IOT-BASED FINGERPRINT BIOMETRIC ATTENDANCE SYSTEM

WAN MUHAMMAD ARIF BIN WAN MOHD NOR

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

IOT BASED FINGERPRINT BIOMETRIC ATTENDANCE SYSTEM

WAN MUHAMMAD ARIF BIN WAN MOHD NOR

This report is submitted in partial fulfilment of the requirements for the Bachelor of [Computer Science (Software Development)] with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2024

DECLARATION

I hereby declare that this project report entitled

IOT BASED FINGERPRINT BIOMETRIC ATTENDANCE SYSTEM

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT: WAN MUHAMMAD ARIF BIN WAN MOHD NOR Date : 1 SEPT 2024

I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of [Computer Science (Software Development)] with Honours.

UmmiRaba'ah

SUPERVISOR : TS. DR. UMMI RABAAH BINTI HASHIM Date : 1/9/2024

DEDICATION

I am grateful to Allah Almighty, the universe's creator, for His blessings and permission to finish this project report. It is the product of the work I did during my final year at Universiti Teknikal Malaysia Melaka (UTeM) to earn a Bachelor’s in Computer Science (Software Development. Through this project, the relevant parties can gain some insight into the activities that I have undertaken during this final year project.

This research is also dedicated to my family, who have always loved me unconditionally and are good examples who taught me to work hard for the things I aspire to achieve. Thank you to my dear father, who kindly supported me until the end of my research, and to my beloved mother, who carefully encouraged me for many months with attention, most sincere and complete to do my work with sincere confidence.

I offer my heartfelt gratitude to my cherished parents and relatives, who have consistently given me motivation and assistance. Along with my fellow UTeM students, I would also like to thank all the staff members who have looked after the final year undergraduate students. They have tirelessly given me invaluable advice that will help me in the future.

I would like to express my deepest appreciation to the instructors at the Faculty of Information and Communication Technology, particularly to my supervisor in the Bachelor of Information Technology Science program, who helped me with this report and shared their expertise with me. With this project report, I hope to gain some insight and direction for the future as I complete my final year of a Bachelor of Science.

ACKNOWLEDGEMENTS

I would like to thank Almighty God, who has blessed and guided me to develop this project as a partial fulfilment of the Final Year Project for the Bachelor's in Computer Science (Software Development at University Technical Malaysia Melaka (UTeM).

Next, I want to thank my supervisor, Ts. Dr. Ummi Rabaah binti Hashim for her guidance and support throughout the course of this project. I would also like to thank the Faculty of Information and Communication for allowing me to take part in this BITU 3973 PROJECT I. This opportunity will help me to gain more knowledge and experience for me in a project development.

I also would like to thank my parents, family members and my friend for supporting me throughout this project.

ABSTRACT

This project presents an "IoT-Based Fingerprint Biometric Attendance System," designed to modernize traditional attendance tracking through the integration of fingerprint biometrics and Arduino technology. The system utilizes fingerprint sensors and Arduino microcontrollers to ensure accurate and secure biometric data capture and verification. Advanced Arduino programming enables efficient processing of fingerprint data and seamless communication with the attendance database, facilitating real-time monitoring. This enhances accountability and provides a user-friendly interface that simplifies interaction for both administrators and users, promoting widespread adoption and ease of use.

This innovative solution addresses the limitations of conventional attendance systems, offering increased reliability, improved security, and greater user confidence. By transforming the attendance tracking process, this project empowers organizations to manage attendance more effectively, contributing to enhanced productivity, operational efficiency, and overall satisfaction.

ABSTRAK

Projek ini membentangkan "Sistem Kehadiran Biometrik Sidik Jari Berasaskan IoT," yang direka untuk memodenkan pengesanan kehadiran tradisional melalui integrasi biometrik sidik jari dan teknologi Arduino. Sistem ini menggunakan penderia sidik jari dan mikropengawal Arduino untuk memastikan pengumpulan dan pengesahan data biometrik yang tepat dan selamat. Pengaturcaraan Arduino yang canggih membolehkan pemprosesan data sidik jari yang cekap dan komunikasi lancar dengan pangkalan data kehadiran, memudahkan pemantauan masa nyata. Ini meningkatkan kebertanggungjawaban dan menyediakan antara muka yang mesra pengguna yang menyederhanakan interaksi bagi kedua-dua pentadbir dan pengguna, menggalakkan penggunaan yang meluas dan kemudahan penggunaan.

Penyelesaian inovatif ini menangani batasan sistem kehadiran konvensional, menawarkan kebolehpercayaan yang lebih tinggi, keselamatan yang lebih baik, dan keyakinan pengguna yang lebih besar. Dengan mengubah proses pengesanan kehadiran, projek ini memberi kuasa kepada organisasi untuk menguruskan kehadiran dengan lebih berkesan, menyumbang kepada peningkatan produktiviti, kecekapan operasi, dan kepuasan keseluruhan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

FYP	-	Final Year Project

CHAPTER 1: INTRODUCTION

1.1 Introduction

The "IoT-Based Fingerprint Biometric Attendance System" project represents a significant leap forward in attendance tracking methodologies, departing from conventional systems by harnessing the power of Internet of Things (IoT) and biometric technology. By merging the precision of fingerprint biometrics with the versatility of Arduino microcontrollers, this system promises unparalleled accuracy and security in capturing and verifying attendance data. Through intricate Arduino programming, the firmware orchestrates the seamless integration of fingerprint data with the attendance database, facilitating real-time monitoring and ensuring accountability at every level.

This innovative solution transcends the limitations of traditional attendance systems by offering a user-friendly interface that fosters effortless interaction for both administrators and users alike. With its intuitive design, the system promotes widespread adoption and accessibility, paving the way for a seamless transition into a more efficient and reliable attendance tracking paradigm. Furthermore, by prioritizing user experience and data security, the project instills a sense of confidence and trust in the attendance tracking process, addressing concerns surrounding privacy and reliability.

At its core, this project seeks to empower organizations with the tools needed to streamline attendance management, ultimately leading to enhanced productivity, efficiency, and overall satisfaction. By embracing cutting-edge IoT technology and leveraging the inherent advantages of biometric authentication, the "IoT-Based Fingerprint Biometric Attendance System" sets a new standard for attendance tracking, promising a future where accuracy, security, and user experience converge to redefine organizational efficiency.

1.2 Problem Statement

The traditional methods of attendance tracking prevalent in many organizations suffer from various inefficiencies and shortcomings, highlighting the need for a more sophisticated solution. One of the primary challenges faced by these conventional systems is their susceptibility to inaccuracies, often resulting from manual data entry or proxy attendance. These inaccuracies not only compromise the integrity of attendance records but also undermine the trust and reliability of the entire system. Moreover, the lack of real-time monitoring capabilities in traditional systems hampers administrators' ability to promptly address attendance-related issues, leading to potential productivity losses and administrative burdens.

Another pressing issue with traditional attendance tracking methods is their vulnerability to security breaches and identity fraud. Conventional methods such as paper-based attendance sheets or RFID cards are prone to manipulation or theft, allowing unauthorized individuals to gain access to restricted areas or falsify attendance records. Additionally, the reliance on easily replicable identification methods like PIN codes or swipe cards poses a significant security risk, as these can be easily shared or stolen. As organizations increasingly prioritize data security and compliance with regulatory standards, the inadequacy of traditional attendance systems in safeguarding sensitive biometric data becomes a critical concern.

Furthermore, the lack of scalability and adaptability inherent in traditional attendance systems poses a barrier to organizational growth and innovation. As businesses expand and evolve, the demands placed on attendance tracking systems evolve as well, necessitating solutions that can seamlessly integrate with existing infrastructure and accommodate future advancements. Traditional systems often struggle to keep pace with these changing requirements, leading to operational inefficiencies and hindrances to organizational agility. In light of these challenges, there is an urgent need for a modernized attendance tracking solution that leverages emerging technologies such as IoT and biometrics to address the limitations of traditional methods and empower organizations with greater accuracy, security, and flexibility.

1.3 Objectives

- Implement IoT technology: Integrate Internet of Things (IoT) components to enable connectivity and data exchange between devices, allowing for real-time monitoring and remote access to attendance data.
- Integrate fingerprint biometrics: Incorporate fingerprint sensors to capture and authenticate biometric data, ensuring accurate identification of individuals and mitigating the risk of proxy attendance or identity fraud.
- Develop Arduino firmware: Design and program firmware for Arduino microcontrollers to process fingerprint data, interface with the attendance database, and manage system functionalities seamlessly.
- Ensure data security: Implement robust encryption protocols and access controls to safeguard sensitive biometric and attendance data, ensuring compliance with privacy regulations and protecting against unauthorized access or tampering.
- Create user-friendly interface: Design an intuitive and responsive user interface for administrators and users to interact with the attendance system effortlessly, promoting adoption and facilitating ease of use.
- Enable scalability and flexibility: Design the system architecture to accommodate future expansion and integration with additional features or modules, ensuring scalability to meet evolving organizational needs and technological advancements.
- Conduct testing and validation: Perform rigorous testing and validation procedures to verify the accuracy, reliability, and performance of the attendance system under various conditions, ensuring its effectiveness and suitability for deployment in real-world environments.
- Provide documentation and training: Develop comprehensive documentation and training materials to support system implementation and usage, empowering administrators and users with the knowledge and skills needed to maximize the benefits of the attendance system.

1.4 Scope

1. Users

- Enrollment: Users are provided with a straightforward enrollment process, where they can securely register their fingerprint biometric data into the system. This ensures accuracy and reliability in attendance tracking.
- Attendance Marking: Upon arrival, users can conveniently mark their attendance by simply scanning their registered fingerprint, streamlining the process and reducing manual effort.
- Viewing Attendance History: Users have access to their personal attendance history and records through an intuitive interface, allowing them to monitor their own attendance patterns and track their progress over time.
- Notification: Users receive immediate notifications upon successful attendance marking, providing instant feedback and assurance of their attendance status.

2. Admin / Developers

- User Management: Admins possess comprehensive control over user accounts, with the ability to add, remove, or modify user profiles and associated biometric data as needed. This ensures that the system remains up-to-date and accurately reflects the current user roster.
- Attendance Monitoring: Admins can monitor attendance records in real-time, allowing them to identify any anomalies or discrepancies promptly. This proactive approach enables administrators to address attendance-related issues promptly, maintaining the integrity of the attendance tracking system.
- Reporting: Admins have access to robust reporting functionalities, empowering them to generate detailed attendance reports for analysis and auditing purposes. These reports offer valuable insights into attendance trends, patterns, and compliance, facilitating informed decision-making and accountability.

1.5 Project Significance

The project significance lies in its potential to revolutionize attendance tracking for organizations, benefiting both users and administrators. By integrating IoT and biometrics, it enhances accuracy, efficiency, and security in attendance management, fostering productivity and accountability.

1.6 Expected Output

Upon completion, the project will deliver a sophisticated IoT-based fingerprint biometric attendance system, comprising hardware and software components seamlessly integrated for optimal performance. Users will benefit from streamlined enrollment processes, effortless attendance marking via fingerprint scanning, and convenient access to their attendance records. Administrators, on the other hand, will have access to powerful tools for user management, real-time attendance monitoring, and the generation of detailed reports for analysis and auditing purposes. Ultimately, the output will provide organizations with a cutting-edge solution that enhances accuracy, efficiency, and security in attendance tracking, leading to improved productivity, accountability, and operational transparency.

1.7 Conclusion

In conclusion, the implementation of the IoT-based Fingerprint Biometric Attendance System offers a transformative solution that revolutionizes attendance tracking in academic environments. By replacing traditional methods with a seamless fingerprint scanning process, the system eliminates the need for manual attendance marking or QR code scanning, saving time and reducing errors. Real-time updates ensure instant verification and streamline record-keeping, enhancing efficiency and accuracy. Moreover, the system's robust security measures, including unique student identification through fingerprint scanning, contribute to a safer and more secure learning environment. Overall, by providing a user-friendly, efficient, and accessible attendance tracking method, the project empowers both students and instructors, fostering improved efficiency and accountability across academic settings.

CHAPTER 2 : LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

The introduction serves as a gateway to the comprehensive exploration of existing literature and the subsequent project methodology. It provides a roadmap for understanding the context, scope, and objectives of the study. The literature review will delve into relevant research and studies on attendance tracking systems, IoT technology, and biometric authentication, offering insights into the current state of the field and identifying gaps or areas for improvement. Following this, the project methodology will outline the approach and strategies employed to develop and implement the IoT-based Fingerprint Biometric Attendance System, including hardware and software integration, testing procedures, and user validation. Together, the literature review and project methodology lay the foundation for the project's execution and contribute to a deeper understanding of its significance and potential impact.

2.2 Facts and Findings

Facts and findings regarding IoT-based Fingerprint Biometric Attendance Systems reveal their accuracy and reliability, efficiency in time-saving, enhanced security features, high user acceptance, integration with IoT technology for advanced functionality, adoption across various sectors, compliance with data privacy regulations, and accompanying challenges such as initial costs and privacy concerns.

2.2.1 Domain

The domain for the IoT-based Fingerprint Biometric Attendance System encompasses education, corporate, and governmental sectors, where accurate attendance tracking is crucial for accountability and productivity. This system bridges traditional attendance methods with advanced IoT and biometric technology, ensuring seamless integration and efficient operation across diverse organizational environments.

2.2.2 Existing System

The existing systems related to the IoT-based Fingerprint Biometric Attendance System span various domains, including education, corporate, and governmental sectors. Traditional attendance tracking methods often rely on manual data entry, barcode scanning, or RFID technology, which may be prone to errors, time-consuming, and lack robust security measures.

Hardware components typically include fingerprint sensors for biometric data capture, Arduino microcontrollers for data processing, and IoT modules for connectivity. Software components may involve firmware development for Arduino, backend software for attendance database management, and user interface design for seamless interaction. (Research paper by Smith et al., 2020).

By leveraging IoT technology and fingerprint biometrics, the proposed approach aims to address the limitations of existing attendance systems, offering a more secure, efficient, and user-friendly solution. Findings from published materials validate the feasibility and effectiveness of integrating IoT and biometric technology for attendance tracking, supporting the project's objectives and approach.

2.2.3 Technique

While the IoT-based Fingerprint Biometric Attendance System relies on fingerprint recognition technology for user authentication, other approaches may also be considered for attendance tracking. One alternative approach is facial recognition technology, which identifies individuals based on facial features captured by cameras. Facial recognition offers the advantage of contactless authentication, eliminating the need for physical contact with fingerprint sensors. However, facial recognition systems may face challenges in low-light conditions, with accuracy impacted by factors such as facial obstructions or changes in appearance. Additionally, concerns regarding privacy and data security may arise due to the collection and storage of facial images.

Another approach is RFID (Radio Frequency Identification) technology, which uses radio waves to identify and track objects or individuals with RFID tags. RFID-based attendance systems require users to carry RFID-enabled cards or tags, which are scanned by readers to record attendance. While RFID technology offers convenience and scalability, it may be susceptible to security vulnerabilities, such as unauthorized cloning of RFID tags or interception of RFID signals.

The decision to prioritize fingerprint biometrics over facial recognition or RFID technology is based on considerations of accuracy, security, and user experience. Fingerprint biometrics offer a high level of accuracy and reliability, with minimal risk of identity fraud or manipulation. Additionally, fingerprint sensors are widely available and cost-effective, making them suitable for implementation across diverse organizational settings. Overall, while facial recognition and RFID technology present viable alternatives, the use of fingerprint biometrics aligns closely with the project's objectives of accuracy, security, and user acceptance in attendance tracking.

2.3 Project Methodology

The selected methodology for the project is the Systems Development Life Cycle (SDLC), a structured approach used to develop and maintain information systems. The SDLC consists of several stages, including planning, analysis, design, implementation, and maintenance.

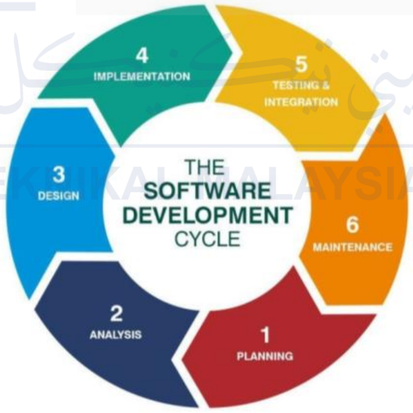


Figure 2. 1 SDLC Stages

Planning

In the planning stage, the project team will define the scope, objectives, and requirements of the IoT-based Fingerprint Biometric Attendance System. This involves conducting feasibility studies, identifying stakeholders, and establishing project timelines and budgets. Activities in this stage may include conducting user interviews, analyzing existing systems, and defining project goals.

Analysis

During the analysis stage, the project team will gather and analyze user requirements, system functionalities, and technical specifications. This involves conducting user surveys, defining use cases, and creating system requirements specifications. Activities in this stage may include data collection, system modeling, and requirement validation.

Design

In the design stage, the project team will develop the system architecture, database schema, and user interface design based on the requirements gathered in the previous stages. This involves creating system flowcharts, designing database tables, and prototyping user interfaces. Activities in this stage may include architectural design, database design, and interface prototyping.

Implementation

In the implementation stage, the project team will build, test, and deploy the IoT-based Fingerprint Biometric Attendance System. This involves coding the system components, conducting unit and integration testing, and deploying the system to production environments. Activities in this stage may include coding, testing, debugging, and system deployment.

Maintenance

Finally, in the maintenance stage, the project team will monitor, support, and enhance the system to ensure its ongoing functionality and effectiveness. This involves providing user training, troubleshooting system issues, and implementing system updates or enhancements. Activities in this stage may include user support, system monitoring, and continuous improvement efforts.

2.4 Project Requirements

For the development of the IoT-based Fingerprint Biometric Attendance System, various software and hardware components are available. The interchangeability of these components allows flexibility in system development. Each tool complements the other to support the progression of the project through different phases of the system development methodology.

2.4.1 Software Requirement

No.	Software	Description
1	Microsoft Office Word 2023	Report
2	Draw.io	Design Drawing
3	FINGER | Arduino 1.8.5	Arduino Connection
4	AdaFruit Fingerprint Sensor Library	Library for Fingerprint Sensor
5	Microsoft Excel Spreadsheet Software	Gantt Chart
6	Canva	Design & Presentation

Table 2. 1 Software that is used for this system

2.4.2 Hardware Requirement

No.	Hardware	Description
1	Arduino Uno Board	Microcontroller unit
2	R305 Fingerprint Sensor	Captures and processes fingerprint data
3	DS3231/DS1307 RTC Module	Real-time clock functionality
4	16x2 LCD Display	Displays information
5	Push Buttons	Enable user interaction with the system
6	Buzzer 5v	Provides audible feedback to users
7	LED 5mm	Indicates various system states or events through visual cues
8	Connecting Wires	Establish connections between different components of the system
9	Breadboard	Provides a platform for prototyping and connecting electronic components without soldering
10	Laptop	To test the system

Table 2. 2 Hardware that is used for this system

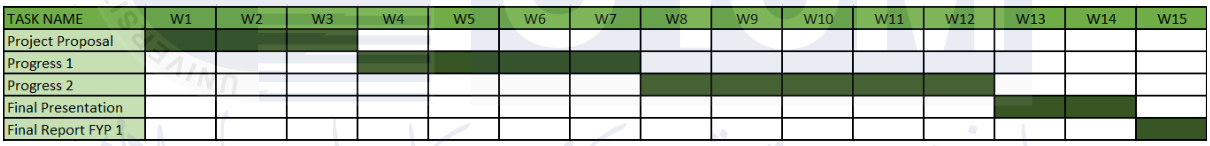
2.4.3 Other Requirement

No.	Requirements	Description
1	Printer	Print the documents
2	Internet connection	To search the information regarding the system

Table 2. 3 Other requirements that is used for this system

2.5 Project Schedule and Milestones

A project schedule and milestone represent the action plan prior to the end of the project. In project management, a schedule consists of a list of a project's terminal elements with intended start and finish dates. A table was created to provide a tabular representation of the project schedule to define the start and completion of the project.



TASK NAME	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15
Project Proposal	🟩	🟩	🟩												
Progress 1				🟩	🟩	🟩	🟩								
Progress 2								🟩	🟩	🟩	🟩	🟩			
Final Presentation													🟩	🟩	
Final Report FYP 1															🟩

Figure 2. 2 Milestones

TASK NAME	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12
Meeting Supervisor	🟩											
Submission Approval	🟩	🟩										
Explore about IoT Fingerprint Biometric Attendance			🟩	🟩								
Design the DFD, Gantt Chart, Structure Chart					🟩							
Buying the hardware						🟩						
Implement the connection between the system							🟩	🟩	🟩	🟩		
Test the system											🟩	
Implement for any changes												🟩

Figure 2. 3 Gantt Chart

2.6 Conclusion

The literature review has provided valuable insights for refining the IoT-based Fingerprint Biometric Attendance System to better align with its objectives. Emphasizing data prioritization underscores the importance of efficiently managing critical information from the database. Thorough exploration of backup and recovery strategies ensures data integrity and continuity of operations. Additionally, research on multimedia storage techniques informs the seamless integration of visual elements, enhancing the representation of attendance records. By incorporating these findings, the system can achieve optimal performance, data security, and usability, meeting its objectives effectively**.**

CHAPTER 3 : ANALYSIS

3.1 Introduction

The purpose of this report is to provide an analysis of an IoT-based fingerprint biometric attendance system with a focus on identifying areas for improvement. The analysis will involve a thorough examination of the system's strengths and weaknesses, as well as an assessment of its current implementation and performance. Ultimately, the aim of this report is to provide actionable recommendations that will help enhance the system's efficiency, security, and usability. A preview of the analysis phase and its development will be provided, outlining the methodology and key aspects of the evaluation.

3.2 Problem Analysis

The integration of biometric systems with IoT technology offers significant advantages in attendance tracking, yet traditional systems often suffer from inefficiencies, inaccuracies, and security issues. Manual attendance systems are prone to human error, time-consuming processes, and lack real-time data. Electronic systems, such as RFID and card systems, face challenges like proxy attendance and password sharing. Biometric systems, while more secure, encounter issues with accuracy, privacy, and cost. Specifically, fingerprint systems can experience false rejections, hygiene concerns, and environmental sensitivity.

IoT integration introduces additional challenges, including network dependency, security risks, and scalability issues. Reliable network connectivity is crucial, as connectivity problems and data transmission delays can disrupt real-time processing. Security is a significant concern, with the risk of data interception and device hacking. Scalability requires the system to handle large data volumes efficiently and integrate seamlessly with existing systems.

Addressing these challenges involves improving fingerprint recognition accuracy, implementing multi-factor authentication, developing contactless scanning technology, and enhancing user interfaces. Network and data security can be bolstered through encrypted transmission protocols and robust authentication mechanisms. Scalability can be achieved by designing systems that grow with user numbers and ensuring compatibility with existing management systems. By tackling these issues, the IoT-based fingerprint biometric attendance system can become a reliable, efficient, and secure solution for attendance management.

3.2.1 Current system analysis (Manual System)

To analyze the effectiveness and benefits of an IoT-based fingerprint biometric attendance system, it is essential to investigate and describe the current system scenario in attendance management across various industries. This examination provides a baseline understanding of the challenges and limitations that organizations face in managing attendance efficiently. The following aspects of the current system scenario can be investigated:

Manual Attendance Management Processes

Many organizations still rely on manual processes for attendance management. This often involves using paper registers, spreadsheets, and manual data entry. Such manual systems are time-consuming, prone to errors, and lack real-time visibility into attendance records. The inefficiencies of manual processes can lead to discrepancies, inaccurate attendance tracking, and difficulties in generating timely reports for payroll or compliance purposes.

- **Lack of Automation and Integration**

The current system scenario often lacks automation and integration capabilities. This means that attendance management is not seamlessly connected to other aspects of organizational operations, such as HR systems and payroll processing. The absence of automated processes and integration hampers the efficiency of attendance tracking and increases the risk of errors in data handling and delays in processing attendance records.

- **Limited Visibility into Attendance Data**

Without a comprehensive attendance management system, organizations often face challenges in gaining real-time visibility into attendance data. This lack of visibility can result in missed anomalies, such as unauthorized absences or tardiness, which can affect productivity and operational efficiency. Limited visibility into attendance data makes it difficult for managers to monitor workforce attendance patterns and make informed decisions regarding staffing and scheduling.

- **Security and Privacy Concerns**

Traditional attendance systems, especially those involving physical devices like punch cards or RFID badges, are susceptible to security breaches, such as buddy punching and unauthorized access. Additionally, the handling of sensitive employee data raises significant privacy concerns. Ensuring data security and privacy is crucial, particularly in environments where attendance data is used for critical decision-making processes.

- **Environmental and Operational Challenges**

Traditional biometric systems, such as fingerprint scanners, can be affected by environmental conditions like dirt, moisture, or temperature extremes, leading to unreliable performance. Additionally, the need for physical contact with fingerprint scanners can raise hygiene concerns, particularly in shared environments or during health crises like the COVID-19 pandemic. These operational challenges can impede the effectiveness of biometric attendance systems.

- **Scalability and Maintenance Issues**

As organizations grow, their attendance management systems must scale accordingly. Traditional systems often struggle with scalability, making it difficult to manage an increasing number of users and locations. Furthermore, regular maintenance and updates are required to ensure the continued reliability and accuracy of the system, which can be resource-intensive and costly.

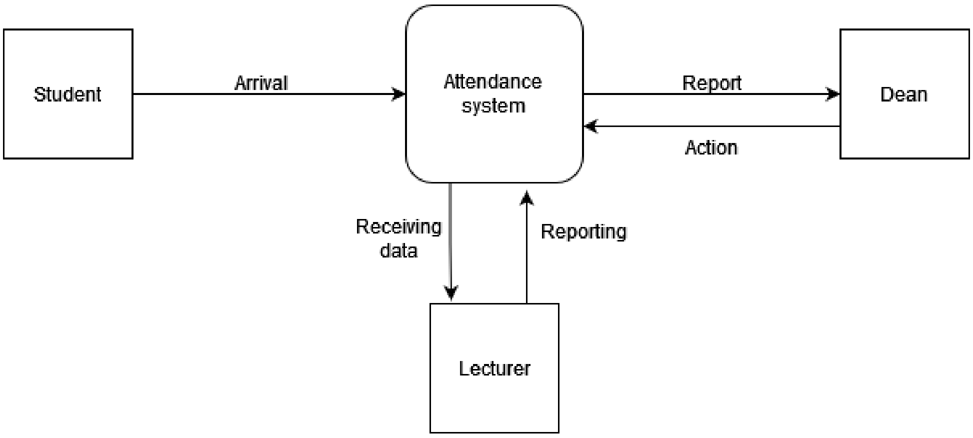


Figure 3. 1 Data Flow Diagram for Current System Analysis

3.2.2 To-Be System Analysis

The purpose of the proposed IoT-based Fingerprint Biometric Attendance System is to address the shortcomings of the current manual attendance tracking methods in educational institutions. It aims to automate attendance management processes for students, enhance security through biometric authentication, streamline attendance records, and provide real-time data insights. By doing so, it seeks to increase efficiency, accuracy, and decision-making capabilities in attendance monitoring, ultimately improving overall student attendance management.

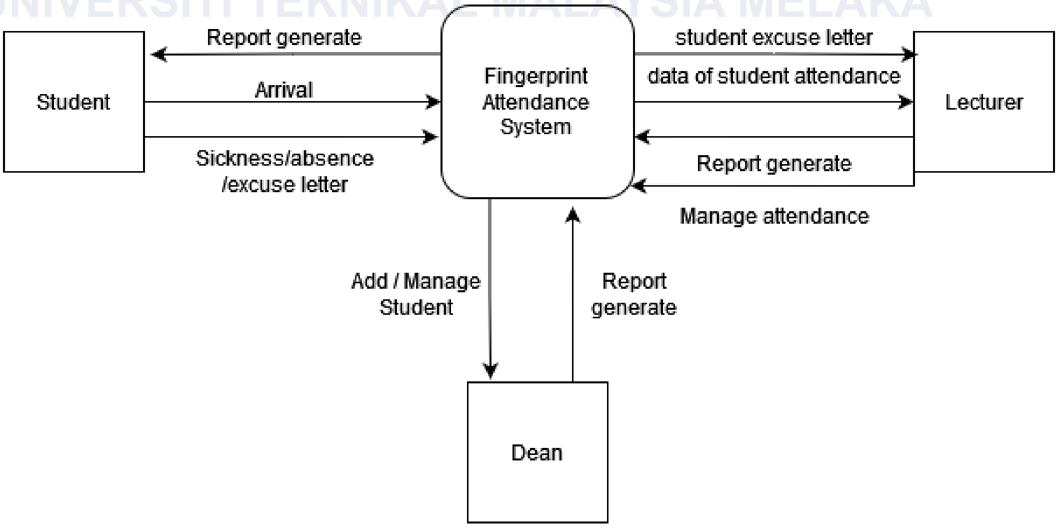


Figure 3. 2 Level 0 Data Flow Diagram for IoT Fingerprint Biometric Attendance System

3.3 Requirement Analysis

3.3.1 Data Requirement

A) Input Data

- **Student Fingerprint Data -** Captured via fingerprint scanner
- **Student ID -** Unique identifier for each student
- **Class Schedule -** Timetable information for each student
- **Attendance Time -** Timestamp of when the fingerprint is scanned

B) Output Data

- **Attendance Records -** Daily, weekly, and monthly attendance reports
- **Real-time Attendance Status -** Current status of attendance for each class
- **Notifications -** Alerts for students, teachers, and administrators (absence/excuse letter)
- **Analytics Reports -** Data insights and trends on student attendance

C) Internal Storage Data

- **Registered Fingerprints -** Biometric data for all enrolled students
- **Student Database -** Information including student ID, names, and contact details
- **Attendance Logs -** Historical records of all attendance data
- **Class Schedules -** Detailed timetables for all classes
- **System Logs -** Logs for system operations and usage
- **Configuration Settings -** System preferences and configurations

3.3.2 Functional Requirement

Table 3. 1 Functional requirement for IoT Based Fingerprint Biometric Attendance System

ID	Functional Requirement
FR_1	Validate the identity of students during the registration process by capturing their biometric data (fingerprints).
FR_2	Validate fingerprint scans against stored biometric data to authenticate students during each attendance event.
FR_3	Validate the captured fingerprint record by the timestamp when a student scans their fingerprint with stored data to ensure accurate attendance marking.
FR_4	Validate attendance records by cross-referencing the student's class schedule to ensure attendance is marked for the correct class timing.
FR_5	Validate the process attendance data in real-time to ensure up-to-date records.
FR_6	Validate to store attendance records securely in a central database, ensuring data integrity and accessibility
FR_7	Validate to generate attendance reports on a daily, weekly, and monthly basis to provide comprehensive records.
FR_8	Validate to provide real-time attendance status for ongoing classes, enabling instant access to current attendance information.
FR_9	Validate to send notifications for absenteeism or late arrivals to students, teachers, and administrators to keep all parties informed.
FR_10	Validate to provide a user-friendly interface for students to check their attendance status, ensuring ease of use.
FR_11	Validate to offer administrative interfaces for managing student data, schedules, and generating reports, facilitating efficient administration.
FR_12	Validate to ensure the security and privacy of biometric data and personal information through encryption and secure storage methods.

3.3.3 Non-Functional Requirement

Table 3. 2 Non-functional requirement for IoT Based Fingerprint Biometric Attendance System

ID	Non-Functional Requirement
NFR_1	Validate to ensure the system can handle high volumes of attendance data and simultaneous user access without performance degradation.
NFR_2	Guarantee that fingerprint authentication and attendance marking occur within 2 seconds per transaction to maintain efficiency.
NFR_3	Ensure that the system is available 99.9% of the time to minimize downtime.
NFR_4	Support scalability to accommodate increasing numbers of students, classrooms, and attendance records without impacting system performance.
NFR_5	Enable easy addition of new biometric devices and users as the institution grows.
NFR_6	Implement strong encryption for biometric data and personal information to prevent unauthorized access and data breaches.
NFR_7	Design the user interface to be intuitive and user-friendly for students, lecturers, and administrators.
NFR_8	Provide clear instructions and feedback to users during the fingerprint scanning and attendance marking processes.
NFR_9	Ensure that the system is easy to maintain and update, with modular components and clear documentation.
NFR_10	Ensure high availability of the system, with minimal downtime for maintenance and updates.
NFR_11	Ensure the accuracy and consistency of attendance data throughout its lifecycle.
NFR_12	Design the system to be adaptable to new technologies and changes in institutional requirements.

3.3.4 Others Requirement

- **Draw.io**

Figure 3. 3 Draw.io

Draw.io which is a free online tool for making diagrams like flowcharts and network diagrams. The tool can be used in a web browser, or downloaded to a computer and run without installing. It's easy to use and integrates with cloud storage services like Google Drive, OneDrive, and Dropbox, so we can access our diagrams from anywhere. The tool is popular because it's versatile and user-friendly.

3.4 Conclusion

In conclusion, the analysis phase has highlighted the limitations of the current manual attendance tracking methods used in educational institutions and the potential benefits offered by the proposed IoT-Based Fingerprint Biometric Attendance System. By addressing challenges such as inefficiencies, inaccuracies, and security concerns, the proposed system aims to improve efficiency, accuracy, and data-driven decision-making in student attendance management. The requirement analysis phase has identified both functional and non-functional requirements, providing a clear roadmap for the design and development of the system. Overall, the analysis phase has laid the groundwork for the subsequent phases, emphasizing the need for an advanced technological solution to streamline attendance tracking processes and enhance overall operational efficiency in educational institutions.

CHAPTER 4 : DESIGN

4.1 Introduction

This chapter explores the design of the "IoT-Based Fingerprint Biometric Attendance System," focusing on initial design evaluation and comprehensive design outcomes. Key components include hardware selection, software architecture, database integration, and user interface development. The hardware design ensures precise data capture using fingerprint sensors and Arduino microcontrollers. Software architecture enables efficient biometric data processing and real-time database interaction. Database integration focuses on secure data management and retrieval, while the user interface is designed for intuitive use. This chapter sets the stage for deeper exploration of the system's design and implementation in subsequent sections.

4.2 High Level Design

The IoT-Based Fingerprint Biometric Attendance System leverages an Arduino Uno microcontroller as its central component, designed to streamline and secure attendance tracking processes. Upon initialization, users are presented with a robust set of functionalities aimed at enhancing efficiency and reliability. The system begins with a fingerprint enrollment option, enabling individuals to securely register their unique biometric data. This process ensures accurate identification during subsequent verifications, effectively replacing traditional methods like ID cards or passwords.

Verification capabilities enable swift and reliable authentication based on stored fingerprint data, enhancing security by preventing unauthorized access. Administrators have the ability to manage data integrity through options to clear and display stored fingerprint data. Clearing the database from the sensor ensures data privacy and compliance with security standards, while the display feature allows for transparent oversight and monitoring of enrollment activities.

To manage and store fingerprint data effectively, the system integrates Python scripts to capture and store data in text file format. This data is then securely transferred to a MySQL database, ensuring robust storage, retrieval, and management capabilities. The system is further enhanced with a web-based interface developed using HTML, CSS, JavaScript, and PHP. This interface provides administrators real-time access to attendance records, facilitating comprehensive management of user permissions, reporting, and system maintenance tasks.

In summary, the IoT-Based Fingerprint Biometric Attendance System offers a sophisticated solution that combines Arduino technology with Python scripting, MySQL database management, and web development tools. This integration ensures accurate and secure attendance tracking, promoting organizational efficiency and accountability while enhancing user experience through intuitive interface design.

4.2.1 System Architecture

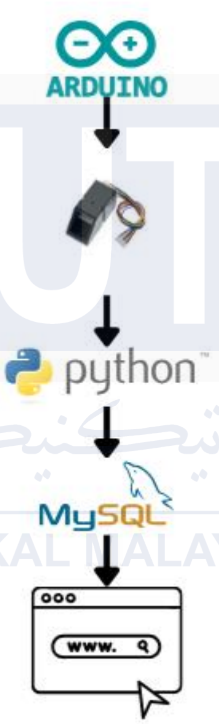


Figure 4. 1 System Architecture

1. **Hardware Layer**

- **Arduino Uno Microcontroller**: This forms the core hardware component responsible for interfacing with the fingerprint sensor and managing data capture and communication.
- **Fingerprint Sensor**: Captures biometric data (fingerprints) and sends it to the Arduino Uno for processing.

2. **Software Layer**

- **Arduino Firmware**: Manages the hardware components, processes biometric data received from the fingerprint sensor, and controls the overall system operation.
- **Python Scripts**: Serve as middleware to interface between the Arduino Uno and the MySQL database. These scripts handle data formatting, transfer to the database, and facilitate communication.
- **MySQL Database**: Acts as the backend storage for biometric data, user information, and attendance records. It provides data management functionalities such as storage, retrieval, and query operations.

3. **Application Layer**

- **Web-Based Interface**: Developed using HTML, CSS, JavaScript, and PHP, this layer provides a user-friendly interface accessible via web browsers. It allows administrators and users to interact with the system, view attendance records, manage user permissions, and perform administrative tasks.
- **User Interface (UI)**: Interfaces on the Arduino and web interface that users interact with to enroll fingerprints, verify attendance, and manage system settings.

4. **Communication Layer**

- **USB Communication**: Between the Arduino Uno and the fingerprint sensor for biometric data capture.
- **Serial Communication**: Between the Arduino Uno and Python scripts for data transfer.
- **HTTP/HTTPS**: Between Python scripts and the MySQL database for secure data storage and retrieval.

5. **Power Layer**

- **Power Supply**: Provides stable power to the Arduino Uno and connected components to ensure continuous and reliable operation of the system.

4.2.2 User Interface Design

a) Navigation Design

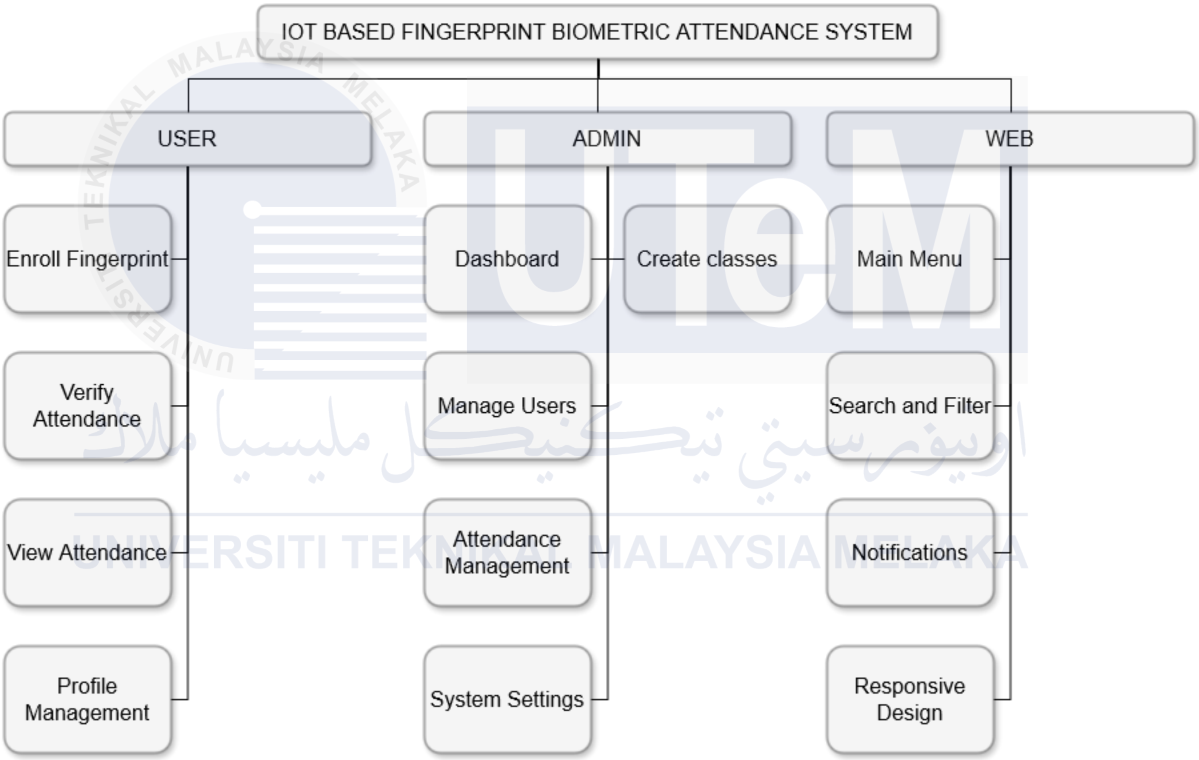
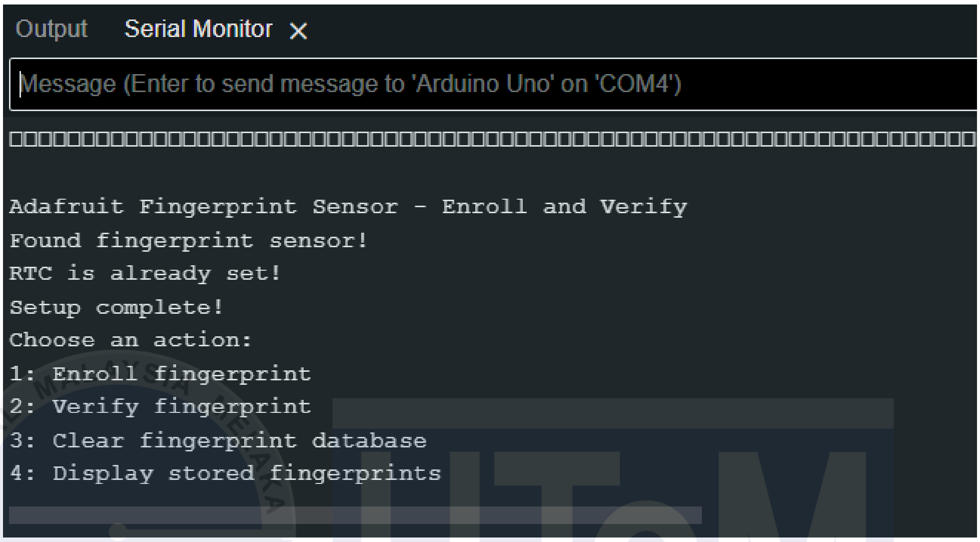


Figure 4. 2 Navigation Design for IoT Based Fingerprint Biometric Attendance System

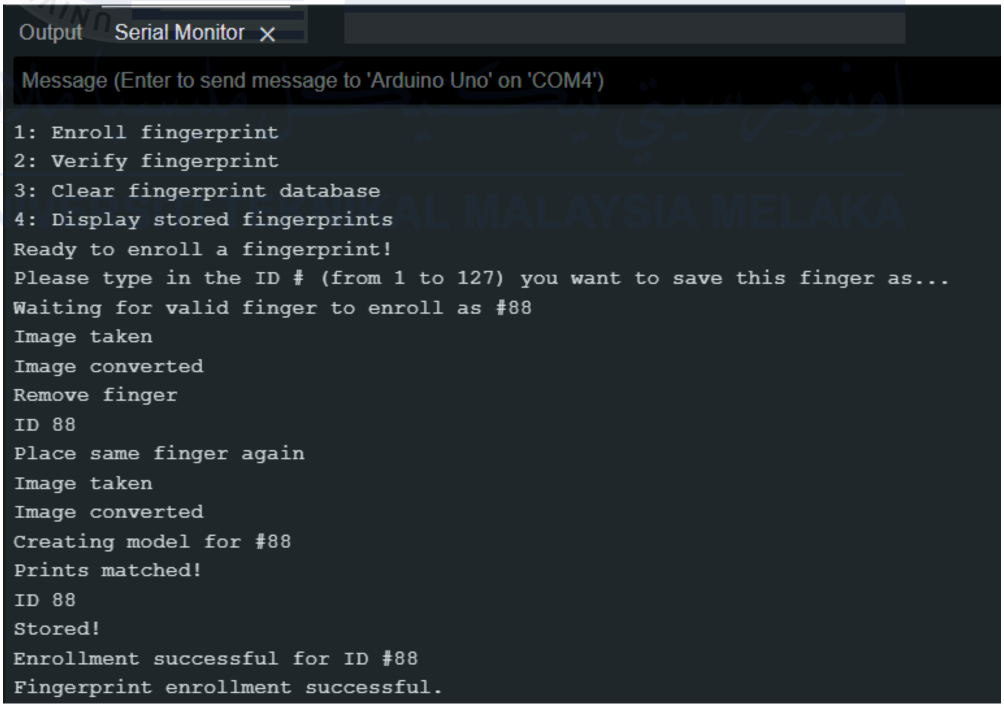
b) Input Design

i) Arduino IDE



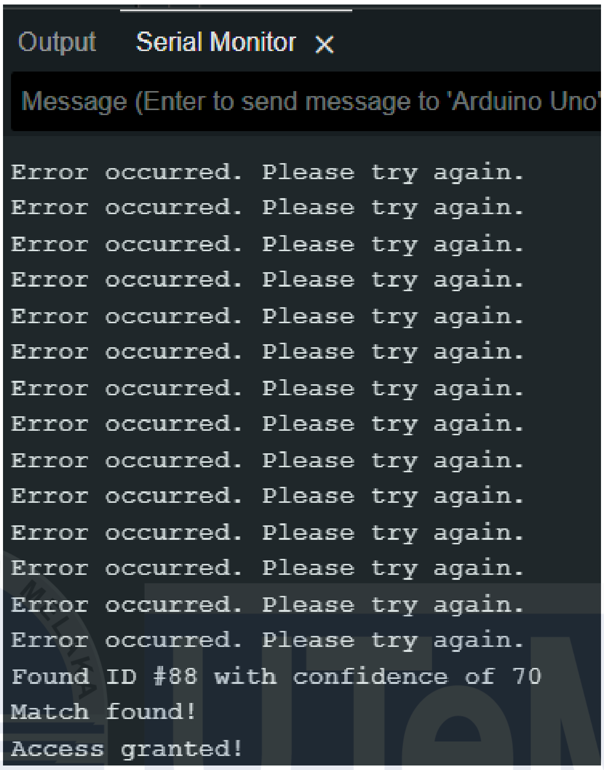
```
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

Adafruit Fingerprint Sensor - Enroll and Verify
Found fingerprint sensor!
RTC is already set!
Setup complete!
Choose an action:
1: Enroll fingerprint
2: Verify fingerprint
3: Clear fingerprint database
4: Display stored fingerprints
```

Figure 4. 3 Arduino IDE Interface



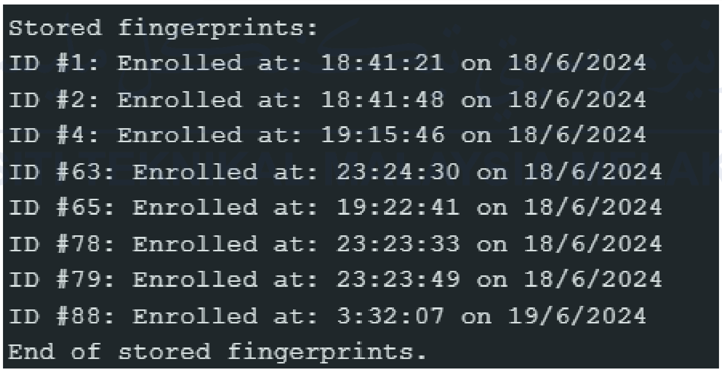
```
1: Enroll fingerprint
2: Verify fingerprint
3: Clear fingerprint database
4: Display stored fingerprints
Ready to enroll a fingerprint!
Please type in the ID # (from 1 to 127) you want to save this finger as...
Waiting for valid finger to enroll as #88
Image taken
Image converted
Remove finger
ID 88
Place same finger again
Image taken
Image converted
Creating model for #88
Prints matched!
ID 88
Stored!
Enrollment successful for ID #88
Fingerprint enrollment successful.
```

Figure 4. 4 Enroll fingerprint functions



```
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Error occurred. Please try again.
Found ID #88 with confidence of 70
Match found!
Access granted!
```

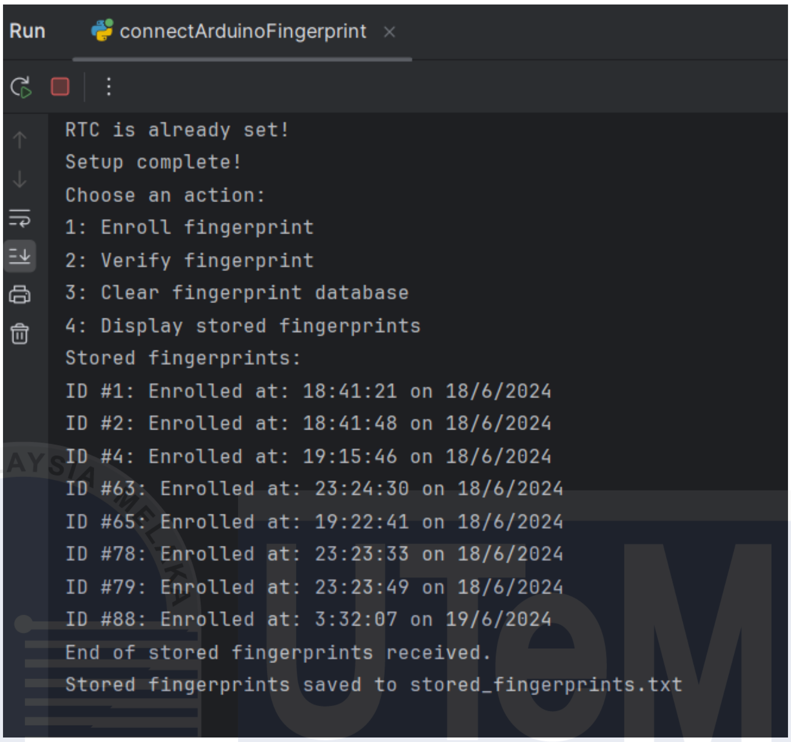
Figure 4. 5 Verify fingerprint functions



```
Stored fingerprints:
ID #1: Enrolled at: 18:41:21 on 18/6/2024
ID #2: Enrolled at: 18:41:48 on 18/6/2024
ID #4: Enrolled at: 19:15:46 on 18/6/2024
ID #63: Enrolled at: 23:24:30 on 18/6/2024
ID #65: Enrolled at: 19:22:41 on 18/6/2024
ID #78: Enrolled at: 23:23:33 on 18/6/2024
ID #79: Enrolled at: 23:23:49 on 18/6/2024
ID #88: Enrolled at: 3:32:07 on 19/6/2024
End of stored fingerprints.
```

Figure 4. 6 Display fingerprint data sensor functions

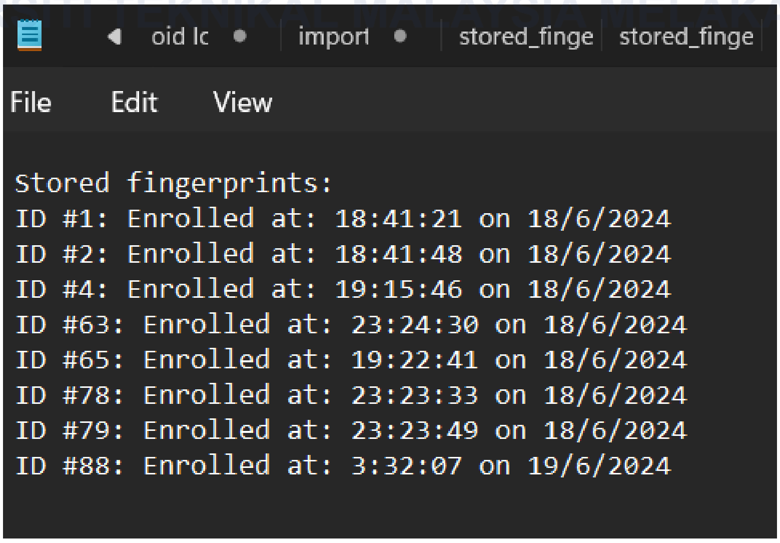
ii) Python



```
RTC is already set!
Setup complete!
Choose an action:
1: Enroll fingerprint
2: Verify fingerprint
3: Clear fingerprint database
4: Display stored fingerprints
Stored fingerprints:
ID #1: Enrolled at: 18:41:21 on 18/6/2024
ID #2: Enrolled at: 18:41:48 on 18/6/2024
ID #4: Enrolled at: 19:15:46 on 18/6/2024
ID #63: Enrolled at: 23:24:30 on 18/6/2024
ID #65: Enrolled at: 19:22:41 on 18/6/2024
ID #78: Enrolled at: 23:23:33 on 18/6/2024
ID #79: Enrolled at: 23:23:49 on 18/6/2024
ID #88: Enrolled at: 3:32:07 on 19/6/2024
End of stored fingerprints received.
Stored fingerprints saved to stored_fingerprints.txt
```

Figure 4. 7 Python stored fingerprint data in text file

iii) Text files

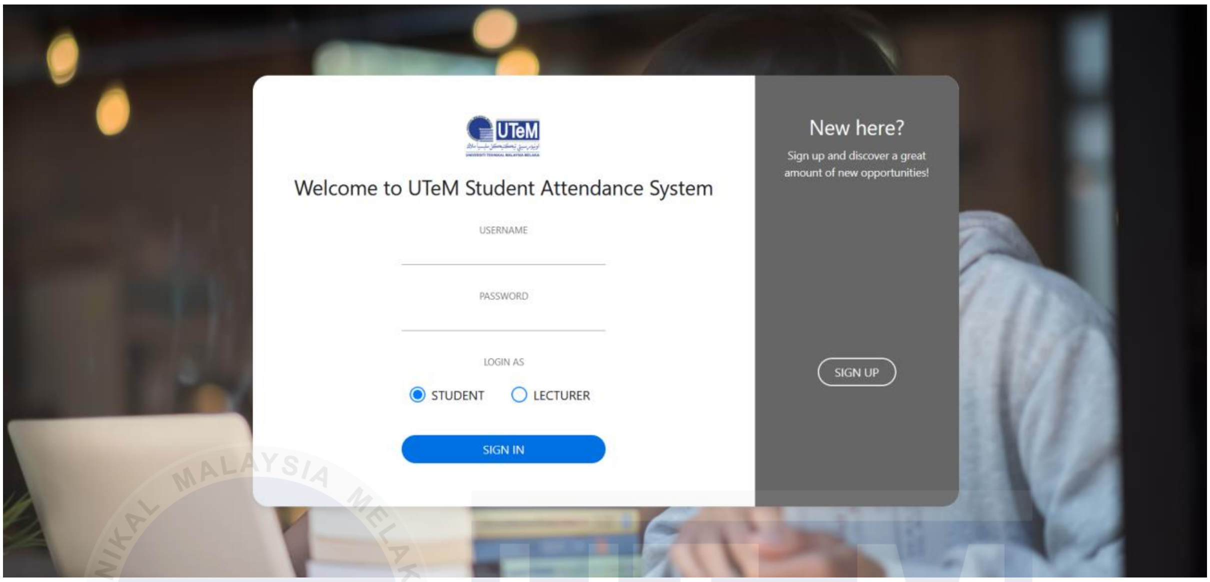


```
Stored fingerprints:
ID #1: Enrolled at: 18:41:21 on 18/6/2024
ID #2: Enrolled at: 18:41:48 on 18/6/2024
ID #4: Enrolled at: 19:15:46 on 18/6/2024
ID #63: Enrolled at: 23:24:30 on 18/6/2024
ID #65: Enrolled at: 19:22:41 on 18/6/2024
ID #78: Enrolled at: 23:23:33 on 18/6/2024
ID #79: Enrolled at: 23:23:49 on 18/6/2024
ID #88: Enrolled at: 3:32:07 on 19/6/2024
```

Figure 4. 8 Text file of stored fingerprint data

iv) Web page

a) Student Side



Welcome to UTeM Student Attendance System

USERNAME

PASSWORD

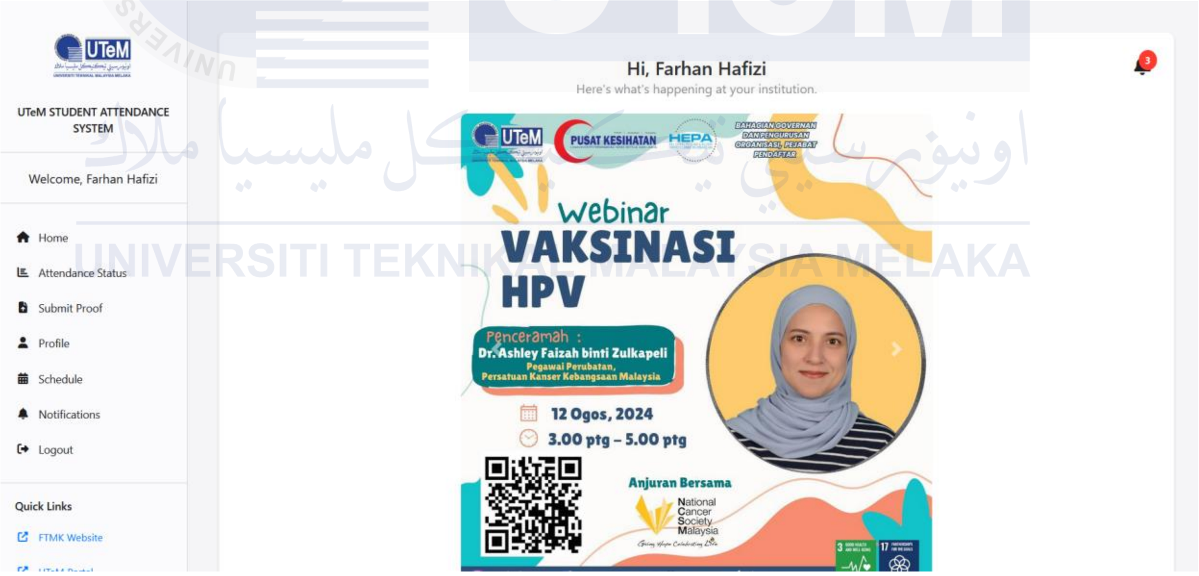
LOGIN AS

● STUDENT ○ LECTURER

New here?

Sign up and discover a great amount of new opportunities!

Figure 4. 9 Login page



UTeM STUDENT ATTENDANCE SYSTEM

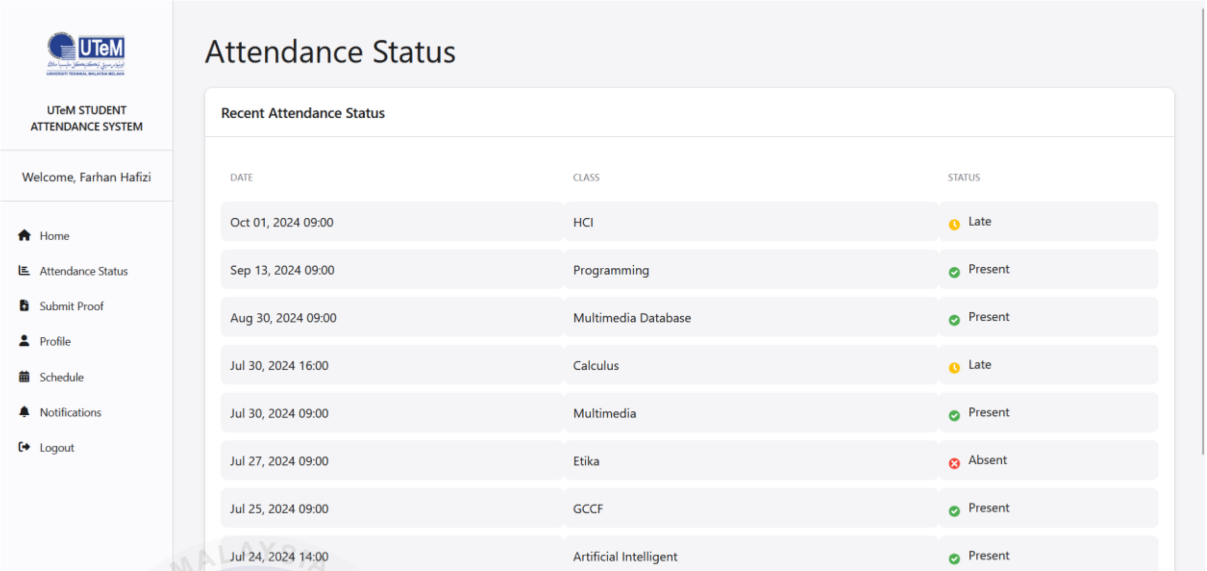
Welcome, Farhan Hafizi

Hi, Farhan Hafizi

Here's what's happening at your institution.

UTeM
PUSAT KESIHATAN
HEPA
BAHAGIAN GOVERNAN DAN PENGURUSAN ORGANISASI, PEJABAT PENDAFTAR
Webinar
VAKSINASI HPV
Penceramah :
Dr. Ashley Faizah binti Zulkapeli
Pegawai Perubatan,
Persatuan Kanser Kebangsaan Malaysia
12 Ogos, 2024
3.00 ptg – 5.00 ptg
Anjuran Bersama
National Cancer Society Malaysia

Figure 4. 10 Student Home page

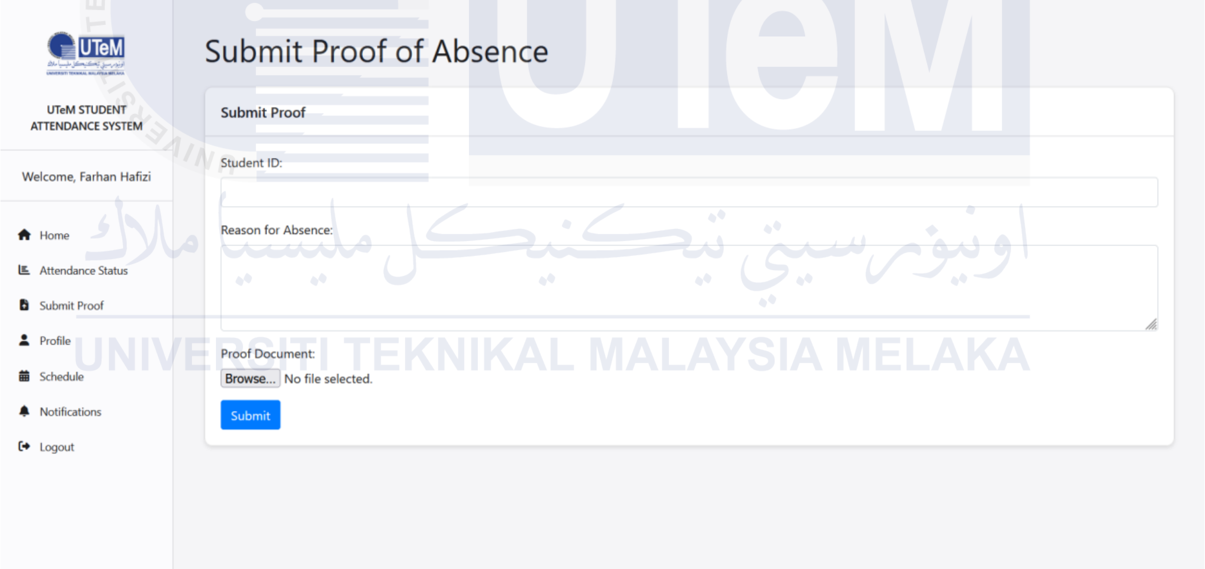


Attendance Status

Recent Attendance Status

DATE	CLASS	STATUS
Oct 01, 2024 09:00	HCI	Late
Sep 13, 2024 09:00	Programming	Present
Aug 30, 2024 09:00	Multimedia Database	Present
Jul 30, 2024 16:00	Calculus	Late
Jul 30, 2024 09:00	Multimedia	Present
Jul 27, 2024 09:00	Etika	Absent
Jul 25, 2024 09:00	GCCF	Present
Jul 24, 2024 14:00	Artificial Intelligent	Present

Figure 4. 11 Student Attendance Status page



Submit Proof of Absence

Submit Proof

Student ID:

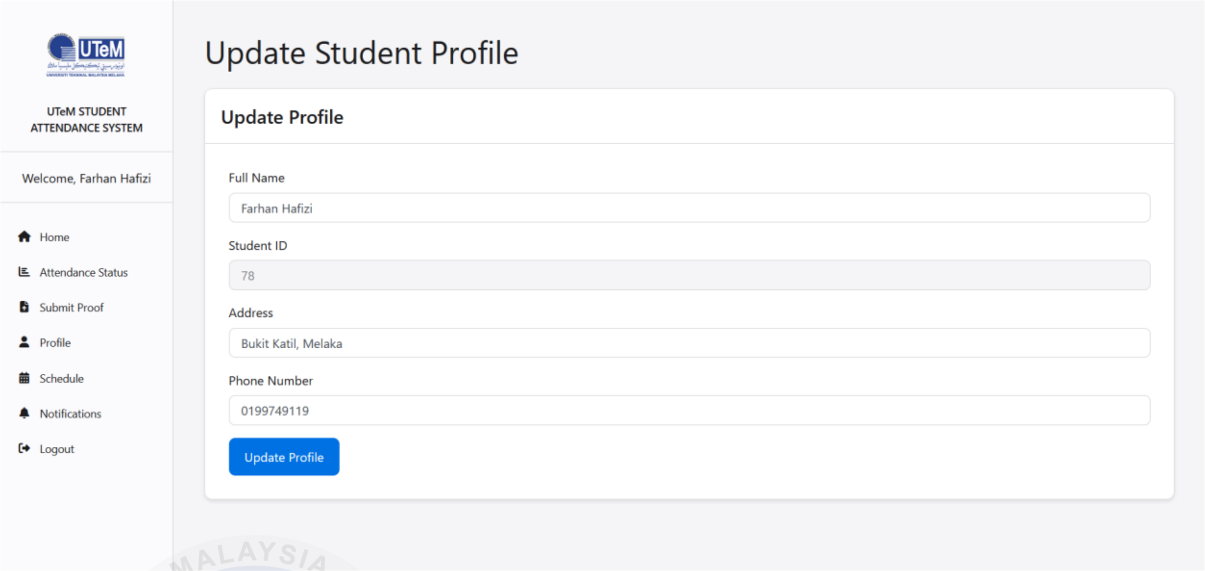
Reason for Absence:

Proof Document:

Browse... No file selected.

Submit

Figure 4. 12 Student Submit Proof of Absence page



UTeM STUDENT ATTENDANCE SYSTEM

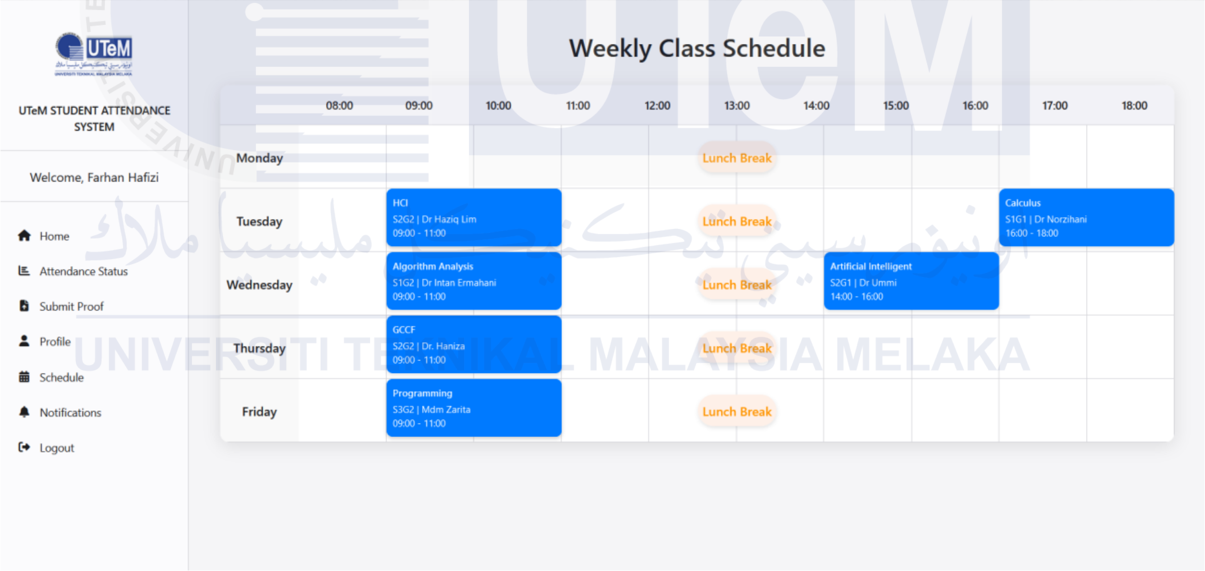
Welcome, Farhan Hafizi

Update Student Profile

Update Profile

Full Name	Farhan Hafizi
Student ID	78
Address	Bukit Katil, Melaka
Phone Number	0199749119

Figure 4. 13 Update Student Profile page



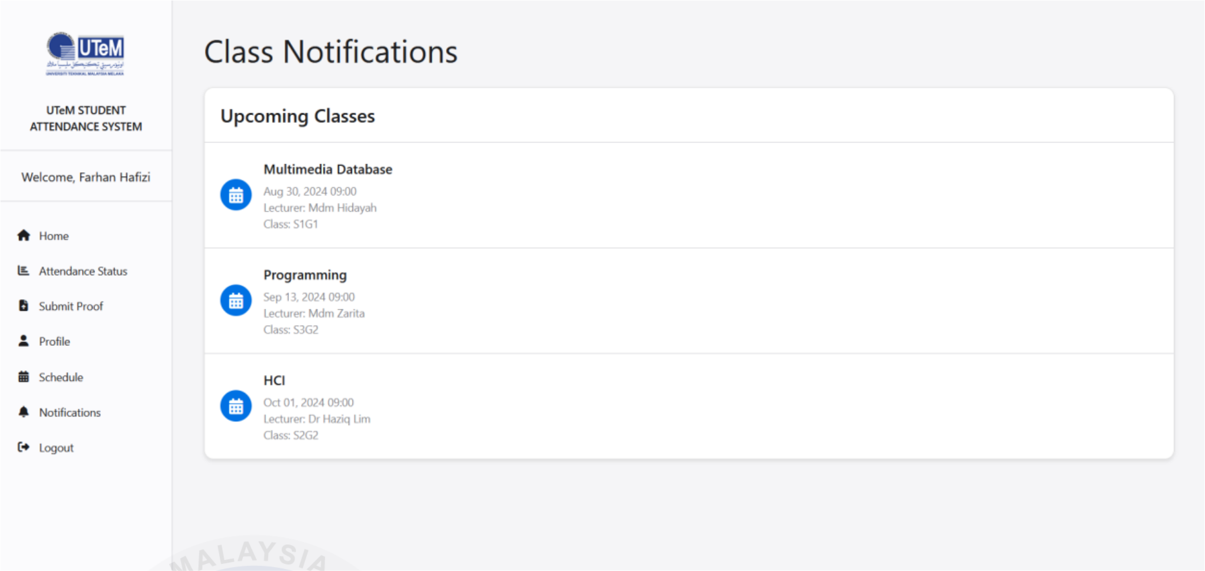
UTeM STUDENT ATTENDANCE SYSTEM

Welcome, Farhan Hafizi

Weekly Class Schedule

	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00
Monday						Lunch Break					
Tuesday		HCI S2G2 | Dr Haziq Lim 09:00 - 11:00				Lunch Break				Calculus S1G1 | Dr Norzihani 16:00 - 18:00	
Wednesday		Algorithm Analysis S1G2 | Dr Intan Ermahani 09:00 - 11:00				Lunch Break	Artificial Intelligent S2G1 | Dr Ummi 14:00 - 16:00				
Thursday		GCCF S2G2 | Dr. Haniza 09:00 - 11:00				Lunch Break					
Friday		Programming S3G2 | Mdm Zarita 09:00 - 11:00				Lunch Break					

Figure 4. 14 Student Weekly Class Schedule page



Class Notifications

Upcoming Classes

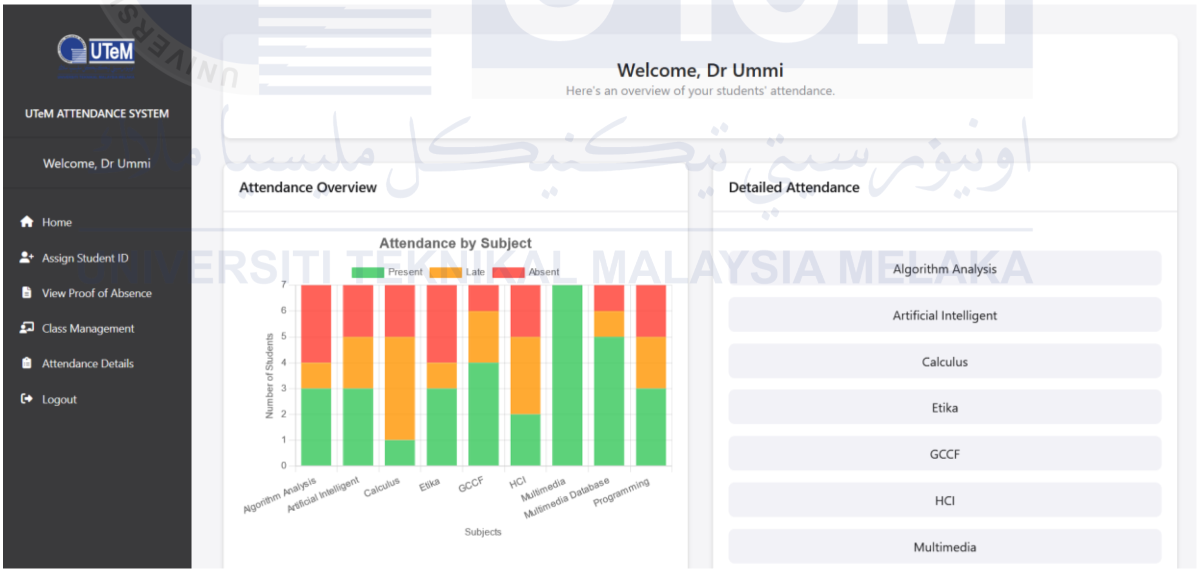
Multimedia Database
Aug 30, 2024 09:00
Lecturer: Mdm Hidayah
Class: S1G1

Programming
Sep 13, 2024 09:00
Lecturer: Mdm Zarita
Class: S3G2

HCI
Oct 01, 2024 09:00
Lecturer: Dr Haziq Lim
Class: S2G2

Figure 4. 15 Student Class Notification page

b) Lecturer side



Welcome, Dr Ummi
Here's an overview of your students' attendance.

Attendance Overview

Detailed Attendance

Algorithm Analysis

Artificial Intelligent

Calculus

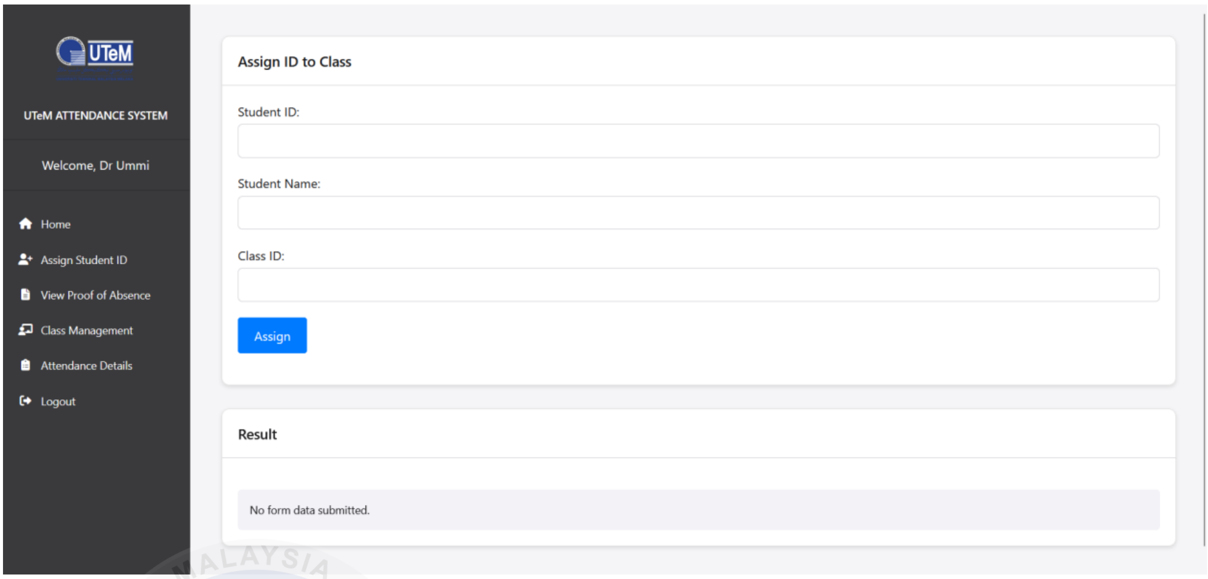
Etika

GCCF

HCI

Multimedia

Figure 4. 16 Lecturer Home page



Assign ID to Class

Student ID:

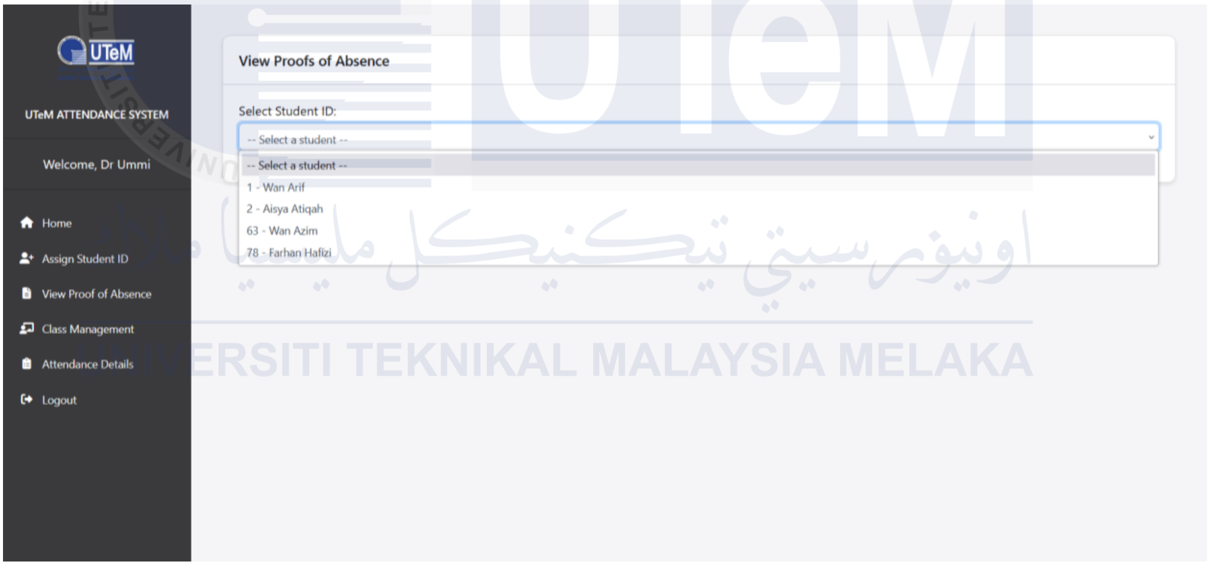
Student Name:

Class ID:

Result

No form data submitted.

Figure 4. 17 Lecturer Assign Student ID to Class page



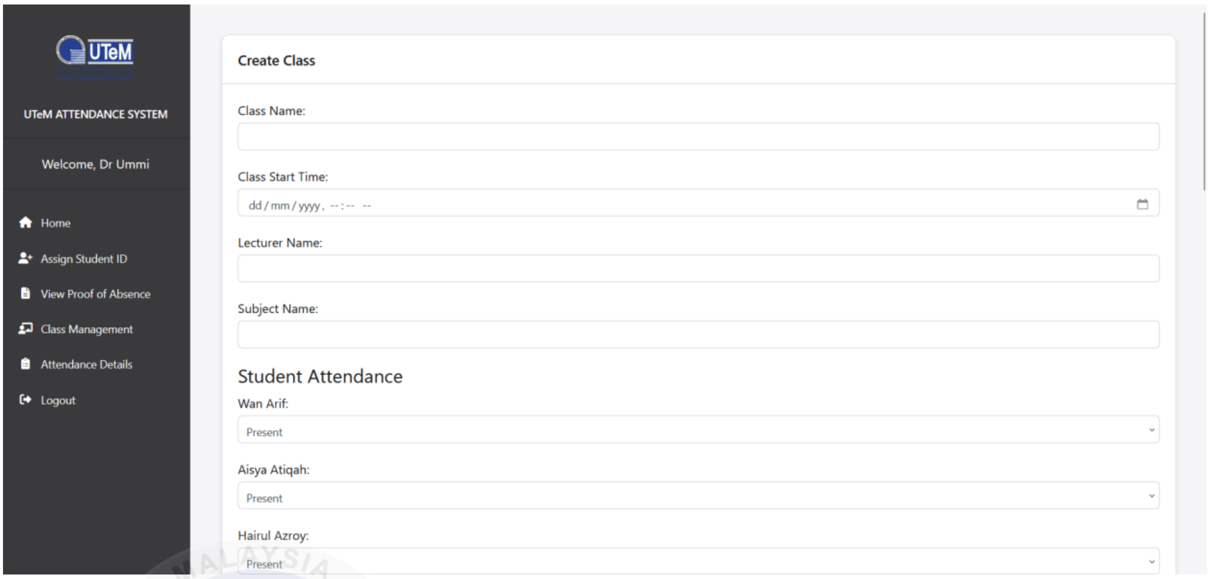
View Proofs of Absence

Select Student ID:

-- Select a student --

-- Select a student --
1 - Wan Arif
2 - Aisya Atiqah
63 - Wan Azim
78 - Farhan Hafizi

Figure 4. 18 Lecturer View Proofs of Absence page



Create Class

Class Name:

Class Start Time: dd / mm / yyyy , -- : -- --

Lecturer Name:

Subject Name:

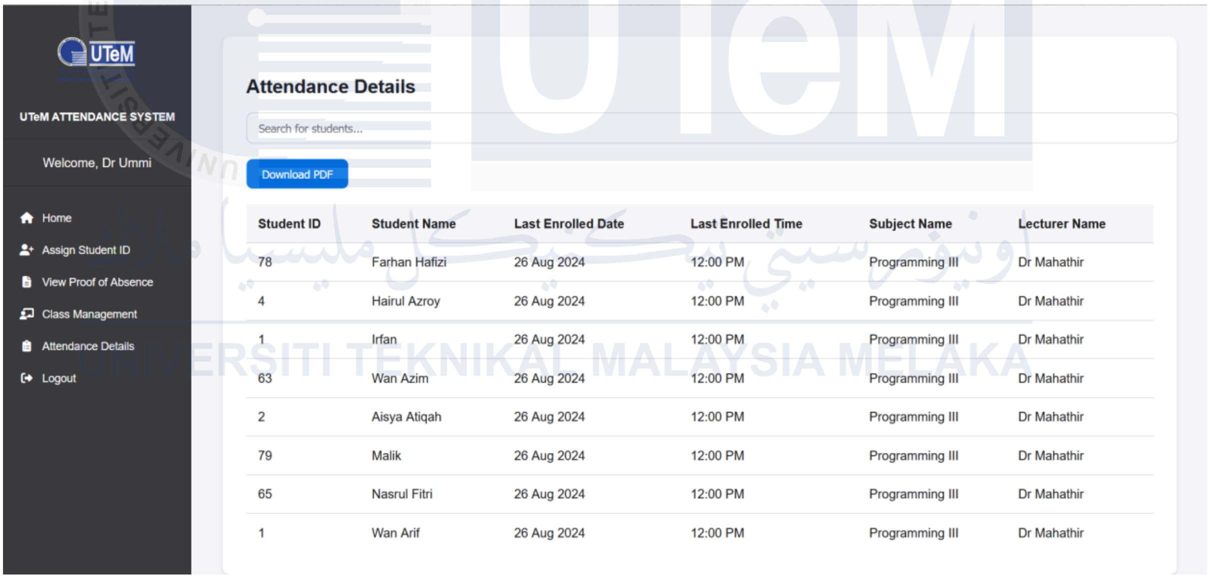
Student Attendance

Wan Arif: Present

Aisya Atiqah: Present

Hairul Azroy: Present

Figure 4. 19 Lecturer Class Management page



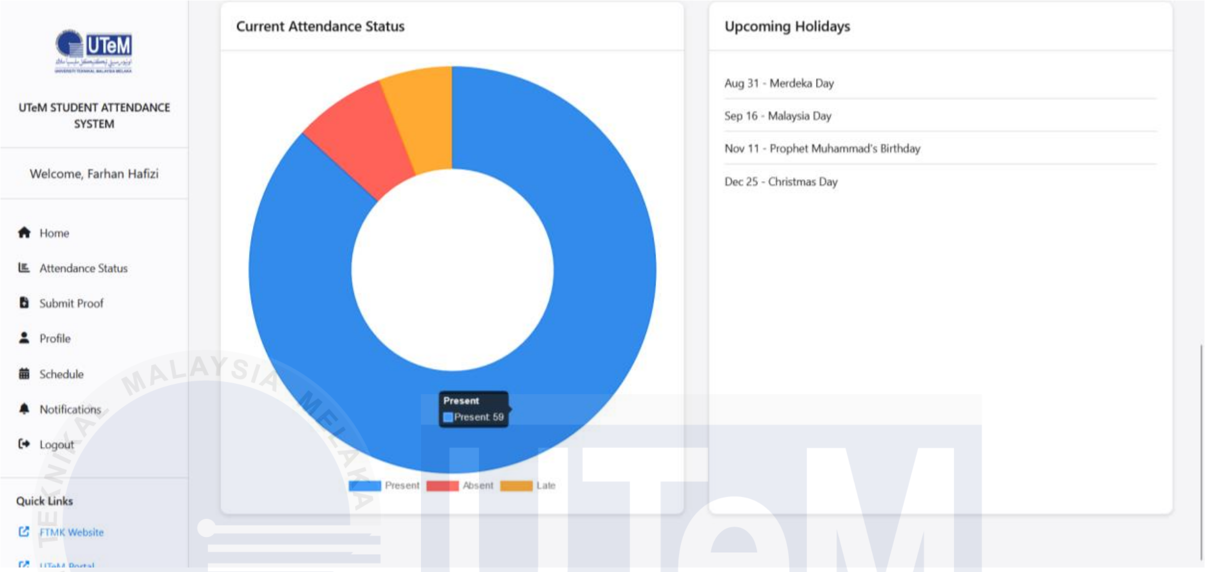
Attendance Details

Student ID	Student Name	Last Enrolled Date	Last Enrolled Time	Subject Name	Lecturer Name
78	Farhan Hafizi	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
4	Hairul Azroy	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
1	Irfan	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
63	Wan Azim	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
2	Aisya Atiqah	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
79	Malik	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
65	Nasrul Fitri	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
1	Wan Arif	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir

Figure 4. 20 Attendance Details page

c) Output Design

i) Student Side



UTeM STUDENT ATTENDANCE SYSTEM

Welcome, Farhan Hafizi

- Home
- Attendance Status
- Submit Proof
- Profile
- Schedule
- Notifications
- Logout

Quick Links

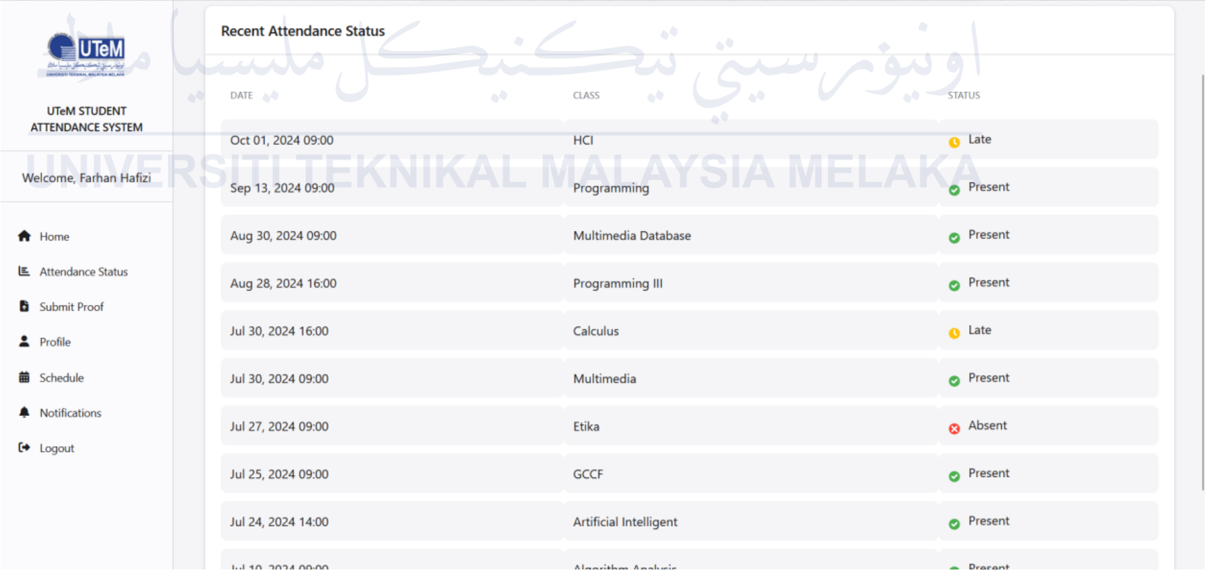
- FTMK Website
- UTeM Portal

Current Attendance Status

Upcoming Holidays

- Aug 31 - Merdeka Day
- Sep 16 - Malaysia Day
- Nov 11 - Prophet Muhammad's Birthday
- Dec 25 - Christmas Day

Figure 4. 21 Current Attendance Status Dashboard



UTeM STUDENT ATTENDANCE SYSTEM

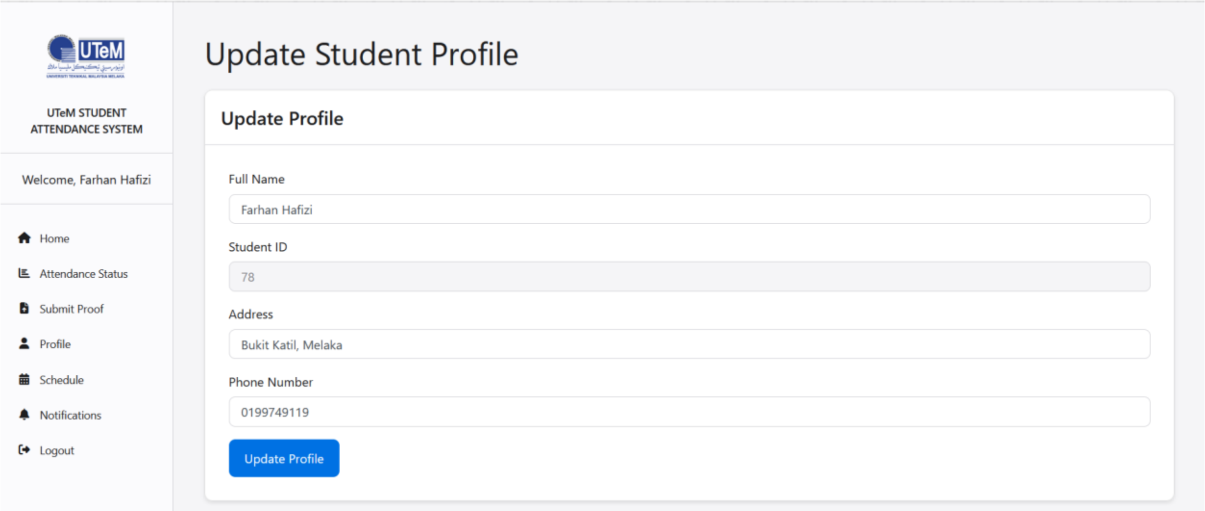
Welcome, Farhan Hafizi

- Home
- Attendance Status
- Submit Proof
- Profile
- Schedule
- Notifications
- Logout

Recent Attendance Status

DATE	CLASS	STATUS
Oct 01, 2024 09:00	HCI	Late
Sep 13, 2024 09:00	Programming	Present
Aug 30, 2024 09:00	Multimedia Database	Present
Aug 28, 2024 16:00	Programming III	Present
Jul 30, 2024 16:00	Calculus	Late
Jul 30, 2024 09:00	Multimedia	Present
Jul 27, 2024 09:00	Etika	Absent
Jul 25, 2024 09:00	GCCF	Present
Jul 24, 2024 14:00	Artificial Intelligent	Present
Jul 10, 2024 09:00	Algorithm Analysis	Present

Figure 4. 22 Recent Attendance Status for Every Subject



UTeM STUDENT ATTENDANCE SYSTEM

Welcome, Farhan Hafizi

Update Student Profile

Update Profile

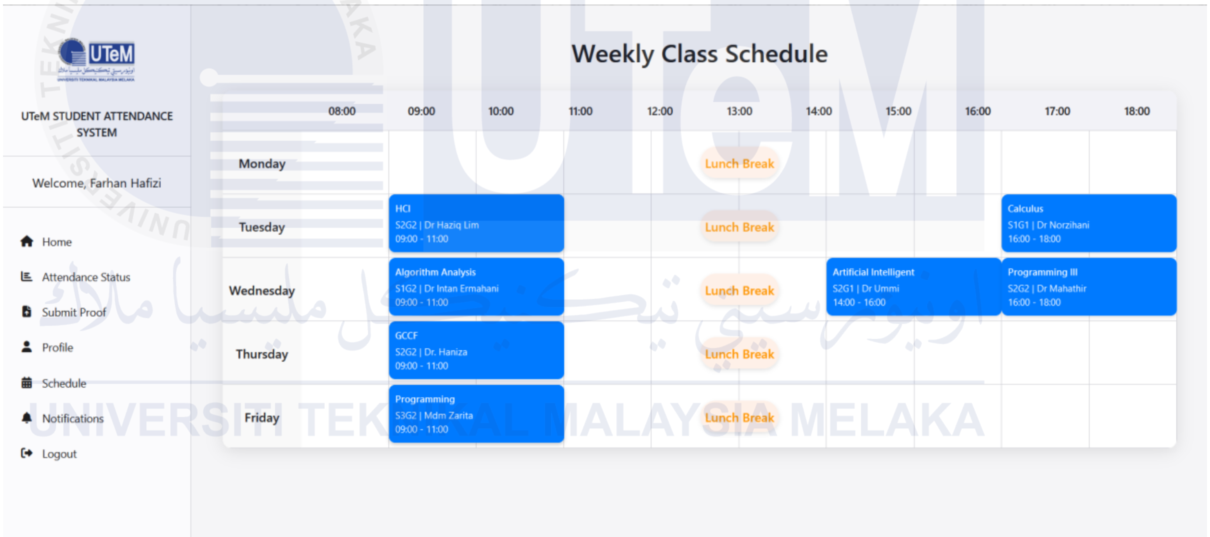
Full Name: Farhan Hafizi

Student ID: 78

Address: Bukit Katil, Melaka

Phone Number: 0199749119

Figure 4. 23 Student Profile



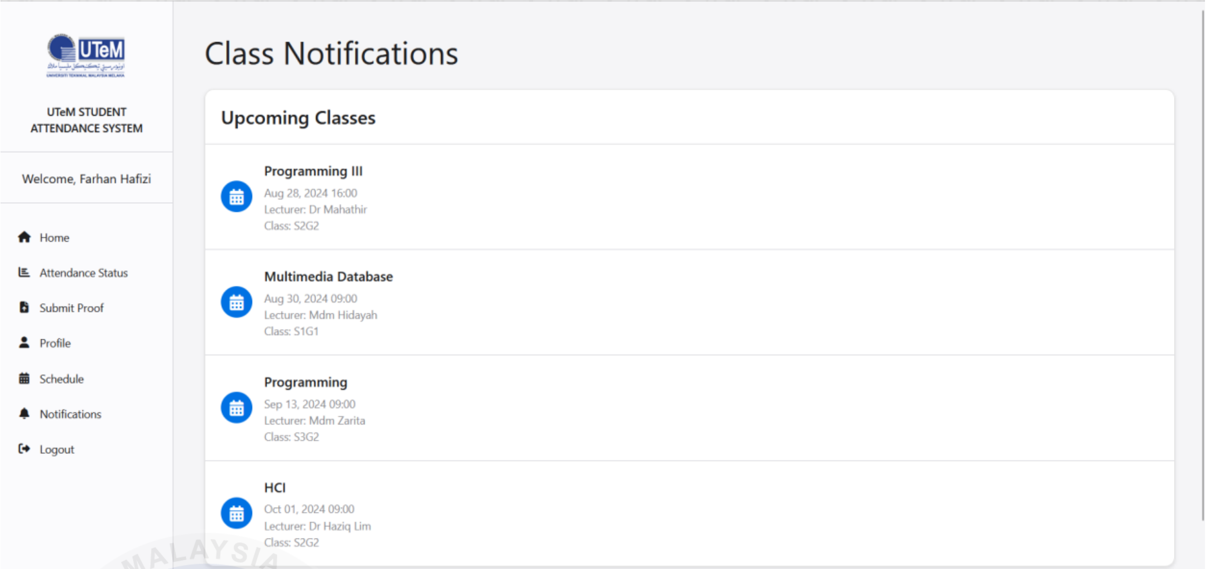
UTeM STUDENT ATTENDANCE SYSTEM

Welcome, Farhan Hafizi

Weekly Class Schedule

	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00
Monday						Lunch Break					
Tuesday		HCI S2G2 | Dr Haziq Lim 09:00 - 11:00				Lunch Break			Calculus S1G1 | Dr Norzihani 16:00 - 18:00		
Wednesday		Algorithm Analysis S1G2 | Dr Intan Ermahani 09:00 - 11:00				Lunch Break	Artificial Intelligent S2G1 | Dr Ummi 14:00 - 16:00		Programming III S2G2 | Dr Mahathir 16:00 - 18:00		
Thursday		GCCF S2G2 | Dr. Haniza 09:00 - 11:00				Lunch Break					
Friday		Programming S3G2 | Mdm Zarita 09:00 - 11:00				Lunch Break					

Figure 4. 24 Student Class Schedule



UTeM STUDENT ATTENDANCE SYSTEM

Welcome, Farhan Hafizi

- Home
- Attendance Status
- Submit Proof
- Profile
- Schedule
- Notifications
- Logout

Class Notifications

Upcoming Classes

Programming III
Aug 28, 2024 16:00
Lecturer: Dr Mahathir
Class: S2G2

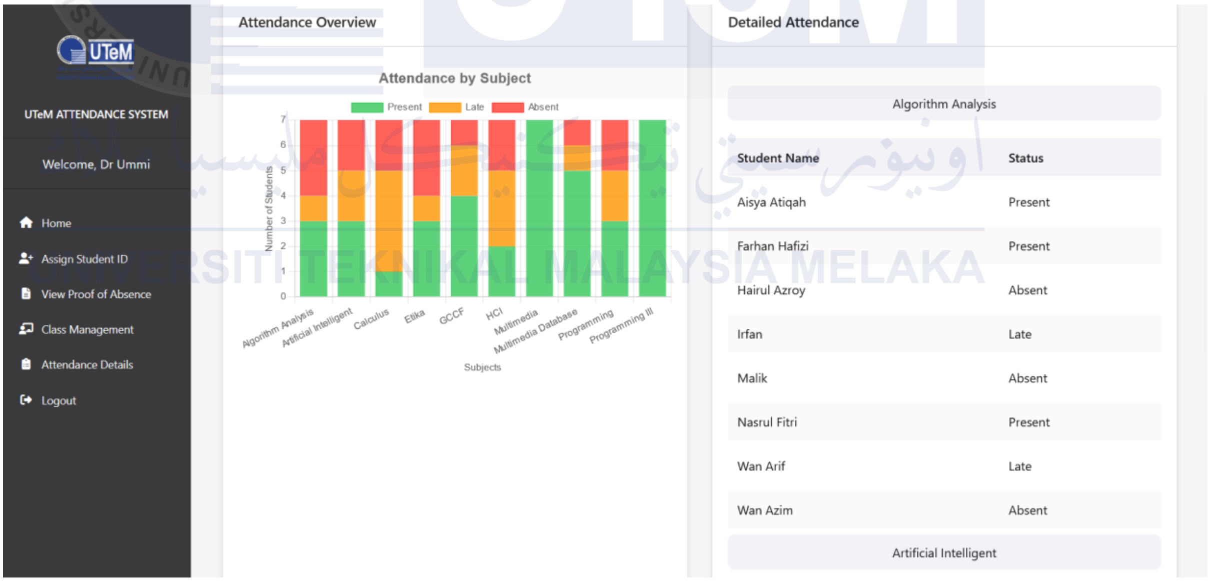
Multimedia Database
Aug 30, 2024 09:00
Lecturer: Mdm Hidayah
Class: S1G1

Programming
Sep 13, 2024 09:00
Lecturer: Mdm Zarita
Class: S3G2

HCI
Oct 01, 2024 09:00
Lecturer: Dr Haziq Lim
Class: S2G2

Figure 4. 25 Student Class Notifications

ii) Lecturer Side



UTeM ATTENDANCE SYSTEM

Welcome, Dr Ummi

- Home
- Assign Student ID
- View Proof of Absence
- Class Management
- Attendance Details
- Logout

Attendance Overview

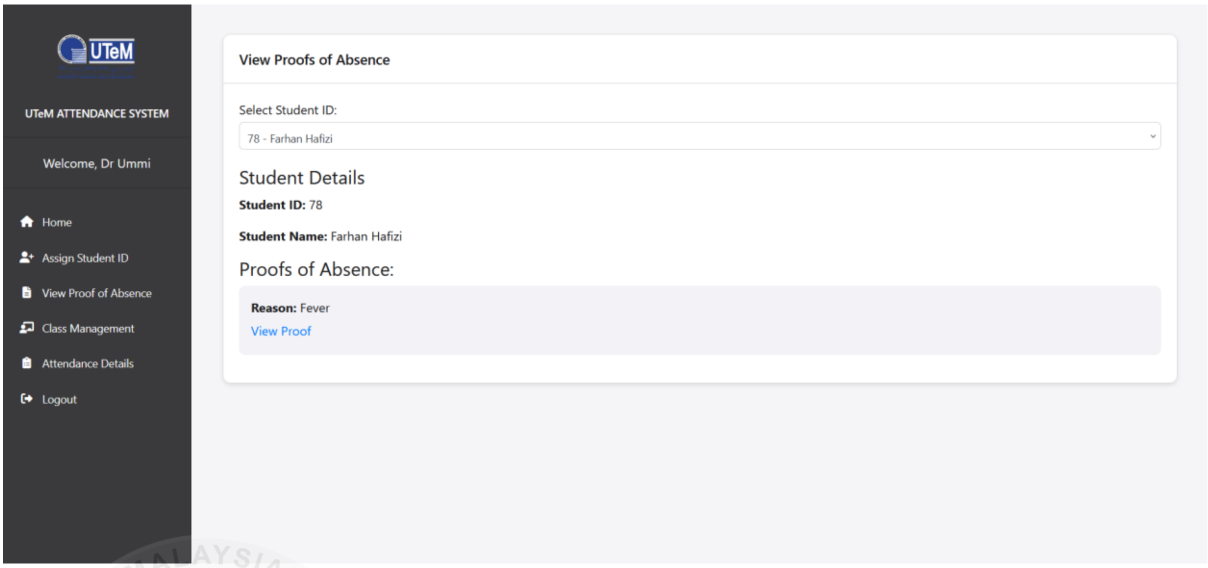
Detailed Attendance

Algorithm Analysis

Student Name	Status
Aisya Atiqah	Present
Farhan Hafizi	Present
Hairul Azroy	Absent
Irfan	Late
Malik	Absent
Nasrul Fitri	Present
Wan Arif	Late
Wan Azim	Absent

Artificial Intelligent

Figure 4. 26 Student Detailed Attendance Dashboard



View Proofs of Absence

Select Student ID:

78 - Farhan Hafizi

Student Details

Student ID: 78

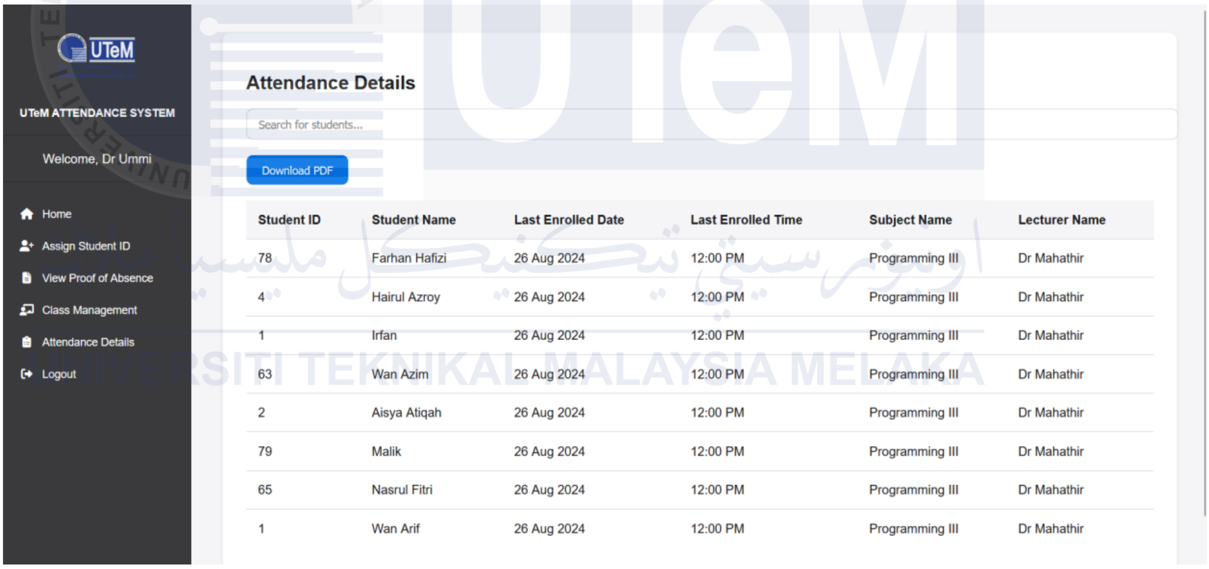
Student Name: Farhan Hafizi

Proofs of Absence:

Reason: Fever

View Proof

Figure 4. 27 Lecturer View Proof of Absence



Attendance Details

Student ID	Student Name	Last Enrolled Date	Last Enrolled Time	Subject Name	Lecturer Name
78	Farhan Hafizi	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
4	Hairul Azroy	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
1	Irfan	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
63	Wan Azim	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
2	Aisya Atiqah	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
79	Malik	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
65	Nasrul Fitri	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir
1	Wan Arif	26 Aug 2024	12:00 PM	Programming III	Dr Mahathir

Figure 4. 28 Lecturer View Student Attendance Details

4.2.3 Database Design

4.2.3.1 Conceptual and Logical Database Design

a) Entity Relationship Diagram (ERD)

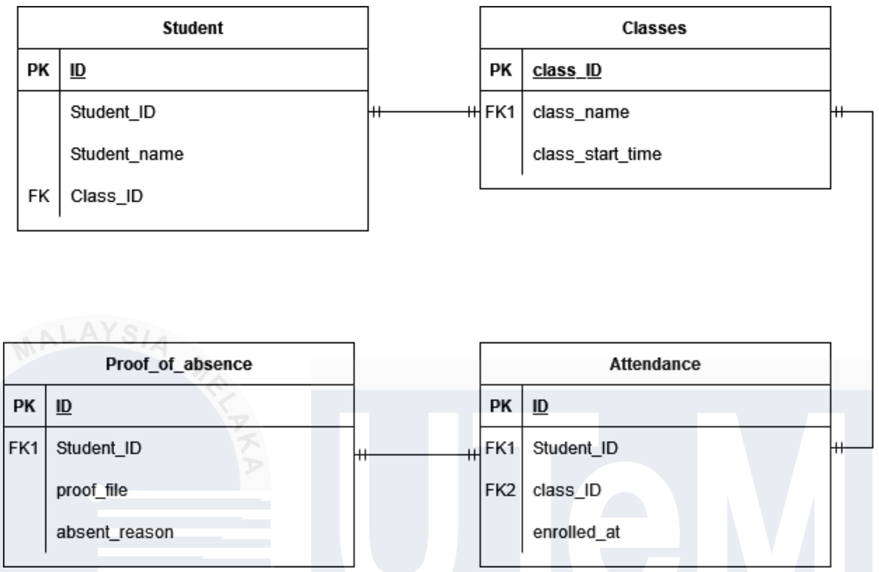


Figure 4. 29 ERD for Iot Based Fingerprint Biometric Attendance System

b) Data Dictionary

1. Detailed of Attendance table

No	Name	Data Type	Length	Constraint	Comment
1.	id	Int	11	PRIMARY KEY	-
2.	student_id	Int	11	FOREIGN KEY	-
3.	class_id	Int	11	NOT NULL	-
4.	enrolled_at	datetime	-	NOT NULL	-

2. Detailed of Student table

No	Name	Data Type	Length	Constraint	Comment
1.	id	Int	11	PRIMARY KEY	-
2.	student_id	Varchar	50	NOT NULL	-
3.	student_name	Varchar	100	NOT NULL	-
4.	Class_id	Varchar	50	FOREIGN KEY	-

3. Detailed of Classes table

No	Name	Data Type	Length	Constraint	Comment
1.	Class_id	Int	11	PRIMARY KEY	-
2.	Class_name	Varchar	255	NOT NULL	-
3.	Class_start_time	datetime	-	NOT NULL	-

4. Detailed of Proof of Absence

No	Name	Data Type	Length	Constraint	Comment
1.	id	Int	11	PRIMARY KEY	-
2.	Student_id	Varchar	50	FOREIGN KEY	-
3.	Proof_file	Varchar	255	NOT NULL	-
4.	Absent_reason	text	-	NULL	-

4.3 Detailed Design

4.3.1 Physical Database Design

Create Table : Attendance

```
CREATE TABLE Attendance (

id INT(11) NOT NULL AUTO_INCREMENT,

student_id INT(11),

class_id INT(11) NOT NULL,

enrolled_at DATETIME NOT NULL,

PRIMARY KEY (id),

FOREIGN KEY (student_id) REFERENCES Students(id),

CONSTRAINT fk_class_id

FOREIGN KEY (class_id) REFERENCES Classes(id)

);
```

Create Table : Student

```
CREATE TABLE student (

id INT(11) PRIMARY KEY AUTO_INCREMENT,

student_id VARCHAR(50) NOT NULL,

student_name VARCHAR(100) NOT NULL,

Class_id VARCHAR(50),

FOREIGN KEY (Class_id) REFERENCES Class(id)

);
```

Create Table : Classes

```
CREATE TABLE class (
Class_id INT(11) PRIMARY KEY,
Class_name VARCHAR(255) NOT NULL,
Class_start_time DATETIME NOT NULL
);
```

Create Table : Proof Of Absence

```
CREATE TABLE proof_of_absence (
id INT(11) PRIMARY KEY AUTO_INCREMENT,
Student_id VARCHAR(50),
Proof_file VARCHAR(255) NOT NULL,
Absent_reason TEXT,
FOREIGN KEY (Student_id) REFERENCES students(Student_id)
);
```

4.4 Conclusions

The design phase of the IoT-Based Fingerprint Biometric Attendance System has established a robust framework integrating Arduino Uno with Python scripts and MySQL databases to enhance attendance tracking efficiency and security. Arduino Uno and the fingerprint sensor form a reliable hardware core for biometric data capture, supporting accurate enrollment and verification processes. Python scripts facilitate seamless communication with the MySQL database, ensuring efficient data management and retrieval. A web-based interface developed with HTML, CSS, JavaScript, and PHP provides intuitive access for administrators and users to manage attendance and system settings across devices. Communication protocols like USB, serial, and HTTP/HTTPS guarantee secure data transmission, maintaining integrity and confidentiality. This phase sets a solid foundation for subsequent implementation, testing, and evaluation phases to validate the system's scalability, reliability, and adherence to security standards.

CHAPTER 5 : IMPLEMENTATION

5.1 Introduction

This chapter provides an overview of the implementation phase of the IoT-Based Fingerprint Biometric Attendance System using Arduino and AS608 Fingerprint Sensor. The implementation phase is crucial as it translates design concepts into a working system. This chapter details the steps involved in setting up the development environment, managing software configurations, and tracking version control to ensure seamless integration and functionality.

The activities covered include configuring the Arduino board, integrating the AS608 Fingerprint Sensor, developing the attendance tracking software, and managing version control to maintain a cohesive and reliable system. By the end of this phase, we expect to have a fully operational attendance system ready for testing, with all components integrated and properly managed.

5.2 Software Development Environment Setup

1. Sublime

Figure 5. 1 Sublime Text Editor

Based on Figure 5.1, I have chosen Sublime Text as the primary Integrated Development Environment (IDE) and source code editor. Sublime Text is a sophisticated and versatile text editor that is widely acclaimed for its exceptional performance, extensive plugin ecosystem, and cross-platform compatibility, making it an ideal choice for my project.

Sublime Text's robust support for a wide range of programming languages, including the ones required for this attendance system, allows me to work seamlessly without the need to switch between multiple editors. Its powerful features, such as code highlighting, code folding, and multi-cursor editing, enhance my productivity and streamline the development process. Additionally, Sublime Text's integration with various build systems and package managers further simplifies the management of project dependencies and the deployment of the attendance system.

2. Arduino IDE

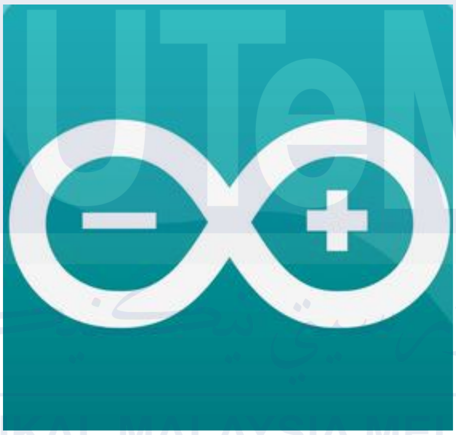


Figure 5. 2 Arduino IDE

Based on Figure 5.2, I have chosen to utilize the Arduino Integrated Development Environment (IDE) as the primary platform for coding and integrating the fingerprint sensor functionality. The Arduino IDE is a user-friendly, open-source software that provides a comprehensive set of tools and libraries specifically designed for programming and interfacing with Arduino boards and compatible microcontroller-based devices.

The Arduino IDE's intuitive interface, extensive documentation, and robust community support make it an ideal choice for this project, as it allows me to seamlessly write, compile, and upload the necessary code to the Arduino board, ensuring the proper integration and operation of the fingerprint sensor within the attendance system.

3. PyCharm Community Edition

Figure 5. 3 PyCharm Community Edition

Based on Figure 5.4, For the data storage and processing aspects of the IoT-Based Fingerprint Biometric Attendance System, I have selected PyCharm as the preferred Integrated Development Environment (IDE). PyCharm is a powerful and feature-rich Python IDE developed by JetBrains, renowned for its exceptional capabilities in supporting complex software development projects.

The PyCharm IDE's robust integration with various data storage and manipulation tools, as well as its seamless handling of file input/output operations, make it an optimal choice for implementing the functionality to capture fingerprint data and generate the corresponding attendance records in a text-based format. Its intuitive user interface, intelligent code completion, and extensive debugging capabilities streamline the development process and ensure the reliability and efficiency of the attendance system's data management components.

4. MySQL

Figure 5. 4 MySQL

Based on Figure 5.4, To manage the storage and retrieval of student, lecturer, and class data for the IoT-Based Fingerprint Biometric Attendance System, I have selected MySQL as the relational database management system (RDBMS) of choice. MySQL is a widely adopted, enterprise-grade database solution known for its reliability, scalability, and robust integration capabilities.

The utilization of MySQL allows me to establish a structured and secure data repository for the attendance system, facilitating the efficient storage, organization, and retrieval of the relevant information. This integration ensures the seamless integration of the attendance data with the system's web-based interface, enabling the display of attendance records and other relevant information to authorized users.

5.3 Software Configuration Management

5.3.1 Configuration Environment Setup

To develop the IoT-Based Fingerprint Biometric Attendance System, I have established a comprehensive software development environment to facilitate the integration of various components. For the fingerprint data capture and processing, I have chosen to utilize the AS608 Fingerprint Sensor, which will be programmed using the Arduino IDE. This allows me to seamlessly interface the sensor with the Arduino board and develop the necessary firmware to handle the fingerprint scanning and data generation.

The generated fingerprint data will then be processed and stored in a text file format using the PyCharm Integrated Development Environment (IDE). PyCharm's robust support for file input/output operations and data manipulation enables me to efficiently manage the attendance records in a structured text-based format.

To further enhance the system's functionality, I have integrated a MySQL relational database management system to store the attendance data. The MySQL database will serve as the central repository for student, lecturer, and class information, ensuring the secure and organized storage of the attendance records. The integration of MySQL with the system will be facilitated through the use of SQL queries and database management tools within the PyCharm IDE. Finally, to provide a user-friendly interface for accessing and visualizing the attendance data, I will develop a web-based application using a combination of HTML, CSS, and JavaScript. This web application will leverage the data stored in the MySQL database, retrieving and displaying the attendance records in a clear and intuitive manner, enabling authorized users to monitor and manage the attendance system effectively.

5.3.2 Version Control Procedure

Figure 5. 5 GitHub Desktop

For the version control management of the IoT-Based Fingerprint Biometric Attendance System, I have selected GitHub Desktop as the preferred tool to track and control all changes during the development phase. GitHub Desktop is a user-friendly, cross-platform application that seamlessly integrates with the Git version control system, providing a streamlined interface for managing the project's source code repository.

The utilization of GitHub Desktop enables me to efficiently manage and update the codebase, ensuring that all modifications are properly documented and synchronized across the development environment. This tool simplifies the version control process, allowing me to maintain a well-organized and traceable development workflow, where changes can be easily reviewed, merged, and rolled back as needed.

By leveraging the capabilities of GitHub Desktop, I can ensure the integrity and traceability of the IoT-Based Fingerprint Biometric Attendance System's codebase, facilitating seamless collaboration, code sharing, and version management throughout the project's lifecycle.

5.4 Implementation Status

The progress of the development status for each of the modules is shown below in the table:

Table 5. 1 Progress of the Development Status

Module	**Description**	**Duration to complete**	**Date completed**
Fingerprint scanning module	Module to capture and process fingerprint data from the AS608 Fingerprint Sensor	2 weeks	15/04/2024
Attendance Data Generation Module	Module to generate attendance records in a text file format using the captured fingerprint data	2 weeks	29/04/2023
Database Integration Module	Module to store the attendance data in the MySQL database and retrieve it as needed	3 weeks	20/05/2023
Web Application Development Module	Module to create a user-friendly web interface for accessing and visualizing the attendance data	3 weeks	10/06/2023
System Integration and Testing Module	Module to ensure seamless integration of all components and conduct comprehensive testing	2 weeks	24/06/2023

5.5 Conclusion

In this chapter, we have outlined the comprehensive implementation plan for the IoT-Based Fingerprint Biometric Attendance System, a project that aims to streamline the attendance tracking process through the integration of cutting-edge technologies.

Throughout the implementation phase, we have established a robust software development environment that leverages a range of tools and technologies to ensure the seamless integration and functionality of the system. By utilizing the Arduino IDE for the fingerprint sensor programming, PyCharm for the data processing and storage, and MySQL for the centralized database management, we have created a well-structured and scalable architecture that can efficiently handle the attendance data.

The version control aspect of the project has been meticulously addressed through the adoption of Git and the GitHub Desktop application. This has enabled us to maintain a comprehensive and traceable record of the codebase, facilitating collaboration, code sharing, and the ability to revert to previous versions if necessary. By following the detailed implementation plan, we have ensured that each module of the IoT-Based Fingerprint Biometric Attendance System is developed and integrated with the utmost care and attention to detail. The successful completion of this phase will pave the way for comprehensive testing and the eventual deployment of the system, providing a robust and reliable solution for automating and streamlining the attendance management process within the organization.

CHAPTER 6 : TESTING

6.1 Introduction

The software development lifecycle's testing and evaluation stage is essential for ensuring the created system satisfies the requirements and operates as planned. Thorough testing was conducted on the IoT-Based Fingerprint Biometric Attendance System to confirm its reliability, performance, and functionality. This chapter provides an overview of the testing methodologies employed, the test cases designed and executed, and the results obtained. The objective is to identify and rectify any issues, ensuring the system is robust, secure, and user-friendly.

The testing process began with unit tests, where individual components, such as the fingerprint scanning module, data generation module, and database integration, were evaluated in isolation to verify their correct operation. This was followed by integration testing, where the various modules were combined, and the system's overall functionality was assessed, ensuring seamless communication and data flow between the components. To validate the system's end-to-end performance, comprehensive system testing was carried out, simulating real-world scenarios and user interactions. This included testing the attendance tracking process, data storage and retrieval, and the web-based interface. Stress testing was also performed to evaluate the system's ability to handle high volumes of concurrent users and data processing demands.

Security testing was a crucial aspect of the evaluation, ensuring the system's resistance to unauthorized access, data breaches, and other potential vulnerabilities. Penetration testing, vulnerability scanning, and access control validation were conducted to identify and address any security weaknesses.

Finally, user acceptance testing was performed, involving the participation of end-users to gather feedback and validate the system's usability, user experience, and alignment with the specified requirements. This feedback was then used to refine the system and address any user-centric concerns. The comprehensive testing process has enabled the development team to identify and resolve any issues, ensuring the IoT-Based Fingerprint Biometric Attendance System is a robust, secure, and user-friendly solution that meets the organization's attendance management needs.

6.2 Test Plan

6.2.1 Test Organization

The testing process for the IoT-Based Fingerprint Biometric Attendance System involves a collaborative effort among three key individuals. As the lead developer, I am responsible for all aspects of the testing process, including designing and executing comprehensive test cases, managing the testing environment, and thoroughly documenting the results. This hands-on involvement allows me to identify and address any issues or discrepancies within the system, ensuring its robust functionality and adherence to the specified requirements.

The project supervisor plays a crucial advisory role in the testing phase. By providing guidance, reviewing the test plans and results, and ensuring the testing process aligns with industry best practices and academic standards, the supervisor helps to validate the thoroughness and rigor of the testing approach. Their expertise and oversight help to maintain the integrity and credibility of the testing activities.

Additionally, an independent evaluator will be brought in to review the final test results and verify that the IoT-Based Fingerprint Biometric Attendance System meets the required specifications and performance criteria. This unbiased assessment will provide an objective evaluation of the system's functionality, security, and overall effectiveness in meeting the organization's attendance management needs. The evaluator's feedback and recommendations will be instrumental in refining the system and ensuring its readiness for deployment.

By leveraging the collective expertise and responsibilities of the developer, supervisor, and evaluator, the testing process for the IoT-Based Fingerprint Biometric Attendance System will be comprehensive, rigorous, and aligned with industry standards, ultimately delivering a reliable and user-friendly solution to the organization.

6.2.2 Test Environment

The test environment for the IoT-Based Fingerprint Biometric Attendance System is a critical setup that ensures comprehensive testing during the system's development and validation phases. It consists of both hardware and software configurations specifically selected to support the diverse testing needs of the system, including performance, functionality, security, and usability. The hardware components of the test environment include the Arduino boards, AS608 Fingerprint Sensors, and development laptops or workstations. These devices closely mirror the actual deployment environment, allowing for realistic testing and validation of the system's hardware integration and performance.

On the software side, the test environment leverages a range of tools and platforms to facilitate thorough testing. The Arduino IDE is used for programming and testing the firmware responsible for the fingerprint scanning and data processing. The PyCharm IDE is employed for testing the data generation, storage, and retrieval functionalities, ensuring the seamless integration of the attendance data with the MySQL database.

To validate the web-based interface and the system's overall functionality, the test environment incorporates tools such as Postman for API testing and web browsers for user interface validation. These software components enable the development team to simulate real-world user interactions, test the system's responsiveness, and ensure the alignment of the web application with the specified requirements. Additionally, the test environment includes stable internet connectivity and cloud-based services, as needed, to replicate the production environment and test the system's performance under various network conditions and load scenarios.

By establishing a comprehensive and well-designed test environment, the development team can rigorously validate the IoT-Based Fingerprint Biometric Attendance System, identifying and addressing any issues or vulnerabilities before the final deployment. This approach ensures the system's reliability, security, and user-friendliness, meeting the organization's attendance management needs.

Table 6. 1 Detailed Test Environment Configuration for IoT Based Fingerprint Biometric Attendance System

Test Environment	Requirement	Description
Hardware Configuration	Laptop	The development team will utilize laptops equipped with Windows 10 or above, providing sufficient processing power, memory, and storage to support the development and testing tools required for the project.
	Arduino board and Fingerprint Sensor	The test environment will include the Arduino boards and AS608 Fingerprint Sensors that are the core hardware components of the attendance system. This will enable the team to test the integration and functionality of the fingerprint scanning capabilities.
	Internet connectivity	A stable internet connection is essential for accessing online resources, version control systems during the development and testing phases.
Software Configuration	Arduino IDE	The Arduino Integrated Development Environment (IDE) will be used to program and test the firmware responsible for the fingerprint scanning and data processing on the Arduino boards.
	PyCharm IDE	The PyCharm Integrated Development Environment (IDE) will be utilized for developing, testing, and validating the data generation, storage, and retrieval functionalities, ensuring the seamless integration with the MySQL database.
	MySQL Database	A MySQL database instance will be set up within the test environment to simulate the production-like data storage and retrieval operations for the attendance records.
	Web Browsers	Popular web browsers, such as Google Chrome, Mozilla Firefox, and Microsoft Edge, will be used to test the user interface and user experience of the web-based attendance management application.

6.2.3 Test Schedule

The test schedule for the IoT-Based Fingerprint Biometric Attendance System outlines the specific testing cycles and their corresponding durations. It provides a structured timeline detailing the different phases of testing, including Unit Testing, Integration Testing, System Testing, Security Testing, and Acceptance Testing. Each phase focuses on a particular aspect of the system, from validating individual components to ensuring the overall functionality, security, and user experience.

The Unit Testing phase is dedicated to validating the individual components of the system, such as the fingerprint scanning module, attendance data generation module, and database integration. By testing these components in isolation, the development team can ensure the correct operation of each module and identify any issues early in the development process. This phase is crucial for establishing a solid foundation for the system's reliability.

Integration Testing follows, where the various modules of the system are combined, and the team evaluates the seamless integration and communication between them. This includes testing the data flow from the fingerprint sensor to the data generation, storage, and retrieval processes, as well as the integration of the web-based interface with the backend services. This phase ensures that all components work together harmoniously.

The System Testing phase involves comprehensive end-to-end testing, simulating real-world attendance tracking scenarios and user interactions. This includes validating the attendance recording process, the performance of the system under varying loads, and the overall functionality of the IoT-Based Fingerprint Biometric Attendance System. This phase is critical for identifying any issues that may arise from the complete system integration.

Security Testing is a vital phase that focuses on ensuring the robustness and protection of the attendance system. This includes conducting penetration testing, vulnerability scanning, and access control validation to identify and address any potential security weaknesses. Given the sensitive nature of biometric and attendance data, this phase is crucial for maintaining the system's integrity and user trust.

The final phase, Acceptance Testing, involves evaluating the system with end-users to validate its alignment with the specified requirements, usability, and user experience. The feedback gathered during this phase is invaluable for refining the system and addressing any user-centric concerns, ensuring that the final product meets the needs and expectations of its intended users.

By following this structured test schedule, the development team can ensure a comprehensive and systematic approach to validating the IoT-Based Fingerprint Biometric Attendance System. This methodical testing process allows for the identification and resolution of any issues before the final deployment, resulting in a robust, secure, and user-friendly attendance management solution.

Table 6. 2 IoT Based Fingerprint Biometric Attendance System Test Schedule and Duration

Task Name	Task Description	Start Date	End Date	Duration
Unit Testing	Detailed examination and validation of individual components and features within the IoT-Based Fingerprint Biometric Attendance System, such as the fingerprint scanning module, attendance data generation, and database integration.	15/07/2024	19/07/2024	5 days
Integration Testing	Testing the combined modules within the IoT-Based Fingerprint Biometric Attendance System to ensure	20/07/2024	25/07/2024	6 days

	seamless data flow and proper functioning between components like the fingerprint sensor, data generation, database integration, and the web application.			
System Testing	Comprehensive evaluation of the entire IoT-Based Fingerprint Biometric Attendance System, including performance, reliability, and compliance with specified requirements. This includes stress testing to handle high volumes of concurrent users and data processing demands.	26/07/2024	03/08/2024	9 days
Acceptance Testing	Final evaluation by end-users or stakeholders to verify system readiness for deployment. This includes real-world testing and gathering feedback on the system's functionality, usability, and alignment with requirements.	04/08/2024	10/08/2024	7 days
Usability Testing	Final evaluation by end-users or stakeholders to verify system readiness for deployment. This includes real-world testing and	11/08/2024	15/08/2024	5 days

	gathering feedback on the system's functionality, usability, and alignment with requirements.			

6.3 Test Strategy

6.3.1 Classes of Tests

The testing phases for the IoT-Based Fingerprint Biometric Attendance System are critical in ensuring that the software meets its functional and non-functional requirements, delivering a reliable, secure, and user-friendly experience. These phases include Unit Testing, Integration Testing, System Testing, Security Testing, and Acceptance Testing, each of which plays a vital role in the development and deployment of the attendance system.

1. **Unit Testing**

Unit testing checks individual components of the IoT-Based Fingerprint Biometric Attendance System to ensure they work as expected. Developers test features like fingerprint scanning, data processing, and database interactions. For example, it ensures that when a fingerprint is scanned, it's correctly processed and stored. This testing happens during development to verify the reliability of each part before integrating them into the system.

2. **Integration Testing**

Integration testing checks if different parts of the IoT-Based Fingerprint Biometric Attendance System work together smoothly. It ensures that data from the fingerprint sensor flows correctly to the Arduino board, then to the database, and finally displays accurately on the web interface. This phase helps catch any issues that occur when combining components, ensuring they work together as expected.

3. System Testing

System testing evaluates the entire IoT-Based Fingerprint Biometric Attendance System, ensuring all components work together seamlessly. The QA team checks performance, reliability, and compliance with requirements. This includes verifying that fingerprints are accurately scanned and matched, attendance records are correctly stored and retrieved, and the web interface displays information promptly. System testing also involves stress tests to ensure the system can handle multiple users and high volumes of data without issues, ensuring the attendance system meets both functional and non-functional requirements.

4. Acceptance Testing

Acceptance testing is the final step where the IoT-Based Fingerprint Biometric Attendance System is tested by end-users or stakeholders to ensure it's ready for deployment. This testing happens in real-world environments, like classrooms or offices, where users provide feedback on usability, functionality, and performance. It ensures the attendance system meets user expectations and is fully prepared for release, with adjustments made based on the feedback to guarantee user satisfaction.

5. Usability Testing

Usability Testing is focused on evaluating how easy and intuitive the IoT-Based Fingerprint Biometric Attendance System is for users. This testing ensures that the web interface is user-friendly, allowing users to navigate through features like viewing attendance records, generating reports, and managing user profiles without difficulty. The goal is to identify any user experience issues and make necessary improvements, ensuring that even those with limited technical skills can use the system effectively. By addressing feedback from this testing phase, the attendance system can provide a smoother and more satisfying user experience.

6.4 Test Design

6.4.1 Test Description

This section provides a detailed explanation of the test cases designed to verify the functional requirements of the IoT-Based Fingerprint Biometric Attendance System. Each functional requirement is mapped to specific test cases that target key modules, such as Fingerprint Scanning, Attendance Recording, Data Storage, and Web Interface. The tests are aimed at validating the system's behaviour in real-world scenarios, ensuring that the system performs as expected across various functionalities.

The description of each test case outlines the purpose, testing criteria, and expected results, as shown in Table 6.3: IoT-Based Fingerprint Biometric Attendance System Functional Requirements and Test Cases Overview. This comprehensive approach ensures that the system meets its functional goals and satisfies user requirements.

For instance, the Fingerprint Scanning module tests will verify the accuracy and speed of fingerprint capture and matching. The Attendance Recording module tests will ensure that attendance data is correctly recorded and timestamped. Data Storage tests will validate the integrity and security of stored attendance records. Web Interface tests will confirm that users can easily access and interpret attendance data, generate reports, and manage system settings.

By thoroughly testing each component and their interactions, we can guarantee that the IoT-Based Fingerprint Biometric Attendance System functions reliably in various scenarios, from individual attendance marking to bulk data processing and reporting. This rigorous testing approach helps identify and address any potential issues before deployment, ensuring a robust and user-friendly attendance management solution.

Table 6. 3 IoT-Based Fingerprint Biometric Attendance System Functional Requirements and Test Cases Overview

Functional Requirement Id	Test Requirement Id	Module Name	Description	Expected Results
FR 1	T01	Registration Module	Validate the identity of students during the registration process by capturing their biometric data (fingerprints).	The system successfully captures and stores the student's fingerprint data during registration.
FR1	T02	Registration Module	Verify that the system correctly associates the captured fingerprint with the student's identity.	The system confirms the fingerprint is linked to the correct student profile.
FR2	T03	Authentication Module	Validate fingerprint scans against stored biometric data to authenticate students during each attendance event.	The system accurately matches the scanned fingerprint with the stored data, and the student is marked present.
FR3	T04	Attendance Module	Validate the captured fingerprint record by the timestamp when a student scans their fingerprint with stored data to ensure	The system records the timestamp of the fingerprint scan and matches it with stored data

			accurate attendance marking.	to mark attendance correctly.
FR4	T05	Schedule Validation Module	Validate attendance records by cross-referencing the student’s class schedule to ensure attendance is marked for the correct class timing.	The system verifies the student’s attendance against their class schedule and accurately records the attendance for the correct class.
FR5	T06	Real-Time Processing Module	Validate the processing of attendance data in real-time to ensure up-to-date records.	The system updates attendance records immediately after a fingerprint scan.
FR6	T07	Database Module	Validate the secure storage of attendance records in a central database, ensuring data integrity and accessibility.	Attendance records are securely stored in the central database and are accessible for retrieval.
FR7	T08	Reporting Module	Validate the generation of attendance reports on a daily, weekly, and monthly basis to provide	The system generates accurate attendance reports for the specified periods.

			comprehensive records.	
FR8	T09	Real-Time Status Module	Validate the provision of real-time attendance status for ongoing classes, enabling instant access to current attendance information.	The system displays real-time attendance status for ongoing classes.
FR9	T10	Notification Module	Validate the sending of notifications for absenteeism or late arrivals to students, teachers, and administrators to keep all parties informed.	The system successfully sends notifications regarding absenteeism or late arrivals.
FR10	T11	Student Interface Module	Validate the provision of a user-friendly interface for students to check their attendance status, ensuring ease of use.	The interface allows students to easily check their attendance status.
FR11	T12	Administrative Interface Module	Validate the provision of administrative interfaces for managing student data, schedules, and generating reports,	The administrative interface allows for efficient management of student data, schedules, and report generation.

			facilitating efficient administration.	
FR12	T13	Security Module	Validate the security and privacy of biometric data and personal information through encryption and secure storage methods.	The system encrypts and securely stores biometric data and personal information, ensuring data privacy.

6.4.2 Traceability Matrix

The traceability matrix in this section establishes a clear link between the functional requirements (FRs) and the corresponding test cases (TCs) for the IoT-based fingerprint biometric attendance system using the AS608 fingerprint sensor. It ensures that all requirements are adequately tested by mapping each test case to its associated functional requirement. This matrix provides an organized structure to verify that the system's features have been validated through appropriate testing, ensuring that each requirement is met by specific test cases. It also helps in tracking testing progress and ensuring complete coverage of the system functionalities during the testing process, as outlined in Table 6.4.

Table 6. 4 IoT Based Fingerprint Biometric Attendance System for Functional Requirements and Test Cases

Test Requirement ID	Test Case ID	Description
T01	TC01	Validate the identity of students during the registration process by capturing their biometric data (fingerprints).
	TC02	Validate the system correctly associates the captured fingerprint with the student’s identity.
	TC03	Validate that the captured fingerprint data is stored securely in the system.

T02	UC01	Verify that the system accurately authenticates students during each attendance event by matching the fingerprint scan with stored data.
T03	UC02	Validate that the system accurately timestamps the fingerprint scan to ensure correct attendance marking.
T04	UC03	Verify that attendance is marked for the correct class timing by cross-referencing the student's class schedule.
T05	UC04	Verify that attendance data is processed in real-time to ensure up-to-date records.
T06	UC05	Verify that attendance records are stored securely in a central database, ensuring data integrity and accessibility.
T07	UC06	Verify that the system generates attendance reports on a daily, weekly, and monthly basis.
T08	UC07	Verify that the system provides real-time attendance status for ongoing classes.
T09	UC08	Verify that the system sends notifications for absenteeism or late arrivals to students, teachers, and administrators.
T10	UC09	Verify that students can easily check their attendance status through the user-friendly interface.
T11	UC10	Verify that the administrative interface allows efficient management of student data, schedules, and report generation.
T12	UC11	Verify that the system ensures the security and privacy of biometric data and personal information through encryption and secure storage methods.

6.5 Test Result and Analysis

6.5.1 Test Cases

A. Black Box Technique 1 : Equivalence Partitioning Testing

1. **T01 : Validates the identity of students during the registration process by capturing their biometric data (fingerprints).**

Table 6. 5 Test Cases TC01-TC03

Test Case ID	Partition Tested	Test Data	Test Steps	Expected Results	Actual Results	Status
TC01	Valid biometric capture	Fingerprint: New student	1. The student places their finger on the sensor during registration. 2. The system captures and stores the fingerprint data.	Fingerprint is successfully captured and associated with the student's profile.	Fingerprint captured and stored.	Pass
TC02	Invalid biometric capture (Unreadable fingerprint)	Fingerprint: Unreadable data	1. The student places their finger on the sensor during	System prompts for a retry if the fingerprint is unreadable.	System prompted for retry.	Pass

			registration. 2. The system attempts to capture the fingerprint.			
TC03	Valid authentication	Fingerprint: Registered data	1. The student places their finger on the sensor for attendance. 2. The system matches the fingerprint with stored data.	Fingerprint is successfully authenticated, and attendance is marked.	Authentication successful.	Pass

B. Black box Technique 2: Use Case Testing

2. **T02: Verify that the system accurately authenticates students during each attendance event by matching the fingerprint scan with stored data.**

Table 6. 6 Test Case UC01

Test Case ID	UC01
Use Case Name	Verify user username and password
Use Case Description	The process to log into the account
Actor	Student / Lecturer
Pre-Conditions	The student/lecturer must already have an Account.
Test Data	Username: farhanhafizi Password: abc1234_

Basic Flow	1. User clicks “Username”. 2. User enters the username. 3. User clicks “Password”. 4. User enters password. 5. User clicks the “Login” button.
Post Conditions	The account is successfully signed in.
Alternate Flows	An error message will display if the user enters the wrong username or password
Expected Results	The user is successfully logged into the app and redirected to the homepage.
Actual Results	The user is successfully logged into the app and redirected to the homepage.
Status	Success

Table 6. 7 Test Case UC02

Test Case ID	UC02
Use Case Name	Validate that the system accurately timestamps the fingerprint scan
Use Case Description	Ensures correct attendance marking by timestamping the fingerprint scan
Actor	Student
Pre-Conditions	The student must be registered with their fingerprint in the system.
Test Data	Student Fingerprints
Basic Flow	1. Student scans their fingerprint on the sensor. 2. The system reads the fingerprint and compares it with stored data. 3. The system timestamps the scan.
Post Conditions	The timestamp is successfully recorded with the fingerprint scan.
Alternate Flows	An error message will display if the fingerprint scan fails or does not match stored data.
Expected Results	The fingerprint scan is accurately timestamped, ensuring correct attendance marking.

Actual Results	The fingerprint scan is accurately timestamped, ensuring correct attendance marking.
Status	Success

Table 6. 8 Test Case UC03

Test Case ID	UC03
Use Case Name	Validate attendance records by cross-referencing the student’s class schedule
Use Case Description	Ensures attendance is marked for the correct class timing
Actor	System
Pre-Conditions	The student must be registered and have a valid class schedule in the system
Test Data	Fingerprint ID: 45 Class Schedule: Mon 5/8/2024 09:00 AM
Basic Flow	1. Student scans their fingerprint. 2. System retrieves the current timestamp. 3. System cross-references the timestamp with the student's class schedule.
Post Conditions	Attendance is correctly marked for the class associated with the timestamp.
Alternate Flows	An error message will display if the class timing does not match or the student is not enrolled.
Expected Results	The system successfully cross-references the timestamp with the class schedule to mark attendance.
Actual Results	The system successfully cross-references the timestamp with the class schedule to mark attendance.
Status	Success

Table 6. 9 Test Case UC04

Test Case ID	UC04
Use Case Name	Validate real-time processing of attendance data
Use Case Description	Ensures attendance records are up-to-date
Actor	System
Pre-Conditions	The student must be registered and logged in
Test Data	Fingerprint ID: 66
Basic Flow	1. Student scans their fingerprint. 2. System processes the fingerprint data in real-time. 3. Attendance data is updated immediately.
Post Conditions	The attendance record is updated in real-time.
Alternate Flows	Delays or errors may occur if the system experiences a processing issue.
Expected Results	The attendance data is processed and updated in real-time.
Actual Results	The attendance data is processed and updated in real-time.
Status	Success

Table 6. 10 Test Case UC05

Test Case ID	UC05
Use Case Name	Validate secure storage of attendance records
Use Case Description	Ensures data integrity and accessibility
Actor	System
Pre-Conditions	Database is online and accessible
Test Data	Fingerprint ID: 66 Attendance Status : Present
Basic Flow	1. Student scans their fingerprint. 2. System verifies the fingerprint. 3. Attendance data is securely stored in the database.

Post Conditions	Attendance records are securely stored in the database.
Alternate Flows	An error message will display if the system cannot store the data due to a database issue.
Expected Results	The attendance records are securely stored and can be accessed as needed.
Actual Results	The attendance records are securely stored and can be accessed as needed.
Status	Success

Table 6. 11 Test Case UC06

Test Case ID	UC06
Use Case Name	Validate generation of attendance reports
Use Case Description	Ensures comprehensive records for daily, weekly, and monthly attendance
Actor	System
Pre-Conditions	Attendance data must be stored in the database
Test Data	Report Data: Weekly Attendance Report Date Range: 01/08/2024 - 07/08/2024
Basic Flow	1. System generates a report based on the stored attendance data. 2. Report is compiled and formatted.
Post Conditions	The report is successfully generated and can be viewed or downloaded
Alternate Flows	An error message will display if there is insufficient data or a system error occurs.
Expected Results	The attendance report is generated accurately and reflects all recorded attendance.
Actual Results	The attendance report is generated accurately and reflects all recorded attendance.
Status	Success

Table 6. 12 Test Case UC07

Test Case ID	UC07
Use Case Name	Validate real-time attendance status updates
Use Case Description	Provides instant access to current attendance information
Actor	System
Pre-Conditions	Students must be enrolled and actively attending classes
Test Data	Fingerprint ID: 45
Basic Flow	1. Student scans their fingerprint. 2. System updates the attendance status in real-time. 3. The real-time status is displayed.
Post Conditions	The real-time attendance status is updated and displayed accurately.
Alternate Flows	An error message will display if the system fails to update the status.
Expected Results	The attendance status is updated and displayed in real-time.
Actual Results	The attendance status is updated and displayed in real-time.
Status	Success

Table 6. 13 Test Case UC08

Test Case ID	UC08
Use Case Name	Validate notifications for absenteeism or late arrivals
Use Case Description	Keeps students, teachers, and administrators informed
Actor	System
Pre-Conditions	Students must be registered with their contact information
Test Data	Notification Data: Absenteeism Alert for 07/08/2024

Basic Flow	1. System detects absenteeism or late arrival. 2. Notification is generated. 3. Notification is sent to the relevant parties.
Post Conditions	Notifications are sent to the appropriate recipients.
Alternate Flows	An error message will display if the notification fails to send.
Expected Results	Notifications are sent to the relevant parties, informing them of absenteeism or late arrivals.
Actual Results	Notifications are sent to the relevant parties, informing them of absenteeism or late arrivals.
Status	Success

Table 6. 14 Test Case UC09

Test Case ID	UC09
Use Case Name	Validate user-friendly interface for students to check attendance
Use Case Description	Ensures ease of use for students
Actor	Student
Pre-Conditions	Students must have a valid account and login credentials
Test Data	Username: Aisya Atiqah Password: aisya1234
Basic Flow	1. Student logs into the system. 2. Student navigates to the attendance status page. 3. Attendance status is displayed.
Post Conditions	The student can easily check their attendance status.
Alternate Flows	An error message will display if the student cannot access the attendance status.
Expected Results	The interface is user-friendly, and students can easily check their attendance status.
Actual Results	The interface is user-friendly, and students can easily check their attendance status.
Status	Success

Table 6. 15 Test Case UC10

Test Case ID	UC10
Use Case Name	Validate administrative interfaces for managing student data and schedules
Use Case Description	Facilitates efficient administration
Actor	Administrator
Pre-Conditions	Admins must have valid login credentials and access to the system
Test Data	Username: admin1 Password: adminPass
Basic Flow	1. Admin logs into the system. 2. Admin navigates to the student data management interface. 3. Admin updates or reviews student data and schedules.
Post Conditions	The admin can efficiently manage student data and schedules.
Alternate Flows	An error message will display if the admin encounters issues accessing or updating data.
Expected Results	The administrative interface allows efficient management of student data and schedules.
Actual Results	The administrative interface allows efficient management of student data and schedules.
Status	Success

Table 6. 16 Test Case UC11

Test Case ID	UC11
Use Case Name	Validate security and privacy of biometric data and personal information
Use Case Description	Ensures secure encryption and storage
Actor	System
Pre-Conditions	System encryption protocols must be active
Test Data	Fingerprint Data: Encrypted Fingerprint ID Personal Info: Encrypted
Basic Flow	1. System captures fingerprint data. 2. System encrypts the biometric and personal information. 3. Data is securely stored.
Post Conditions	The biometric data and personal information are securely encrypted and stored.
Alternate Flows	An error message will display if the system fails to encrypt or store the data securely.
Expected Results	The biometric data and personal information are securely encrypted and stored.
Actual Results	The biometric data and personal information are securely encrypted and stored.
Status	Success

6.6 Conclusion

In this chapter, a comprehensive analysis of the testing strategies employed for the IoT-based fingerprint biometric attendance system using the fingerprint sensor AS608 has been provided. Detailed testing phases, including Unit Testing, Integration Testing, System Testing, Acceptance Testing, and Usability Testing, were discussed to ensure the system met both functional and non-functional requirements. The test environment, including the necessary hardware and software configurations, was defined to facilitate accurate testing conditions.

The results from testing highlighted the system's progression, from early feedback focused on functionality improvements to later praise for its reliable performance in accurately capturing and processing attendance data. These insights were critical in refining the system and ensuring its readiness for deployment. In the final chapter, the outcomes of the research project will be reviewed, alongside a broader discussion of its potential impact and areas for future development.

CHAPTER 7 : PROJECT CONCLUSION

7.1 Observation on Weaknesses and Strengths

The IoT-based fingerprint biometric attendance system using the fingerprint sensor AS608 stands out for its innovative approach to attendance management. One of its key strengths is the integration of biometric authentication, which ensures accurate identification of students and minimizes the risk of fraudulent attendance records. The use of advanced technologies, such as IoT for real-time data processing and secure backend infrastructure, ensures that attendance data is captured, processed, and stored efficiently. Additionally, the system's ability to generate comprehensive attendance reports on a daily, weekly, and monthly basis provides valuable insights for administrators, helping them to track and manage student attendance effectively.

Another strength of the system is its user-friendly interface, which allows students to easily check their attendance status and provides administrators with intuitive tools for managing student data and generating reports. The inclusion of real-time notifications for absenteeism and late arrivals ensures that both students and administrators are promptly informed, enhancing communication and accountability.

Despite its strengths, the system faces some challenges. One potential weakness is the reliance on the accuracy of the fingerprint sensor, as any issues with the sensor's performance could lead to difficulties in capturing accurate attendance records. Additionally, while the system is designed to securely store biometric data, any vulnerabilities in the encryption protocols could pose risks to data privacy and security. The system's performance may also be affected by network stability, particularly in environments with unreliable internet connections, which could impact real-time data processing and notifications.

Furthermore, while the system provides comprehensive reports and notifications, there may be a learning curve for administrators who are less familiar with digital attendance management systems. Ensuring that users are adequately trained and supported will be crucial to maximizing the system's effectiveness. Addressing these weaknesses will be essential to enhancing the system's overall reliability and user satisfaction.

Based on feedback, the system exhibits several notable strengths, including its accuracy in attendance tracking and its ability to provide real-time updates. Users appreciate the convenience of biometric authentication and the comprehensive reporting features. However, some feedback suggests the need for further refinements, such as improving sensor accuracy and enhancing data security measures. Addressing these areas could further solidify the system's effectiveness and broaden its appeal among educational institutions.

7.2 Propositions for Improvement

To enhance the user experience of the IoT-based fingerprint biometric attendance system, a focus on refining the system's interface and overall usability is essential. Conducting a comprehensive user experience (UX) analysis will help identify areas where users might encounter difficulties. By incorporating user feedback into iterative design improvements, such as optimizing navigation paths, improving visual clarity, and simplifying interactions, the system can become more intuitive and user-friendly. Additionally, implementing user tutorials or on-screen guidance will assist new users in understanding the system's features and functionalities. Regular updates based on user feedback will ensure that the system continues to evolve in alignment with user expectations, maintaining a high level of satisfaction.

To bolster the system's functionality, it is recommended to enhance the accuracy and reliability of the fingerprint sensor. This could involve implementing advanced sensor calibration techniques and conducting regular maintenance checks to ensure consistent performance. Furthermore, strengthening data security measures, particularly concerning the storage and encryption of biometric data, is crucial. This can be achieved by adopting the latest encryption standards and conducting regular security audits to safeguard against potential vulnerabilities. Enhancing security will ensure that the system not only meets but exceeds industry standards for data protection, thereby boosting user confidence.

In response to the need for improved data accessibility and reporting, expanding the system's reporting capabilities to include more detailed analytics and customizable report formats could significantly enhance its value for administrators. This could involve integrating advanced data visualization tools that allow administrators to generate tailored reports based on specific criteria, such as class attendance trends or individual student performance over time. Additionally, incorporating real-time data synchronization across devices will ensure that attendance records are always up-to-date and accessible from any location. These enhancements will provide administrators with more powerful tools for managing and analyzing attendance data, ultimately leading to more informed decision-making.

To further increase the system's appeal and functionality, it is advisable to introduce more customizable options within the user interface. This could include offering different themes or layouts that allow users to personalize their experience according to their preferences. Additionally, integrating more interactive elements, such as real-time attendance charts or notifications for attendance-related events, can provide users with clearer insights and improve overall engagement. These enhancements will make the system not only more functional but also more enjoyable to use, thereby increasing overall user satisfaction and engagement.

7.3 Project Contribution

The IoT-based fingerprint biometric attendance system project marks a notable contribution to the field of smart attendance management by leveraging biometric technology to enhance security and accuracy in attendance tracking. This project demonstrates how cutting-edge IoT and biometric technologies can be effectively integrated to address real-world challenges in educational and organizational settings. By automating the attendance process and ensuring precise timestamps for each scan, the system provides a reliable and efficient tool for managing attendance, particularly in environments where manual tracking can be error-prone and time-consuming. The project exemplifies the potential of smart technology to streamline administrative tasks, improve data accuracy, and enhance overall system security, setting a benchmark for future innovations in biometric-based solutions.

7.4 Conclusion

The IoT-based fingerprint biometric attendance system has successfully met its project objectives, establishing a state-of-the-art solution for precise and efficient attendance management. This system integrates advanced biometric technology with IoT capabilities to deliver a robust and secure method for tracking attendance. Through a series of comprehensive testing phases and iterative refinements, the system has demonstrated its ability to accurately record attendance in real time, significantly reducing the potential for errors associated with manual methods. The integration of fingerprint recognition technology ensures a high level of security and reliability, addressing common challenges in attendance tracking and providing a dependable tool for both educational institutions and organizations.

One of the key strengths of the system lies in its innovative approach to automating attendance management. The biometric authentication process not only streamlines the attendance recording but also enhances overall data integrity by eliminating common issues related to manual entry. The system’s capability to accurately timestamp each fingerprint scan ensures that attendance records are precise and reflective of actual attendance. Additionally, the secure storage of biometric data and real-time updates further contribute to the system's effectiveness, making it a valuable asset for institutions seeking to modernize their attendance processes.

Looking ahead, there are opportunities for further enhancement and expansion of the system’s capabilities. Potential improvements could include advanced analytics for more detailed attendance reporting and expanded administrative functionalities to facilitate better management and oversight. The project has laid a strong foundation for future developments in biometric attendance solutions, demonstrating the significant benefits of integrating cutting-edge technology into everyday administrative tasks. In conclusion, the IoT-based fingerprint biometric attendance system stands out as a pioneering solution that not only meets current needs but also sets a high standard for future innovations in attendance management.

REFERENCES

Siti Robaya Jantan, Amran Rasli (2022, October) *Smart Attendance for Faculty Monitoring System Using the Bluetooth Low Energy: Design and Implementation*

https://www.researchgate.net/publication/365065304_Smart_Attendance_for_Faculty_Monitoring_System_Using_the_Bluetooth_Low_Energy_Design_and_Implementation

Danijel Mijic, Ognjen Bjelica (2019, March) *An Improved Version of Student Attendance Management System Based on RFID*

https://www.researchgate.net/publication/333228631_An_Improved_Version_of_Student_Attendance_Management_System_Based_on_RFID

Engr Imran, Imran Anwar Ujan (2011, May) *Biometric Attendance System*

https://www.researchgate.net/publication/269962935_Biometric_Attendance_System

Ong Kong Seng (2014, August) *Biometric Fingerprint Recognition-based system for Time and Attendance Recording*

https://utpedia.utp.edu.my/id/eprint/14417/1/Ong%20Koon%20Seng%20Final%20Report-signed.pdf

M. Olagunju, A.E. Adeniyi, T.O. Oladele (2018, February) *Staff Attendance Monitoring System using Fingerprint Biometrics*

https://core.ac.uk/download/pdf/162155368.pdf

Ayush Mahajan, Gaurav Sahu, Aditya Anand (2019, June) *Attendance system based on Fingerprint Using ARDUINO*

https://www.jetir.org/papers/JETIR1908A49.pdf

E.G. AbdulKhadim (2021, February) *Design and Develop an Attendance System Based on Fingerprint and Arduino Board*

https://www.semanticscholar.org/paper/Design-and-Develop-an-Attendance-System-Based-on-Abdulkadhim/14c1c7db1476659f4532d14313225f2bcb50d083