MQTT-Enabled Smart Door Access System: Design and Implementation Using NodeMCU ESP 8266 and HiveMQ

1st Ahmad Anwar Zainuddin
Department of Computer Science, Kuliyyah of ICT,
International Islamic University Malaysia
Kuala Lumpur, Malaysia
anwarzain@iium.edu.my

2ndRizal Mohd Nor
Department of Computer Science, Kuliyyah of ICT,
International Islamic University Malaysia
Kuala Lumpur, Malaysia
rizalmohdnor@iium.edu.my

3rdAmir 'Aatieff Amir Hussin
Department of Computer Science, Kuliyyah of ICT,
International Islamic University Malaysia
Kuala Lumpur, Malaysia
amiraatieff@iium.edu.my

4th Muhammad Nurzikry Mohd Sazali
Department of Electrical and Computer Engineering, Kuliyyah of Engineering,
International Islamic University Malaysia
Kuala Lumpur, Malaysia

2023 IEEE 9th International Conference on Computing, Engineering and Design (ICCED) | 979-8-3503-7012-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCED60214.2023.10425368

***Abstract*— The security of one's residence or property is an essential consideration that warrants careful attention to safeguard the premises and its contents. It has become increasingly apparent today that physical key door locks are susceptible to damage and can be compromised by unauthorized individuals. The inherent vulnerability of physical key door locks stems from their susceptibility to misplaced keys and duplication, as individuals are required to always carry them. This work presents a novel Internet of Things (IoT) enabled smart door access system designed to improve the security of homes or premises. The system offers keyless access to individuals who have been granted authorization. The system's architectural design incorporates the utilization of a NodeMCU ESP 8266 microcontroller to oversee door operations. Access control functionality is facilitated through the implementation of the Virtuino IoT application, which enables the unlocking of doors using smartphones. Additionally, a MQTT broker, specifically the HiveMQ, is implemented to facilitate effective machine-to-machine communication within the IoT components. The rationale behind the adoption of this IoT-based solution stems from the inherent weaknesses of traditional physical key door locks, which are prone to damage and replication, consequently jeopardizing security measures. The proposed system aims to address these limitations by rendering traditional keys obsolete, thereby improving both security and convenience for users. The system has undergone comprehensive development, testing, and operationalization, resulting in a highly functional system. The success rate of all functions has consistently achieved a 100% level, which serves as an indication of the system's robustness and effectiveness. In addition, the practical implementation of the system in the Centre of Excellence for Cybersecurity (CoExCys) office at Kuliyyah of ICT IIUM exhibited smooth operation and the absence of any operational challenges throughout a trial period lasting one week. The findings highlight the potential of the system as a feasible solution for enhancing security and regulating access in diverse environments.**

Keywords—Smart door access system; NodeMCU ESP 8266; Virtuino IoT; MQTT; HiveMQ.

I. Introduction

The main concern of a door locking system is its accessibility and security. Traditionally, people use keys to lock their houses and offices. However, physical keys and their locks provide limited security as they can be easily duplicated providing access to anyone who has the key. Furthermore, the key door locks are easy to break, and the keys can be misplaced since the keys are often carried everywhere [1]. Due to this concern, people nowadays are implementing keyless door lock systems as they can provide a better secure environment for the workplace and home[2].

Moving toward Industrial Revolution 4.0 (IR4.0) and wireless technology generation, the implementation of the Internet of Things (IoT) can give better security to the door system. It can offer a reliable door access protection system by providing multiple layers of security on its software program and hardware sensors, enhance people's productivity as they do not need to bring physical keys with them anymore, and can monitor and control the door access remotely using Wi-Fi and Bluetooth and the usage of sensors [2]. Therefore, the implementation of IoT IoT-based smart door access system should be an essential thing. People should ensure better security and a safe environment for their workplaces and houses.

This work proposes the implementation of an IoT-based smart door access system that can provide wireless and keyless control of door access using a smartphone. In this project, NodeMCU is used as it can support a Wi-Fi connection between the hardware and the software. Virtuino IoT is used as an application to control the door access on the mobile device with Message Queuing Telemetry Transport (MQTT) to provide machine-to-machine communication.

This paper is arranged as follows: Section I gives a brief introduction to the concept and purpose of the implementation of a smart door access system. Section II focuses on the study and implementation of existing smart door development and research. Section III describes the proposed model for this paper. Section IV shows the testing of the model and its results. Finally, section V summarizes and concludes this paper.

II. LITERATURE REVIEW

A. Recent Trends on IoT Applications on Smart Door Access Systems

Over the past decade, IoT development and application have experienced robust growth, driven by the advancement of technology that enables effortless connectivity and also the adoption by various industries. Cisco estimated that there will be 50 billion IoT connections in 2020, while Huawei predicted that the number of IoT connections will reach 100 billion by 2025 [3]. For IoT applications in smart door systems alone, records almost a thousand studies on this project as shown in Fig. 1.

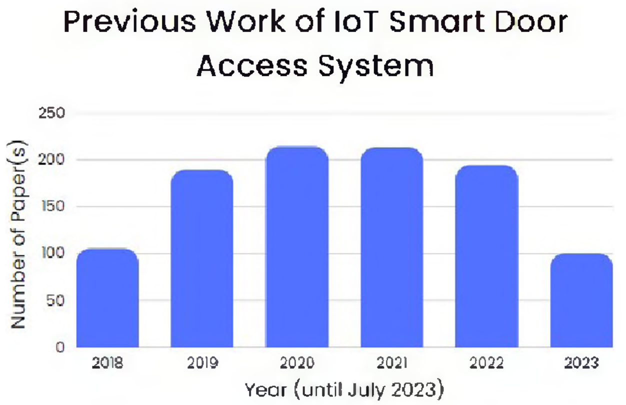


Fig. 1. Studies were done on IoT-based Smart Door Systems from 2018 until July 2023

The preliminary phase of IoT development, which has been discussed in the article, represents the previous work in this field [4-7].

B. Smart Door Access System

Smart door systems have undergone significant advancement in recent years to enhance the security of the system. This includes the implementation of multiple layers and phases of security in the smart door design through many technologies from the basic Bluetooth and Wi-Fi technology system to the variation of the usage of smartphone devices, embedded systems, sensors, and actuators. This variation creates various types of smart door systems as in Table I:

TABLE I. LIST OF SMART DOOR SYSTEM

Type of smart door system	Description	Advantage & Drawback
Wireless smart door lock	Mobile applications are implemented as a medium to lock and unlock the door[2], [8-12]. The mobile application transmits a signal via Wireless Fidelity (Wi-Fi) or Bluetooth, and the door will respond accordingly based on the signal received from the mobile application.	Advantage: Convenience, Enhance security. Remote access Management Keyless. Drawback: Connectivity and power source dependence Cybersecurity concerns Potential malfunction
Biometric recognition door lock	This system relies on biometric technology, which utilizes human biology characteristics to initiate the signal to unlock the door. The system will recognize the users by identifying their fingerprints facial features or voices. Upon successful identification, the system will transmit the signal to the lock mechanism.	Advantage: Enhance security Reduce the risk of identity theft Fast and convenient. Drawback: False biometric detection, Environmental factors may reduce accuracy Privacy and data security concerns
RFID card door lock	This system implements the usage of Radio Frequency Identification (RFID) to access the lock mechanism[11]. The system will detect the ID card with an RFID chip planted inside it. When the system recognizes the ID card, it requires the user to insert a password using the keypad. Once both authentications are successful, the system will transmit the signal to the door lock	Advantage: Durable and scalable Enable audit trails Enable user access management Drawback: Risk of card loss Power source dependency Vulnerable to cloning and spoofing attacks
QR-based door lock	This system implements the Quick Respond (QR) barcode to access the door[13]. The user is required to register for his/her ID before obtaining the generated QR code. Then the system will detect if the QR is identical to the system. When the QR detection is successful, the system will send a signal to open the door.	Advantage: Easy to use Cost-effective Enable temporary access Drawback: Limited range, Smartphone dependency Require internet connectivity
Visible Light Communication (VLC) LED color-coded door lock	This system operates by the user device recognizing the LED that transmits a grid color-coded pattern from the facility, then it will recognize the user authentication code and send a response signal to the door lock camera sensor. The door lock camera sensor then will recognize the grid color pattern from the user device before enabling the door access to the user [10].	Advantage: Secure communication Fast High accuracy Energy efficient Drawback: Complex implementation Indoor use only Distance limitation Limited adoption Compatibility

C. Microcontroller

Microcontrollers play a significant role in developing IoT systems. Microcontroller functions to connect the electrical hardware parts and the software system. It consists of CPU, memory, and Input/Output (I/O) peripherals as the main parts. The microcontrollers work by processing the data and information received from the I/O and processing it in the CPU before transmitting the signal to control the device. The memory will store the temporary information received by the microcontroller to be accessed by the processor to process the incoming data. Table II explains various types of controllers that are usually used in developing IoT systems.

TABLE II. LIST OF MICROCONTROLLERS

Type of microcontroller	Description	Key Feature
NodeMCU ESP8266 / ESP 32	NodeMCU ESP8266 is an open-source board development that is widely used in Internet of Things (IoT) projects and can be programmed using Arduino IDE[2], [14]. It also incorporates firmware designed to run on the ESP8266 Wi-Fi system-on-a-chip (SoC) from Espressif System. NodeMCU also provides a convenient platform for building IoT projects as it combines the microcontroller unit (MCU) with built-in Wi-Fi that makes it easy to connect with the internet and communicate with other devices.	1.Wi-Fi connectivity 2.Low cost 3.GPIO pin availability
Raspberry Pi	Raspberry Pi (RPi) is an affordable computer alternative that operates on the Linux Operating System[10], [13]. It offers a set of General Input/Output (GPIO) pins that allow users to connect and control a wide array of devices and peripherals. Raspberry Pi is often used in IoT projects due to its versatility which makes it suitable for a diverse range of projects and applications.	1.Runs on Linux OS environment 2.GPIO and other interfaces' pin availability 3.HDMI output availability 4.Extensive software support 5.Expensive
Arduino UNO	Arduino UNO is a popular microcontroller board from the Arduino family that is widely used for prototyping and DIY electronics projects [8][11][15]. The board features an ATmega328P microcontroller as its core, along with digital input/output pins, analog input pins, and other dedicated pins for specific functionalities making it accessible even for electronics and programming field beginners.	1.Beginner-friendly 2.Cheap 3.Compatible with various shield 4.Open source 5.Wide variety of sensors and actuators 6.Not support Wi-Fi.
STM 32	STM 32 is a microcontroller developed by STMicroelectronics and based on ARM Cortex-M processor cores. It is widely used in embedded systems and IoT applications due to its wide range of integrated peripherals including GPIO, communication interface, timers, analog-to-digital converters, and others.	1.Arm Cortex-M cores 2.Rich peripherals set. 3.Comprehensive development ecosystem 4.Enable low power mode.
Silicon Labs EFM 32	Silicon Labs Energy Friendly Microcontroller (EFM) 32 is developed for energy efficient and low energy operation which is suitable for battery-operated IoT applications.	1.Ultra-low power 2.Support Gecko Technology 3. Advanced peripherals integration 4.Comprehensive software development tools and libraries

III. Methodology

This project consists of two parts which are the software part and the hardware part. The software parts focus on the coding of the NodeMCU to create a topic and subscription for communication between the application and the IoT device using HiveMQ protocol. The hardware part consists of a combination of the power supply, the hardware connection between NodeMCU with buzzer, touch switch, front desk switch, kill switch, and electromagnetic door.

A. *Software Parts*

The system will operate when the Virtuino IoT application detects the smart door via the internet network. Once the mobile is connected to the smart door, the door status will be shown whether it is open, closed or door initialized. The user who has access to the project file on the apps can control the operation of the door by simply touching the key icon to open the door the door will then open and give access for the user to enter and in 10 seconds the door will automatically be locked. The function process is explained in Fig. 2 below.

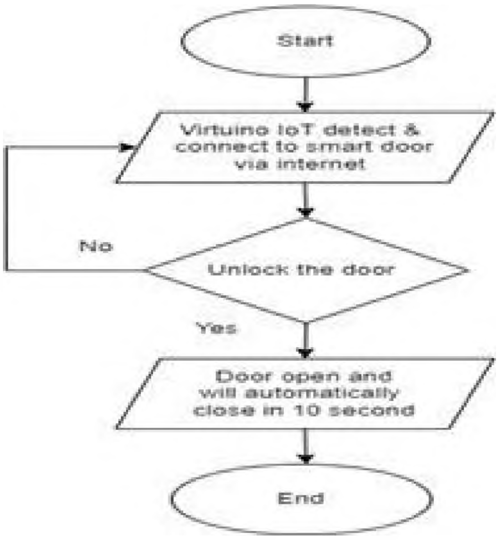

Start
Virtuino IoT detect & connect to smart door via internet
No
Unlock the door
Yes
Door open and will automatically close in 10 second
End

Fig. 2. Process flowchart of the door access

B. *Hardware Parts*

For the hardware parts, the NodeMCU is connected to the power source to provide voltage to lock the electromagnetic door. The hardware part also consists of a combination of kill switches outside the premises for emergency and maintenance purposes which will cut the voltage supply to the right door which will open the door. The hardware design also includes a touch switch and front desk switch located inside the premises to ease people inside to open the door or give access to unauthorized users, and a buzzer to indicate the door is unlocked. Fig. 3 and Fig. 4 show the block diagram for the connection with the NodeMCU and the hardware parts.

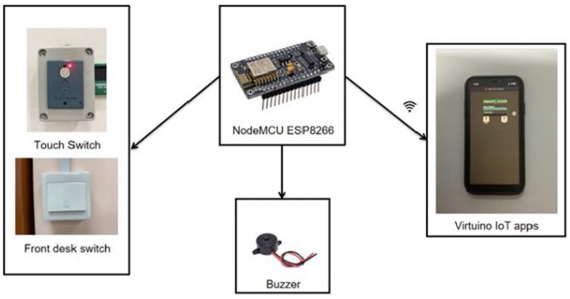


Fig. 3. Block diagram of NodeMCU connection

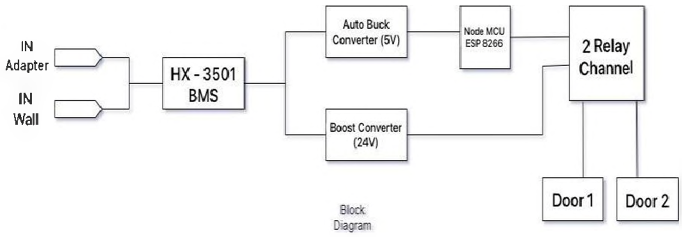


Fig. 4. Block diagram of the prototype hardware

C. Operation Block Diagram

Fig. 5 shows the UML for the use case combining the operation of the door access between the hardware and software parts.

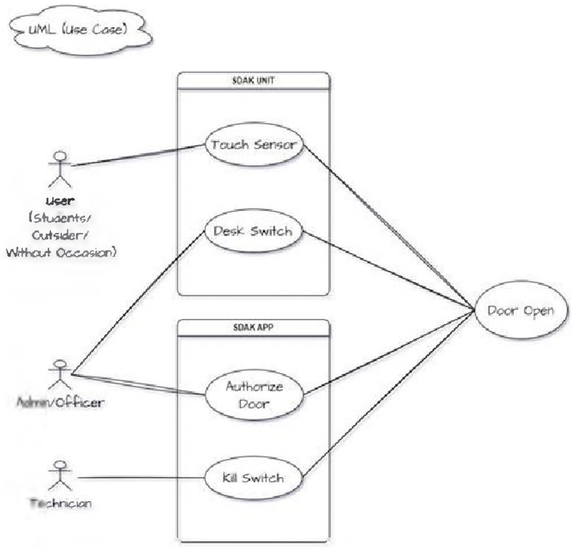


Fig. 5. Block diagram for full operation

The figure illustrates that only the actor (user) can utilize access to the door wirelessly via a mobile application. On the contrary, an unauthorized user would require permission from the people inside the premises and access is given through the use of a touch switch or a front desk switch. Alternatively, they can also use the mobile application to give access to unauthorized users. In emergency cases, only the technician is authorized to use the kill switch for emergency and maintenance purposes.

D. List of Materials

This IoT work is delivered through its controlling device that controls door access using a mobile application. A microcontroller is programmed to make communication between the public protocol and to initiate the signal of the sensor, electromagnetic door, and all switches by connecting it all to the microcontroller. Table III provides the details of the list of main materials and components.

TABLE III. LIST OF MATERIAL

Component	Function	Specification
NodeMCU ESP 8266	Act as a backbone and connector between the hardware components and software devices. It can be connected to the internet without aid from other electronic components.	Open-source firmware and development kit that was widely used to build IoT prototypes. It includes firmware that runs on ESP8266 Wi-Fi SoC by Espressif System.
Virtuino IoT Application	Act as an IoT platform to control door lock mechanisms. The user interface is created and customized based on the IoT application's suitability. These apps are used to open the door wirelessly and enable the door to unlock for 10 seconds before it automatically locks again	An application where users build their interface, widgets, and dashboard that is suitable for IoT projects. Supports various communication protocols for information transfer.
HiveMQ	The MQTT broker for a communication protocol for IoT applications. Follows a publish-subscribe architecture. Enabling devices and applications to publish messages to designated topics such as “Door Initialized” when the door is unlocked, which are then received by subscribed devices or applications.	Provide a Publish-Subscribe Architecture model that can handle control and deliver messages between devices.
Buzzer	To alert the user when the door is unlocked	5V buzzer that can give sound ranging from 70dB-100dB
TTP 223 Touch Switch & Front Desk Switch	Switch to open the door manually from the inside to allow visitors who have no access to enter. Both the left and right doors will open for 10 second	An embedded touch switch that installed on the hardware box. Utilize capacitive touch sensing technology. Able to detect the touch input and trigger the output in milliseconds
Electromagnetic Door	The door is locked when the power voltage is supplied and unlocked when the is no power voltage supplied to the door	Require 24V voltage power to provide a strong holding force of the electromagnetic to lock the door
Kill Switch	To shut down the smart door system for maintenance and emergency purposes. Enable the right door to open until the switch is off	Switching off to disconnect the connection of the circuit to the door

E. Topology

In this study, MQTT is being implemented to connect mobile apps and ESP8266 that control door operation. MQTT works by using the topic publish-subscribe concept where the publisher needs to send data to the receiver (publish) and the receiver receives the data (subscribe).

In Fig. 6, the connection and communication process between the private Wi-Fi and Cloud HiveMQ is shown. It functions as follows: Virtuino IoT sends an operation signal to open the left right or both doors using the key button on the application. The Virtuino IoT itself acts as a MQTT client and publishes a topic as an operation message to open the door and to receive the door update whether it is unlocked or locked to the Cloud HiveMQ. HiveMQ operates as an MQTT broker and routes messages to the private Wi-Fi connection to distribute the message to the electromagnetic door that also acts as a MQTT client. The electromagnetic door will subscribe to the messages and operate as requested to unlock the door and consequently send back a MQTT message of the door status to the Virtuino IoT application.

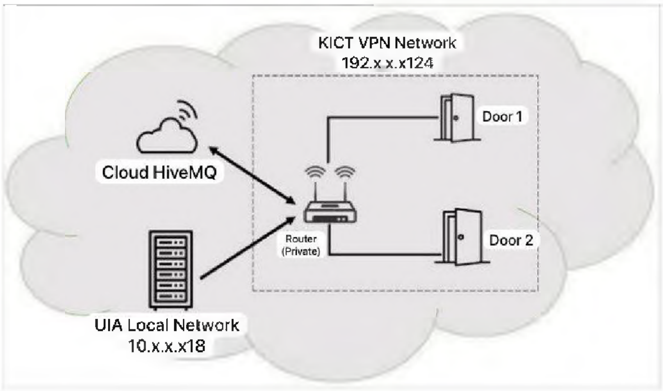
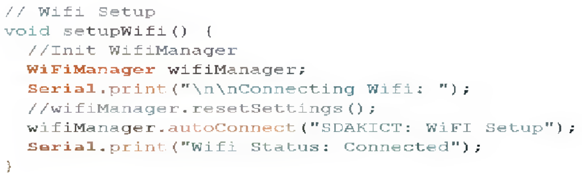


Fig. 6. Topology connection between Wi-Fi and Cloud HiveMQ

F. Software Development

To develop all the instructions for the IoT device, NodeMCU ESP 8266 is programmed using Arduino IDE. The program codes include the establishment and connection from the Wi-Fi with the NodeMCU of the smart door to enable the whole smart door to function. After the connection is established, the other operation and function controlled by the NodeMCU to unlock and auto-lock the door will be functioning. The program includes the coding of IoT devices to connect to the premise Wi-Fi as in Fig. 7.



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

Fig. 7. Coding to establish the connection between the IoT device to Wi-Fi

IV. Result and Discussion

The development of smart door access is tested and objectively successful. In the IoT environment, door access can communicate and function well. The button function, and door status update on the Virtuino IoT working perfectly. Meanwhile, the hardware parts which include the touch switch, front desk switch, and kill switch button also work as what has been proposed and programmed. Table IV below explains the results of the input and output functions of the door access using the mobile application.

TABLE IV. PROTOTYPE OUTPUT

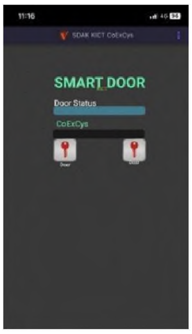
<table>
<tr><th>Input</th><th>Output</th></tr>
<tr><td colspan="2">
SMART DOOR
Door Status
CoExCys

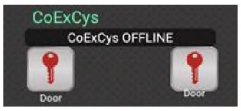
Fig. 8. Virtuino IoT user interface</td></tr>
<tr><td>
CoExCys
CoExCys OFFLINE

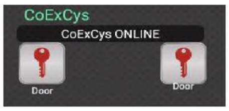
Fig. 9. Virtuino IoT did not detect the door</td><td>
CoExCys
CoExCys ONLINE

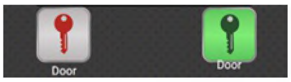
Fig. 10. Virtuino IoT detects the door and the "Door Online" status is updated.</td></tr>
<tr><td>

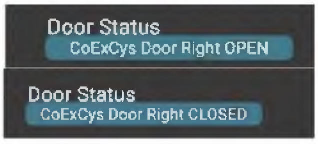
Fig. 11. The door button becomes green indicating "open"</td><td>
Door Status
CoExCys Door Right OPEN
Door Status
CoExCys Door Right CLOSED
Fig. 12. (a) "Door Open" status updated; (b) "Door Close" status updated after 10 seconds.</td></tr>
</table>

TABLE V. TESTING RESULT

Testing Function	Specification		
	Number of Testing	Success	Success Rate (%)
Virtuino IoT left key button	10	10	100
Virtuino IoT right key button	10	10	100
Touch Switch	10	10	100
Front desk Switch	10	10	100
Kill Switch	10	10	100

According to Table V, all functions reach a 100% success rate indicating the whole system is working well. The door is also already being implemented in the Centre of Excellence for Cybersecurity (CoExCys) office in Kuliyyah of ICT IIUM for a week and the result also shows the system is working without any arising issues. Fig. 13 shows the IoT smart door circuit box that has been installed at CoExCys office KICT IIUM to control the whole door access system.

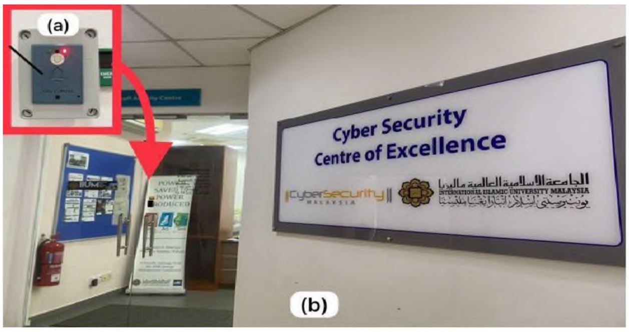


Fig. 13. (a) smart door hardware circuit box. (b) The installation of smart door circuit box at CoExCys office.

Several initiatives will be undertaken, guided by the following principles: Initially, an examination will be conducted regarding alternative microcontrollers or IoT platforms that can be utilized in smart door access systems. Furthermore, a comprehensive examination will be conducted to explore supplementary security measures aimed at enhancing the overall security of smart door access systems. Furthermore, a comprehensive evaluation of the proposed system will be carried out in various contexts to determine its performance and efficacy. Furthermore, the development of a mobile application will be undertaken to provide users with an enhanced and intuitive interface for the smart door access system. There will be endeavors to integrate the intelligent door access system with additional IoT devices or systems, to establish a comprehensive smart home or smart building solution.

V. Conclusion

To conclude, the study and development of IoT-based smart door access systems enable to provide a more secure environment for the premises and ease users to not use the physical key anymore. The study gave a better understanding of how to develop door access using the NodeMCU ESP 8266 microcontroller, Virtuino IoT application with the implementation of HiveMQ public protocol. The study also gave a better grasp of how IoT works and its implementation of door access. The outcome of this study and work has fulfilled the objective where the NodeMCU ESP8266 integrated with Virtuino IoT has been implemented to enhance the security of the door access system. This work is preliminary to understand the implementation of IoT smart door access that allows keyless access for the staff and authorizes users. In future development, the improvement of this work will be made to reduce its errors and enhance its security, smoothness of door operation, and improve its function.

Acknowledgement

This research work is fully sponsored by the IIUM RIGS grant KICT-RG20-010-0010, Cybersecurity (CoExCys), Kuliyyah of ICT, IIUM and Silverseeds Lab Network, for their significant contributions, which have undoubtedly enhanced the quality and impact of this work.

References

[1] M. Pavelic, Z. Loncaric, M. Vukovic, and M. Kusek, “Internet of Things Cyber Security: Smart Door Lock System,” in 2018 International Conference on Smart Systems and Technologies (SST), Osijek: IEEE, Oct. 2018, pp. 227–232. doi: 10.1109/SST.2018.8564647.

[2] U. A. B. Norarzemi et al., “Development of Prototype Smart Door System With IoT Application,” vol. 1, no. 1, 2020.

[3] B. C. Ervural and B. Ervural, “Overview of Cyber Security in the Industry 4.0 Era,” in Industry 4.0: Managing The Digital Transformation, in Springer Series in Advanced Manufacturing. Cham: Springer International Publishing, 2018, pp. 267–284. doi: 10.1007/978-3-319-57870-5_16.

[4] Zainuddin, A. A., Bhattacharjee, S., Kalliat, S., Shrestha, S., Sivaraman, S., Khalique, M. M., ... & Manokaran, P. (2021). Trends and Challenges of Internet-of-Things in the Educational Domain. Malaysian Journal of Science and Advanced Technology, 81-88.

[5] Rajiv, S. A., & Zainuddin, A. A. (2021). Review of New Trends and Challenges of Android-Based Home Security Robot. Malaysian Journal of Science and Advanced Technology, 103-108.

[6] Jusat, N., Zainuddin, A. A., Sahak, R., Andrew, A. B., Subramaniam, K., & Rahman, N. A. (2021, August). Critical Review In Smart Car Parking Management Systems. In 2021 IEEE 7th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA) (pp. 128-133). IEEE.

[7] Zainuddin, A. A., Sahak, R., Jusat, N., Kaitane, W. S., Rahman, S. H. A., Mansor, A. F. M., ... & Subramaniam, K. (2022). Modelling a Smart Parking Management System (SPMS) based on Integrated IoT. Multidisciplinary Applied Research and Innovation, 3(4), 72-81.

[8] Sialee Leekongxue, Li Li, Tomas Page, and Tianjin University of Technology and Education, “Smart Door Monitoring and Locking System using SIM900 GSM Shield and Arduino UNO,” Int. J. Eng. Res., vol. V9, no. 04, p. IJERTV9IS040011, Apr. 2020, doi: 10.17577/IJERTV9IS040011.

[9] A. Zhang and R. V. P. Kandubai, “Access Control Schema for Smart Locks using a Wifi Bridge: An exploration of a smart lock access control system based around the SimSim retrofitting smart lock.,” in 2020 6th International Conference on Robotics and Artificial Intelligence, Singapore Singapore: ACM, Nov. 2020, pp. 174–178. doi: 10.1145/3449301.3449331.

[10] S. H. Yoon et al., “IoT Open-Source and AI based Automatic Door Lock Access Control Solution,” Int. J. Internet Broadcast. Commun., vol. 12, no. 2, pp. 8–14, May 2020, doi: 10.7236/IJIBC.2020.12.2.8.

[11] M. I. Mohamed Ariff, F. D. Mohamad Fadzir, N. I. Arshad, S. Ahmad, K. A. Salleh, and J. A. Wahab, “Design and Development of a smart garage door system,” in 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada: IEEE, Jun. 2022, pp. 1–6. doi: 10.1109/IEMTRONICS55184.2022.9795768.

[12] Y. T. Park, P. Sthapit, and J.-Y. Pyun, “Smart digital door lock for the home automation,” in TENCON 2009 - 2009 IEEE Region 10 Conference, Singapore: IEEE, Nov. 2009, pp. 1–6. doi: 10.1109/TENCON.2009.5396038.

[13] A. F. M. Fauzi, N. N. Mohamed, H. Hashim, and M. A. Saleh, “Development of Web-Based Smart Security Door Using QR Code System,” in 2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), Shah Alam, Malaysia: IEEE, Jun. 2020, pp. 13–17. doi: 10.1109/I2CACIS49202.2020.9140200.

[14] T. Kadak and S. ÖzdemiR, “Security-Oriented Smart Door Lock à la Internet of Things,” Eur. J. Sci. Technol., Apr. 2021, doi: 10.31590/ejosat.898085.

[15] S. B. Saleh et al., “Smart Home Security Access System Using Field Programmable Gate Arrays,” Indones. J. Electr. Eng. Comput. Sci., vol. 11, no. 1, p. 152, Jul. 2018, doi: 10.11591/ijeecs.v11.i1.pp152-1