Web-Based Access Control System using Wi-Fi Technology

Najwa Husna Mohd Ishak[1], Rashdan Rashid[2], Farizah Ariffin[3]
[1] Kolej Komuniti Tanjung Piai
[2,3] Politeknik Tuanku Syed Sirajuddin
husna@kktanjungpiai.edu.my, rashdanrashid@ptss.edu.my, farizahariffin@ptss.edu.my

Abstract: The Web-Based Access Control System utilizing Wi-Fi Technology aims to streamline the management of door access in spaces such as labs, lecture halls, and meeting rooms. This system enables the designated administrator to remotely lock or unlock doors via Wi-Fi, provided they are connected to the same network. Additionally, the administrator can track door usage by reviewing a log stored in a server database, which records who locked or unlocked each door. The project consists of two primary components: hardware and software. The hardware features a NodeMCU ESP8266 microcontroller with Wi-Fi capability, paired with a TowerPro SG90 servo motor that operates the door locks. The software is developed using the Arduino IDE for microcontroller programming and PHP for creating the web interface, where the administrator logs in using a username and password to monitor the system. The primary goal of this system is to enhance security and efficiency by automating door control and enabling real-time monitoring of room access. Only users with authorized credentials can interact with the system, ensuring its security. Ultimately, the project provides a reliable and convenient solution for managing access to rooms, improving both control and accountability.

Keywords: *IoT; Microcontroller; Arduino; Wi-Fi Technology*

1.0 INTRODUCTION

Security systems have evolved greatly over time, particularly with the advent of Internet of Things (IoT) technology. Access control systems, which are essential for regulating entry to secure areas, have seen the transition from mechanical locks to modern systems using smart devices. This project focuses on the development and implementation of a web-based access control system that leverages Wi-Fi technology to monitor and control access to rooms. The introduction references the importance of modern access control systems, drawing on foundational studies (Kassem et al., 2017). IoT technology has significantly advanced the functionality of these systems, enabling remote control and monitoring (Jain & Shah, 2016).

This system is designed for use at the Faculty of Computer and Mathematical Sciences (FSKM) at Universiti Teknologi MARA (UiTM). The web-based system allows administrators to lock and unlock doors remotely via Wi-Fi, improving efficiency and flexibility. This document will cover the problem statement, objectives, literature review, methodology, and the findings of the research.

1.1 Problem Statement

The traditional key-based access system used in FSKM is inefficient, requiring the physical presence of personnel to lock and unlock rooms. This can lead to delays in room access and over-reliance on certain individuals. There is also no way to track who accessed the rooms and when.

1.2 Objective

The primary objective of this project is to develop a Wi-Fi-enabled web-based access control system, allowing for remote monitoring and control. Another key goal is to establish a database that logs room usage and access by authorized personnel.

2.0 LITERATURE REVIEWS

The concept of access control dates back thousands of years, originally developed to restrict unauthorized entry to specific areas. Modern access control systems have advanced significantly, incorporating various models and technologies. The literature review includes in-depth analysis of access control models such as Discretionary Access Control (DAC) and Role-Based Access Control (RBAC) (Lopez & Rubio, 2018; Sandhu & Samaranti, 1994). Previous research on wireless access technologies indicates that Wi-Fi is a flexible and scalable option for access control (Potts & Sukittanon, 2012). However, the use of Wi-Fi introduces security concerns, which have been explored in studies on access control system vulnerabilities (Adalan & Bursa, 2014; Huang & Lee, 2015). In FSKM, it can be concluded that they use Role-Based Access Control as only the users with roles is guarding the key are allowed to lock and unlock all door in the faculty.

The primary models of access control include:

1. Discretionary Access Control (DAC): Access permissions are granted based on the user's identity and managed at the discretion of the resource owner.
2. Mandatory Access Control (MAC): This model enforces strict access rules determined by the organization, and permissions are managed by a central authority.
3. Role-Based Access Control (RBAC): Users are granted access based on roles within an organization, allowing for more streamlined permission management.

Technologies in Access Control Systems

With the rise of IoT, access control systems have incorporated technologies such as RFID, biometrics, and Wi-Fi. Wi-Fi technology, in particular, provides convenience for remote control and monitoring. However, it also presents security challenges, requiring robust encryption to prevent unauthorized access. Research indicates that Wi-Fi-enabled access control systems are well-suited for environments requiring flexibility and real-time control. Such systems allow for centralized monitoring, reducing the need for manual intervention. Previous studies show that while Wi-Fi technology provides ease of access and scalability, it also necessitates security measures to address potential vulnerabilities.

Table 1: Comparison of Access control System Technology

Access Control System Technologies	Pros	Cons
PIN/Keypad	• Keyless entry system. • No losses incurred by the organization since appliances or devices such as keys, cards or smart phones are not used.	• Forgetting the password making the lock system unable to be operated. (Kumar et. al., 2016)
RFID	• RFID enables data to be captured automatically, and tasks to be automated. (Roberti M., 2009).	• Losing the device used to control the lock system which might be taken over by irresponsible people (Kumar et. al., 2016) • This frame work is quite costly (Kumar M. et. al., 2016).
NFC	• Use less energy which can preserve battery life for device owners (Ray R.,2015)	• Additional purchases need to be made to maintain related machines and other equipments (Viswanathan P., 2018).
Bluetooth	• Requires less power (Khan Md. A.A., 2016).	• Only a limited number of devices can be connected (Uttarwar P., 2014)

Wi-Fi Technology	• Wi-Fi technology has a higher range in terms of distances covered (Khan Md. & Ali A., 2016).	• The security of Wi-Fi technology would be higher if it has been programmed and secured correctly (Khan Md. Ali A., 2016)

3.0 METHODOLOGY

This project followed a structured methodology, consisting of several phases to design, develop, and test a web-based Wi-Fi access control system. The phases included information gathering, system design, hardware and software setup, and system testing. The system design is based on earlier implementations of Wi-Fi-enabled access control, utilizing the NodeMCU ESP8266 microcontroller for effective wireless communication (Kassem & Lin, 2016). Additionally, PHP and MySQL were used to manage data logging, which aligns with standard practices in IoT environments (Ismail et al., 2014).

3.1 Research Framework and Phases

Below is an overview of the key components:

1. Information Gathering: Initial research focused on understanding access control requirements within the Faculty of Computer and Mathematical Sciences (FSKM) and gathering specifications for both hardware and software.

2. System Design: The system consists of two primary components:
   - Hardware: The NodeMCU ESP8266 microcontroller and a TowerPro SG90 Servo motor were selected for controlling the door mechanism. Figure 1 shows the block diagram with explanation with for this paper.

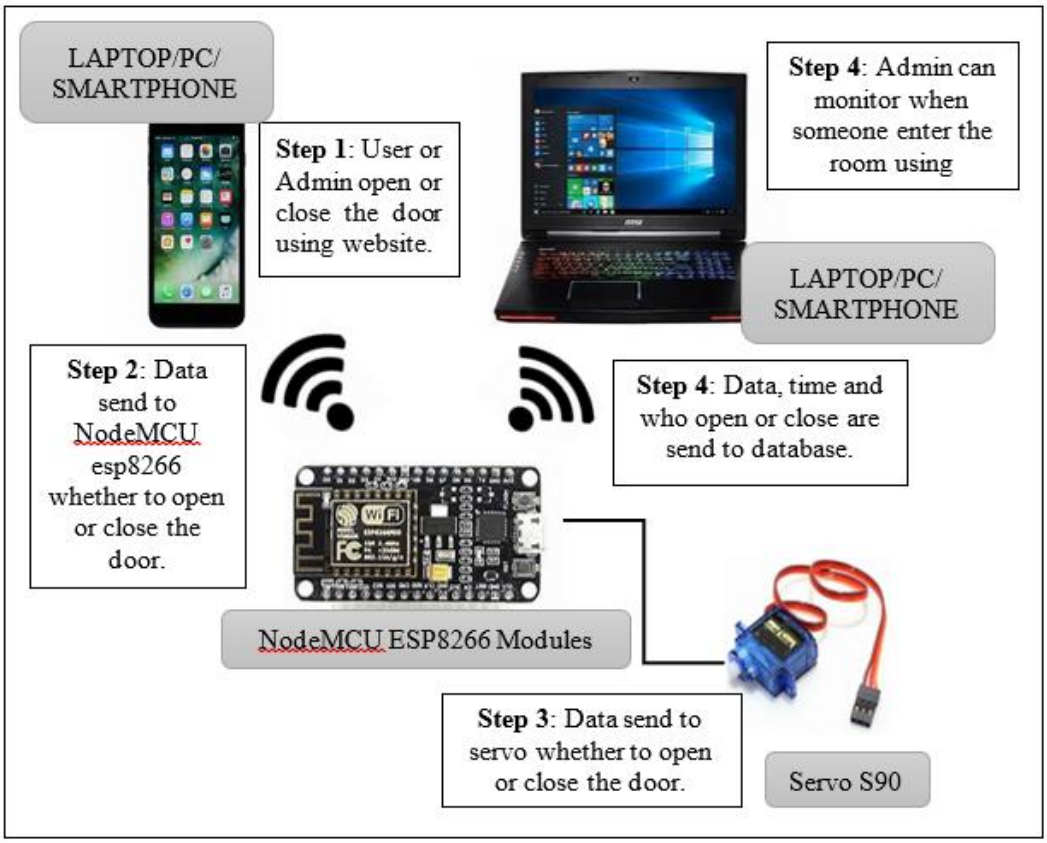

Figure 1: Block Diagram with explanation

- Software: Arduino IDE was used to program the microcontroller, while Notepad++ was used to create PHP scripts for the web interface. The design for the website are shown in Figure 3 until Figure 5.

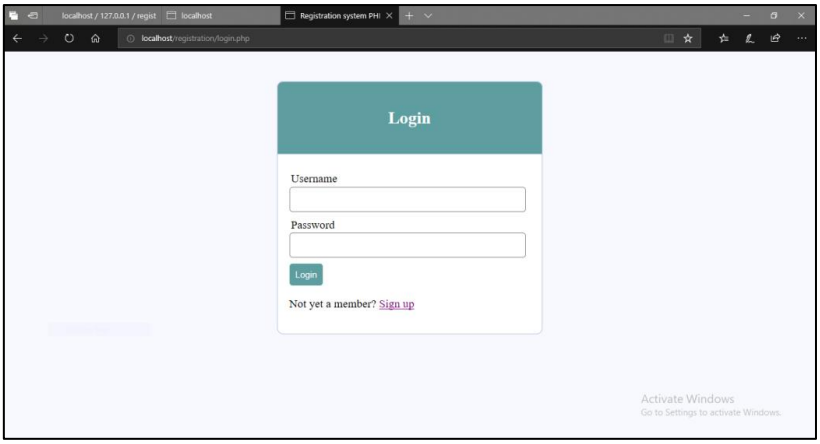

Figure 2: The design for admin interface to login

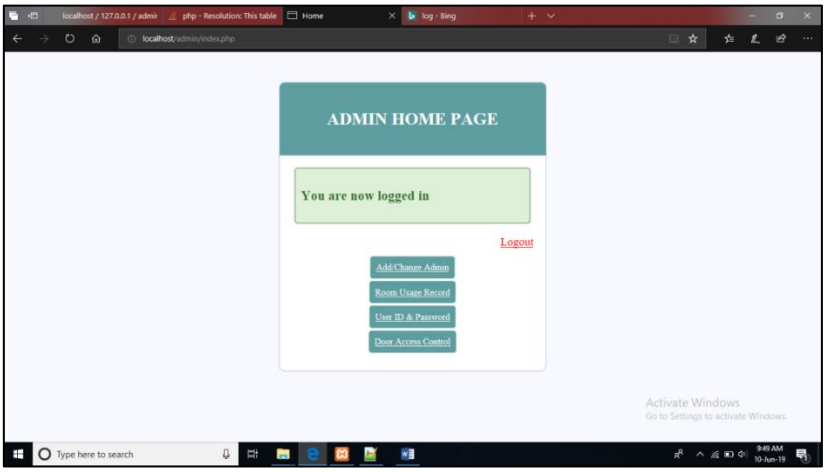

Figure 3: The design for admin homepage interface

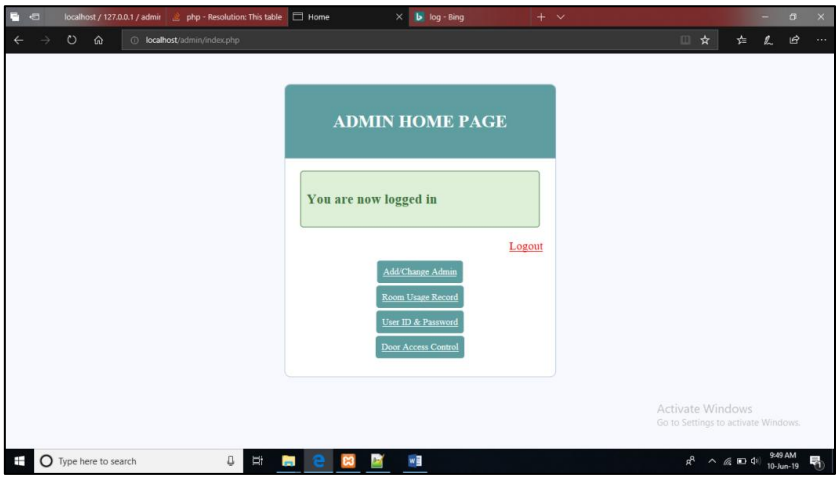

Figure 4: The design for admin interface to monitor the door being lock or unlock

3. Hardware and Software Integration:
    - Wi-Fi Module (NodeMCU): The NodeMCU microcontroller connects to a Wi-Fi network, allowing remote commands for locking and unlocking.

Figure 4: Unlock and lock the door

Purpose	To allow the person in charge to lock and unlock the door in just one click from a distance.
Role	The person in charge presses the lock or unlock button on the website.
Base Scenario	1. The system already works in the background. 2. The person in charge presses unlock or lock button on the website. 3. When NodeMCU receives the signal, it will know what actions need to be taken. 4. After that the servo will change position based on what action is chosen by the person in charge.
System Scenario	It will send the data of locking and unlocking the door to the database.

Table 2: Unlock and lock the door

- Web Interface: The web-based interface, created using PHP, enables the administrator to control access and view logs of room usage.

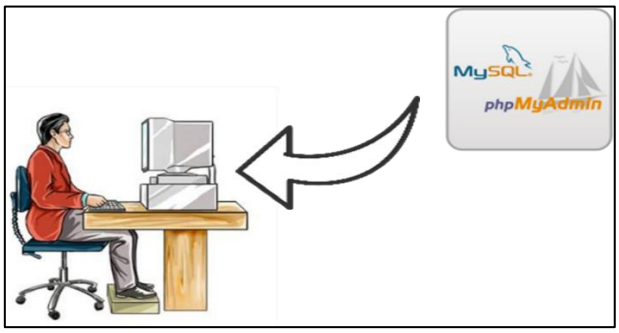

Figure 5: Monitor the room log

Purpose	To allow the person in charge to monitor the room usage.
Role	The person in charge will be able to know who or when someone enters or exits a room.
Base Scenario	1. The system already works in the background. 2. The person in charge has opened the page in the server. 3. Login into the admin page. 4. After login is successful the person in charge can view the room record data which will be shown in a table.
System Scenario	It will send the data to the PHP file to allow data to be displayed.

Table 3: Monitor the room log

4. Database Configuration: The system logs all access events in a MySQL database, managed through phpMyAdmin. This allows the system to store information about who accessed the room and when, accessible only by authorized personnel.

3.2 Development and Testing

Each component was tested independently and then integrated to assess the system's overall functionality. Testing involved checking the servo motor's response to lock/unlock commands, verifying Wi-Fi connectivity, and ensuring that access logs were accurately recorded in the database.

4.0 DATA ANALYSIS AND FINDINGS

The web-based access control system was successfully developed, tested, and met its objectives. Testing showed the effectiveness of remote control systems using Wi-Fi, as previously documented (Potts & Sukittanon, 2012). The reliability of real-time data logging was assessed in accordance with established IoT protocols for secure access (Jain & Shah, 2016).

Below are the key results from the testing phase:

4.1 System Functionality

1. Servo Motor and Door Lock Mechanism: The servo motor responded effectively to commands sent via the web interface, consistently locking and unlocking the door without delay.
2. Wi-Fi Connectivity: The NodeMCU ESP8266 module successfully connected to the Wi-Fi network, enabling remote control of the system from any device on the same network.
3. Data Logging and Monitoring: The system accurately recorded access events in the MySQL database, capturing the date, time, and user information for each room entry and exit. This feature allows administrators to track room usage and verify access history as shown in Figure 6.
    - Server: Localhost
    - Password & Username: Admin
    - Database name: Monitoring
    - Table name: userusage

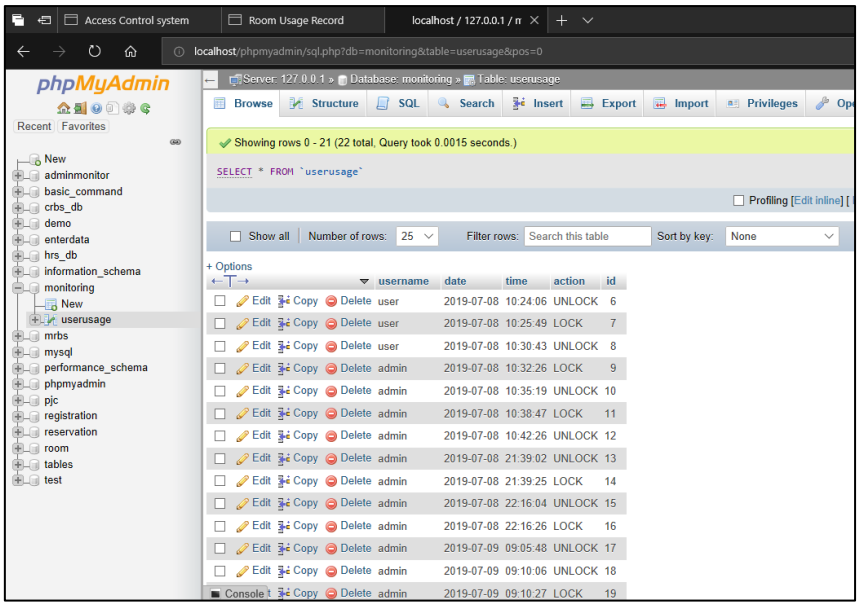

Figure 6: Database that keeps a record on the room log

4.2 Analysis of Web-Based Control

During testing, the web interface proved effective for remote management. Authorized personnel could log in, access the control page, and operate the door remotely. The system was also tested for security, ensuring that only users with correct credentials could access the control interface.

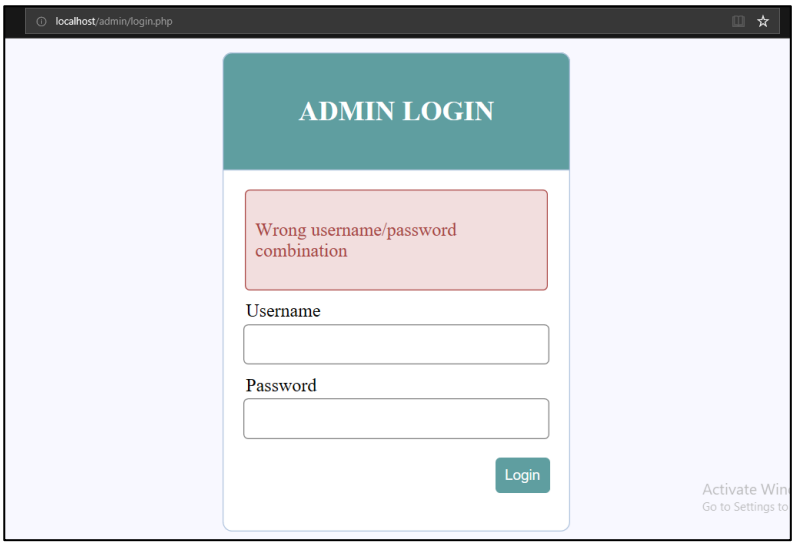

Figure 7: Admin login page that shows an error message if the username/password does not match the data in the database

Only the admin will be able to view the data that is sent by the NodeMCU into the database in the monitoring page as shown in Figure 4.22. It allows the admin to know who and at what time or date the room has been locked or unlocked. Other than that, the admin will also able to delete the record that had been created.

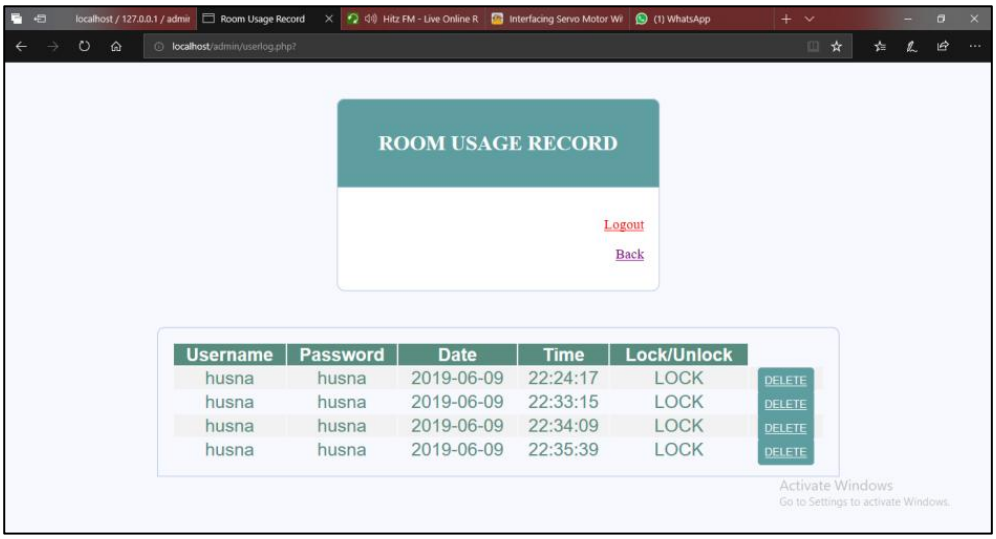

Figure 8: The design for the admin interface to monitor the door being locked or unlocked

4.3 Performance Assessment

The system demonstrated reliable performance in terms of speed and response time, with minimal delays. The results suggest that the web-based Wi-Fi control system is practical for environments that require flexible access management and remote monitoring.

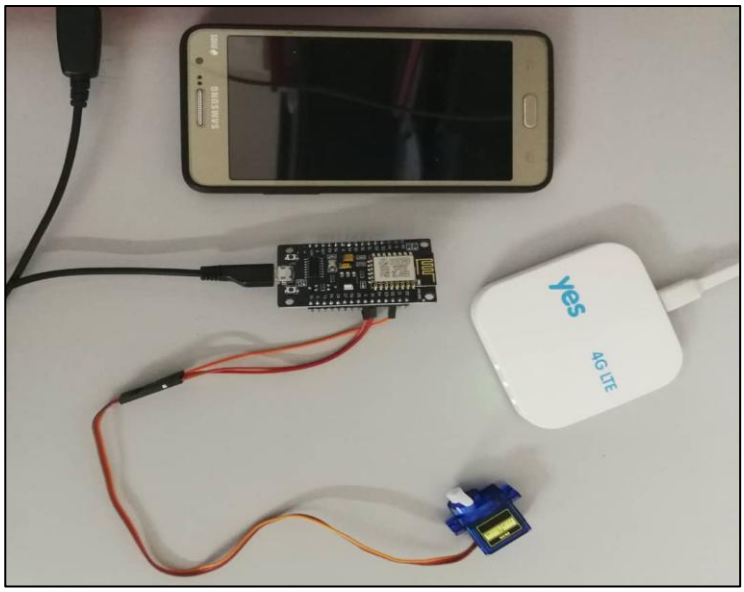

Figure 9: Setup for range testing and response time to lock and unlock the door using the website

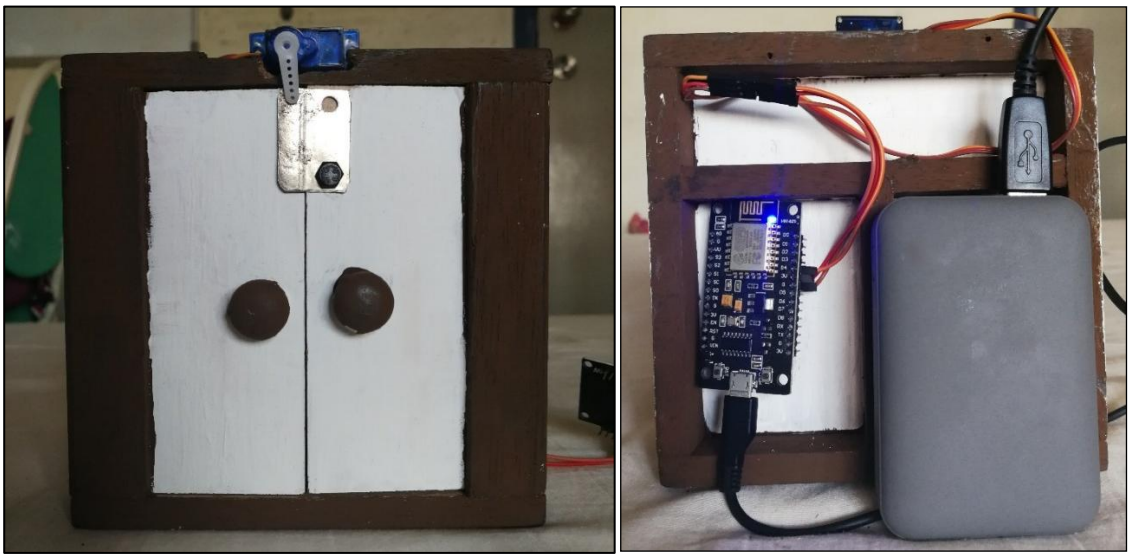

Figure 10: Front view and back view after combining the door prototype and the circuit

5.0 DISCUSSION AND CONCLUSIONS

The Web-Based Access Control System using Wi-Fi technology offers a flexible, efficient, and secure solution for managing access to rooms and facilities remotely. By integrating IoT components, such as the NodeMCU and a web-based interface, the system allows administrators to control and monitor room access from any device on the network.

The report concludes that Wi-Fi technology has proven practical for flexible access control systems, consistent with findings by Lopez and Rubio (2018). However, future work should aim to address network security issues noted in prior studies (Huang & Lee, 2015). The successful implementation at the Faculty of Computer and Mathematical Sciences (FSKM) at UiTM demonstrates its practical applications for institutions needing modern access solutions. The system effectively reduces the reliance on physical keys and manual monitoring, allowing for streamlined access control. Real-time monitoring and logging of access events provide security and accountability, ensuring that only authorized individuals can access specific rooms.

5.1 Limitations and Future Work

The limitation of this project is the project was only created for a situation with only one room with one door only and how the lock will be implemented on the real door instead of prototype. Other than that, the password and username created by the admin for the user will not be given automatically to the user and there is no case sensitive ability in checking the username or password.

While effective, the system's reliance on Wi-Fi means it may be susceptible to network issues or unauthorized access attempts. Future improvements could focus on:

1. Enhancing security protocols to further prevent unauthorized access.
2. Expanding the system's scalability to cover larger facilities or integrate with other IoT security devices.

Overall, this project demonstrates the potential of Wi-Fi technology in access control and sets a foundation for further research and development in IoT-based security systems.

REFERENCES

Adalan, K., & Burch Bursa. (2014). *Smart access control systems*. Journal of Emerging Technologies in Computing, 7(2), 56-63.

Huang, H. C., & Lee, Y. (2015). *Development of mobile-based access control solutions*. International Journal of Security, 10(4), 90-95.

Ismail, N. H., Ahmad, S., & Shafiee, A. (2014). *IoT-enabled access control in smart environments*. International Conference on Advanced Networking, Kuala Lumpur.

Jain, R., & Shah, K. (2016). *Password-based access control systems for IoT*. International Journal of Computer Applications, 12(3), 44-50.

Kassem, A., & Lin, J. (2016). *Mobile applications for access control using Wi-Fi and IoT*. IEEE Internet of Things Journal, 4(1), 8-15.

Kassem, A., Karmouch, M., & Marshall, T. (2017). *The evolution of access control systems*. Journal of Information Security, 9(3), 14-22.

Lopez, J., & Rubio, J. E. (2018). *Access control models in IoT environments*. ACM Computing Surveys, 51(2), 30-43.

Potts, J., & Sukittanon, S. (2012). *Wireless access control systems*. International Journal of Computing and Security, 6(1), 17-22.

Sandhu, R. S., & Samaranti, P. (1994). *Access control: Models and applications*. IEEE Transactions on Computers, 9(12), 1232-1245.