

An internet of things-driven smart key system with real-time alerts: innovations in hotel security

Putra Jaya, Ryan Fikri, Agariadne Dwinggo Samala, Dimas Sanjaya

Department of Electronics Engineering, Faculty of Engineering, Universitas Negeri Padang, Padang, Indonesia

Article Info

Article history:

Received Nov 20, 2023

Revised Aug 14, 2024

Accepted Aug 30, 2024

Keywords:

Agile methodology

Arduino Uno

Internet of things

Real-time alerts

Smart key system

ABSTRACT

This paper presents an innovative smart key system designed to enhance the safety and convenience of hotel guests. The system employs an iterative, agile approach encompassing the phases of requirement analysis, design, implementation, and testing. Key components of the input circuitry include limit switches, RFID-RC522 and SW420 vibration sensors, which collectively gather data. This data is processed using an Arduino Uno microcontroller and integrated with internet of things (IoT) technology. On the output side, the system incorporates a solenoid lock and is capable of promptly notifying users via Telegram in response to unauthorized access attempts. Importantly, the system can distinguish between vibrations caused by unauthorized entry and those from legitimate usage. Rigorous testing validates its efficacy, issuing Telegram alerts promptly when detecting security breaches. This technological advancement significantly enhances hotel room security, providing an intelligent real-time solution. The fusion of IoT, Arduino microcontroller, and precise sensor configuration underscores the system's reliability, setting new benchmarks for security in the hospitality sector. The comprehensive approach detailed in this paper offers valuable insights applicable to a wide range of security applications.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Ryan Fikri

Department of Electronics Engineering, Faculty of Engineering, Universitas Negeri Padang

Prof. Dr. Hamka Street, Air Tawar Barat, Padang Utara, Padang, West Sumatera 25171, Indonesia

Email: ryanfikri@ft.unp.ac.id

1. INTRODUCTION

According to data from Central Bureau of Statistics of Indonesia (*Badan Pusat Statistik*) [1], the statistics on the number of tourists staying in hotels in Indonesia, encompassing both starred and non-starred hotels, have closely correlated with global situation over the past five years. In 2018, the total number of travelers who opted for hotel accommodation was 63,011,126, indicating positive growth in the hotel industry. However, in 2019, due to the impact of the COVID-19 pandemic and subsequent travel restrictions, this number decreased to 57,736,804. Due to the pandemic, the number of tourists in 2020 dropped significantly to 14,914,273.

In particular, the year 2021 marked a rebound, signaling the gradual recovery of the hotel industry after the pandemic. These fluctuations in statistics serve as a testament to the resilience of the hospitality industry in the face of unexpected global developments. They underscore the need for collaboration between government authorities, industry stakeholders, and the public to revitalize the tourism sector. Multiple stakeholders have taken proactive measures to increase tourist visits, including conducting research in the field of information and communication technologies (ICT) within hotel environments [2], [3], improving hotel facilities [4], [5], conducting guest satisfaction feedback surveys [6], and establishing smart hotels [7], [8]. Figure 1 illustrates the fluctuations in the number of tourists visiting and staying in hotels.

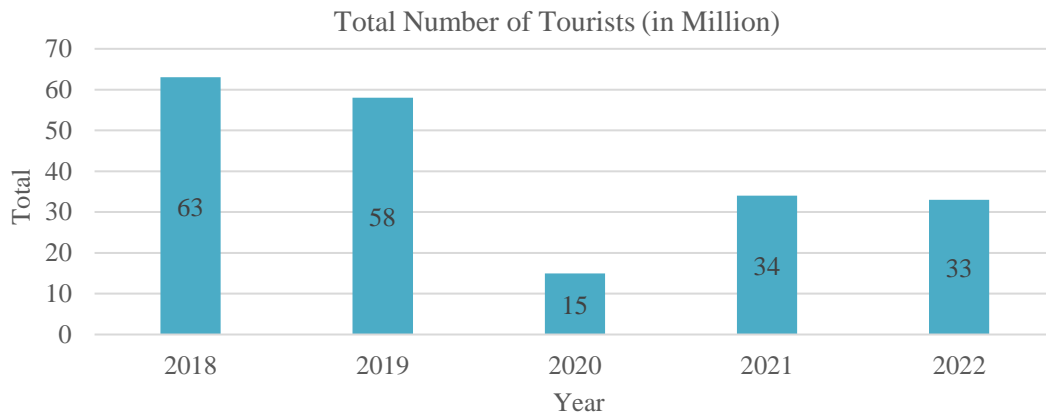


Figure 1. Total number of Indonesian and foreign tourists staying in hotels rated with and without stars

Due to the large number of tourists who visit and stay in hotels, security is an issue that cannot be neglected. To improve hotel security, a study of essential components must be carried out [7]. Hotel room security, such as access to and from rooms, plays a vital role and is a top priority for hotel owners. This emphasis on security aligns seamlessly with the core mission of hotels: to provide guests with a safe and comfortable environment during their stay. It is noteworthy that hotel doors, in general, are equipped with various security features specifically tailored to their intended use, ensuring that guests can feel secure in their accommodations.

The availability of smart key systems that integrate internet of thing (IoT) technology, as shown in [9]-[11], allows hotel managers to provide a higher level of security through the implementation of electronically controlled door access [12]-[14]. Hotel guests can benefit significantly from an IoT-driven smart key system, such as real-time monitoring of their room doors via smart devices such as smartphones. As a result, everyone can ensure the security of their hotel room doors without being physically present. This monitoring instrument provides additional security and convenience to visitors, removing concerns about undesirable acceptance or alterations to their room doors.

Addressing the security issue, a smart key system driven by IoT has been purposefully designed to enhance hotel room door security. This system aims to solve several potential difficulties. A significant concern involves the risk of misplacing the radio frequency identification (RFID) key card for hotel room door access or being discovered by unidentified individuals. This ensures that only authorized personnel can use the card. Also, to prevent unwanted access and interference with hotel room doors. If the door is damaged or forcibly opened, causing vibrations, the system will transmit a warning to the hotel room occupants as a potential danger sign. As a result, they can take the appropriate action immediately.

This innovation facilitates interactions between devices and users for accessing information about hotel room door security through the Telegram application. This system is assembled by integrating three types of security sensors. The RFID-RC522 sensor enables access to the hotel room door by recognizing the electronic key card. The SW420 sensor detects door vibrations, potentially indicating suspicious activity. Lastly, the limit switch is a sensor that identifies forced door openings and quickly alerts potential security breaches.

To control this system, an Arduino device is the central controller that collects data from these various sensors. As a result, IoT technology is used to connect this device to the internet directly. Users can receive real-time notifications via the Telegram app when an activity or issue affects hotel room door security. The combination of sensor technology, Arduino, and IoT provides a comprehensive solution to improve safety while offering hotel guests greater peace of mind during their stay.

2. METHOD

In this research, we have adopted the Agile approach. The selection of the Agile approach is motivated by the continuously evolving nature of IoT systems, making them susceptible to changes over time. The Agile approach is implemented in the device design process of an IoT-driven smart key system, covering system needs analysis, design (both hardware and software), implementation, and testing. This Agile methodology allows flexibility and responsiveness to changing requirements throughout the development cycle, ensuring that the IoT-driven smart key system can effectively adapt to technological advancements and evolving user needs. The stages of this process are illustrated in Figure 2.

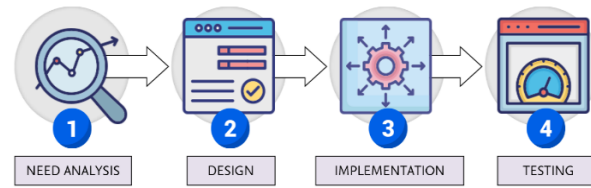


Figure 2. Agile approach in the development process of the IoT-driven smart key system

2.1. Needs analysis

The initial stages of designing a system to aid in the development of an IoT-based smart key for hotel rooms have revealed several crucial insights into the current state of hotel room doors. Through a comprehensive needs analysis, it became evident that several key issues need to be addressed. First, many existing hotel room doors lack the necessary infrastructure to support advanced IoT technology. Additionally, the analysis highlighted the importance of ensuring compatibility with the various types of door locking mechanisms currently in use. These insights are pivotal for guiding the subsequent stages of the smart key system development.

The needs analysis underscores the necessity of enhanced guest security through the implementation of a smart key system. This system aims to bolster hotel guests' security by offering real-time surveillance and an immediate response to unauthorized entry attempts. Leveraging IoT technology, this innovative solution ensures that guests are safeguarded around the clock. Features such as rapid alerts to both hotel security and guests' mobile devices not only deter potential intruders but also enable immediate action in the event of a security breach, aligning with current hotel safety standards.

To ensure a secure and dependable locking system, the smart key system will utilize a solenoid lock, which relies on electromagnetic mechanics. This technology not only improves the reliability and efficiency of the locking mechanism but also facilitates seamless interaction with the smart key system. By requiring electronic signals to operate, the solenoid-based lock offers an additional layer of protection, reducing the likelihood of unauthorized access and enhancing overall guest safety.

Remote access and monitoring will be facilitated through the Telegram application, enabling hotel management to oversee room access in real-time via the internet. This feature allows guests to receive updates and notifications directly to their devices, while staff can swiftly address any security concerns. Integration with Telegram ensures that both guests and hotel personnel can easily and securely regulate and monitor access, thereby improving overall operational efficiency and the guest experience.

In the event of a hazardous situation at the hotel room door, such as forced entry with vibrations or unauthorized door access without vibrations, the system will immediately notify the hotel guests staying in that room. These real-time warnings ensure that guests are promptly aware of any potential security breaches, allowing them to take appropriate action or seek assistance. This proactive approach not only enhances guest safety but also demonstrates the hotel's commitment to providing a secure and responsive environment.

Finally, the system can be discreetly installed on the back or inside the hotel room door, ensuring it does not detract from the room's appearance or the guest's comfort. This invisible installation approach allows modern security technologies to function seamlessly without being obtrusive, giving guests peace of mind while maintaining the hotel's elegance and style. By keeping the security system out of sight, hotels can offer an enhanced sense of security while preserving the room's aesthetic appeal.

As a result of these methods, the IoT-driven smart key system significantly enhances the security of hotel guests by providing real-time monitoring and immediate response capabilities. This system enables easier monitoring of hotel room doors and allows for swift preventive actions in potentially harmful situations. With features like remote access and security notifications, guests can have peace of mind knowing they are protected from unauthorized access and other security threats. Overall, the implementation of this smart key system ensures a safer and more secure environment for hotel guests.

2.2. Hardware design

Overall, the components of this system consist of an RFID-RC522, limit switch, SW420 vibration sensor, Arduino Uno Atmega328, ESP8266 module, and a solenoid lock. These components are combined to form a system that performs its intended purpose. Figure 3 shows an illustrative design of the device's development. Actualizing a design concept in the structure of a block diagram throughout the development phase is also known as design implementation. The multiple components in this block diagram each have a particular purpose. The input block diagram, which is the first phase in this process, is one of them. The input block diagram represents the initialization of the necessary data, which is then transferred to the microcontroller.

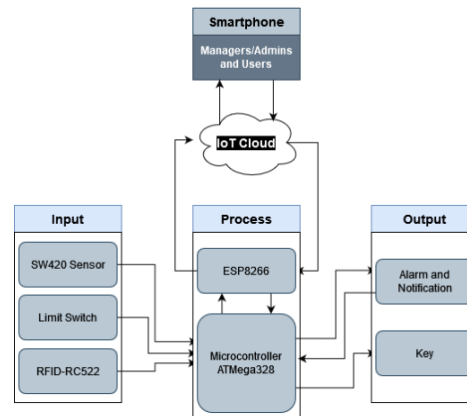


Figure 3. Overall process block diagram of the device design

Multiple sensors perform important functions in this study. For example, the SW420 vibration sensor is responsible for sensing vibrations at the hotel room's door. Likewise, the limit switch is critical in determining whether the door is open or closed. Meanwhile, the RFID-RC522 component uses RFID technology to unlock the door to the hotel room.

The three types of sensors are responsible for acquiring the required data. Subsequently, the data from each sensor is sent to the microcontroller, which serves as the central control unit. Furthermore, the data collected by these sensors will be routed into the IoT network to allow further integration and accessibility. This process enables the more efficient and automatic tracking and management of hotel room doors.

The process block diagram states the system's essential components, such as the Arduino Uno microcontroller and the IoT infrastructure. This process block represents the entity responsible for processing data from the input block. The Arduino microcontroller will direct the data from the input block through processing steps. Data will be delivered to the next level through richer informational data via IoT technology. The output block diagram shows the final step of the process flow. This block is the receiver of informational data that the Arduino microcontroller has processed. The processed data will be delivered to an electronic key to be sent via notifications.

The hardware design method includes selecting and customizing many components that meet the device's needs. The purpose is for each component to blend effortlessly. Figure 4 shows the schematic design of the smart key system to optimize the circuit structure. This graphic shows the complete configuration required to meet functional requirements and ensure the smart key system's design can run optimally.

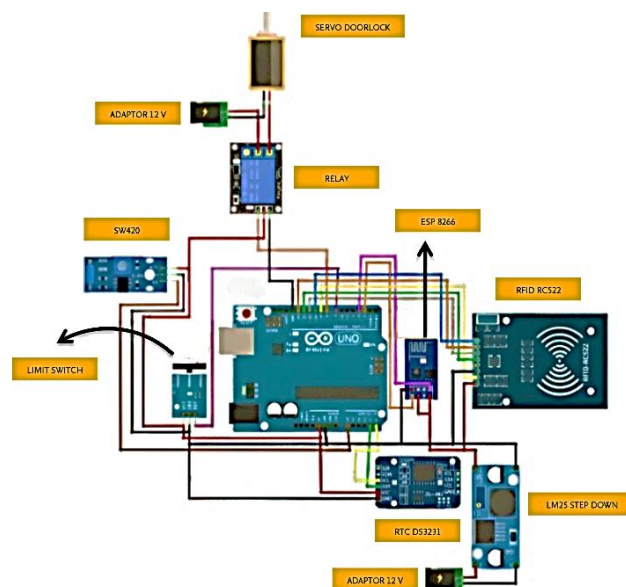


Figure 4. Overall circuit schematic

2.2.1. Microcontroller ATmega 328

The Arduino microcontroller is critical to processing input and output data in the IoT-based smart key device. The Arduino microcontroller processes all sensor information and instructions to the linked devices. The ATmega328 chip, which has 14 digital port pins and six analog port pins, is used in Arduino, a microcontroller development device. In addition, Arduino includes a 16 MHz crystal oscillator, a USB port, a reset button, and a power jack. As the primary data processor, Arduino is critical in processing sensor data and organizing duties that other components of the smart key system must complete. Arduino can connect various sensors and actuators that play a role in the device's functioning using its diversified digital and analog pins [15]-[17].

2.2.2. ESP8266

The ESP8266 module is vital to connect the device to the internet through Wi-Fi [18]. This module contains an ESP8266 chip built and connected with other components of internet connectivity [19]. The ESP8266 module is typically used with a microcontroller, which makes it an additional device that allows it to connect to the internet. Integrating the ESP8266 module with a microcontroller improves the ability of the device to work online in numerous areas of life [20], [21], allowing it to communicate, send, and receive data, and participate in internet-based research [22], [23].

2.2.3. SW420 vibration sensor

The SW420 vibration sensor can detect vibrations or shocks from many directions [24]. This sensor operates using a metal float with two electrodes within. The sensor remains attached without vibration, which causes a low output value. The connection is broken when the sensor detects vibrations, producing a high output value [25]. When vibrations occur in this gadget, the Arduino microcontroller and IoT systems process the input data received by the sensor. The processed data are then transmitted as a notice to the Telegram application. This method allows users to receive real-time information on vibrations or shocks in the monitored system. As a result, integrating the vibration sensor with Arduino and IoT provides an effective solution to monitor activities or circumstances that require special attention.

2.2.4. RFID-RC522

RFID is a radio wave-based identification system that may wirelessly transfer identification information as a PIN. The RFID reader and the RFID tag are the two main elements that play an essential role in this technology. It operates similarly to radio waves in that the RFID reader transmits radio waves that are subsequently received by the RFID tag's antenna. A chip within the RFID tag holds a unique ID code for each tag. The RFID tag antenna then transmits the data to be read by the RFID reader. RFID technology is used in this system to unlock the doors of hotel rooms [26], [27].

As input, the SW420 vibration sensor and RFID technology are implemented in this system. The system also uses a limit switch to detect when the hotel door is forced open without legitimate control. The limit switch functions as an electromechanical switch that can change the position of the contact terminals from normally closed to open or vice versa. This limit switch is manually adjusted in use by pushing [28]. This system provides an effective and integrated security layer for the safe and controlled opening of hotel room doors by combining RFID technology, the SW420 vibration sensor, and the limit switch.

2.2.5. Solenoid

A solenoid is an electronic component that operates under the concept of electromagnetic and consists of a conductor wire twisted around an iron core [29]. Solenoids typically function at a voltage of 12 VDC. When an electric current flows through the iron core, the solenoid generates a magnetic field, causing the solenoid to open. When there is no electric current flowing, the solenoid remains locked.

The solenoid controls access in its operation, while other components, such as RFID-RC522 and the limit switch, detect legal entry and prevent unwanted attempts [30]. The SW420 vibration sensor detects unusual shocks or vibrations on the door, while the Arduino Uno Atmega328 and ESP8266 modules manage data and network connectivity. Combining all these components produces a complex system for hotel room door security.

2.2.6. Software design

The software is designed according to the system flow represented in Figure 5. This diagram outlines the steps the software must follow to ensure efficient and effective operation. Each component in the system flow has been carefully integrated to ensure smooth processes. By adhering to the guidelines in Figure 5, the software development process can be more structured and organized.

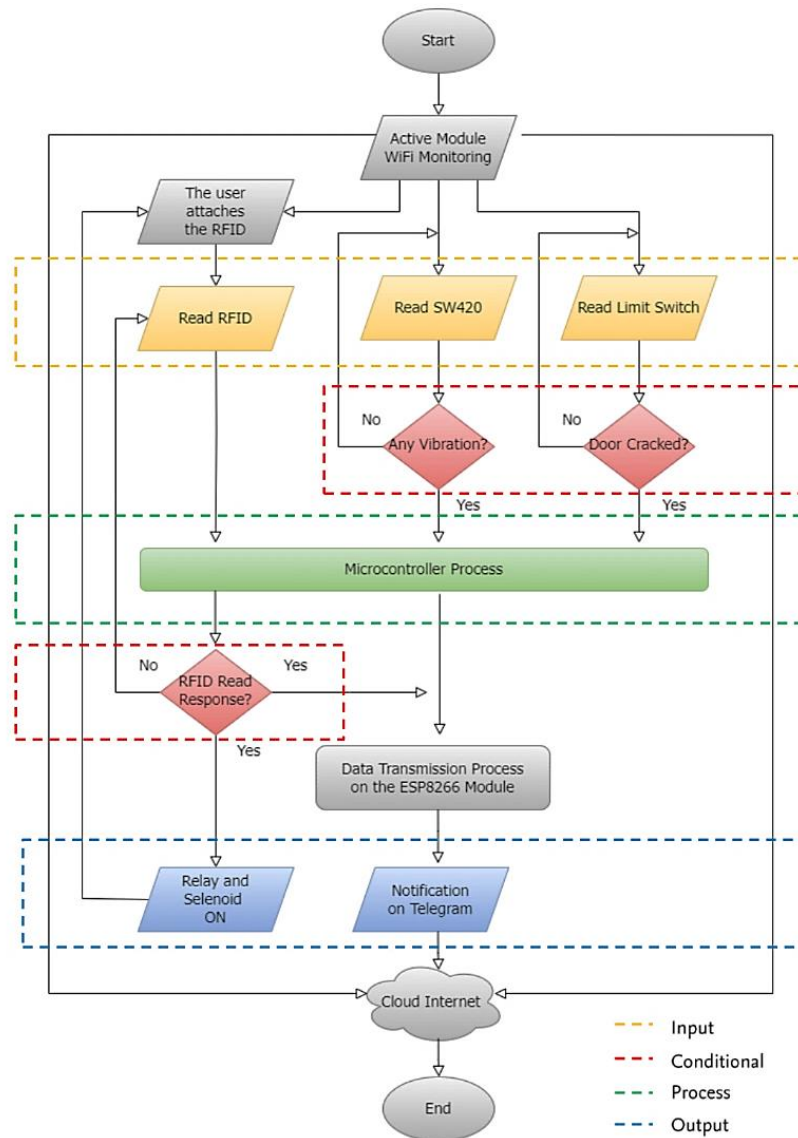


Figure 5. Flowchart software system

2.3. Implementation

As specified in the requirements mentioned above, the development of devices and supplies is the first step towards developing an IoT-based smart key for hotels. Following that, the program design process will be carried out in the form of software, with Arduino IDE software functioning as the platform for developing the program in the C programming language, which has been optimized for microcontroller programming. The component installation process is then carried out, which involves the use of a hand drill to produce holes in the base materials such as plywood and acrylic. These holes will secure the device by securing the components and installing bolts. Finally, the necessary components will be systematically assembled according to the circuit design previously planned.

Jumper cables connect one component to another in this construction, and these connections are reinforced with solder and tin to ensure strong and durable connections. Arduino Uno, ESP8266 module, RFID-RC522, SW420 vibration sensor, limit switch, relay, key solenoid, 12 VDC adapter, and other design-related components are utilized in the assembly. Figures 6 illustrate the circuit diagrams and the application of the created device. Figure 6(a) showcases the physical utilization of the assembled device in everyday scenarios, providing a clear view of how the device integrates into its intended environment. Figure 6(b) depicts an electronic circuit diagram detailing the connections between these components, offering a technical perspective on the device's internal workings and how each part interacts to achieve the desired functionality.

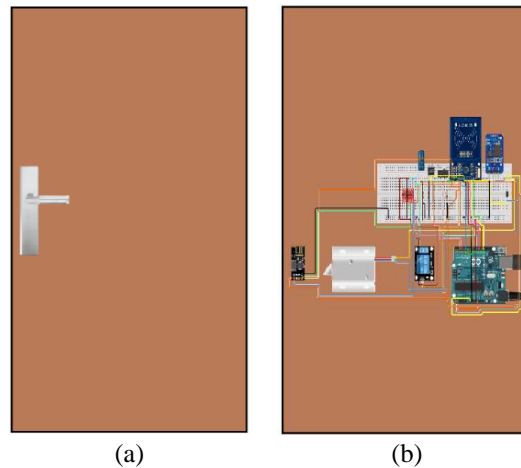


Figure 6. Illustrate the circuit diagrams and the application of the created device (a) showcases the physical utilization of the assembled device in everyday scenarios and (b) depicts an electronic circuit diagram detailing the connections between these components

3. RESULTS AND DISCUSSION

Different kinds of sensors are employed in the smart key input circuit. The RFID-RC522 sensor is the first to be used. The RFID sensor was tested to determine its performance concerning the reading distance between the RFID reader and the RFID card. The RFID card was connected to the RFID reader from various distances during testing. The results of this test indicated that the RFID reader could successfully read the RFID tag from up to 3 cm away. However, distances over 3 centimeters did not produce accurate results. During this test, the RFID sensor was given a voltage input of 3.4 VDC. Table 1 and Figure 7 show voltage readings at specific positions on the Arduino, notably pins D9, D10, D11, D12, and D13.

Table 1. Arduino voltage measurements to evaluate RFID-RC522

Pin location	Voltage measurement in RFID (V)
VCC	3.4
SCK	0.4
SDA	2.4
RST	3.2
MISO	0.2
MOSI	3.4

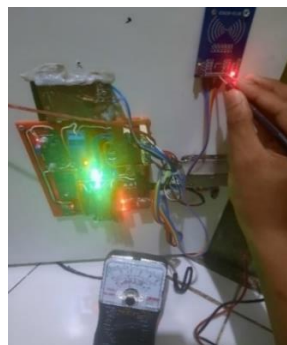


Figure 7. Experimentation and measurements on the smart door device

Based on these measurements, it is possible to conclude that the RFID sensor works normally and follows the expected specifications. Furthermore, the device's functionality was tested when the door was opened without vibration. According to the results of this testing, if the door were opened without vibration, a notification alert would be sent to the user through the Telegram scheme. Figure 8 shows the notification display.

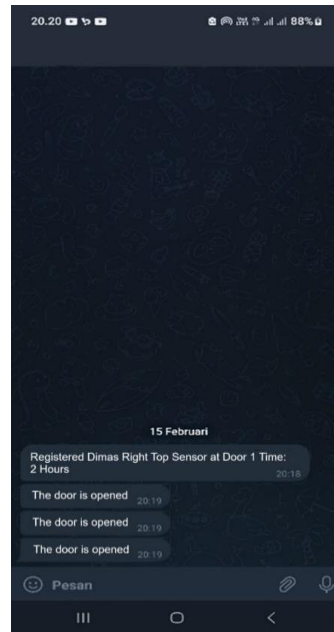


Figure 8. Telegram notification for open-door event

The limit switch is the second sensor in the smart key input circuit. The limit switch was tested by taking measurements with a multimeter at the terminals of the limit switch. The measurement should yield a certain value if the limit switch is in good working condition and connected. The measurement should change after pressing the limit switch with a multimeter probe, showing that the limit switch is engaged. The limit switch voltage was measured at pin D7 of the Arduino Uno and the ground connection was connected at the Arduino ground pin, which yields the measurement data shown in Table 2.

Table 2. Voltage measurements of Arduino input reaction to limit switch

Condition	Voltage in limit switch (V)
Push	0
Not push	3.8

Based on the results of this testing, it is possible to conclude that the limit switch works correctly and follows the expected conditions. Furthermore, the devices were operated when the limit switch detected the hotel door being severely opened. This testing showed that a notification alert would be sent to the user via the Telegram application in such a scenario. This testing showed that a notification alert would be sent to the user via the Telegram application in such a scenario. Figure 9 shows the notification display, which provides a visual representation of how the alert appears on the user's device. This feature ensures that users are promptly informed of relevant events or updates, enhancing the overall functionality and user experience of the system. The SW420 vibration sensor is the third sensor tested. The vibration sensor was tested to ensure that it performs by the pre-programmed program. The test was carried out on the output of the SW420 vibration sensor, which was connected to pin A0 on the Arduino Uno microcontroller. A 5 VDC supply operated the vibration sensor, and the ground connection was connected to the Arduino Uno ground pin.

The following conditions are standard criteria: when vibration is detected, the voltage output from the SW420 vibration sensor is supposed to be 5 VDC. Based on the test results, the measured output voltage is 4.6 VDC when vibration is detected. The Arduino Uno microcontroller will process the input via this vibration sensor. The results will be returned to the ESP8266 module, which will notify the user and the administrator if any vibration is detected on the hotel door. When the SW420 vibration sensor detects vibrations, a notification recognition is issued to the user through the testing-based Telegram application. Figure 9(a) depicts the notification system designed to alert users and administrators in the event of unauthorized door opening, enhancing security measures. Furthermore, Figure 9(b) illustrates the utilization of the Telegram application for notifying users of door vibrations, complementing the previously described notification system

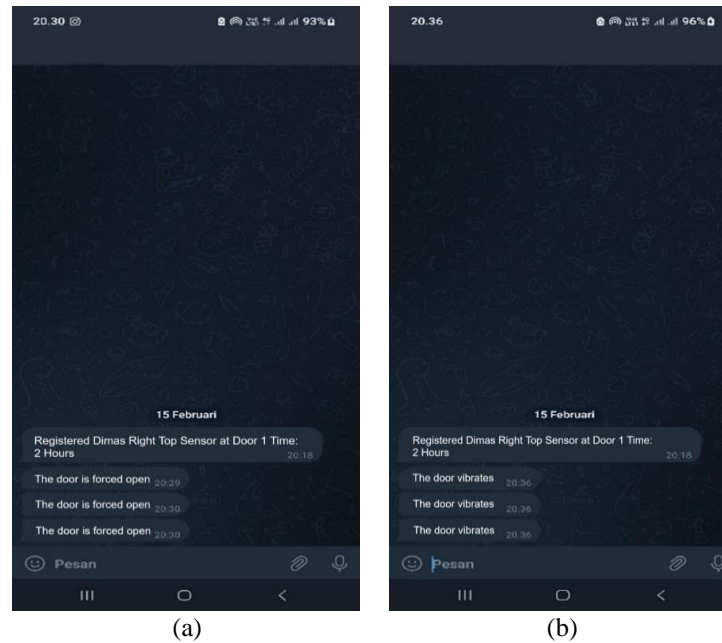


Figure 9. Telegram notification (a) for the forced-open door event and (b) with vibration for the door event

The Arduino Uno and the ESP8266 module construct the electronics of this system. The output voltage was measured at the Arduino Uno I/O port pin positions linked to the module and sensors utilized in this device during testing. The Arduino Uno was given a 12 VDC input voltage to activate the module's red LED indication. This testing includes digital ports from D0 to D13 and analog ports from A0 to A5. The test results showed that the Arduino Uno's output voltage is 12 VDC and that all ports are active.

The Arduino Uno module was tested using the Arduino IDE, with the results displayed on the serial monitor. The objective of this test was to verify that the output of the SW420 vibration sensor and limit switch corresponded to the previously programmed code. The test was successful if striking the hotel door resulted in a vibration display on the serial monitor. Furthermore, if the hotel door were opened without approval, the serial monitor would display the phrase "*pintu dibobol.*" Figure 10 shows an illustration of the serial monitor display.

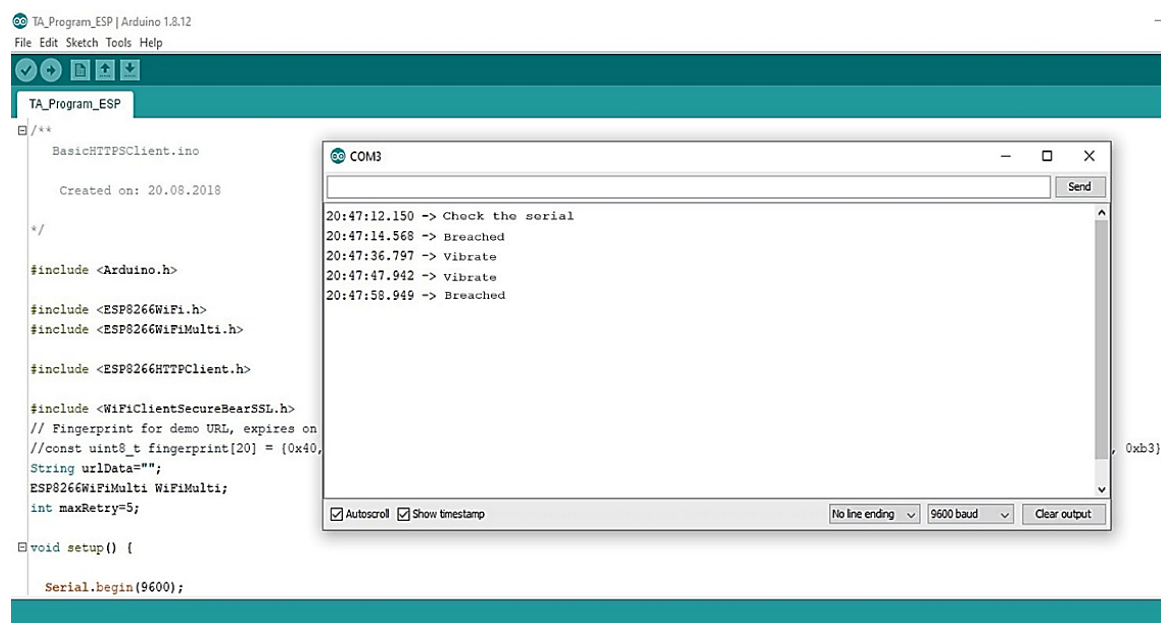


Figure 10. Arduino sensor system test results displayed on the serial monitor

Furthermore, the ESP8266 Wi-Fi module was tested with a 3.4 VDC power supply provided by a step-down regulator DC to DC converter with a 3.4 VDC output voltage. To establish a connection from the ESP8266 module to the Arduino, connect pin D2 on the Arduino to pin GPIO-1 on the ESP8266 module and connect pin D3 on the Arduino to pin GPIO-3 on the ESP8266 module. This test's main objective was the measurement point on the VCC pin of the ESP8266 module, which shows the active status and the connection to the Wi-Fi network.

AT command instructions were used to configure the ESP8266 module as an access point, connecting the module to the internet network. The module was also detected using a laptop during this testing. The ESP8266 Wi-Fi module testing results indicate that the module can be properly noticed and connected to the Wi-Fi network, as shown in Figure 11.

```

BasicHttpServer | Arduino 1.8.12
File Edit Sketch Tools Help

BasicHttpServer

if (Serial.available() > 0) {
  String dataIN = Serial.readString();
  if (dataIN.substring(0,1) == "0") {
    //error
    cekPendaftar(1,dataIN.substring(dataIN
  } else if (dataIN.substring(0,1) == "1") {
    //habis
    cekPendaftar(2,dataIN.substring(da
  } else if (dataIN.substring(0,1) == "2") {
    //getar
    cekPendaftar(3,dataIN.substring(da
  } else if (dataIN.substring(0,1) == "3") {
    //Barang Disimpan
    cekPendaftar(4,dataIN.substring(da
  } else if (dataIN.substring(0,1) == "4") {
    //getar
    cekPendaftar(5,dataIN.substring(da
  }
}

//Serial.println("Wait 10s before next round...");
delay(1000);
}

COM4
14:58:11.846 -> ===
14:58:11.846 ->
14:58:11.846 ->
14:58:11.846 -> Start
14:58:11.846 -> ===
14:58:11.846 -> 56
14:58:11.846 -> Finish
14:58:15.882 -> Add Wifi
14:58:15.882 ->
14:58:15.882 -> ===
14:58:15.882 -> Add Wifi
14:58:15.882 -> ===
14:58:15.926 -> 56
14:58:15.926 -> Finish

[Autoscroll] [Show timestamp] [No line ending] [9600 baud] [Clear output]

```

Figure 11. System test results of the ESP8266 module

A solenoid lock is used in the smart key system's output circuit. The solenoid lock was tested by investigating the results of the operation, specifically whether or not the hotel door locked by the solenoid lock could be opened. This procedure depends on whether or not the RFID card tag reading was successful. If RFID card tag detection is successful, the solenoid lock is pushed into the door, and the door opens. If the RFID card tag reading fails, the solenoid lock will remain in a specific position, preventing the hotel door from opening. The solenoid lock operation was tested with a 12 VDC input voltage adaptor. The voltage measurement point of the solenoid lock, located at the relay's NC pin, was the focus of this testing. When the solenoid lock is open, the measured voltage is 0 volts, based on the test results. When the solenoid lock is closed, the measured voltage is 12 VDC. Based on the results of these tests, it is possible to determine that the solenoid lock action works properly and within the required parameters.

4. CONCLUSION

Overall, the IoT-enabled smart door lock system for hotel devices accomplished significant goals, including the development of both software and hardware for security notifications capable of detecting suspicious activities such as forced use of room keys and doors opening without vibration. The development of the operational configuration software for the Atmega328 and ESP8266 modules also improved the system's capabilities regarding data processing and notification via the IoT network. Furthermore, the implementation of this smart key device adds a new dimension by adding remote real-time monitoring capabilities, boosting security holistically, and allowing users to oversee security remotely. As a result, an effective solution is established to protect both guests and hotel management.




REFERENCES

- [1] Data Badan Pusat Statistik (BPS) Indonesia, "Number of Indonesian guests in star hotels (thousand people) (in Indonesian: *Jumlah Tamu Indonesia pada Hotel Bintang (Ribu Orang)*), 2021-2023," BPS - Statistics Indonesia, 2024, [Online]. Available: <https://www.bps.go.id/id/statistics-table/2/MzI4IzI=/jumlah-tamu-indonesia-pada-hotel-bintang--ribu-orang-.html>. (Accessed: Feb. 03, 2024).
- [2] T. Makoondlall-Chadee, N. P. Goolamally, P. V. R. Coolen, and C. Bokhoree, "Sustainable tourism, technology and internet 4.0: opportunities and challenges for small island developing states," in *2021 IoT Vertical and Topical Summit for Tourism*, IEEE, Sep. 2021, pp. 1–4, doi: 10.1109/IEEECONF49204.2021.9604866.
- [3] T. Y. Xin, N. Katuk, and A. S. C. M. Arif, "Smart home multi-factor authentication using face recognition and one-time password on smartphone," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 24, pp. 32–48, Dec. 2021, doi: 10.3991/IJIM.V15I24.25393.
- [4] P. Verma, M. Singh, and N. Aggarwal, "Analysing the opportunities for technological entrepreneurship: a conceptual framework for hospitality-housekeeping industry," in *Proceedings of 2nd International Conference on Computation, Automation and Knowledge Management, ICCAKM 2021*, IEEE, Jan. 2021, pp. 254–259, doi: 10.1109/ICCAKM50778.2021.9357749.
- [5] S. M. Elwageeh and H. F. Karoui, "A framework of integrating VR and IoT technology to test users' preferences of artificial lighting variations in hotel guest room," in *IET Conference Proceedings*, Institution of Engineering and Technology, 2020, pp. 392–397, doi: 10.1049/icp.2021.0867.
- [6] R. Goel, T. Singh, S. L. Sahdev, S. K. Baral, and A. Choudhury, "Impact of AI & IoT in sustainable & green practices adopted in hotel industry and measuring hotel guests' satisfaction," in *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2022*, IEEE, Oct. 2022, pp. 1–5, doi: 10.1109/ICRITO56286.2022.9965152.
- [7] C. M. Chen and K. S. Zhang, "Research on the critical factors of adopting smart hotel," in *2019 IEEE Eurasia Conference on IOT, Communication and Engineering, ECICE 2019*, IEEE, Oct. 2019, pp. 377–379, doi: 10.1109/ECICE47484.2019.8942757.
- [8] Z. B. Chen and Y. Liu, "Application of face recognition in smart hotels," in *2nd IEEE Eurasia Conference on IOT, Communication and Engineering 2020, ECICE 2020*, IEEE, Oct. 2020, pp. 180–182, doi: 10.1109/ECICE50847.2020.9302014.
- [9] F. Aman and C. Anitha, "Motion sensing and image capturing based smart door system on android platform," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing, ICECDS 2017*, IEEE, Aug. 2018, pp. 2346–2350, doi: 10.1109/ICECDS.2017.8389871.
- [10] M. Shanthini, G. Vidya, and R. Arun, "IoT enhanced smart door locking system," in *Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020*, IEEE, Aug. 2020, pp. 92–96, doi: 10.1109/ICSSIT48917.2020.9214288.
- [11] R. Priyakanth, N. M. S. Krishna, G. Karanam, M. L. Prassna, S. B. Poojitha, and J. Mounika, "IoT based smart door unlock and intruder alert system," in *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, IEEE, Oct. 2021, pp. 6–11, doi: 10.1109/ICOSEC51865.2021.9591822.
- [12] P. Ruiyu, A. Lagorio, M. Cadoni, and E. Grosso, "Enhancing eID card mobile-based authentication through 3D facial reconstruction," *Journal of Information Security and Applications*, vol. 77, p. 103577, Sep. 2023, doi: 10.1016/j.jisa.2023.103577.
- [13] I. S. Akila, P. Pratheek, and A. Poonia, "Smart identity card for campus automation," in *2023 Innovations in Power and Advanced Computing Technologies, i-PACT 2023*, IEEE, Dec. 2023, pp. 1–5, doi: 10.1109/I-PACT58649.2023.10434674.
- [14] S. Alazmi, A. R. Khan, and Q. Yu, "A Comprehensively secure smart card access controls," in *21st Saudi Computer Society National Computer Conference, NCC 2018*, IEEE, Apr. 2018, pp. 1–4, doi: 10.1109/NCG.2018.8592961.
- [15] P. Naveen, K. R. Teja, K. S. Reddy, S. M. Sam, M. D. Kumar, and M. Saravanan, "ATMEGA 328-based gas leakage monitoring and alerting IoT system with SMS notification," in *2023 9th International Conference on Advanced Computing and Communication Systems, ICACCS 2023*, IEEE, Mar. 2023, pp. 1300–1305, doi: 10.1109/ICACCS57279.2023.10112899.
- [16] D. D. P. Rani, D. Suresh, P. R. Kapula, C. H. M. Akram, N. Hemalatha, and P. K. Soni, "IoT based smart solar energy monitoring systems," *Materials Today: Proceedings*, vol. 80, pp. 3540–3545, 2023, doi: 10.1016/j.matpr.2021.07.293.
- [17] D. Thirumoorthy, U. Rastogi, B. B. Sundaram, M. K. Mishra, B. Pattanaik, and P. Karthika, "An IoT implementation to ATM safety system," in *Proceedings of the 3rd International Conference on Inventive Research in Computing Applications, ICIRCA 2021*, IEEE, Sep. 2021, pp. 744–749, doi: 10.1109/ICIRCA51532.2021.9544638.
- [18] M. Gergeleit, "Autotree: connecting cheap IoT nodes with an auto-configuring WiFi tree network," in *2019 4th International Conference on Fog and Mobile Edge Computing, FMEC 2019*, IEEE, Jun. 2019, pp. 199–203, doi: 10.1109/FMEC.2019.8795311.
- [19] F. Ertam, I. F. Kilincer, O. Yaman, and A. Sengur, "A new IoT Application for dynamic WiFi based wireless sensor network," in *2020 International Conference on Electrical Engineering, ICEE 2020*, IEEE, Sep. 2020, pp. 1–4, doi: 10.1109/ICEE49691.2020.9249771.
- [20] D. Parida, A. Behera, J. K. Naik, S. Pattanaik, and R. S. Nanda, "Real-time environment monitoring system using ESP8266 and thingspeak on internet of things platform," in *2019 International Conference on Intelligent Computing and Control Systems, ICCS 2019*, IEEE, May 2019, pp. 225–229, doi: 10.1109/ICCS45141.2019.9065451.
- [21] M. Karpagam, S. S. Sahana, S. Sivadharini, and S. Soundharyasri, "Smart energy meter and monitoring system using internet of things (IoT)," in *IDCIoT 2023 - International Conference on Intelligent Data Communication Technologies and Internet of Things, Proceedings*, IEEE, Jan. 2023, pp. 75–80, doi: 10.1109/IDCIoT56793.2023.10053541.
- [22] P. MacHeso, T. D. Manda, S. Chisale, N. Dzupire, J. Mlatho, and D. Mukanyiligira, "Design of ESP8266 smart home using MQTT and Node-RED," in *Proceedings - International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021*, IEEE, Mar. 2021, pp. 502–505, doi: 10.1109/ICAIS50930.2021.9396027.
- [23] P. F. Gabriel and Z. Wang, "Design and implementation of home automation system using Arduino Uno and NodeMCU ESP8266 IoT platform," in *International Conference on Advanced Mechatronic Systems, ICAMechS*, IEEE, Dec. 2022, pp. 161–166, doi: 10.1109/ICAMechS57222.2022.10003361.
- [24] N. S. Sayem *et al.*, "IoT-based smart protection system to address agro-farm security challenges in Bangladesh," *Smart Agricultural Technology*, vol. 6, p. 100358, Dec. 2023, doi: 10.1016/j.atech.2023.100358.
- [25] M. Noorin and K. V. Suma, "IoT based wearable device using WSN technology for miners," in *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2018 - Proceedings*, IEEE, May 2018, pp. 992–996, doi: 10.1109/RTEICT42901.2018.9012592.
- [26] R. Colella, L. Catarinucci, and L. Tarricone, "Improved RFID tag characterization system: use case in the IoT arena," in *2016 IEEE International Conference on RFID Technology and Applications, RFID-TA 2016*, IEEE, Sep. 2016, pp. 172–176, doi: 10.1109/RFID-TA.2016.7750760.




- [27] M. A. Omran, B. J. Hamza, and W. K. Saad, "The design and fulfillment of a smart home (SH) material powered by the IoT using the Blynk app," *Materials Today: Proceedings*, vol. 60, pp. 1199–1212, 2022, doi: 10.1016/j.matpr.2021.08.038.
- [28] S. Kurundkar, G. Bhole, S. Bele, B. Bhoge, and A. Bhosale, "Advance security system," in *2023 IEEE 8th International Conference for Convergence in Technology, I2CT 2023*, IEEE, Apr. 2023, pp. 1–4, doi: 10.1109/I2CT57861.2023.10126415.
- [29] D. Reçber, B. Kayserilioglu, I. C. Koçum, and D. Cökeliler Serdaroglu, "Configuration of hardware for medical plasma based surgical device and features," in *2018 Medical Technologies National Congress, TIPTEKNO 2018*, IEEE, Nov. 2018, pp. 1–4, doi: 10.1109/TIPTEKNO.2018.8596784.
- [30] T. Nonthaputha, U. Torteanchai, M. Kumngern, and J. Phookwantong, "Design of smart key box using IoT," in *International Conference on ICT and Knowledge Engineering*, IEEE, Nov. 2021, pp. 1–4, doi: 10.1109/ICTKE52386.2021.9665693.

BIOGRAPHIES OF AUTHORS






Putra Jaya    received his master's degree in engineering from Gadjah Mada University, Indonesia. He is a full-time associate professor at Universitas Negeri Padang. His research lines are signal processing, automatic control, and electronic instrumentation. Before his current role, he served as the head of the Department of Electronic Engineering for two consecutive terms. He currently holds the Secretary of the Majelis Wali Amanat position at Universitas Negeri Padang. He can be contacted at email: putrajaya1962@ft.unp.ac.id.






Ryan Fikri    earned a master's degree in engineering from Institut Teknologi Bandung in 2019, specializing in research on high altitude platform station for his thesis. As a dedicated full-time lecturer, he has extensively researched electronics, telecommunications, and the internet of things. Notably, in 2021, he actively contributed to regulating frequency usage in Indonesia, working under the auspices of the Ministry of Communication and Informatics. Furthermore, he served as a Taskforce 5G Indonesia member, showcasing his commitment to advancing telecommunications technology in the country. He can be contacted at email: ryanfikri@ft.unp.ac.id.



Agariadne Dwinggo Samala    is a professional educator, a futurologist and an Assistant Professor at the Faculty of Engineering, Universitas Negeri Padang (UNP), Indonesia, specializing in informatics and computer engineering education. Additionally, he is the Coordinator of the Emerging Technologies and Multimedia in Education Research Group Env. (EMERGE) based in Indonesia, where he contributes to advancing research initiatives. He is an external member of the Digital Society Lab at the Institute for Philosophy and Social Theory, University of Belgrade, Serbia. With a deep passion for education, he has conducted impactful research on technology-enhanced learning (TEL), emerging technologies in education, educational technology, informatics education, and technology, vocational education, and training (TVET). He can be contacted at email: agariadne@ft.unp.ac.id.



Dimas Sanjaya    earned his B.Ed. from, Universitas Negeri Padang, Indonesia, in 2022. Dimas discovered his interest in the internet of things (IoT) field in high school, which led him to pursue higher education at the university level. Throughout his college years, Dimas actively participated in various extracurricular projects, demonstrating his dedication to the development of electronic engineering skills. With a keen interest in IoT using Arduino, he firmly believes that technological innovation can shape a more connected and intelligent future. He can be contacted at email: dimassanjaya1786@gmail.com.