MJSAT

Malaysian Journal of Science and Advanced Technology

journal homepage: https://mjsat.com.my/

Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology

Ahmad Anwar Zainuddin[1,*], Ammar Daniel Abd Rahman[1], Rizal Mohd Nor[1], Amir Aatief Amir Hussin[1], Nik Nor Muhammad Saifudin Nik Mohd Kamal[1,4], Abu Ubaidah Shamsudin[2], and Muhamad Syariff Sapuan[3,4]

[1]*Kuliyyah of Information Communication Technology, IIUM Gombak, Malaysia.*
[2]*Industry and Community Relation Centre Universiti Tun Hussein Onn Malaysia.*
[3]*Jabatan Fizik Gunaan, Fakulti Sains and Teknologi, Universiti Kebangsaan Malaysia.*
[4]*Silverseeds Lab Network, Kuala Lumpur, Malaysia.*

KEYWORDS

Internet of Things
Smart door
NodeMCU ESP 8266
RFID
Fingerprint

ARTICLE HISTORY

Received 11 June 2024
Received in revised form 2 August 2024
Accepted 13 August 2024
Available online 26 August 2024

ABSTRACT

Security concerns in residential and working environments are more critical than ever, yet traditional door locks that rely on physical keys still hold significant vulnerabilities. Those key risks include loss, misplacement, or copying and may result in unauthorized access. Moving into Industry 4.0, there is great potential to integrate IoT technology to create a far more sophisticated and resilient door access system to handle such concerns. This paper analyze the design and development of a new IoT-based smart lock system enhancing security with fingerprint recognition, RFID technology, and application control via Wi-Fi as an additional to conventional lock such as kill switch and also front desk switch. In the discussed system, the ESP8266 microcontroller is used for wireless communication. Then, Virtuino IoT applications provided the function for real-time monitoring, while HiveMQ MQTT broker secured data transmissions. Therefore, the electromagnetic locking mechanism at the door was improved by using multi-layer access control. As mentioned, the methodology would provide an integration of critical hardware parts, such as NodeMCU ESP8266, Arduino Uno and electromagnetic locks, with robust software solutions in terms of secure communication and control. Once developed, the system architecture will be simulated and tested for its effectiveness in achieving better security and operational efficiency. The opted multi-layered security system can be beneficial to residential and working environment and is designed to overcome the limitations of conventional locks. Thus, enhancing the implementation of IoT-based security solutions in everyday life.

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 choose smart door locks over standard keyed locks to increase the security of homes or places of business [1].

As a transition towards the era of Industrial Revolution 4.0 (IR4.0) and embrace wireless technology advancements, the integration of the Internet of Things (IoT) holds immense potential in revolutionizing door access systems. By leveraging IoT technology, a new paradigm of door security emerges, offering a multifaceted approach to protection. Through sophisticated software programs and hardware sensors, IoT-based smart door access systems can provide robust layers of security, bolstering both physical and digital defences [2]. This not only enhances productivity by eliminating the need for physical keys but also enables remote monitoring and control via Wi-Fi and Bluetooth connectivity. As long as people want security, convenience and control, solutions will be developed, whether physically present or not [1]. As highlighted in recent research, the implementation of IoT-based solutions for door access is imperative in ensuring heightened security and fostering safe environments for both workplaces and residences.

*Corresponding author:
E-mail address: Ahmad Anwar Zainuddin <anwarzain@iium.edu.my>.
https://doi.org/10.56532/mjsat.v4i4.335

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 [3]. 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 [3].

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, fingerprint sensor, RFID sensor 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.

Fig.1. Vulnerabilities of traditional key-based system

This paper follows a structured approach to explore the implementation of a smart door access system. Section I introduces the concept and objectives. Section II reviews existing research in smart door technology. Section III outlines the proposed model. Section IV presents testing and results. Finally, Section V summarizes key findings and conclusions, contributing to academic discourse on smart door access systems.

2. LITERATURE REVIEW

Smart door technology integrates advanced door lock systems to enhance security using digital data such as fingerprints, facial recognition and smart cards for authentication. The implementation of fingerprint and RFID sensors in door security systems ensures a more secure access control by authenticating users based on stored data. Security is very important in home automation to prevent theft and ensure safety of residents and their belongings. The ESP8266 module is used in IoT applications for its ability to provide Wi-Fi connectivity and enable communication between devices, making it suitable for smart door systems. The objective of this literature review is to explore the current state of smart door technologies and the integration of fingerprint and RFID sensors to enhance the security of door lock systems.

2.1 Overview of IoT Devices in Security Systems

Utilising Internet of Things (IoT) technology in security systems such as smart doors can enhance both security protocols and operational efficiency. The application of IoT technology in security systems such as smart doors aims to improve user authentication and access control measures [4]. Additionally, The Internet of Things allows devices to interact and exchange information, leading to the creation of smart systems that improve people's daily lives, offer economic advantages, conserve energy, and enhance human safety [5].

2.2 ESP8266 in Smart Door Applications

The ESP8266 microcontroller module offers Wi-Fi connectivity, which is ideal for Internet of Things (IoT) applications that need wireless communication. It's designed to be energy efficient, using no more than 2 Watts whether it's idle or active. The ESP8266 is commonly used in smart home systems to manage devices like RGB lamps, curtains, and sensors for detecting gas leaks and fires, as well as electric fans with advanced features. Its affordable and efficient design makes the ESP8266 a cost-effective choice, widely adaptable for various uses [6].

2.3 Fingerprint Sensors in Home Security

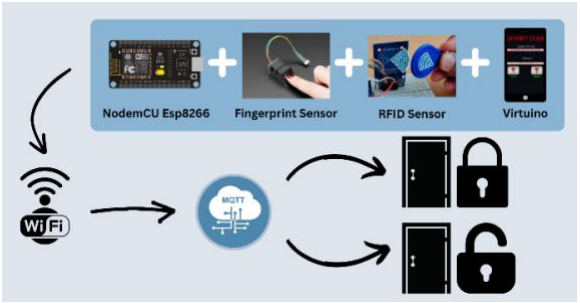

Fig. 2. The Integration of the smart door

Using a fingerprint for security enables us to manage access to the house door. Based on the article, the project aims to develop a system for automating household tasks through an Android app, integrating a microcontroller for robotic functions, switching devices with an electrical mechanism, creating an accurate circuit diagram, and designing the system [7].

2.4 RFID Technology in Access Control

RFID is short for radio frequency identification, a wireless communication technology used uniquely to identify tagged objects or people. It employs radio frequency for automatic identification of items. RFID can maintain data integrity even

in harsh environments and offers strong security measures due to its resistance to counterfeiting [8].

The inclusion of power resources in active RFID tags has diminished some of their benefits, like cost-effectiveness and durability over time. However, the RFID sensor network inherits several characteristics from wireless sensor networks that could potentially overcome the limitations experienced by passive and semi-passive tags, as discussed in the "Tag as a sensor" section [9].

2.5 Integration of Fingerprint and RFID Sensors with ESP8266

Every component within the security system, like the imprisonment modules, has its pros and cons. Relying solely on one module can't ensure security. Thus, to enhance system reliability, multiple modules should be integrated during construction. Additionally, the system should be capable of handling unforeseen circumstances [10].

Numerous experts have applied RFID technology in discussing access control systems for door security [12-15]. In one study, the authors focused solely on RFID sensor-based protection. Another paper details a security system with a single keypad sensor. Conversely, reference features a security system reliant only on Bluetooth technology, while outlines a setup employing two sensors: RFID and fingerprint recognition. Research delves into a smart door lock system incorporating RFID and a keypad. To address potential security concerns with systems lacking a password, the authors suggest integrating one. Additionally, in the proposed setup, only the owner possesses the password for the automatic door [9].

door. The bar is magnetized when there is a 12 V power. The bar will be magnetized and shut the door when it receives the 12 V. 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, the front desk switch and the touch switch. 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. 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 illustrates the topology diagram of the system. The Cloud HiveMQ acts as a cloud-based MQTT broker, facilitating efficient message communication between IoT devices. This system is connected to IIUM's Local network to handle internal communications. A private router manages both internal and external network traffic. KICT VPN network is implemented to allow devices to communicate securely over the Internet. Then they are connected to the doors to control remotely using Virtuino IoT app. The doors can also be accessed using fingerprint and RFID sensors.

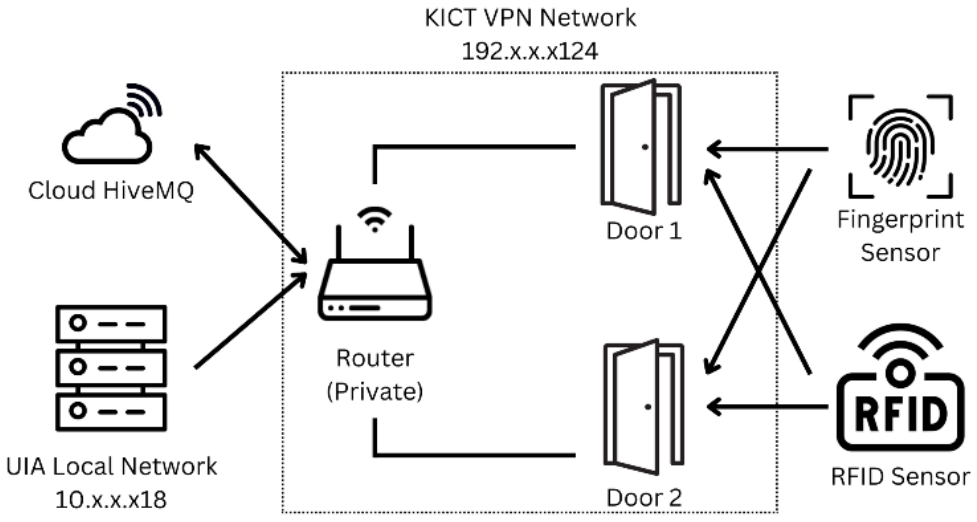

Fig. 3. Topology connection between components

3. MATERIAL AND METHODS

Figure 4 indicates the flowchart of smart door access system. The smart door access system consists of three parts which are the software, hardware, programming and the process part.

3.1 Hardware

The door is an electromagnetic door that have an electromagnetic bar that attracts the metal bar located on the

3.2 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.

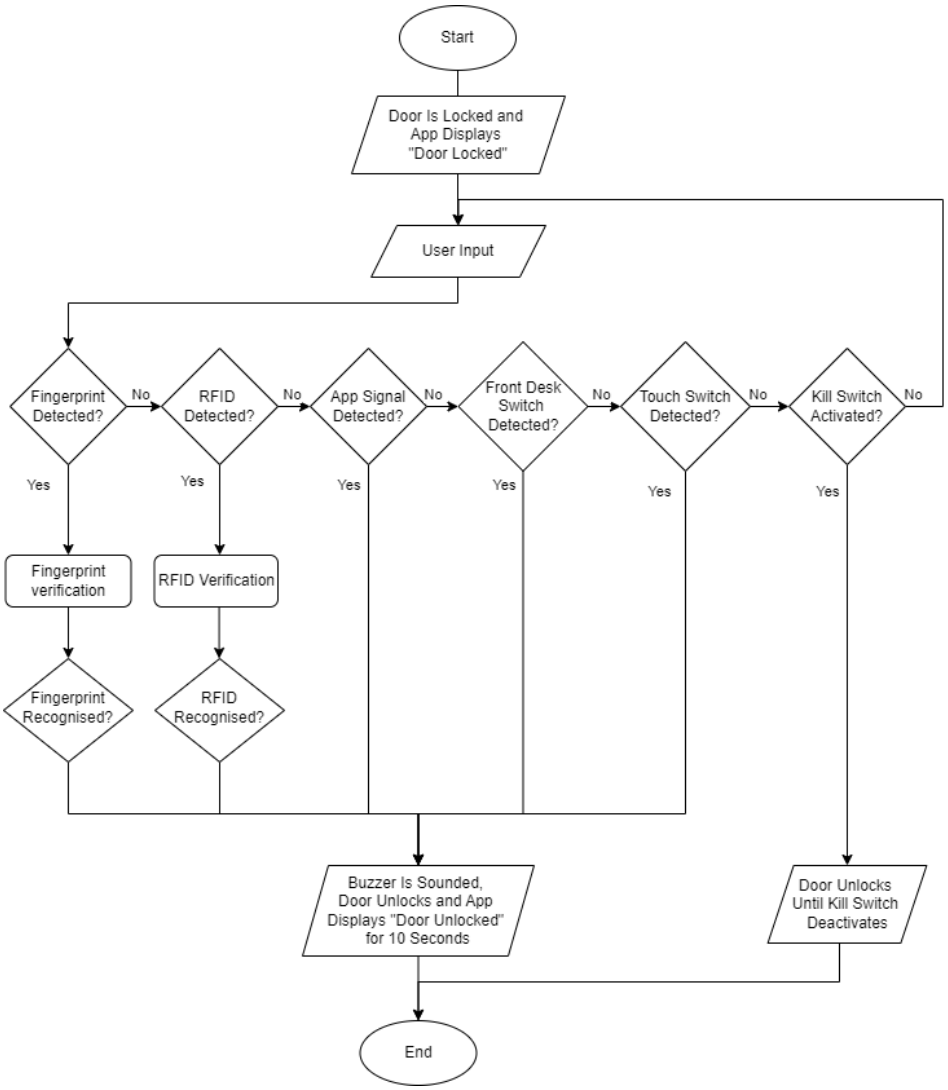

Fig. 4. The flowchart of smart door access system

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.

3.3 Arduino IDE Programming

The application used for the programming is the Arduino IDE. The programming sets up the connection to the internet 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.

3.4 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.

4. RESULTS AND DISCUSSIONS

The previous development of smart door has been covered in details as in [3].

4.1 RFID and fingerprint sensors prototype

There are two access methods are added currently in this work. The access methods are RFID and fingerprint sensors. The system will be able to store multiple fingerprints and RFID tags for access. The system will remain idle until a user inputs their fingerprint or RFID tag which will then be verified. If the input matches the data stored, it will unlock the door for 10

seconds and ring the buzzer to alert the user. As a starting point, Figure 5 shows the prototype created using a circuit simulator Proteus 8. The microcontroller used in the prototype is an Arduino Uno since it is not possible to simulate NODEMCU ESP8266 using Proteus 8 as discussed in Table 1. Two virtual terminals are used in the prototype, one for the inputs of RFID tags or fingerprints and the other for the output. An LED is used to simulate a door being locked (light off) and unlocked (light on). A buzzer had also been added to alert the user of the door being unlocked.

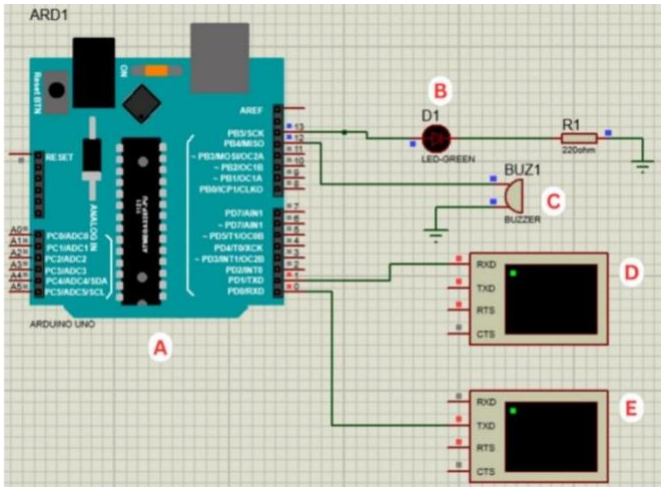

Fig. 5. Simulated prototype of RFID and fingerprint sensors

Table 1. Simulation of RFID and fingerprint sensors.

LABEL	DESCRIPTION
A	Arduino Uno
B	LED (represents door lock)
C	Buzzer
D	Virtual Terminal for Output
E	Virtual Terminal for Input (Fingerprint & RFID)

Figure 6 shows the RFID and fingerprint ID being input to the first virtual terminal and Figure 7 shows the output on the second virtual terminal. For simplicity, all data are stored using arrays in the Arduino IDE code and consists of 6-character strings. RFID tags start with the letter 'R' and fingerprints starts with the letter 'F'. If the IDs are recognized, it will display "Valid RFID/Fingerprint" and turns on the LED for 10 seconds as well as the buzzer for 2 seconds. Otherwise, it will display "Invalid ID". Moreover, if the input is more or less than 6 characters, it will display "invalid format".

Table 2 outlines a detailed methodology for testing the smart door system. This comprehensive approach ensures that each component and the overall system function correctly and reliably. The methodology is divided into several stages, each focusing on different aspects of the testing process.

4.2 PCB Improvisation Compared to Normal Circuit

A printed circuit board represents an organized platform for electronic components, just like a blueprint, contrary to the wires' scattered arrangement. By holding the electronic components in their places securely, PCBs greatly increase the reliability of electronic devices by reducing the chances of loose or broken connections and inconsistencies in the performance of devices over time. Moreover, they facilitate the transmission of electrical signals efficiently because the routes provide better speed and efficiency to the device.

Fig. 6. Proteus 8 prototype of RFID and fingerprint sensors (Input)

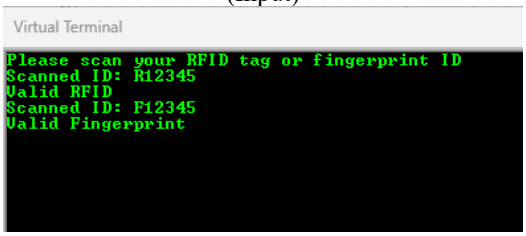

Fig. 7. Proteus 8 prototype of RFID and fingerprint sensors (Output)

Table 2. Comprehensive Methodology for Testing

Component Validation	Authentication process: Check every single part including the microcontroller, sensors and actuators if it functions as it should by its technical specification.
Design Verification	PCB Design Accuracy: Check if the printed circuit board's design corresponds precisely to general design rules of keeping components' places and running paths.
Prototyping	PCB Assembly: Mounting of the components onto the PCB. This may include soldering and physical mounting supports on the board.
Functionality Checks	Initial Power-Up Test: Check that the PCB powers up correctly and all the parts such as relay, fan, buzzer work as expected.
	Testing of Sensor Performance: Testing of sensor responsiveness with variable input such as touch, RFID and fingerprint.
	Testing for Communication: Inter-communication checking between microcontroller and MQTT server.
Testing for Durability	Stress Testing: Involves the long-term running of the PCB to test the continuous working performance.
Integration of System	Combined System Testing: Test how the PCB interacts with other parts of the system, including the magnetic door lock and the mobile app.

These are also highly versatile, working well with various scales of production. The standard design simplifies the process of mass production, hence easily replicated. Again, it aids

miniaturization; hence the creation of compact devices at a higher power rating is possible. With the minimized usage of wires, the result in using PCBs will result in a much more streamlined and beautiful circuit board with an added advantage of easy troubleshooting.

4.3 Findings

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.

Table 3 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 3. Testing result

	Triplicate of Testing	**Success Rate (%)**
Virtuino IoT left key button	Success	100
Virtuino IoT right Key button	Success	100
Haptic Switch	Success	100
Front Desk Switch	Success	100
RFID Sensor	Success	100
Fingerprint Sensor	Success	100

Several initiatives guided by following principles have been introduced. Firstly, a review of alternative Internet of Things platforms or microcontrollers for smart door entry systems would be conducted. A comprehensive examination will also be conducted to look for the weakness so that additional security measures aimed at enhancing the general security of smart door entry systems can be done. Users' satisfaction is also our main concern. Thus, an improved and more user-friendly interface for the smart door access system, a mobile application will also be developed.

5. CONCLUSION

In conclusion, the smart door access system is an essential component to provide security to important premises and enables keyless access system which ease the access for users. The implementation of the door using the Virtuino IoT application, the HiveMQ as the MQTT broker, Ardiono Uno 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.

ACKNOWLEDGEMENT

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

REFERENCES

[1] Chathuri Paranagama and Budditha Hettige, "A Review on Existing Smart Door Lock Systems," 2022, doi: 10.13140/RG.2.2.18892.08325.

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

[3] A. A. Zainuddin, R. M. Nor, A. 'Aatieff A. Hussin, and M. N. M. Sazali, "MQTT-Enabled Smart Door Access System: Design and Implementation Using NodeMCU ESP 8266 and HiveMQ," in 2023 IEEE 9th International Conference on Computing, Engineering and Design (ICCED), Kuala Lumpur, Malaysia: IEEE, Nov. 2023, pp. 1–6. doi: 10.1109/ICCED60214.2023.10425368.

[4] N. P. I. Widiantari, N. Karna, Sussi, I. P. Y. N. Suparta, and I. K. Gowinda, "Implementation of Panic Button and Fingerprint Sensor on Security System RFID Using Internet of Things and e-KTP," in 2022 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia: IEEE, Nov. 2022, pp. 375–382. doi: 10.1109/ICITSI56531.2022.9971021.

[5] S. Kaya, E. Aşkar Ayyildiz, and M. Ayyildiz, "Smart Door Lock Design With Internet of Things," Int. J. 3D Print. Technol. Digit. Ind., vol. 6, no. 2, pp. 201–206, Aug. 2022, doi: 10.46519/ij3dptdi.1074468.

[6] S. Fuada and H. Hendriyana, "UPISmartHome V.2.0 – A Consumer Product of Smart Home System with an ESP8266 as the Basis," J. Commun., pp. 541–552, 2022, doi: 10.12720/jcm.17.7.541-552.

[7] M. A. Al Rakib et al., "Fingerprint Based Smart Home Automation and Security System," Eur. J. Eng. Technol. Res., vol. 7, no. 2, pp. 140–145, Apr. 2022, doi: 10.24018/ejeng.2022.7.2.2745.

[8] N. K. Daulay and M. N. Alamsyah, "Monitoring Sistem Keamanan Pintu Menggunakan Rfid dan Fingerprint Berbasis Web dan Database," Jusikom J. Sist. Komput. Musirawas, vol. 4, no. 02, pp. 85–92, Nov. 2019, doi: 10.32767/jusikom.v4i2.632.

[9] J. W. Simatupang and R. W. Tambunan, "Security Door Lock Using Multi-Sensor System Based on RFID, Fingerprint, and Keypad," in 2022 International Conference on Green Energy, Computing and Sustainable Technology (GECOST), Miri Sarawak, Malaysia: IEEE, Oct. 2022, pp. 453–457. doi: 10.1109/GECOST55694.2022.10010367.

[10] G. Ju, C. Sim, C. Kim, and Y. Kim, "Development of a Quadruple Security System Combining Keypad, RFID, Fingerprint, and Bluetooth modules," 2021.

[11] Khan, M. R. B., Jidin, R., & Pasupuleti, J. (2016). Energy audit data for a resort island in the South China Sea. Data in brief, 6, 489-491. https://doi.org/10.1016/j.dib.2015.12.033

[12] Khan, M. R. B., Jidin, R., & Pasupuleti, J. (2016). Data from renewable energy assessments for resort islands in the South China Sea. Data in brief, 6, 117-120. https://doi.org/10.1016/j.dib.2015.11.043

[13] Zahraoui, Y., Alhamrouni, I., Mekhilef, S. and Khan, M.R.B., 2022. Machine learning algorithms used for short-term PV solar irradiation and temperature forecasting at microgrid. In Applications of AI and IOT in Renewable Energy (pp. 1-17). Academic Press https://doi.org/10.1016/B978-0-323-91699-8.00001-2

[14] Almeida, D., Pasupuleti, J., Raveendran, S. K., & Basir Khan, M. R. (2021). Performance evaluation of solar PV inverter controls for overvoltage mitigation in MV distribution networks. Electronics, 10(12), 1456. https://doi.org/10.3390/electronics10121456

[15] Seet, C. C., Pasupuleti, J., & Khan, M. R. B. (2019). Optimal placement and sizing of distributed generation in distribution system using analytical method. International Journal of Recent Technology and Engineering, 8(4), 6357-6363. https://doi.org/10.35940/ijrte.D5120.118419