Received June 30th 2025; accepted December 26th 2025. Date of publication December 31st 2025
Digital Object Identifier: https://doi.org/10/25047/jtit.v12i2.421

Optimizing Security with an Iot: A Data-Driven Visitor Identification Framework

CHOIRUL HUDA[1], LUKMAN HAKIM[2]

[1] Department of Information Technology, Politeknik Negeri Jember, Jember, Indonesia
[2] Department of Business, Politeknik Negeri Jember, Jember, Indonesia

CORESPONDING AUTHOR: CHOIRUL HUDA (email:chuda@polije.ac.id)

ABSTRACT Security is a critical factor in academic environments, where assets such as computers, sensor devices, teaching aids, and other equipment must be maintained in optimal condition for continuous use. The loss or misuse of these resources can disrupt learning activities and hinder the achievement of expected learning outcomes. In response, visitor identification systems have evolved through the adoption of IoT devices, facial recognition, and voice recognition technologies. However, existing solutions still face challenges, including slow identification processes, the need for large training datasets, and limited application platforms. To address these issues, this study proposes an IoT-based visitor identification framework enhanced with Data-Driven Modelling and an integrated Identification Information System (IIS). The framework integrates RFID and passive infrared (PIR) sensors with a Raspberry Pi microcontroller for real-time data acquisition, supported by a cloud-based platform for storage, processing, and monitoring. Experimental evaluations conducted in a simulated institutional environment demonstrate notable improvements in authentication accuracy, reduced verification response time, and higher reliability compared to conventional approaches. The findings highlight that combining Data-Driven Modelling, IoT technologies, and IIS not only strengthens room security but also establishes the foundation for predictive visitor management systems, offering adaptive and intelligent security solutions for the future. Overall, experimental results confirm that the proposed system performs optimally across various test scenarios.

KEYWORDS: Identification, Internet of Things, Data-Driven, Raspberry Pi, Magnetic Lock, RFID

I. INTRODUCTION

Security is a fundamental requirement to ensure that individuals can carry out their activities safely and without threat. This applies not only to personal safety but also to the protection of valuable assets, such as computers, sensor devices, teaching aids, and other instructional media. The loss or damage of such equipment poses a significant risk, particularly for those responsible for their maintenance. The risk becomes even more critical when the items are expensive, rare, or difficult to replace. Moreover, if these items are part of a laboratory's inventory, their unavailability can disrupt students' learning processes and hinder the achievement of intended learning outcomes.

Currently, visitor identification technology to enhance room security is increasingly advancing. Initiated with face recognition and biometrics to the utilization of an IoT such as sensors, Bluetooth, and more [1], [2], [3]. It indicates that technological developments have a positive impact, particularly on visitor identification systems.

However, some technologies can't be easily implemented because many factors need to be considered, especially during the Covid-19 pandemic. Face recognition is one technology that has garnered attention, but it becomes very vulnerable when applied during the pandemic. Users have to remove their face masks and bring their faces close to the device to be detected. Removing masks during the pandemic can expose individuals to the risk of Covid-19 infection [4]. Meanwhile, the implementation of biometric methods requires a large dataset, necessitating devices with very high specifications to process the data quickly. This is inefficient as it takes a long time, whereas the identification process needs to be fast to easily recognize visitors.

To address these issues, a visitor identification system has now been developed using an Internet of Things (IoT) approach, combined with smartphones by adding facial and voice recognition [5], [6], [7], [8]. This shows that everyone is striving

to enhance security, particularly in the identification process to recognize visitors easily.

The implementation of an-IoT and smartphones is a choice worth considering. Moreover, most people view gadgets as a basic necessity to assist daily communication [9], [10]. However, the development of an IoT system integrated with smartphones takes a long time. Additionally, the Android operating system has API levels that require regular maintenance. Furthermore, adding features such as facial and voice recognition demands higher operating system specifications and other resources. A system that is not adaptive and not responsive will discourage users from using it.

Therefore, this study proposes a visitor identification system that is effortless for the public to implement while still using advanced technology. The system is developed with an IoT approach, especially in the era of Industry 4.0. Data-driven modelling is employed as the method for recognizing visitors based on the identification card. The room door will automatically lock using a Magnetic Lock and will open when the system is capable of recognizing the visitor. The system is also equipped with a Radio Frequency Identification (RFID) Reader to identify room visitors. Additionally, a Passive Infrared (PIR) device is added to verify visitors once they have entered the room. To facilitate visitors, the RFID Tag is replaced with the e-KTP as it serves the same function.

II. METHOD

1. Data Driven Modelling

Data-driven is a modelling approach where data regulates the flow of whole program. The output is the result of system processing based on the given input. Different inputs will produce different outputs. Therefore, this modelling allows input to act as a trigger to execute a specific process [11].

Nowadays, the data-driven approach is applied in various fields such as IoT, energy, and industry. Although the terminology may vary slightly, such as data-driven architecture or data-driven approach, the core idea remains the same: data acts as the trigger for the next action [12], [13].

In this study, the trigger is initiated by actions such as visitors bringing their e-KTP near the RFID Reader and verification from the PIR sensor. The E-KTP is utilized in security system because it has a unique serial number like RFID Card. This card is also used as identification ID for people that live in Indonesia [7].

The E-KTP triggers the program to perform data-matching processes in a database using a Raspberry Pi. If the visitor is registered, the Raspberry Pi instructs the magnetic lock to open the door. The system also stores data of registered and unregistered visitors.

2. Internet of Things

IoT describes how various machines interact with their surrounding environment and vice versa. Interactions range from simple to complex tasks such as monitoring devices to sensing devices. These machines include microprocessors, microcontrollers, sensors, monitoring devices, and other electronic devices. IoT also involves ensuring connectivity among these devices (things) and maintaining continuous communication [14].

In this research, the devices used include Raspberry Pi Model B, Magnetic Lock, RFID, Passive Infrared (PIR), and Driver Modules. The following subsection will explain the implementation of devices into the proposed system.

3. Raspberry Pi

The Raspberry Pi is a device equipped with RAM, CPU, GPU, USB ports, audio jack, HDMI, and other features resembling a computer. This device is also known as a single-board computer due to its capabilities similar to a computer but in a very small size, like an ATM card. Raspberry Pi is capable of running various applications, making it easier for developers to develop programs according to their needs [15].

Raspberry Pi is widely utilized in various fields such as robotics, security systems, healthcare, smart homes, and even simple devices like plant watering systems [16]. This demonstrates the diverse applications of Raspberry Pi in supporting and simplifying everyday life.

In this research, Raspberry Pi Model B was chosen for its specifications, including 512MB of memory, 2 USB ports, HDMI port, and Ethernet. It only requires 3.5 watts of power, sufficient to be powered by a smartphone charger. After several implementations and tests, this device performed optimally. Additionally, this model is affordable compared to newer types.

The Magnetic Lock is used to lock the room door due to the magnetic field generated when electricity flows through it. The Magnetic Lock 300 with ZL Bracket was chosen because it can withstand loads up to 300 kg and comes with a bracket for easy installation on doors and frames. This device also features I/O (Input/Output) pins, making it easy to integrate with the Driver Module.

4. Magnetic Lock

The Magnetic Lock is used to lock the room door due to the magnetic field generated when electricity flows through it. The Magnetic Lock 300 with ZL Bracket was chosen because it can withstand loads up to 300 kg and comes with a bracket for easy installation on doors and frames. This device also features I/O (Input/Output) pins, making it easy to integrate with the Driver Module.

5. Radio Frequency Identification

Radio Frequency Identification (RFID) is a technology used to read digital data from an object via radio waves. RFID consists of two main components: Tags and Readers. Tags store digital data of an object, typically used as a serial number. To read the serial number, a Reader is required. Currently, tags are implemented in Electronic Identity Cards, known as e-KTP.

In this research, e-KTP is utilized for ease of implementation. The RFID Reader chosen is the RFID Proximity Card Tag Reader EM4100. This device was selected because it has a USB port for direct connection to the Raspberry Pi. Additionally, the EM4100 reader can easily read the serial number on e-KTPs and is cost-effective.

6. Passive Infrared

In this research, Passive Infrared (PIR) is used as a method to verify visitors entering the room. This device has three pins: VCC, GND, and an output pin to send data to the Raspberry Pi. To efficiently identify room visitors, the PIR sensor is mounted on the inner door frame. When it is activated, the PIR sensor continuously emits pairs of infrared signals. When a visitor opens the door and passes through the door frame, the PIR sensor detects a change in potential due to the obstruction of its signal by the visitor's body. As the body approaches, the sensor experiences a positive potential change. Conversely, when the visitor moves away from the sensor, the PIR sensor experiences a negative potential change. This condition causes the PIR sensor to send an active high signal (1) from its output pin [17].

7. Modul Driver

The Driver Module is an electronic component designed specifically for this research. It serves as a medium to connect the Raspberry Pi with the Magnetic Lock, PIR sensor, and push-button, enabling them to work together. Additionally, this module acts as a safeguard to prevent damage to the devices during electrical current surges. It can be easily assembled and replaced if damaged.

The Driver Module consists of a 46ND05-P Relay, BC337 Transistor, 1kΩ Resistor, and two LEDs (green and red). Figure 1 illustrates the schematic of the driver module used in this research. This module also features I/O pins for connection to the Raspberry Pi, indicated by the 1x10 PIN HEADER, and a push-button indicated by the 1x3 PIN HEADER. The push button is used to unlock the door from inside the room when a visitor wants to exit.

The Relay is used to activate and deactivate the magnetic field of the magnetic lock through signals sent by the Raspberry Pi. LEDs are used as indicators to check visitor data on the database server. If a visitor is registered in the system, the LED lights up green. Conversely, if the visitor is not recognized, the driver module lights up the red LED.

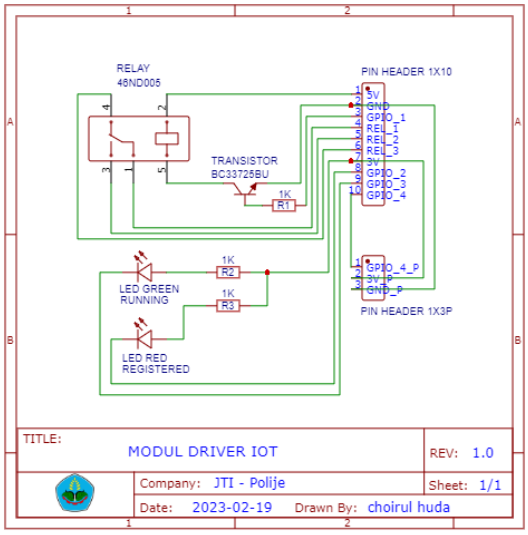

FIGURE 1. The IoT Modul Driver

8. Identification Information System

Identification Information System (IIS) is a web-based information system designed to show and manage visitor and room data. CodeIgniter was chosen as the framework for this application due to several advantages such as speed, lightweight nature, and ease of integration with databases. This framework smoothly adds other libraries to create responsive designs that adapt to user device resolutions, whether on smartphones, tablets, or computers.

IIS includes several menus, such as Registration, Visitors, Locking, and Intruder. The Registration menu features visitor data input into the system, including Card Serial Number, Visitor Name, Employee ID Number, Telephone Number, Email, and Visitor Status. The Visitors menu displays Name, ID Number, Card Serial Number, Telephone Number, and Email data. Administrators can modify visitor data as needed.

Locking is one of the standout features in this research. Administrators are capable of locking individual rooms or all rooms within the same building. When a room is locked, visitors cannot enter even if they are registered. This feature is designed to assist administrators in maintaining room security. The system can be implemented in various rooms as long as there is internet access, such as Wi-Fi or LAN cable connections.

III. RESULT AND DISCUSSION

In this research, the visitor identification process is divided into four stages: Inspection, Searching, Verification, and Recognition. Figure 2 illustrates proposed method of the research. Each stage will be further discussed in the following subsections. Before the system is implemented,

visitor data must be entered into IIS to be stored in the database. The data entered includes Name, Employee ID Number, e-KTP Serial Number, Telephone Number, Email, and Visitor Status.

IoT devices are installed near the room door for easy inspection when issues arise. The Magnetic Lock is installed on the upper door frame. This is done by the device capable of securely pulling the metal plate attached to the door. Each step will be discussed further below.

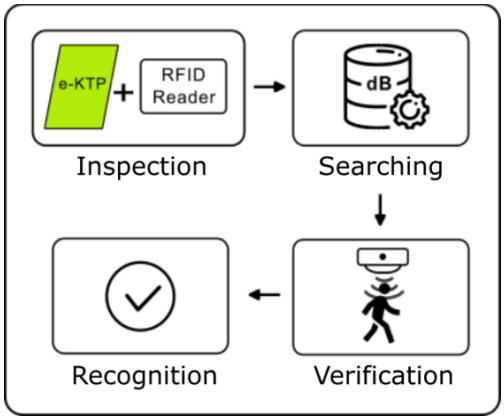

FIGURE 2. The Proposed Method

1. Inspection

When a visitor walks into the room, they must bring their e-KTP close to the RFID Reader located outside. The RFID works to capture the serial number of the e-KTP and transmits it into the Raspberry Pi via the USB port. Next, the serial number will be matched to data within the database in the subsequent stage.

The Inspection phase involves the General-Purpose Input/Output (GPIO) pins within the Raspberry Pi. Pins 13 and 3 are employed and responsible for sending high signal to turn on the LED indicator and activating the locking system. Pin 13 is used to turn on the light while pin 3 is used to send a high signal to the relay to the magnetic lock. Pseudocode 1 shows the algorithm within the Inspection phase.

PSEUDOCODE 1. The Inspection functions

```
function_capture_input_rfid
declare:
    system_run,magnetic_lock =integer;
    rfid_id =string;
    system_run =GPIO(13);
    magnetic_lock =GPIO(3);
    usb_port= Serial('/dev/ttyUSB0',19200,timeout = 5);
begin:
    system_run (HIGH);
    magnetic_lock (HIGH);
    while(1):
        READ(usb_port );
    rfid_id=usb_port (value);
    return rfid_id;
end
```

Variables must be initialized first, initiating GPIO pins 3 and 13 as well as the RFID serial number. The USB port path must be defined to ensure the Raspberry Pi executes the program quickly and smoothly. The path is continually called in a loop and stops staying for the input of the e-KTP serial number from the visitor.

Pseudocode 1 must be executed immediately while the Raspberry Pi starts up. To achieve this, you need to modify the *rc.local* file located in */etc/rc.local* using the command *$ sudo nano /etc/rc.local*. Consider the program from Pseudocode 1 is named *checking_input.py*. Next, add the line *$ /usr/bin/python /home/pi/checking_input.py &* at the existing code. Finally, end the code with exit 0 to ensure the program runs constantly at startup.

2. Searching

Next, the system will match the Serial Number in the database. This process applies to search the Serial Number based on the input data obtained from the RFID Reader in the previous section. Pseudocode 2 summarizes the steps involved in the Searching phase.

When *is_person* is true, the system will turn on the green LED and the process moving forward to the Verification phase. Conversely, if *is_person* is false, the green LED remains off and the identification will be stopped. Finally, the system will be disconnected from the database to prevent burdening IoT performance and secure visitor data.

PSEUDOCODE 2. The Searching Functions

```
function_searching
declare:
    rfid_id =string;
    is_person=boolean;
begin:
    open_connection ();
    connection(mySQL);
    query(SQL)=compare→rfid_id;
    if query(SQL)== rfid_id then
    is_person=true;
    verification_method();
    else
    is_person=false;
    identification→stop();
   close_connection ();
end
```

The advantages of the system are the presence of Visitors and Room Status. Visitor Status serves as a flag for the system indicating whether access is permitted or not. The flag is divided into two categories: Active and Inactive. Similarly, Room Status is also divided into two categories: Opened and Locked. Room Status is used as a locking feature that is performed by the room administrator to lock rooms one by one or multiple

rooms in a specific sector within a building at the time.

If both the Visitor Status is Active and the Room Status is opened, then the visitor is allowed to enter the room. In this case, both statuses are positive. Conversely, if either status is negative (Visitor Status is Inactive, or Room Status is Locked), the door will remain locked even if the visitor is registered. These status checks are only by the room administrator. The process enhances the protection of the identification system to prevent undesirable incidents.

3. Verification

This phase serves as a confirmation method to ensure that the visitor has indeed entered the room. The method initiates after the system identifies the visitor based on the e-KTP Serial Number detected by the RFID Reader. Next, the system triggers the PIR sensor to become active and detect movement when the door opens. The PIR sensor operates by continuously emitting two infrared beams and will send a *HIGH* signal when one of the beams is obstructed. Therefore, the sensor is utilized in the Verification phase. If the PIR sensor catches the movement, the system will deactivate the magnetic lock to allow the visitor to open the door. Otherwise, the magnetic lock remains active and of course, the door stays locked.

Although the system halts the magnetic field, the door does not remain open indefinitely. If the system unlocks the magnetic lock for 3 seconds but the PIR sensor does not catch any movement entering the room, the system withdraws this step and does not proceed to the next phase. Otherwise, if within 3 seconds the system notices the movement of the visitor opening the door, the identification process proceeds to the next phase, which is the Recognition phase.

4. Recognition

After the Inspection, Searching, and Verification phases have been completed, the system will get into the final phase, which is Recognition. The Recognition phase is the stage of the identification process where the visitor's data is stored in the database and displayed in the Identification Information System (IIS). This aims to enable the system to track where the visitor has entered the last room.

Based on these advantages, the system can be implemented in office areas, schools, and campuses. It is reasonable since the system is capable display the visitor's last location. For instance, students are able to utilize the system to discover the last room where a lecturer is located. It can be beneficial for discussion, submitting reports, or simply requesting a signature, among other purposes.

The stored data includes the e-KTP Serial Number. Next, the system will execute a query to show other related data such as Name, Employee ID, Email, Phone Number, and Visitor Status. The system also holds records of unregistered visitors. The process allows the room administrator to discover who tried to attempt. The system also stores logs when a visitor brings the RFID Tag or e-KTP and is close to it, providing information that can be used to determine when the identification process needs enhanced security.

IV. IMPLEMENTATION

The experiment was conducted in a laboratory located in one of the buildings at the Politeknik Negeri Jember. The laboratory has a code A2, where A represents the building and 2 is the room number. An RFID Reader was installed right next to the laboratory entrance to allow visitors to easily present their e-KTP.

1. Testing Cases

At this stage, there were five test cases consisting of T1-T5 as shown in Table 1. In Test Case 1 (T1), the IoT system is capable of recognizing the serial number from the visitor's e-KTP effectively. T1 begins when the system receives the e-KTP card number via the RFID Reader, matches the serial number in the database, verifies the visitor through the PIR sensor, and the process of unlocking the door with the magnetic lock. In T1, some processes include Inspection, Searching, Verification, and Recognition. A Data-Driven is also working in this phase to regulate the data for verifying the person who tries to enter into a specific room.

TABLE 1. List of Functional Testing Cases

Number	Cases	Status
T1	The system capable to recognize the visitor's e-KTP that registered	Complete
T2	The system capable to register and modify visitor data easily	Complete
T3	The system capable to display complete visitor data	Complete
T4	The system effectively locks door based on the room status	Complete
T5	The system smoothly locks door based on visitor status	Complete

In T2, the admin performs the registration process and modifies visitor data on the system. Then, the data is displayed and reviewed to see if it is correct or not in Test Case 3 (T3). In Test Case T4, the administrator simulates locking the room based on Room Status. The status is divided into two categories: Open and Locked. If the status is Open, the room can be accessed. If Locked, the room remains closed even if the visitor is registered.

In T5, the administrator simulates room locking based on Visitor Status. If the status is

Active, the visitor can easily access the room. However, if the visitor status is Inactive, the visitor is unable to walk into the room. This is due to the Raspberry Pi continuously sending an active signal to the magnetic lock.

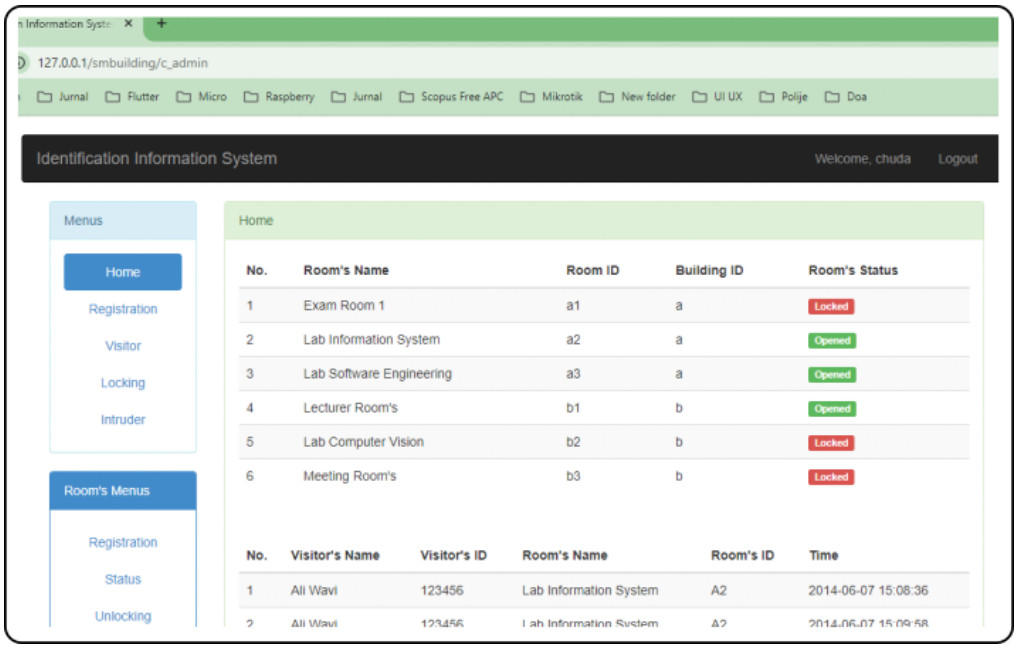

FIGURE 3. The Implementation of the IIS in a browser that runs on a desktop

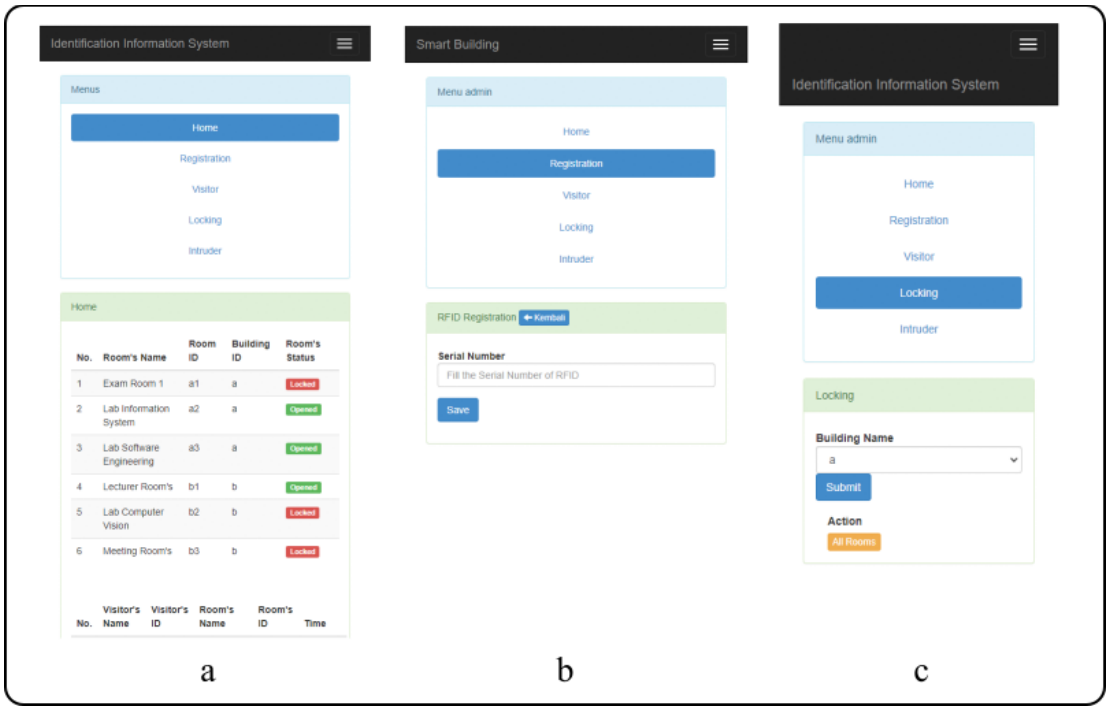

FIGURE 4. The Implementation the IIS that runs on a mobile version: a) Home menu; b) Registration menu, and; c) Locking Feature

Figures 3 & Figure 4 demonstrate the Identification Information System (IIS) that runs on different screen sizes. Figure 4 displays some of the capabilities of the system which are mentioned in T2, T3, and T4 respectively. Figure 4c) shows some information within a room conditions and visitor data performed on T5 in the mobile version. In this picture, the system performs room locking by Visitor Status which runs smoothly.

2. Evaluation

The number of visitors was 104, with 12 registered and 92 unregistered. The unregistered are referred as intruders. The system was installed for a month inside a room namely A2, and 150 attempts were captured. Visitors included students, room administrators, and lecturers who had access to a laboratory. The system was implemented during working hours, which were 08:00 to 16:00 Western Indonesian Time (WIB).

During the implementation process, the proposed system is capable of running optimally by triggering the next actions since the visitor brings the e-KTP close to the RFID Reader. All stages were working very well on every stage, beginning with the Inspection to Recognition phase. Doors were locking perfectly due to the Raspberry Pi being capable of transmitting a HIGH signal to the magnetic lock in an efficient way. Visitors' data were stored in a database and able to display quickly.

V. RESULT AND DISCUSSION

The proposed system has been proven to operate optimally based on the implementation described in the previous subsection. Furthermore, the system demonstrates better performance when compared to prior studies.

TABLE 2 shows a comparison with previous research. One of the key advantages of the proposed system is its ability to run features in parallel (multi-tasking). This is achieved through the use of a microcomputer, namely the Raspberry Pi, which enables the identification process to proceed more efficiently without the need to complete one specific task before initiating another. In contrast, previous studies utilized microcontrollers such as the ESP8266 and Arduino Uno, which are limited to single-task execution and less suitable for multi-tasking environments.

Another strength of the proposed system lies in its cross-platform accessibility. It can be accessed seamlessly from both computers and smartphones without requiring separate development or adjustments under varying lighting conditions [18]. By comparison, some earlier systems could only be accessed via a website or smartphone [7]. Furthermore, unlike prior approaches that required large training datasets, the proposed system minimizes the computational burden on IoT devices and servers [6]. In addition, it eliminates the need for direct physical interaction with users, such as removing masks or glasses, since authentication is performed by simply tapping an e-KTP against the RFID reader. This characteristic makes the system highly relevant and practical for implementation during the COVID-19 pandemic.

TABLE 2. List of comparison with some previous researches

Authors	Sensors	Methods	Data Training	Tasking Performance	Transmission Media	Capabilities
Zhang et al (2020) [19]	Unknown	Multimodal Biometric	Yes	Multi-Tasking	Unknown	Unknown
Najib et al (2021) [20]	NodeMCU V3 ESP8266, PIR, Relay, RFID, Selenoid	Unknow	No	Single Tasking	Wi-Fi	Mobile Application
Proposed Method	Raspberry Pi, Magnetic Lock, RFID, Modul Driver	Data-Driven Modelling	No	Multi-Tasking	LAN or Wi-fi	Web dan Mobile Application

VI. CONCLUSION

Based on some experiment that have been done, the proposed system capable to identify visitors using Data Driven Approach utilizing an IoT optimally. The system is easy to install within a room, affordable, and is able to improve room security. This approach is suitable for implementation in visitor identification systems since it triggers subsequent actions, such as visitor verification through motion using the PIR, and the sending and displaying of data to the IIS.

In future research, the system will be developed using RFID devices capable of capturing Serial Numbers from a greater distance. This enhancement is necessary to allow users to keep their RFID Tags in their pockets, thereby increasing the efficiency of the identification system.

VII. ACKNOWLEDGEMENT

Acknowledgments are extended to the Department of Information Technology at Politeknik Negeri Jember for providing research facilities and other equipment. Authors also appreciation to all parties who have assisted in this research.

REFERENCE

[1] J.-J. Lin and S.-C. Huang, "The implementation of the visitor access control system for the senior citizen based on the LBP face recognition," in *2017 International Conference on Fuzzy Theory and Its Applications (iFUZZY)*, IEEE, Nov. 2017, pp. 1–6. doi: 10.1109/iFUZZY.2017.8311817.

[2] K. Gautam, N. Sharma, P. Kumar, and V. P. Mishra, "COVID 19 Visitor Management System,"

Proceedings of 2nd IEEE International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2021, pp. 560–564, 2021, doi: 10.1109/ICCIKE51210.2021.9410724.

[3] P. Drozdowski, C. Rathgeb, B.-A. Mokros, and C. Busch, "Multi-Biometric Identification With Cascading Database Filtering," *IEEE Trans Biom Behav Identity Sci*, vol. 2, no. 3, pp. 210–222, Jul. 2020, doi: 10.1109/TBIOM.2020.2977215.

[4] M. Andriansyah, M. Subali, I. Purwanto, S. A. Irianto, and R. A. Pramono, "e-KTP as the basis of home security system using arduino UNO," in *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, IEEE, Aug. 2017, pp. 1–5. doi: 10.1109/CAIPT.2017.8320693.

[5] X. Zhang, D. Cheng, P. Jia, Y. Dai, and X. Xu, "An Efficient Android-Based Multimodal Biometric Authentication System with Face and Voice," *IEEE Access*, vol. 8, pp. 102757–102772, 2020, doi: 10.1109/ACCESS.2020.2999115.

[6] A. A. Najib, R. Munadi, and N. B. Aditya Karna, "Security system with RFID control using E-KTP and internet of things," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 3, pp. 1436–1445, Jun. 2021, doi: 10.11591/eei.v10i3.2834.

[7] L. Tan, N. Shi, K. Yu, M. Aloqaily, and Y. Jararweh, "A Blockchain-empowered Access Control Framework for Smart Devices in Green Internet of Things," *ACM Trans Internet Technol*, vol. 21, no. 3, pp. 1–20, Jun. 2021, doi: 10.1145/3433542.

[8] L. Y. Rock, F. P. Tajudeen, and Y. W. Chung, "Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective," *Univers Access Inf Soc*, vol. 23, no. 1, pp. 345–364, Mar. 2024, doi: 10.1007/s10209-022-00937-0.

[9] A. Koohang, C. S. Sargent, J. H. Nord, and J. Paliszkiewicz, "Internet of Things (IoT): From awareness to continued use," *Int J Inf Manage*, vol. 62, p. 102442, 2022, doi: https://doi.org/10.1016/j.ijinfomgt.2021.102442.

[10] I. Sommerville, *Software engineering (10th edition)*, 10th ed. Harlow: Pearson, 2016.

[11] Y. Sun, F. Haghighat, and B. C. M. Fung, "A review of the-state-of-the-art in data-driven approaches for building energy prediction," *Energy Build*, vol. 221, p. 110022, 2020, doi: https://doi.org/10.1016/j.enbuild.2020.110022.

[12] A. Bousdekis, K. Lepenioti, D. Apostolou, and G. Mentzas, "A review of data-driven decision-making methods for industry 4.0 maintenance applications," *Electronics (Switzerland)*, vol. 10, no. 7, 2021, doi: 10.3390/electronics10070828.

[13] S. Greengard, *The Internet of Things, Revised and Updated Edition*, vol. 59. Cambridge: The MIT Press, 2021.

[14] G. Halfacree, *The Official Raspberry Pi Beginner's Guide - How to use your new computer*, 2nd ed. Cambridge: Raspberry Pi Press, 2019.

[15] C. Huda, B. Etikasari, and P. S. D. Puspitasari, "A Smart Greenhouse Production System Utilizes an IoT Technology," *JUITA : Jurnal Informatika*, vol. 11, no. 1, p. 117, 2023, doi: 10.30595/juita.v11i1.16191.

[16] L. Fried, "PIR Motion Sensor," 2021. [Online]. Available: https://learn.adafruit.com/pir-passive-infrared-proximity-motion-sensor

[17] I. Chatisa, Y. A. Syahbana, A. Urip, and A. Wibowo, "A building security monitoring system based on the internet of things (IoT) with illumination-invariant face recognition for object detection," *Kinetik*, vol. 4, no. 1, pp. 485–497, 2023, doi: doi.org/10.22219/kinetik.v8i1.1622.

[18] X. Zhang, D. Cheng, P. Jia, Y. Dai, and X. Xu, "An Efficient Android-Based Multimodal Biometric Authentication System with Face and Voice," *IEEE Access*, vol. 8, pp. 102757–102772, 2020, doi: 10.1109/ACCESS.2020.2999115.

[19] A. A. Najib, R. Munadi, and N. B. Aditya Karna, "Security system with RFID control using E-KTP and internet of things," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 3, pp. 1436–1445, Jun. 2021, doi: 10.11591/eei.v10i3.2834.

CHOIRUL HUDA, was born at Jember, East Java Indonesia in 1992. He received the Bachelor's degree of Informatic Engineering from Universitas Brawijaya Malang in 2014. He spent more than two years working as a mobile application developer for a private company. In 2020, he earned a Master's degree in Computer Science from Brawijaya University, Malang. He currently works as a lecturer at Politeknik Negeri Jember. His research interests include Mobile Application Development, Computer Vision, and the Internet of Things.

LUKMAN HAKIM, was born at Bondowoso, East Java Indonesia in 1989. Received the Bachelor's degree of Informatic Engineering from Universitas Muhammadiyah Jember in 2012. In 2019, he earned a Master's degree in Computer Science from Institut Teknologi Sepuluh Nopember, Surabaya. He currently works as a lecturer at Politeknik Negeri Jember. His research interests include Web Application Development, Digital Business, Word Classification, and Digital Services.