience in using the system. It is to test how well the system's functions respond to the real user interaction in certain situations.

#### 5.4.3 Usability Testing

After the developer completes functional testing, usability testing is conducted to evaluate the system. This phase involves real users interacting with the system to assess its efficiency, ease of use, and overall user-friendliness. The results of this testing are presented in the tables provided in **Appendix B**.

### 5.5 Conclusion

This chapter provides a detailed discussion of the various tests conducted to evaluate the system's efficiency. The testing process is categorized into three main sections which are prototype testing ,functionality testing and usability testing. According to the results, the system not only meets its objectives but also functioning properly.

# CHAPTER 6: CONCLUSION AND FUTURE WORK

## 6.1 Introduction

This chapter presents an analysis of the project, discusses the limitations of the prototype system, and highlights the key achievements. During the development phase, certain constraints emerged due to resource and technical challenges. Consequently, recommendations for enhancing the prototype system are proposed for future research.

## 6.2 Objective Achievement

The Smart Access Hotel System Using Fingerprint Technology has been successfully developed, fulfilling the objectives outlined in Chapter 1. The table below summarizes the system objectives alongside their corresponding achievements in the prototype implementation.

Table 6.1: Project Objective

| Objective | Achievement |
|---|---|
| To design and develop finger recognition system for hotel. | The system has been designed according to the suitable for the hotel. |
| To evaluate the proposed system using a prototype, usability and functionality testing | The proposed system was successfully evaluated using a prototype, usability and functionality testing |

## 6.3 Limitations

Although the project provides improved security and convenience through biometric and IoT-based access control, it also has some limitations that need to be considered. These issues come from factors such as the limits of the hardware used, environmental conditions that can affect performance, and the system's dependence on a stable network connection.

a) **Network Dependence**

The system's remote management features depend on Wi-Fi connectivity. Any network instability or downtime could disrupt real-time monitoring and control, limiting the system's functionality during such periods

**b) Hardware Constraints**

The project relies on specific hardware components such as the Arduino Nano 33 IoT, fingerprint sensor, and keypad. The performance and accuracy of the system are limited by the capabilities of these components. For instance, the fingerprint sensor may struggle with wet or dirty fingers, leading to authentication failures. Additionally, the Arduino Nano 33 IoT's processing power may restrict the complexity of tasks the system can handle simultaneously.

**c) Environmental Factors**

The effectiveness of fingerprint recognition can be affected by environmental conditions such as humidity, temperature, or dirt on the sensor. These factors may reduce the reliability of the system in certain scenarios, requiring manual intervention or alternative authentication methods like the keypad.

### 6.4 Future Work

The Smart Access Hotel System Using Fingerprint Technology presents several opportunities for enhancement and expansion. Future work can focus on improving system performance, scalability, security, and user experience. Below are key areas for further development

**a) Multi-Modal Biometric Integration**

Incorporate additional biometric methods such as facial recognition or iris scanning to provide alternative authentication options, improving accessibility for users with fingerprint recognition difficulties.

**b) Improved Fault Tolerance & Backup Systems**

Develop an offline mode that allows the system to function during Wi-Fi outages by storing access logs locally and syncing once connectivity is restored.

**c) Hardware & Processing Upgrades**

To enhance system performance, the Arduino Nano 33 IoT can be replaced with a more powerful microcontroller like the ESP32 or Raspberry Pi, enabling faster processing, improved multitasking, and quicker response times.

### 6.5 Summary

This chapter concludes the project by examining the achievements, the challenges encountered, and potential ideas for future enhancements. The fingerprint-based hotel access system was successfully developed and tested, meeting its primary objectives. However, some issues were found, such as the fingerprint scanner not functioning well with wet fingers and the system requiring a constant internet connection to work properly. For future improvement, the system could add other methods to unlock doors, such as face recognition, work without an internet connection, and use powerful hardware. These changes would make the system more reliable and useful for hotels. The project shows considerable potential but still has room for improvement.

## REFERENCES


Hassan, M. Y., Mahdi, A. J., Al-Sharhanee, K. a. M., Ayad, M., Shutnan, W. A., & Najim, A. H. (2023, October 25). *Designing a Prototype Smart Hotel with High Security, Solar Tracking, and IoT Lighting Control*. https://doi.org/10.1109/iceans58413.2023.10630464

Balaji, M., N, P., Swathi, N., Atheek, S., Manasa, M., & Kumar, K. C. (2023, October 11). *Biometric-based Smart Door Locking System using Biometric and OTP*. https://doi.org/10.1109/i-smac58438.2023.10290425

Wang, H., Wang, Z., Sun, G., Zhang, L., Gao, Y., Zhang, Y., & Bi, C. (2021). Design of a biometric access control system based on fingerprint identification technology. In *Lecture notes in electrical engineering* (pp. 34–42). https://doi.org/10.1007/978-981-15-8599-9_5

Alnabhi, H., Al-Naamani, Y., Al-Madhehagi, M., & Alhamzi, M. (2020b). Enhanced security methods of door locking based fingerprint. *International Journal of Innovative Technology and Exploring Engineering*, *9*(3), 1173–1178. https://doi.org/10.35940/ijitee.b7855.019320

Devharsh, T. (2021). Agile Methodologies. International Journal of Computer Science & Communication, 12(2), 91-100.

Waja, G., Shah, J., & Nanavati, P. (2021). Agile software development. International Journal of Engineering Applied Sciences and Technology, 5(12), 73-78.

S, K., S, R., M, K., & A, K. (2024). *Arduino-Powered Fingerprint Authentication for Door Access Control*. https://doi.org/10.1109/icesc60852.2024.10689965

Baidya, J., Saha, T., Moyashir, R., & Palit, R. (2017). Design and implementation of a fingerprint based lock system for shared access. *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 1–6. https://doi.org/10.1109/ccwc.2017.7868448

Esekhaigbe, E., & Okoduwa, E. O. (2022). Design and implementation of a fingerprint-based biometric access control system. Journal of Advances in Science and Engineering, 7(1), 18–23. https://doi.org/10.37121/jase.v7i1.183

Aguayo Publicidad. (n.d.). Agile Methodology in UX | Aguayo's blog. https://aguayo.co/en/blog-aguayp-user-experience/agile-methodology-in-ux/

Arduino. (n.d.). Arduino Official Store. https://store.arduino.cc/products/arduino-nano-33-iot?srsltid=AfmBOoo8JRrhCLIZYrzj-U4jSgA1IfSP0pZuWJwSIipKxuQYIcft3cO5#product-docs

MYBOTIC. (n.d.). AS608 FINGER PRINT MODULE. https://mybotic.com.my/finger-print-module/as608-finger-print-module

I2C 1602 Serial OLED for Arduino & RPI. (n.d.). Cytron Technologies Malaysia. https://my.cytron.io/p-i2c-1602-serial-OLED -for-arduino-and-rpi?r=1

Electronation Pakistan. (2024, March 25). *Keypad 3x4 - Electronation Pakistan*. https://electronation.pk/shop/arduino-iot-boards/keypads/keypad-3x4/

Module Buzzer Passif pour Arduino. (n.d.). Souilah - Composants Électroniques Et Robotique En Tunisie. https://souilah-electronique.tn/modules-et-capteurs/887-module-buzzer-passif-pour-arduino.html

Make Computer Science Great Again. (2024, November 29). Agile Methodology: Flexibility and efficiency in project management. Medium. https://medium.com/@MakeComputerScienceGreatAgain/agile-methodology-flexibility-and-efficiency-in-project-management-eda8bc1c6201

Rashid, M., & Zaki, H. (2014). RSA Cryptographic Key Generation using Fingerprint Minutiae. *Iraqi Journal for Computers and Informatics*, *41*(1), 66–69. https://doi.org/10.25195/ijci.v41i1.101

Yeap, A. (2023, November 17). S'porean says intruder entered JB hotel room at 3am; ongoing hotel probe finds no sign of unauthorised access. *TODAY*. https://www.todayonline.com/singapore/sporean-intruder-jb-hotel-room-3am-probe-no-sign-unauthorised-entry-2307516

# APPENDICES

## APPENDIX A: FUNCTIONAL TEST

**Functionality Testing**

| **Module:** Guest and Admin | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Test Objective:** To test functionality of Guest and Admin module in the application | | | | | | | |
| Test Id | Test Case | Input Data | Expected Result | Actual Result | Pass/Fail | Summary of Defect | Comment |
| F001 | Login into the system | Validate the email and password | The user is able to log in and access the application | The user is able to log in to the system | Pass | None | - |
| F002 | Logout from the system | Tap the logout button on the homepage | The user went back to the login page and require to log in back to access the application | The user went back to the login page and require to log in back to access the application | Pass | None | - |

| **Module:** Guest | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Test Objective:** To test functionality of Guest module in the application | | | | | | | |
| Test Id | Test Case | Input Data | Expected Result | Actual Result | Pass/Fail | Summary of Defect | Comment |
| F003 | Register as new user | Fill in all the required details on the registration page | The guest will be redirected to the login page after tapping the “Register” button | The guest managed to create a new account in the database and was automatically redirected to the login page | Pass | None | - |
| F003 | Book a room | Enter the duration of the stay on the book room page | The guest will be redirected to the room dashboard page after tapping the “Confirm Booking” button | The guest managed to create a new booking in the database and was automatically redirected to the room dashboard page | Pass | None | - |
| F004 | View ongoing booking | Select the room logo on the bottom bar | The Guest was able to see their ongoing booking details and room PIN 5 minutes before the booking time | The details about their ongoing booking form database showed after tapping the room logo on the bottom bar and get the generated PIN 5 minutes before their booking | Pass | None | - |
| F005 | View room dashboard | Select the room logo on the bottom bar | The Guest was able to see their ongoing room dashboard and all the security alerts during their stay | The Guest was able to see their ongoing room dashboard and all the security alerts during their stay that been filterd by their User Id and the booking detail from database | Pass | None | - |

| **Module:** Admin | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Test Objective:** To test functionality of Admin module in the application | | | | | | | |
| Test Id | Test Case | Input Data | Expected Result | Actual Result | Pass/Fail | Summary of Defect | Comment |
| F006 | Create new Room | Fill in all the required details on the create room page | The admin will see the new created room on the home page | The admin manages to create a new room in the database and will be redirected to the homepage | Pass | None | - |
| F007 | View room status | Tap any room in the homepage list | The admin will be redirected admin room dashboard and see the current status of the room | The admin managed to fetch the correct room details from the database | Pass | None | - |
| F008 | Locked/ Unlocked Room | Tap the Lock/Unlock button | The admin is able to lock lock/unlock | The admin successfully change the state of the isLocked variable in the database to lock/ unlock the lock | Pass | None | - |
| F009 | Enable/Disable Room | Tap the Enable/Disable button | The admin is able to Enable/Disable | The admin successfully change the state of the isDisabled variable in the database to enable/ disable the lock | Pass | None | - |

## APPENDIX B: NON-FUNCTIONAL TEST

**Usability Testing**

| **Module:** Guest and Admin | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Test Objective:** To test the usability of the Guest and Admin module in the application | | | | | | | |
| Test Id | Task | Success | Time Taken | Errors | User Feedback | Observations | Comment |
| U001 | Login into the system | Yes | 1 minutes | 0 | Simple and straightforward | Smooth interaction | - |
| U002 | Logout from the system | Yes | 5 seconds | 0 | The logout button is quite noticeable | Smooth interaction | - |

| **Module:** Guest | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Test Objective:** To test the usability of Guest module in the application | | | | | | | |
| Test Id | Task | Success | Time Taken | Errors | User Feedback | Observations | Comment |
| U003 | Register as new user | Yes | 4 minutes | 0 | Easy to understand and familiar with the interface | User completed with no hesitation | - |
| U003 | Book a room | Yes | 4 minutes | 0 | Simple and easy to understand | User completed with no hesitation | - |
| U004 | View ongoing booking | Yes | 5 seconds | 0 | Easy to see their booking detail | Smooth interaction | - |
| U005 | View room dashboard | Yes | 5 seconds | 0 | Good layout and easy to find the intended info | Smooth interaction | - |

| **Module:** Admin | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Test Objective:** To test the usability of Admin module in the application | | | | | | | |
| Test Id | Task | Success | Time Taken | Errors | User Feedback | Observations | Comment |
| U006 | Create a new Room | Yes | 4 minutes | 0 | Finds it easy to understand the form and process flow | User completed with no hesitation | - |
| U007 | View room status | Yes | 5 seconds | 0 | Easy to see specific information of the room status | Smooth interaction | - |
| U008 | Locked/ Unlocked Room | Yes | 5 seconds | 0 | The button design is easy to distinguish | Smooth interaction | - |
| U009 | Enable/Disable Room | Yes | 5 seconds | 0 | The button design is easy to distinguish | Smooth interaction | - |