APPLIED INFORMATION TECHNOLOGY AND COMPUTER SCIENCE
e-ISSN: 2773-5141

AITCS

Vol. 6 No. 2 (2025) 416-432
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

Web-Based IoT Smart Door Lock System for Secure Access Building Management

Umi Umairah Nordin[1], Nayef Abdulwahab Mohammed Alduais[1]*

[1] *Faculty of Computer Science and Information Technology,*
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

*Corresponding Author: nayef@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2025.06.02.023

Article Info

Received: 12 June 2025
Accepted: 3 November 2025
Available online: 30 November 2025

Keywords

IoT (Internet of Things), Smart Door Lock System, Web-Based System, remotely control door lock, Arduino, RFID, Laravel framework, ThingSpeak

Abstract

The conventional lock and key or pass code security of office and building set ups are prone to real time security, remote security set-ups and prone to hacking. This project proposes a safe, using IoT Smart Door Access System as the filing of these deficits by providing linked, programmable, and real-time authorizing. The system incorporates essential features such as user registration, login, profile management, password recovery, door access monitoring, and access logs. By employing RFID technology alongside the ESP8266 microcontroller, it guarantees secure and effective authentication. The backend is constructed using the Laravel web framework integrated with a MySQL database, while real-time data visualization is facilitated through ThingSpeak The system comprises extensive modules for door monitoring and control, user administration, report generation, and profile management. All project goals have been thoroughly met, and the final functioning prototype successfully merges both hardware and software elements. The system exhibits excellent performance in managing door access, delivering real-time updates, and ensuring precise access records. This solution provides a scalable and reliable method for securing entry points in office settings, educational institutions, and various smart facilities.

1. Introduction

The swift progression of the Internet of Things (IoT) has transformed numerous sectors, allowing for effortless communication between tangible devices and digital platforms. The adoption of IoT technology in security systems enables enhanced real-time control and monitoring, significantly improving the efficiency and effectiveness of access management solutions [1]. This project presents a Web-Based IoT Smart Door Lock System for Effective Building Access Control, tackling the shortcomings of conventional locking systems by providing a flexible, remote-access, and secure alternative. Traditional methods that depend on physical keys, or passcodes often lack real-time monitoring, adaptability, or sufficient security against unauthorized entry. The proposed system combines IoT technology with an online interface, enabling administrators to manage access rights, oversee entry attempts, and address incidents in real-time. Its features include Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), access logs, notifications, and immediate alerts to improve both security and usability. Tailored for multi-story office complexes, this system supports centralized management and comprehensive reporting to reduce risks and enhance access control procedures. By integrating cutting-edge

security features, this project aims to deliver a practical and versatile solution for contemporary access management, significantly advancing IoT-driven security innovations.

2. Related Work

Prior studies, such as those conducted at [], have shown the efficacy of Radio Frequency Identification (RFID) technology in creating advanced Door Access Management Systems [2]. These systems employ RFID tags for user identification and authentication, allowing or restricting access to secure areas. By combining RFID with additional technologies like microcontrollers, databases, and IoT platforms, researchers have developed complex systems that provide real-time access control, remote monitoring, and centralized management functions. These systems exhibit considerable potential in improving security and operational efficiency across a range of applications, including in businesses, residential communities, and educational facilities. For instance, RFID-based systems can enable contactless access, enhance audit trails, and ensure seamless integration with other security protocols. Moreover, the incorporation of IoT facilitates remote management, immediate alerts, and insights driven by data, resulting in more effective and informed security oversight. Building on these developments, this research intends to further investigate the capabilities of IoT-enabled smart door locks in bolstering security for homes and buildings.

2.1 Reviewing Existing System

System Application of an Internet of Internet of Things Door Lock Network Bridge for Classroom Access Control Management is designed to retrofit current electronic locks with IoT features, with the goal of improving access control in classrooms without needing to replace the entire locking system [3]. This strategy could lead to cost savings and less disruption during the implementation process. By connecting to an IoT network bridge, the system facilitates centralized management of classroom access through an online platform. This capability enables administrators to remotely oversee access, monitor usage trends, and potentially automate specific tasks. However, the system has notable shortcomings in several key areas. Most importantly, it does not offer role-based access control, which is crucial for managing different access levels for various user groups (such as teachers, students, and staff). This gap presents a security concern as it fails to provide detailed control over who has access to classrooms. Additionally, the system utilizes QR codes for access, which might not be as secure or user-friendly as alternatives like RFID cards or biometric authentication. QR codes are susceptible to easy sharing or compromise, which could weaken the overall security of the system. In summary, while this system showcases the promising capabilities of IoT in enhancing classroom access control, its absence of critical security features and dependence on potentially insecure authentication methods highlight the need for further development and improvement to establish a reliable and secure solution.

Designing a Securable smart Home Access Control System using RFID Cards aims to improve home security through the implementation of an RFID-based access control mechanism [4]. RFID cards provide a convenient and relatively secure approach for granting entry to authorized users while preventing access to unauthorized individuals. The system likely consists of an RFID reader that works with a central controller to validate card credentials and allow access. The integration of role-based access control is a notable advantage of this system, as it facilitates differentiated access rights for various users (e.g., family members, guests, service personnel). This adaptability boosts security and enables better oversight of who can enter particular areas of the home. However, the system seems to be missing essential features such as real-time monitoring and the ability for remote management. In the absence of real-time monitoring, it becomes challenging to identify and respond swiftly to security infractions or attempts at unauthorized access. Likewise, the lack of remote management functionality restricts flexibility and ease of use, as it may necessitate being physically present to modify access settings or resolve issues. These shortcomings impede the system's capacity to offer thorough and agile security management. To sum up, although the adoption of RFID cards and role-based access control is a constructive advancement in boosting home security, the deficiency of real-time monitoring and remote management features diminishes the system's overall effectiveness.

Smart Lock system illustrates a straightforward application of an RFID-based smart lock [5]. It leverages RFID technology to verify users and allow entry to a restricted area. The system likely incorporates an RFID reader within the locking mechanism, which checks the validity of the RFID card or tag presented. If verification is successful, the lock is unlocked electronically, allowing access. Although this method provides a basic level of security and convenience compared to traditional key locks, it lacks several essential features that are present in more sophisticated access control systems. Specifically, the system seems to be missing web-based integration,

which would facilitate remote management, access tracking, and other advanced functionalities. In the absence of web capabilities, the system's operations are restricted to on-site use, reducing its flexibility and responsiveness. Furthermore, the system likely lacks more advanced security elements, such as multi-factor authentication, access logs, and the ability to block users. These features are vital for boosting security and minimizing potential hazards, such as lost or stolen RFID cards. To sum up, this system offers a basic approach to RFID-based access control but misses the complexity and advanced features characteristic of more comprehensive and secure systems. Table 1 shows the comparison for existing system and proposed system.

Table 1: Comparison Table for Existing System and Proposed System

System / Characteristic	**Application of an Internet of Things Door Lock Network Bridge for Classroom Access Control Management [3]**	**Designing a Securable Smart Home Access Control System using RFID Cards. [4]**	**Smart Lock System Using RFID [5]**	**Web-Based IoT Smart Door Lock System for Secure Building Access Management**
Web-Based System	✗	✓	✗	✓
IoT Integration	✓	✓	✓	✓
Role-Based Access Control	✗	✓	✗	✓
Multi-Factor Access Control	✗	✗	✗	✓
Real-time door control and monitoring	✓	✗	✗	✓
Access log and reporting	✗	✗	✗	✓
User blocking functionality	✗	✗	✗	✓
Remote access and management	✗	✗	✗	✓

3. Methodology

3.1 Parallel Development Methodology

Parallel Development Methodology is a software development strategy aimed at improving efficiency by permitting the simultaneous development of multiple components or subsystems. This approach is especially advantageous in projects involving intricate and interrelated systems, such as IoT applications, as it shortens

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 416-432

development timelines while ensuring that all components are effectively coordinated and integrated. As noted by Mohseni et al. (2022), parallel computing significantly contributes to the improved effectiveness of IoT systems, facilitating enhanced scalability and performance [6]. By employing parallel processes, developers can more adeptly meet the complex requirements of IoT systems, including data processing, real-time communication, and security.

This methodology segments the system into smaller modules that are developed independently by various teams or processes, which are then integrated later in the development timeline. This strategy alleviates the bottlenecks commonly found in traditional sequential models by allowing simultaneous advancement across multiple subsystems [7]. For example, in an IoT Smart Door Lock System, the hardware elements, mobile application, and cloud infrastructure can be developed concurrently, with regular checkpoints to ensure compatibility and integration.

By facilitating concurrent development and iterative testing, the Parallel Development Methodology promotes the swift creation of resilient and dependable systems, making it particularly suitable for complex and evolving projects like IoT applications. This method also enables ongoing enhancements and early identification of potential problems, which can greatly mitigate risks and enhance overall project results. Figure 3.1 shows the software development life cycle of parallel development methodology.

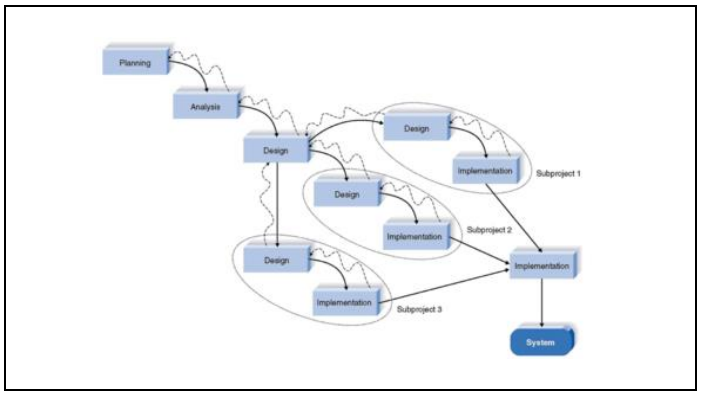


Figure 1: Software Development Life Cycle of Parallel Development [8]

The Planning Phase laid the groundwork for the entire development process, creating specific objectives, scope, and resources for the project. The project officially started in October 2024, with an expected completion date of June 2025. A detailed project proposal was created, outlining the system's goals, scope, and expected results. This proposal encompassed technical specifications, system components, and the necessary hardware and software requirements for development. After being finalized, the proposal was presented to a supervisor for further deliberation and enhancement, with a strong emphasis on articulating the system requirements, features, modules, users, and both software and hardware tools. Following these discussions, the proposal was subjected to a defense process in front of a panel of experts, where feedback was gathered to confirm the project's feasibility and alignment with expectations. The panel's endorsement signified the successful conclusion of the phase, ensuring that the project had a well-defined direction, timeline, and clearly articulated deliverables.

4. System Analysis and Design

This system merges IoT technology with web-based oversight to provide effortless management, improved security, and the ability to access remotely. Unlike conventional lock-and-key systems, this smart locking mechanism enables users to supervise and control door access through an easy-to-use web interface. It delivers real-time alerts, the option to lock and unlock from afar, and strong authentication methods to block unauthorized entry. By utilizing IoT functionalities, this solution minimizes the hazards linked to physical keys, provides detailed access tracking, and gives users authority and insight into their security, no matter where they are located. The IoT Web-Based Smart Door Lock System symbolizes the next generation of security, merging state-of-the-art technology with practicality to transform how we protect our environments.

4.1 System Architecture Design

The process starts with the User and Admin accessing the Web Interface, which acts as the main interaction hub. Users can undertake actions such as logging in or signing up, managing their accounts, and checking the status of the door. Administrators possess additional functions, including managing user accounts, limiting user access, and observing or adjusting the door status. Login and registration functionality provides secure authentication for both users and administrators, giving proper access rights based on their credentials. After logging in, users can manage their information and send requests to change door status or monitor door status, with the system responding accordingly. Administrators can supervise these actions and have access to enhanced features like restricting user access, managing users, and generating access logs and reports to track activities and system usage. Figure 2 shows the system architecture design.

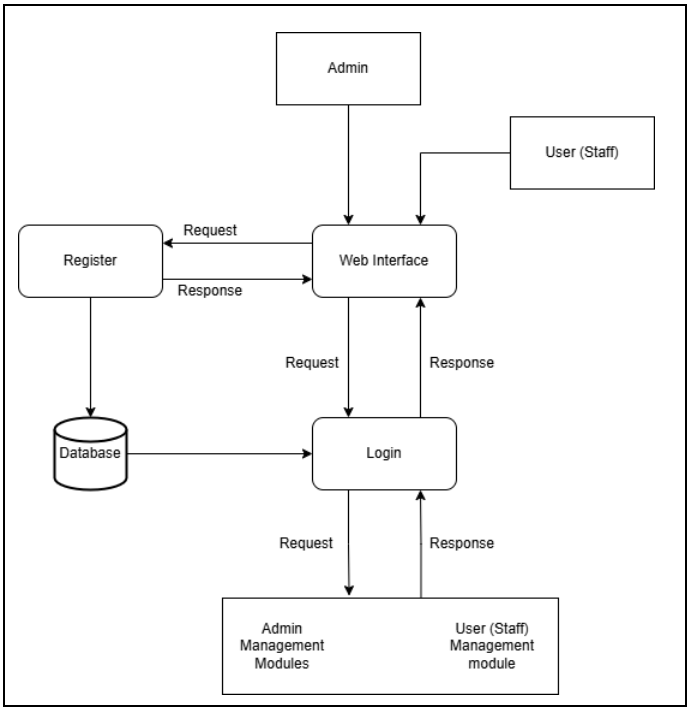


Figure 2: System Architecture Design

4.2 Requirement Analysis

Requirement analysis is a vital step in system development, where the needs and expectations of stakeholders are collected, examined, and recorded to guarantee the successful design and execution of the system. This procedure determines what the system needs to accomplish and how it ought to operate, establishing the groundwork for development. Requirements are generally divided into functional and non-functional requirements, with each focus on various aspects of the system.

Table 2: Functional Requirements

No.	Modules	Functionalities
1.	User Authentication	The system should enable users to sign in or create an account using valid credentials.
2.	Door Lock/Unlock Control	The system must allow users to remotely lock and unlock doors through the web interface.
3.	User Management	Administrators need to handle user accounts, involves add, modify, and remove users.

Table 2: Continued

4.	Access Logs and Reports	The system must create and show logs of door activities available for administrators.
5.	Block User Access	Administrators need to have the capability to prevent certain users from accessing the system.

Table 3: Non-Functional Requirement

No.	Functions	Functionalities
1.	Security	The system needs to secure user information and messages to block unauthorized access.
2.	Scalability	The system must accommodate various users and devices without a decline in performance.
3.	Performance	The system needs to react to commands (e.g., lock/unlock) in under 2 seconds.
4.	Availability	The system needs to guarantee 99.9% uptime for continuous access.
5.	Usability	The web interface must be user-friendly and simple to navigate for users.

4.3 Unified Modelling Language

Unified Modelling Language is a standardized modelling framework that consists of an integrated set of diagrams meant to aid system and software developers in defining, visualizing, constructing, and documenting the artifacts of software systems. It is also applicable to business modelling and various non-software systems. UML encapsulates a range of established engineering practices that have proven effective in modelling intricate and extensive systems. By primarily employing graphical representations, UML enhances the visualization and design of software projects, allowing project teams to communicate efficiently, investigate design options, and verify the system's architectural structure [9].

4.4 Use Case Diagram

The use case diagram illustrates the primary functions and interactions within the IoT Web-Based Smart Door Lock System, highlighting two key actors, the administrator and the staff. The system initiates with a login and registration process, permitting both actors to verify their identity and access their designated functionalities. The administrator possesses greater authority over the system, which includes user management, allowing them to create, modify, or remove user profiles to ensure appropriate access levels and organization of users. Both the administrator and staff can engage with the central feature of door control & monitoring, which entails remotely locking, unlocking, and checking the status of doors. Moreover, the administrator has access to access logs and reports, which offer a comprehensive history of door activities for both accountability and security oversight. Finally, the block user capability allows the administrator to prohibit specific users from entering the system, when necessary, thereby strengthening security protocols. This diagram effectively demonstrates how the system's functionalities are allocated between the two user roles, highlighting their duties and interactions. Figure 4.2 shows the use case diagram of IoT Smart Door Lock System. Figure 3 shows the use case diagram.

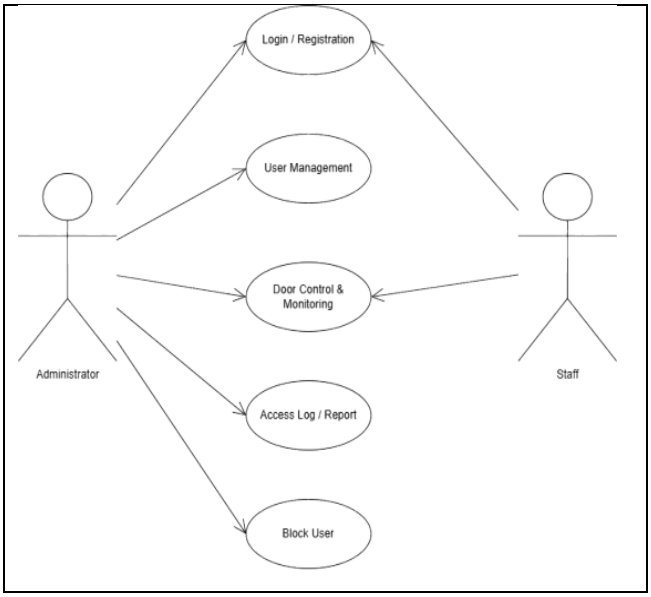


Figure 3: Use Case Diagram of IoT Web-Based Smart Door Lock System

4.5 Sequence Diagram

The system sequence diagram emphasizes the automated interactions involving the smart door lock system, sensors, the Arduino IDE, and the database. When data is transmitted by a sensor, the system captures this information and sends it to the Arduino IDE for analysis. The data that has been processed is subsequently saved in the database to keep a historical record. When the sensor is operational, the system transmits refreshed data to the Arduino IDE for additional examination. Alternatively, if the sensor is not active, the system seeks extra information to guarantee ongoing monitoring and responsiveness of the system. These interactions facilitate immediate updates and the smooth functioning of the IoT-driven smart door lock system, guaranteeing its dependability and safety. Figure 4 shows the sequence diagram for Smart Door Lock System.

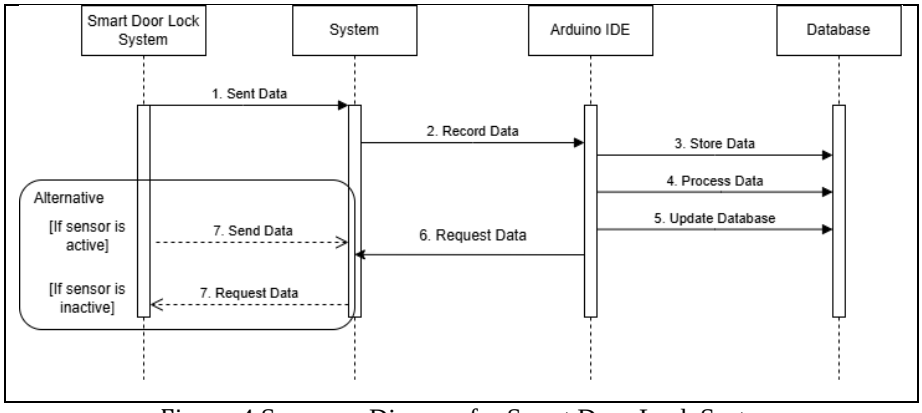


Figure 4 Sequence Diagram for Smart Door Lock System

4.6 Activity Diagram

The activity diagram represents the process flow of a secure IoT-enabled door lock system, highlighting the importance of role-based access control and decision-making steps involved. It starts with a login procedure where users are asked to verify their credentials. After authorization, admin users are given options to oversee system-level functions, such as reviewing access logs and reports or managing user accounts. These functions guarantee that admins maintain complete authority over system operations and user privileges. In contrast, staff users have restricted access, enabling them to manage their profiles or alter the door status. These options allow staff to fulfill their specific duties while observing the system's role-based access policies.

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 416-432

The workflow guarantees that all user interactions remain secure and comply with established guidelines. Ultimately, both admin and staff users meet at the logout stage, indicating the conclusion of their session. This organized process underscores the smooth integration of registration, authentication, and user-specific tasks, thereby ensuring a safe and effective system. The activity diagram clearly illustrates the logical sequence of tasks and decision points, offering a straightforward overview of the system's functionality. Figure 5 shows the activity diagram for the Smart Door Lock System.

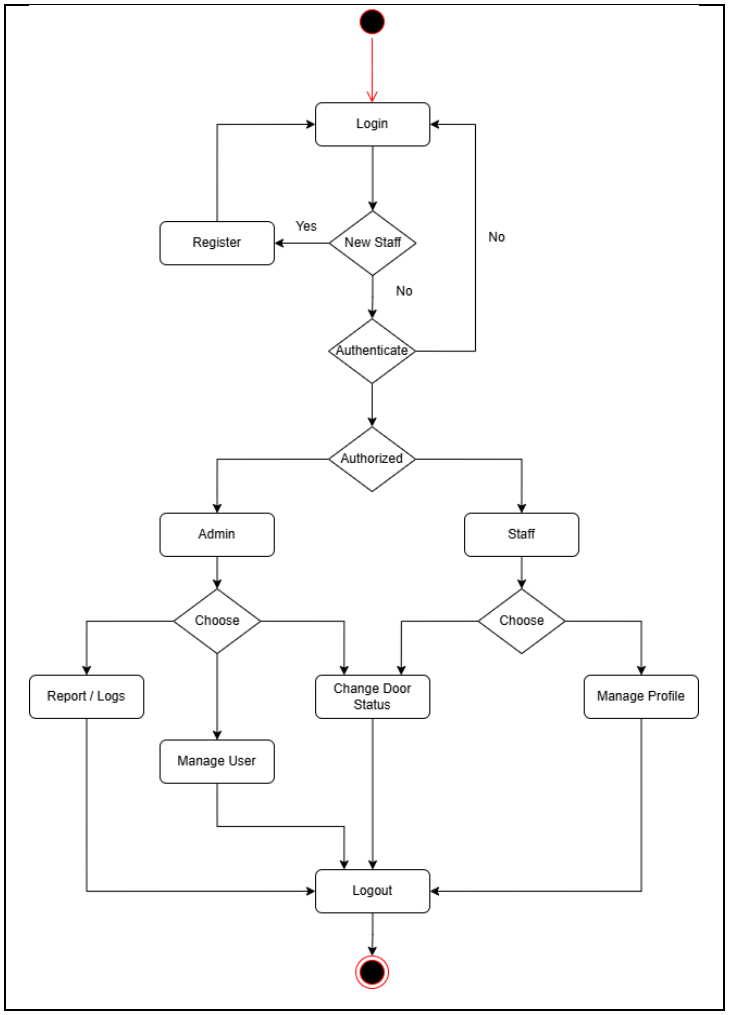


Figure 5 Activity Diagram for Smart Door Lock System

4.7 Class Diagram

A class diagram is a kind of structural diagram utilized in object-oriented modelling to visually depict the classes, their attributes, methods, and the relationships among them within a system.

The Admin class is designed to represent administrators, featuring attributes like admin_id, username, password, and email. Administrators possess functionalities for logging in, managing users, blocking users, viewing logs, generating reports, and altering door statuses. The Staff class depicts staff members with comparable attributes, which include user_id, username, password, and email. Staff can log in, manage their accounts, and modify door statuses.

The Door class represents physical doors, characterized by attributes such as door_id, location, and status, along with a method for updating the door's status. The Logs class monitors system activities, containing attributes like log_id, action, timestamp, user_id, and door_id. It offers methods to generate reports and view logs. Admins are linked to the logs, meaning they are responsible for managing and viewing them.

The Notification class is responsible for managing notifications sent to users, featuring attributes like notification_id, message, timestamp, and user_id. It includes a method for dispatching notifications, which is associated with staff

members. The relationships illustrate that admins supervise multiple staff members, and both admins and staff can interact with doors. Logs are related to actions executed by users, while notifications are connected to users. Figure 6 shows the class diagram for Smart Door Lock System.

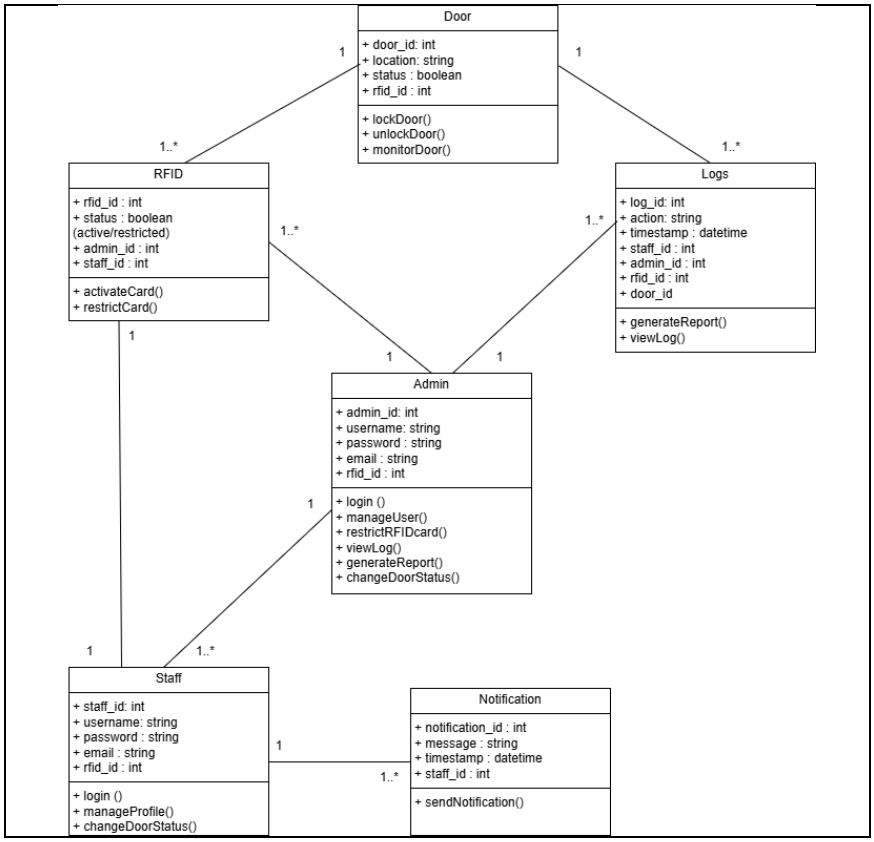


Figure 6 Class Diagram for Smart Door Lock System

5. Implementation & Testing

The Web-Based IoT Smart Door Lock System is developed by combining hardware and software elements to facilitate remote access management and live monitoring. At the heart of the hardware setup is the ESP8266 Wi-Fi microcontroller, serving as the main unit for processing access requests and interfacing with the cloud-based web server. The ESP8266 was selected for its affordability, built-in Wi-Fi features, and IoT compatibility. Figure 7 shows the the smart door lock system's wiring linking the RFID module and various sensors to the ESP8266 microcontroller. Proper wiring is crucial for precise signal transmission, with the RFID reader connected to specific GPIO pins for authentication and the relay module set up to manage the electronic door lock mechanism. The green LED indicated that the door is unlocked.

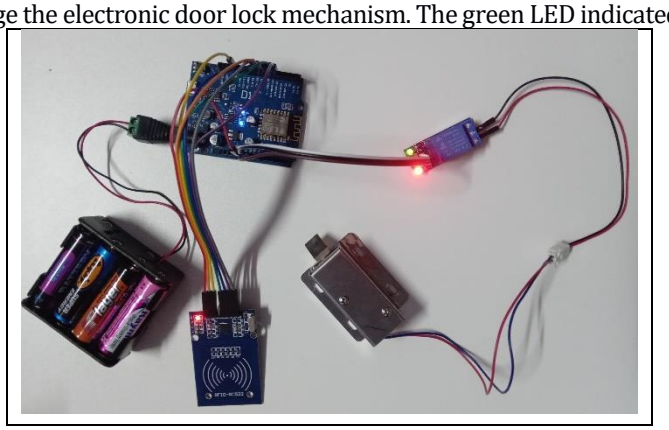


Figure 7: Wiring diagram of smart door lock system

5.1 User Registration and Login

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 416-432

The user registration and login component are a vital aspect of the smart door lock system because it governs authentication and access control. This component enables users and administrators to set up accounts, sign in, recover lost passwords, and safely log out. These capabilities are crucial for maintaining system security and monitoring access events. Each function is designed with appropriate validations and connected to the backend database to guarantee data consistency and secure user administration. Figure 8 shows the web pages for login and registration.

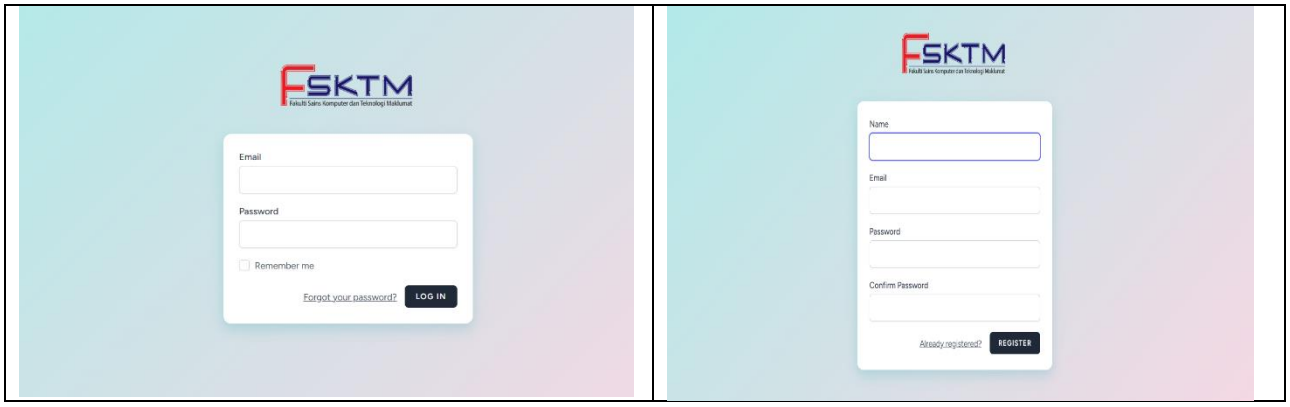


Figure 8: Login & Registration Page

5.2 User Management

This module offers administrative capabilities for managing user accounts within the Laravel application. It features functionalities such as creating new users, viewing lists of users, modifying user details, and deleting user accounts. Built with Laravel's MVC architecture, the module ensures a distinct separation of concerns. This module is essential for upholding the security and organization of the application's user base. Figure 9 shows the user management webpages.

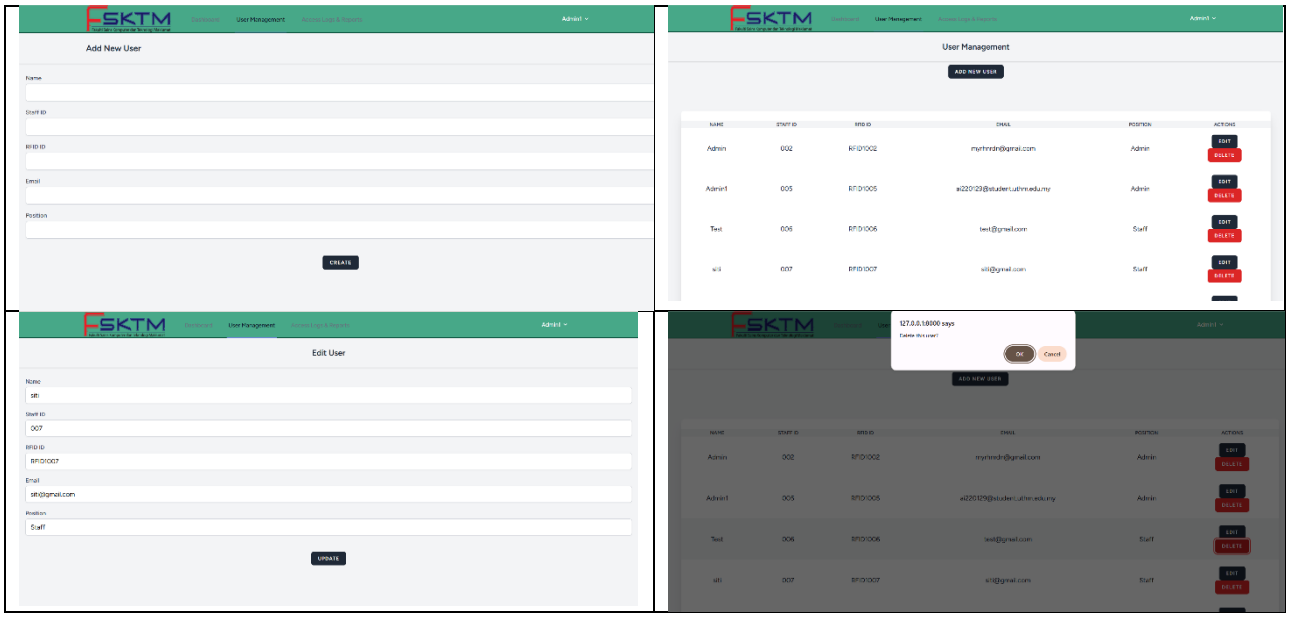


Figure 9: User management module

5.3 Door Access and Management

The Door Access Monitoring and Management Module is an essential part of the IoT Smart Door Lock System, aimed at delivering thorough oversight and control over room access within the facility. This module allows administrators to observe the real-time status of doors (locked or unlocked), thereby helping to maintain security and operational effectiveness. Besides viewing door statuses, users have the capability to access in-depth room details, alter existing room information, and add new rooms to the system using an easy-to-navigate interface. The

option to manually adjust door status enables swift action in emergencies or for administrative exceptions. By bringing all access points together into one management platform, this module improves safety, streamlines room and door management, and facilitates informed decision-making with precise and current access information. It acts as the foundation for effective access control in intelligent building settings. Figure 10 shows the door access monitoring and management web pages.

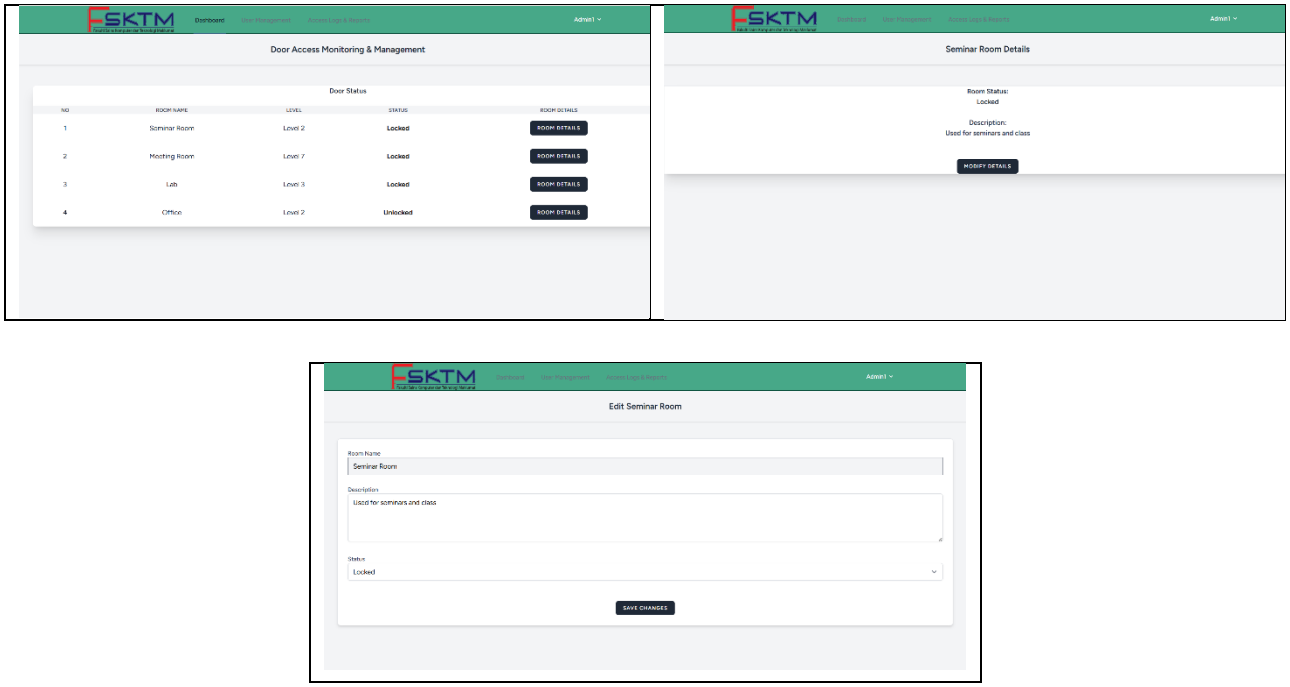


Figure 10: Door access monitoring and management module

5.4 ThingSpeak

Figure 11 demonstrates how the ThingSpeak IoT platform is integrated with the system to emulate and oversee activities related to room access. Simulated information, including RFID tag identifiers, staff identifiers, door status, and timestamps, is regularly sent to ThingSpeak through HTTP requests. This configuration is valuable for testing the real-time logging and visualization of room access incidents prior to the implementation of actual hardware devices. The gathered data can subsequently be retrieved and processed within the web system for purposes such as display, analysis, or report creation.

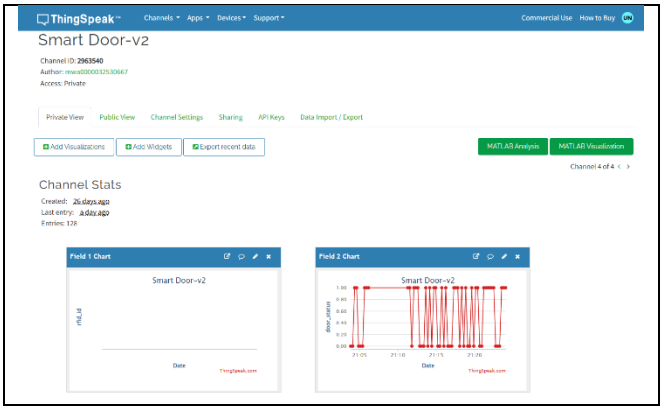


Figure 11: ThingSpeak Channel for Smart Door Lock

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 416-432

5.5 Logs and Reports

The Logs and Report module acts as a key element for overseeing and documenting all access activities within the system. It collects crucial information such as room identifiers, user details like name, timestamps of access, and the status of doors either Lock or Unlock in real time. By integrating with the ThingSpeak API and cross-referencing RFID and staff IDs with records in the database, the system guarantees precise monitoring of all entries and exits. This module not only improves transparency and security but also equips administrators with robust tools for analyzing historical usage trends, identifying irregularities, and preserving audit trails. Moreover, users can export these logs into PDF format for official documentation, compliance checks, or offline use, thereby enhancing the organization's operational efficiency and accountability. Figure 12 shows the logs and reports module where the data was retrieved from ThingSpeak. The data also can be downloaded into PDF version.

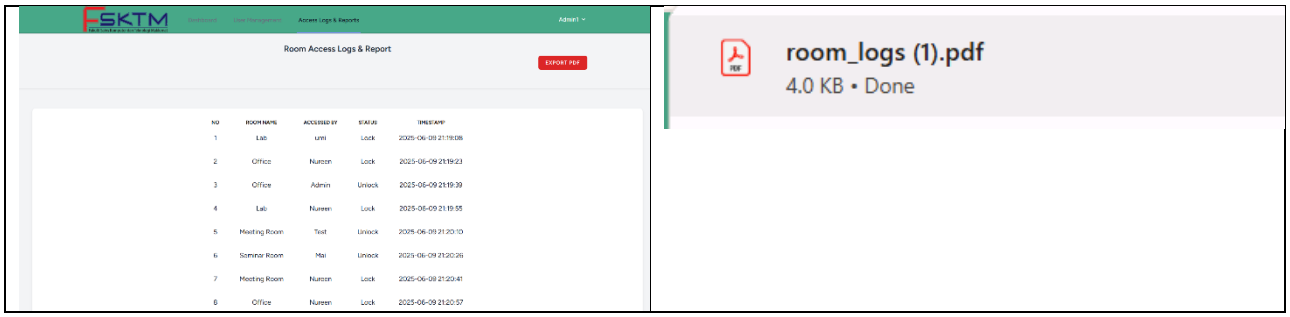


Figure 12: Logs and report module

5.6 System Testing

A test plan details the strategy for system testing, objectives, schedule, deliverables, estimates, and resources. It provides guidance for testing activities and outlines the testing procedures. Tables 4 to Table 8 present examination strategies customized for each module.

Table 4: User Authentication Module

Test	Expected Result	Actual Result
Register with name, email and password	User registered successfully and redirect to dashboard	Pass
Register using existed email	Error message: “The email has already been taken”	Pass
Register using weak password	Error message: “The password field must be at least 8 characters”	Pass
Login with correct credentials	Redirect to dashboard	Pass
Login using incorrect password	Error message: “These credentials do not match our records”	Pass
Login using unregistered email	Error message: “These credentials do not match our records”	Pass
Forgot password with registered email	Message: “We have emailed your password reset link”	Pass
Forgot password using unregistered email	Error message: “We can’t find a user with that email address”	Pass
Logout from dashboard	The user session has ended and being redirected to the homepage.	Pass

Table 5: Door Access Monitoring & Management Module

Test	Expected Result	Actual Result
View current door status	System displays latest door status (locked/unlock)	Pass
View list of rooms and details	List of rooms along with level, status, room details	Pass
Update room details (description/status)	Changes saved and updated in database and list of rooms	Pass
Add new room to system	New room is added, saved in database and visible in the room list	Pass
Change door status from the system	The status of the door updates and displays the new status right away.	Pass

Table 6: User Management Module

Test	Expected Result	Actual Result
Display list of users	All registered users and users added by admin displayed with details	Pass
Add new user	New user added and had message "User created successfully"	Pass
Edit user details	User details updated and had message "User updated successfully"	Pass
Delete user	Alert message pop-up "Delete this user?" and have 2 buttons: "OK", "Cancel". If user clicked on "OK", the registered user will be deleted and no longer listed	Pass

Table 7: Access Logs and Reports Module

Test	Expected Result	Actual Result
View list of door access logs	Access logs utilizing RFID technology with timestamps shown.	Pass
Pull data from ThingSpeak	Latest sensors data successfully retrieve and displayed	Pass
Export logs to pdf	Access logs exported to pdf format and downloaded	Pass

Table 8: Profile Management Module

Test	Expected Result	Actual Result
View current user profile	Users view their profile details (name, email)	Pass
Update profile details	Name and email updated successfully with message "Saved"	Pass
Change account password	The password has been changed; the user can log in again using the new password.	Pass
Delete account	User account removed and redirected to the homepage.	Pass

5.7 User Acceptance Testing

To ensure that the technology meets user expectations in practical environments, User Acceptance Testing, or UAT, is conducted during the later stages of developing the Internet of Things and Web-Based System for Smart Door Lock System. This testing phase emphasizes usability, user needs, and specific requirements related to door lock system. In this process, five carefully selected users will participate, with one designated user focusing solely on testing the administrative panel. According to the results from user acceptance testing, the system fulfils all

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 416-432

essential requirements in both user interface and system functionality areas. Users reported that the interface is intuitive and easy to navigate, with an attractive design. Key functionalities such as login, registration, door monitoring, user and profile management, data visualization, and reporting have all been successfully verified. Furthermore, the admin panel and dashboard features were confirmed to operate effectively, suggesting that the system is prepared for deployment and meets user expectations well. Table 9 shows the result of user acceptance testing for admin user.

Table 9: Result of user acceptance testing for admin user

No.	Acceptance Requirement	Actual Result				
		1	2	3	4	5
User interface						
1	Easy to use and understand				✓	
2	Navigation				✓	
3	Interface design					✓
System Function						
1	Login & registration				✓	
2	Door monitoring function				✓	
3	Users' management function				✓	
4	Profile management function					✓
5	Data visualization function			✓		
6	Logs and report function				✓	
7	Admin panel effectiveness				✓	
8	Admin dashboard functionality				✓	

The User Acceptance Testing (UAT) chart indicates a trend of positive responses across different system modules and usability metrics. Most features such as login, door monitoring, user management, and profile capabilities earned high satisfaction ratings, mostly scored as 4 or 5 by the users. This suggests that the system is positive regarding both its functionality and user interface. Some minor variations in a few criteria like interface design and data visualization highlight opportunities for enhancing the user experience. Nonetheless, the overall findings confirm that the system effectively fulfills user expectations and operates reliably in essential functions. Figure 14 shows the chart result of user acceptance testing for admin user.

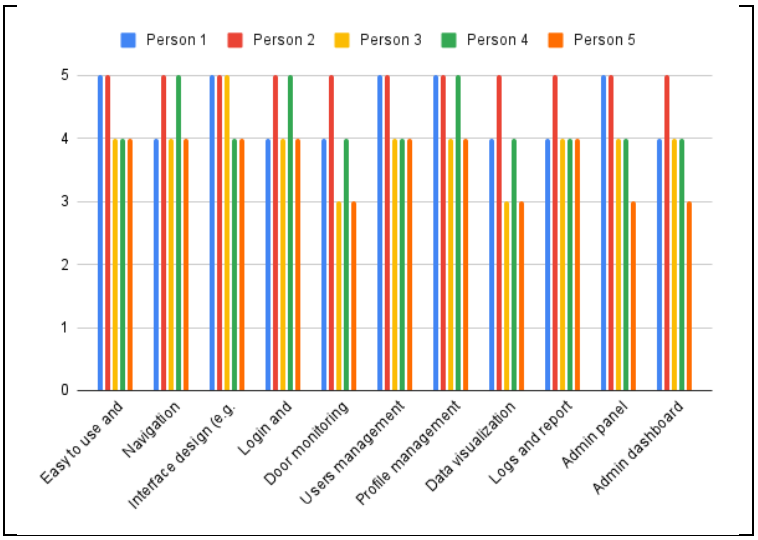


Figure 14: User acceptance result

6. Conclusion

Although the project achieved successful results, it faced various limitations during its development. A primary challenge was maintaining a stable and reliable internet connection, as the system relies heavily on network accessibility for optimal performance. Furthermore, the hardware elements, such as the ESP8266 and sensors, had specific constraints regarding their communication range and connection reliability. In terms of security, while multi-factor authentication was put in place, there has yet to be a thorough exploration of more sophisticated safeguards against cyber threats like spoofing or man-in-the-middle attacks. Additionally, the user interface (UI) could be enhanced to create a more intuitive and user-friendly experience.

In future development, several improvements can be made to enhance the system's performance and features. This could include the integration of a mobile app that enables users to unlock doors, receive notifications, and manage access directly from their smartphones. Additionally, exploring the use of technologies like facial recognition or voice authentication could increase security measures. Implementing artificial intelligence (AI) could also help analyse access patterns and identify any suspicious behaviour. Furthermore, the system could be adapted for use in other settings, such as schools, hospitals, or residential areas, with minor modifications to meet specific requirements.

Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support.

Conflict of Interest

Authors declare that there is no conflict of interest regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: **study conception and design:** Umi Umairah Binti Nordin, Author Nayef Abdulwahab Mohammed Alduais; **data collection:** Umi Umairah Binti Nordin; **analysis and interpretation of results:** Umi Umairah Binti Nordin, Author Nayef Abdulwahab Mohammed Alduais; **draft manuscript preparation:** Umi Umairah Binti Nordin, Nayef Abdulwahab Mohammed Alduais. All authors reviewed the results and approved the final version of the manuscript.

References

[1] *Sowmya, G., Jyothi, G. D., Shirisha, N., Navya, K., & Padmaja, B. (2018). Iot based Smart Door lock system. International Journal of Engineering & Technology, 7(3.6), 223-225.*

[2] *Shahid Ul Haq, Singh, Y., Sharma, A., Gupta, R., & Gupta, D. (2023). A survey on IoT & embedded device firmware security: architecture, extraction techniques, and vulnerability analysis frameworks. Discover Internet of Things, 3(1). https://doi.org/10.1007/s43926-023-00045-2*

[3] *Li, C. H., Chen, C. Y., Huang, X. R., Tsai, T. F., & Liu, B. Y. (2021, March). Development and application of an Internet of Things door lock network bridge for classroom access control management. In IOP Conference Series: Materials Science and Engineering (Vol. 1113, No. 1, p. 012022). IOP Publishing. https://doi.org/10.1088/1757-899X/1113/1/012022*

[4] *Baykara, M., & Abdullah, S. (2020). Designing a securable smart home access control system using RFID cards. Journal of Network Communications and Emerging Technologies (JNCET), 10(12), 1–12.*

[5] *Gindi, S., Shaikh, N., Beig, K., & Sabuwala, A. (2020). Smart lock system using RFID. International Research Journal of Engineering and Technology (IRJET), 7(7).*

[6] *Mohseni, M., Othman, B. A., Raturi, P., Mishra, A. B., Priya, S. J., & Saravanan, V. (2022, April). The role of parallel computing towards implementation of enhanced and effective industrial Internet of Things (IoT) through MANOVA approach. In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 160–164). IEEE.*

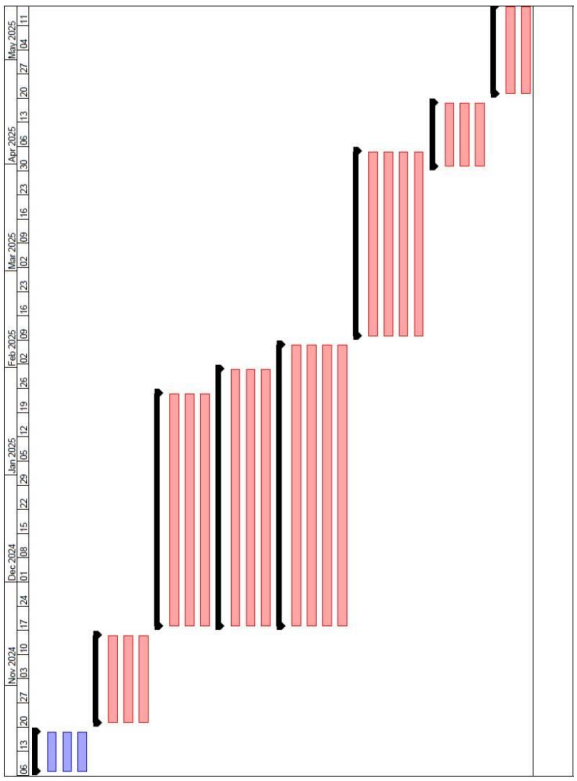
[7] *Parallel Development. (n.d.). TechDocs. Broadcom. https://techdocs.broadcom.com/us/en/ca-mainframe-software/devops/ca-endevor-software-change-manager/18-1/using/parallel-development.html*

[8] *Darmawan, P. (n.d.). Metodologi dalam Rekayasa Perangkat Lunak (RPL). https://philipdarmawan.blogspot.com/2011/09/blog-post.html*

[9] *Visual Paradigm. (2019). What is Unified Modeling Language (UML)? Visual-Paradigm.com. https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-uml/*

Appendix A:

Gantt Chart



	Name	Duration	Start	Finish
1	**Project Initialization**	**10 days**	**10/7/24 8:00 AM**	**10/18/24 5:00 PM**
2	Define Project Scope	10 days	10/7/24 8:00 AM	10/18/24 5:00 PM
3	Gather Requirement	10 days	10/7/24 8:00 AM	10/18/24 5:00 PM
4	Initial Stakeholder Meeting	10 days	10/7/24 8:00 AM	10/18/24 5:00 PM
5	**System design**	**20 days**	**10/21/24 8:00 AM**	**11/15/24 5:00 PM**
6	Create system architecture	20 days	10/21/24 8:00 AM	11/15/24 5:00 PM
7	Hardware Design	20 days	10/21/24 8:00 AM	11/15/24 5:00 PM
8	IoT Communicatio Flow	20 days	10/21/24 8:00 AM	11/15/24 5:00 PM
9	**Hardware Implementa...**	**50 days**	**11/18/24 8:00 AM**	**1/24/25 5:00 PM**
10	Assemble IoT hardware	50 days	11/18/24 8:00 AM	1/24/25 5:00 PM
11	Develop firmware for Io...	50 days	11/18/24 8:00 AM	1/24/25 5:00 PM
12	test hardware component	50 days	11/18/24 8:00 AM	1/24/25 5:00 PM
13	**Backend Development**	**55 days**	**11/18/24 8:00 AM**	**1/31/25 5:00 PM**
14	setup backend infrastruc...	55 days	11/18/24 8:00 AM	1/31/25 5:00 PM
15	develop core backend fe...	55 days	11/18/24 8:00 AM	1/31/25 5:00 PM
16	test backend modules	55 days	11/18/24 8:00 AM	1/31/25 5:00 PM
17	**frontend development**	**60 days**	**11/18/24 8:00 AM**	**2/7/25 5:00 PM**
18	setup frontend framework	60 days	11/18/24 8:00 AM	2/7/25 5:00 PM
19	develop ui component	60 days	11/18/24 8:00 AM	2/7/25 5:00 PM
20	integrate with backend ...	60 days	11/18/24 8:00 AM	2/7/25 5:00 PM
21	test frontend features	60 days	11/18/24 8:00 AM	2/7/25 5:00 PM
22	**system integration & t...**	**40 days**	**2/10/25 8:00 AM**	**4/4/25 5:00 PM**
23	integrate hardware	40 days	2/10/25 8:00 AM	4/4/25 5:00 PM
24	conduct unit testing	40 days	2/10/25 8:00 AM	4/4/25 5:00 PM
25	conduct system testing	40 days	2/10/25 8:00 AM	4/4/25 5:00 PM
26	fix bugs and optimize	40 days	2/10/25 8:00 AM	4/4/25 5:00 PM
27	**deployment preparation**	**15 days**	**3/31/25 8:00 AM**	**4/18/25 5:00 PM**
28	prepare deployment env...	15 days	3/31/25 8:00 AM	4/18/25 5:00 PM
29	write documentation	15 days	3/31/25 8:00 AM	4/18/25 5:00 PM
30	create testing protocol f...	15 days	3/31/25 8:00 AM	4/18/25 5:00 PM
31	**system optimization a...**	**20 days**	**4/21/25 8:00 AM**	**5/16/25 5:00 PM**
32	optimize performance	20 days	4/21/25 8:00 AM	5/16/25 5:00 PM
33	finalization and handover	20 days	4/21/25 8:00 AM	5/16/25 5:00 PM