ACADEMICA PRESS SOLUTIONS

APS PROCEEDINGS

Editors:
Mohamad Rahimi Mohamad Rosman
Izzatil Husna Arshad
Nurulannisa Abdullah
Amira Idayu Mohd Shukry
Noor Rahmawati Alias
Nik Nur Izzati Nik Rosli
Faizal Haini Fadzil
Mohamad Sayuti Md.Saleh
Mohd Zafian Mohd Zawawi
Meida Rachmawati

VOLUME 14 2024

APS Proceedings Volume 14

Published 23 July 2024

e ISBN 978-629-99506-4-6

Published by:
Academica Press Solution [003428568-X]
Batu 23, Kg Jias,
17000 Pasir Mas,
Kelantan, MALAYSIA
Email: contact.digit360@gmail.com

Table of Contents

Research Article

IoT-Powered Protection: The Smart Door Access System

Ahmad Anwar Zainuddin[1,*], Rizal Mohd Nor[2], Amir Aatieff Amir Hussin[3], Muhammad Nurzikry Mohd Sazali[4], Muhammad Irfan Zaki Mohd Razali[5], Muhammad Nor Syahmi Khalid[6], Muhammad Nazmi Fazail[7], and Nik Muhammad Faris Firdaus Norazman[8]

1 Department of Computer Science, International Islamic University Malaysia; anwarzain@iium.edu.my; ORCID ID (https://orcid.org/0000-0001-6822-0075)

2 Department of Computer Science, International Islamic University Malaysia; rizalmohdnor@iium.edu.my; ORCID ID (https://orcid.org/0000-0002-8994-2234)

3 Department of Computer Science, International Islamic University Malaysia; amiraatief@iium.edu.my; ORCID ID (https://orcid.org/0000-0002-1508-7650)

4 Department of Electrical and Computer Engineering, International Islamic University Malaysia; nurzikrysazali@gmail.com

5 Department of Computer Science, International Islamic University Malaysia; irfanzaki1085@gmail.com

6 Department of Computer Science, International Islamic University Malaysia; syahmii.wolford@gmail.com

7 Department of Computer Science, International Islamic University Malaysia; nazmifazail749@gmail.com

8 Department of Computer Science, International Islamic University Malaysia; nikfaris055@gmail.com

* Correspondence: anwarzain@iium.edu.my; (+603) 6421 5646.

Abstract: *The proliferation of Internet of Things (IoT) technology has catalysed innovations in home security systems, particularly in the realm of smart door access. This study proposes a robust and efficient IoT-enabled smart door lock system. Traditional physical key door locks are fraught with vulnerabilities, ranging from susceptibility to damage to the risk of unauthorized duplication. In response, this research introduces a novel IoT Smart Door Lock system designed to alleviate these concerns. Utilizing Wi-Fi connectivity and smartphone integration, the system provides keyless access control, rendering traditional keys obsolete. Through the incorporation of NodeMCU ESP 8266 microcontroller and Virtuino IoT application, users can securely unlock doors with their smartphones, bolstering both security and convenience. Furthermore, the HiveMQ MQTT broker is used to enable efficient machine-to-machine communication within the IoT component, improving the efficiency and interoperability of the system. The practical implementation and testing of the system demonstrated its efficacy, achieving a 100% success rate across all functions. Moreover, a trial deployment at the Centre of Excellence for Cybersecurity (CoExCys) office yielded positive results, underscoring its potential applicability in diverse environments. By leveraging IoT technology, this innovative smart door access system represents a significant advancement in home security, offering users a seamless and reliable solution to safeguard their premises while enhancing accessibility and peace of mind.*

Keywords: Internet of Things; Smart door; NodeMCU ESP 8266.

1. INTRODUCTION

Ensuring the security of one's residence or workplace has always been paramount, with the door serving as the primary defence mechanism against intruders. Traditionally, physical keys were

the sole means of locking and unlocking doors, but with technological advancements, the landscape has evolved. The conventional reliance on physical keys poses inherent vulnerabilities, as keys can be duplicated, lost, or misplaced, compromising the security of the premises. As a result, a lot of people decide to upgrade their homes and businesses security by installing smart door lock rather than traditional keyed locks.

As humanity transitions to the era of Industrial Revolution 4.0 (IR4.0) and the advancement of wireless technology, the integration of the Internet of Things (IoT) holds enormous potential for revolutionizing door access systems. Leveraging IoT technology creates a novel security paradigm that offers diverse approaches to protection. Through sophisticated software programs and hardware sensors, IoT-based smart door entry systems can provide robust security layers, thereby strengthening both physical and digital defenses (Norarzemi et al., 2020). This not only increases productivity by eliminating the need for physical keys but also enables remote monitoring and control via Wi-Fi and Bluetooth connectivity. Solutions are developed to enhance security, comfort, and control, whether users are physically present or not (Chathuri Paranagama & Budditha Hettige, 2022). As highlighted in recent research, implementing IoT-based door access solutions is essential to enhancing security and promoting safe environments both at work and at home.

By harnessing the power of wireless technology and keyless control functionalities, this system offers unprecedented convenience and security. Central to this project is the utilization of NodeMCU, chosen for its ability to facilitate seamless Wi-Fi connectivity between hardware and software components. Complementing NodeMCU is the Virtuino IoT application, serving as the interface for controlling door access via mobile devices. Crucially, the integration of Message Queuing Telemetry Transport (MQTT) enables efficient machine-to-machine communication, enhancing the system's functionality and responsiveness (Zainuddin et al., 2023). Through this innovative combination of hardware and software, this IoT-based smart door access system represents a significant leap forward in door security solutions, promising enhanced accessibility and peace of mind for users. The previous work has been discussed (Zainuddin et al., 2023).

The adoption of IoT-based smart door access systems, as advances in Industry 4.0 continue, offers significant advantages over traditional key-based systems by addressing inherent vulnerabilities such as key duplication, loss, misplacement and susceptibility to damage as shown in Figure 1. Leveraging digital credentials and wireless connectivity through Wi-Fi and Bluetooth, these smart systems enable real-time remote monitoring and control, enhancing security and convenience. Integration of NodeMCU and the Virtuino IoT application provides seamless mobile device control, while MQTT ensures efficient communication between components, allowing for responsive and dynamic access management as shown in Figure 2. This technology not only streamlines administrative processes by eliminating physical key exchanges but also enhances productivity and safety through detailed logging and immediate response capabilities. Ultimately, IoT-based smart door systems represent a major advancement in securing residential and commercial properties, aligning with the goals of Industry 4.0 to utilize cutting-edge technology for improved efficiency and protection.

This paper adopts a structured approach to investigate the integration of a smart door entry system. Section I introduces the concept and outlines the objectives. Section II reviews existing research on smart door technology. Section III details the proposed model. Section IV presents the methodology, tests, and results. Finally, Section V summarizes the key findings and conclusions, and discusses their implications for the scientific discourse on smart door access systems.

Figure 1. Vulnerabilities of traditional key-based system.

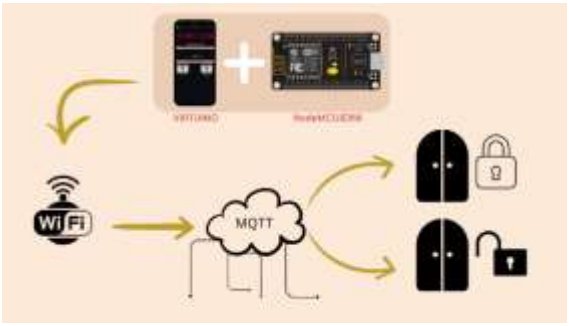

Figure 2. The Integration of the smart door**.**

2. METHOD & MATERIAL

The smart door access system consists of three parts which are the software, hardware, programming and the process part.

2.1 Hardware

The door is an electromagnetic door that have an electromagnetic bar that attracts the metal bar located on the door. The bar is magnetized when there is a 12 Voltage power. The bar will be magnetized and shut the door when it receives the 12 Volt. A buzzer is also used in the system as an alert when the door is unlocked. For accessing through the smart door, there are three access method physically which are the kill switch, as shown in Figure 3, the front desk switch and the touch switch, both shown in Figure 4. The touch switch is located on the circuit box, and can be accessed by any personnel in the premise to open the door. The front desk switch is located at the front desk of a premise, only able to be accessed by the authorised user such as the receptionist, as they can unlock easily from the desk, allowing access into and out of the premise. The kill switch is a permanent unlock, used only in case of emergency and maintenance. Only the admin or the technician should have the access to the kill switch. As shown in Figure 5, the microcontroller used in the smart door is the NodeMCU ESP 8266, used to connect the hardware and the hardware component while also can be connected to the internet by itself.

Figure 3. Circuit box and the touch switch represented by the bell icon.

Figure 4. The front desk switch and the kill switch located on the top.

Figure 5. The NodeMCU ESP 8266.

2.2 Software

The software used by the smart door is the Virtuino IoT application, a customizable IoT user interface app. The application used the HiveMQ MQTT broker that uses a Publish-Subscribe model

that allows messages to be sent from the HiveMQ to the subscribed devices, which in this case the door. Any custom message for the door can be displayed here by utilising the abundant of free-to-use widget that's responsive as long as it receives messages from the HiveMQ server. For the use of each door, implementation of the subject door must be made to the application first and the proper HiveMQ broker must be entered. Then, topics are entered under the door which are the door status, door ID, the door key. After implementing the topics, the appropriate widgets are implemented to enable the user to be able to interact with the smart door through the application. Accessing the door can be done by pressing the unlock switch on the app represented by the key widget. The finished user interface can be seen in Figure 6.

2.3 Arduino IDE Programming

The application used for the programming is the Arduino IDE. The programming sets up the connection to the internet, as can be seen in Figure 7, and the MQTT broker, which in this case, the broker is HiveMQ. Then, programming also writes up the instruction for the status of the door, the door ID, and the unlocking and locking of the door.

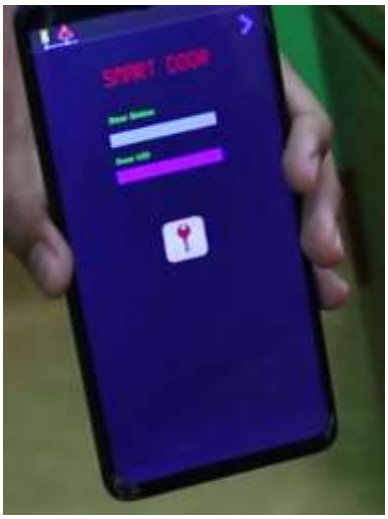

Figure 6. The Finished User Interface.

```
void setupWifi() {
  //Init WifiManager
  WiFiManager wifiManager;
  Serial.print("\n\nConnecting Wifi: ");
  //wifiManager.resetSettings();
  wifiManager.autoConnect("SDAKICT: WiFI Setup");
  Serial.print("Wifi Status: Connected");
}
```

Figure 7. Setting up the Internet connection.

2.4 The flowchart of smart door access system

When the user unlocks the door by any means except through the kill switch, a buzzer will be sounded for 3 seconds. The power source is cut from the magnet bar and the bar will be demagnetised. The application will display that the door is opened to the user in the door status section. The door will be opened for 10 seconds, allowing access into and out of the premise. After 10 seconds, the power source will be connected back to the bar and it'll be magnetized, which then after the door is closed physically, the door will be locked. The application will display that the door is locked. The kill switch activation has the same process but the power is cut and the door is unlocked permanently until the kill switch is deactivated.

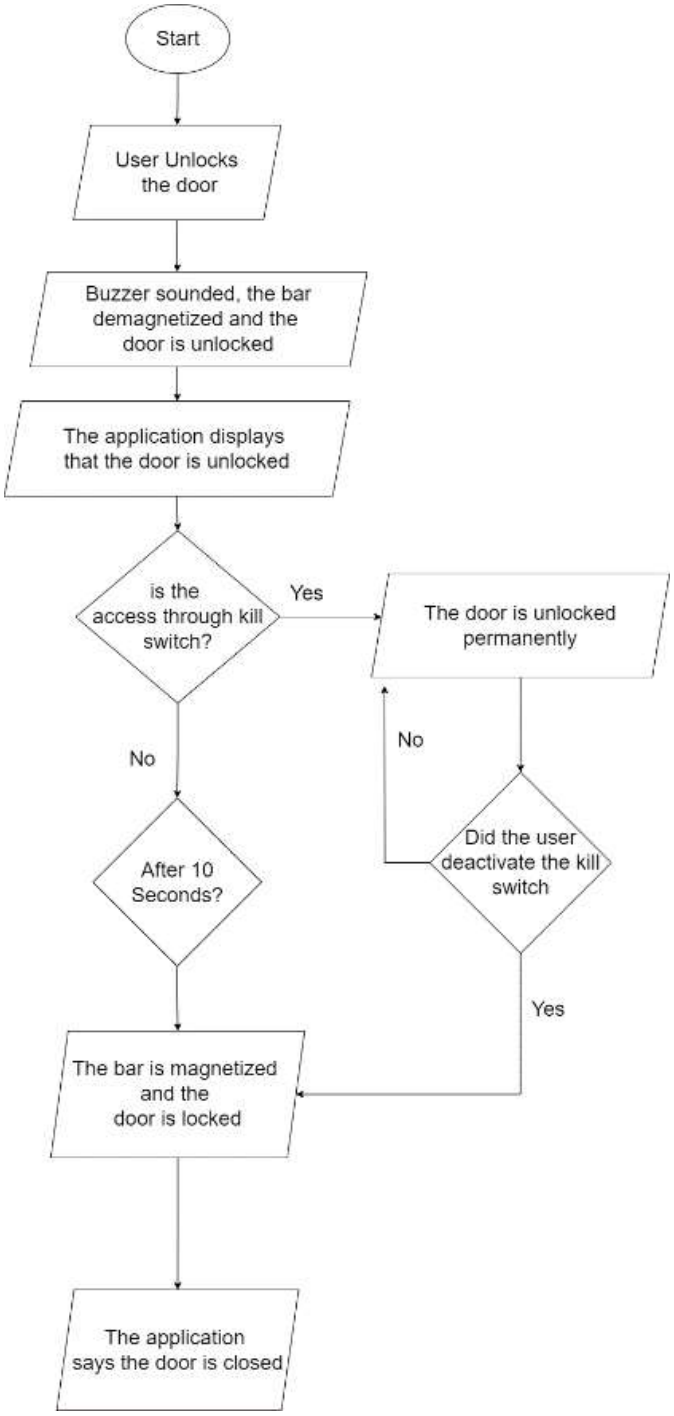

Figure 8. The flowchart of smart door access system.

3. FINDINGS

The creation of smart door access has been tried and proven to be effective. Door access can be functional and communicate in an IoT setting. The button function and door status update are perfectly connected and updated on the Virtuno IoT. In the meantime, the haptic switch, front desk switch, and kill switch button function are designed by the hardware components. The results of the door access using the mobile application's input and output functionalities are explained in Figure 9.

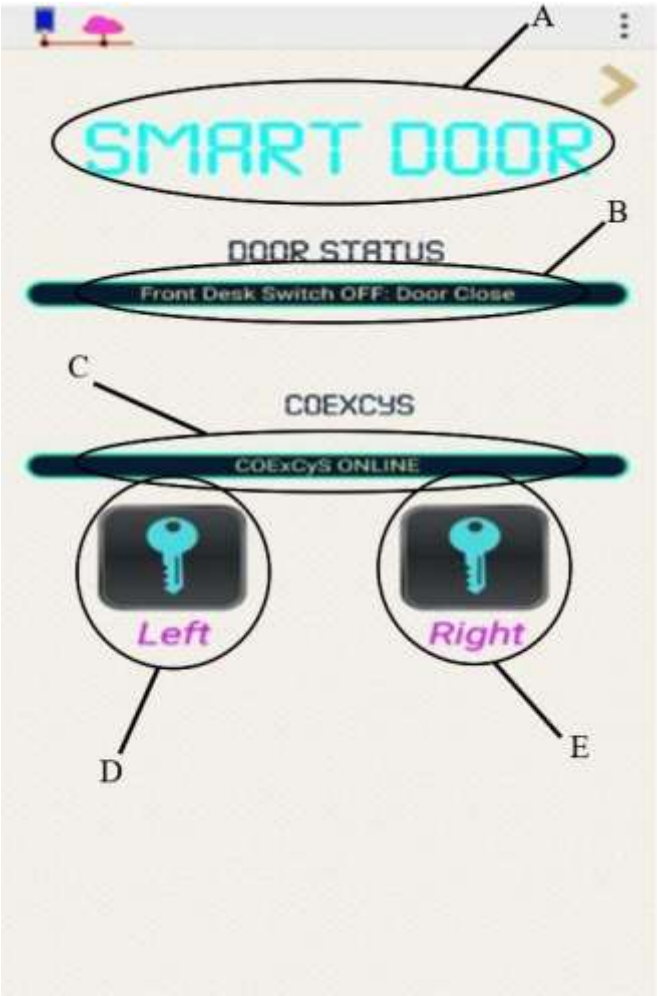

Figure 9. Door system user interface; a) User Interface heading b) Front Desk door status

c) COExCyS door status d) Left key icon e) Right key icon

Figure 9 is the user interface for the door system application. User will be informed whether the door is close or open at the door status section (b). The door can be access using either Left (d) or right (e) key depends on which door the user would like to open.

Table 1 illustrates the overall performance of the system by showing that every tested function has a 100 % success rate of triplicate testing. These doors have shown its potential on improving security. This consistency of the result indicates that the smart doors are highly dependable and could be an instrument in improving access control and security in various applications.

Table 1. Testing result

Testing Function	Smart door prototype		Smart door at CoExCyS	
	Triplicate of checking	Success Rate (%)	Triplicate of Testing	Rate of Success (%)
Application (Virtuino IoT) - left key button	Success	100	Success	100

Application (Virtuino IoT) - right Key button	Success	100	Success	100
Haptic Switch	Success	100	Success	100
Front Desk Switch	Success	100	Success	100

4. DISCUSSION

The smart door has been developed from a prototype, as shown in Figure 15, which then implemented at The Centre of Excellence for Cyber Security (CoExCyS), Kulliyah of Information and Communication Technology (KICT), International Islamic University Malaysia (IIUM), Gombak, Malaysia as can be seen in Figure 16. The implementation proves to be an enhancement towards security at CoExCyS, far better than the traditional physical lock. Figure 10 shows the final prototype, before the implementation at CoExCyS, which has been done as can be seen in Figure 11.

Figure 10. Prototype of smart door.

Figure 11. Implementation of smart door at CoEXCyS; a) The circuit box; b) Magnet bar.

The authors will introduce several initiatives guided by following principles. Firstly, a review of alternative Internet of Things platforms or microcontrollers for smart door entry systems would be conducted. A thorough checking and examination will be carried out to look for the weakness so that additional security precaution intended on improving the general security of the smart door system can be executed. Users' satisfaction is also our main concern. As a result, the application with an enhanced and more user-friendly interface for the smart door access system will also be developed.

5. CONCLUSION

In conclusion, the smart door access system is the future of security that must be expanded and thoroughly developed. The integration of the door using the Virtuino IoT application, the HiveMQ as the MQTT broker and NodeMCU as the microcontroller provides a modern solution towards the issue of security by providing a process of access that's easier, wireless and more secure. In the future, enhancement towards the system can be made such as implementing a much more complex

microcontroller to reduce the compactness of the circuit box and adding in additional security measure such as face recognition and keycode.

Acknowledgments: Special thanks to Silverseeds Lab Network, Centre for Excellence of Cyber Security and IoTeams for supporting this project.

References

Chathuri Paranagama & Budditha Hettige. (2022). *A review on existing smart door lock systems*. https://doi.org/10.13140/RG.2.2.18892.08325

Norarzemi, U. A. B., Zainal, M. S., Hassan, O. A., Zohari, M. H., Nor, D., Hamzah, S. A., & Mohamed, M. (2020). *Development of prototype smart door system with IoT application*. *1*(1).

Zainuddin, A. A., Nor, R. M., Hussin, A. 'Aatieff A., & Sazali, M. N. M. (2023). *MQTT-enabled smart door access system: design and implementation using NodeMCU ESP 8266 and HiveMQ*. *2023*

ACADEMICA PRESS SOLUTIONS

PREFACE

This book is a comprehensive compilation of articles covering various topics in social science, science and technology, literature, and product innovation. Each article is carefully selected and peer-reviewed by experts in the respective fields. This ensures that the content is of the highest quality and provides valuable insights into the latest developments. Moreover, these proceedings also aim to guide readers towards emerging mainstream topics, making it a valuable resource for researchers, academics, and professionals seeking up-to-date information and guidance in these areas. The collections are available online (https://zenodo.org/communities/apsproceedings/) and indexed by OpenAire and DOI provided by Zenodo.

e ISBN 978-629-99506-4-6