Indonesian Journal of Artificial Intelligence and Data Mining (IJAIDM)
Vol. 8, No. 1, March 2025, pp. 102 – 109
p-ISSN: 2614-3372 | e-ISSN: 2614-6150

Implementation of Fingerprint Biometrics on Smart Door Entrance Access Integrated with Internet of Things-based PINs

[1]Wulan Trihandini, [2]Jon Endri, [3*]Irma Salamah
[1,2,3]Telecomunication Engineering, State Polytechnic of Sriwijaya, Indonesia
Email: [1]wulantrihandini12@gmail.com, [2]jon_endri@polsri.ac.id, [3]irma.salamah@yahoo.com

Article Info
Article history:
Received Jul 20th, 2024
Revised Sep 3rd, 2024
Accepted Dec 29th, 2024

Keyword:
Fingerprint
Internet of Things
Optical Scanning Sensor
Smart Door

ABSTRACT
Security is something that must often be ignored by most people and think it is safe, but it turns out that someone can still lose their valuables. In this final project, we will design an Internet of Things (IoT)-based smart door access tool that uses a fingerprint and pin password using the Optical Scanner Sensor method. The purpose of making and designing a smart door tool based on the IoT is one of them to apply the optical method as a method used to recognize fingerprint biometric identification. By using a smartphone (android) as a controller using the NodeMCU contained in the ESP2866 WiFi module via an internet connection connected to an application made with MIT App Inventor. In the application of fingerprint sensors using the optical method, the scanning process is obtained through finger scanning based on the effect of light reflection that occurs on the optical sensor on the fingerprint. So as to produce digital image retrieval on identified fingerprints. The communication that uses the fingerprint sensor and Arduino uno as a data processing unit uses serial data communication. When the command has run according to its function, the results of the data obtained enter in realtime at the data processing place.

Corresponding Author
Irma Salamah
Telecomunication Engineering,
State Polytechnic of Sriwijaya,
Palembang, South Sumatera, Indonesian.
Email: irma.salamah@yahoo.com

DOI: http://dx.doi.org/10.24014/ijaidm.v8i1.31738

1. INTRODUCTION

With the rapid advancement of technology in modern times, human needs will become more complex. In particular, the increasing use of communication technology by people. As long as technology remains stable and connected, rapid technological advances can be seen as a means to foster creativity and communication in unexpected ways[1]. Modern industry has produced a wide variety of technologies in this era, ranging from newly developed technologies to technologies that are the result of evolution from previous technologies. In addition, advanced technology is also needed for security systems, especially private door security systems [2]. One of the most important components of every home is the door. Opening the door manually will be difficult or worrying because to open and close the door of the house [10].

As technological capabilities increase, consideration should also be given to automated door security systems when replacing manual methods [11]. Basically, when replacing manual methods, the full potential of technological considerations also needs to be given to automatic door security systems [3]. The main problem that needs to be addressed is the door that is often lost due to the use of manual methods. There are many people who experience problems in the process of moving from a public space to a private space, such as a waiting room or a private space stacked with items that are more expensive than those used by many people [12]. There are many methods that can be used to improve home security. One of them is using Internet of Things (IoT) technology as a method to create doors, which are sometimes referred to as “smart doors”. The technological advancement demonstrated by the IoT, allows any object, including those with arches, to be

connected to the internet. Through the development of the Internet of Things, any object, including those with arches, can be connected to the internet [5].

Institute of Electrical and Electronics Engineers (IEEE) defines the IoT as a network consisting of individual devices connected to sensors in an internet-based network [4]. Smart door lock is a type of lock that can be operated with a keypad, fingerprint, or even a smartphone (android)[6]. In previous research there is a comparison, namely making a smart door using RASPBERRY PI 3 on a smartphone that is connected to the internet and bluetooth, then giving data to ULN 2803 as an IC to increase the voltage so that it can use the selenoid as a door lock according to the voice command that has been given [13]. Create a smart door lock with a QR code as a means of scanning the baecode that has been programmed by a microcontroller [14]. Make a smart keypad for motorcycles using Near Field Communication (NFC) cards to display notifications from DF Mini Player to further design bicycle engines [15]. The author will answer these needs, namely the design of the IOT system on samrt door lovk using the blynk application in combining ESP32 CAM with selenoid [16].

In this research, I designed a smart door entrance that uses a fingerprint, PIN password and smartphone (android) as a substitute for a manual key to open and close the door [7]. In this study I used the optical method as the method used to recognize fingerprint biometric identification[8]. In the process of making this tool, 2 designs are made, namely hardware design (hardware) and software design (software). So from this, the idea to make this smart door uses a fingerprint, PIN password and smartphone (android) as a controller for opening and closing the door [9].

2. RESEARCH METHOD

2.1 Research framework

The research findings are presented in clear and concise graphical form. The block diagram is the most important type of diagram as it can be used to understand the different types of tasks that will be performed during the testing process. As a result, the final form of the diagram used to describe the analysis process will result in a system that can function effectively. The Research Framework can view figure 1.

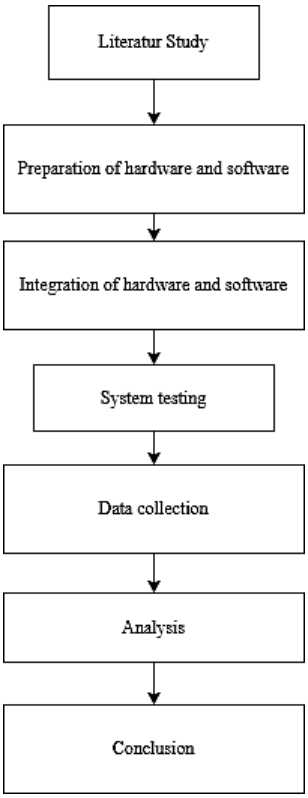

Figure 1. Block Diagram of Research Framework

The first stage in this research is a literature study, where the researcher collects various literatures that discuss relevant research topics and variables. This process involved searching for journals, e-books on the internet, and sorting out the literature to be used. The next stage is hardware and software preparation. Hardware preparation includes physical components that will run the system, such as LoRa transmitter and receiver modules, Arduino, power supply circuit, and keyboard interface and Liquid Crystal Display (LCD)

display. While software preparation includes software that will control the hardware, such as Arduino IDE and serial terminal. After all the hardware and software are prepared, the next stage is hardware and software integration, where the hardware is connected and the software is installed to ensure everything is working properly. The system testing stage is carried out after hardware and software integration is complete. This test includes several steps, namely testing or.

2.2 Device Design

In this research, the design process is divided into two parts, namely design for hardware and design for software. Designing a comprehensive system block diagram is the first step in hardware design. One of the most important elements in the diagramming process is the tool. An overview of how the circuit works can be obtained from the circuit block diagram. Therefore, the overall circuit block diagram will produce a system that can function.

2.2.1 Hardware Design

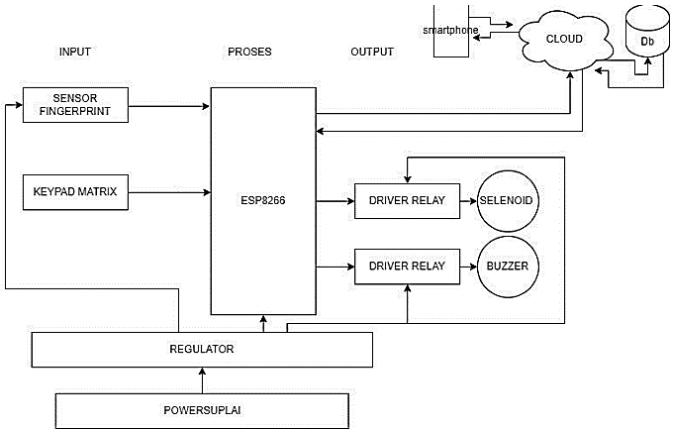

Figure 2. Hardware System Block Diagram

Based on the figure 2, we can see a block diagram design that describes a whole system. Broadly speaking, the block diagram is divided into three main parts. First, the input block, which consists of two system inputs, namely input from the keypad which functions as a receiver of user code data and input from the fingerprint sensor which functions to scan fingerprints. Second, the data processing block, which is carried out by a microcontroller. This microcontroller is tasked with translating input data from the matrix keypad and fingerprint sensor by validating the data that has been read, matching it with the code and fingerprint that has been determined. The microcontroller also directs the information data that has been processed to the LCD display as an input board that provides information to the user, and controls the output block in the form of a servo motor that moves the door leaf mechanism. The three output blocks, which consist of a data display on the LCD sc.

2.2.2 Software Design

The results of thissoftware design produce a program that is used to process keypad and fingerprint scanning data based on the protocol of each device and produce an application as a control tool to open the door. This application is made through MIT App Inventor which will be displayed on a smartphone (android) which will be directly connected to the internet network. Then, the keypad uses the column and row scanning method while the fingerprint uses serial data communication. In the source coding program code in the Arduino IDE application using the C++ program language. The software design can be described in the following flowchart description on figure 3.

3.3. Devices used

3.3.1 Hardware used

The hardware used in this hardware design includes several important components, including: Arduino UNO as the main microcontroller, 3x4 keypad for user input, fingerprint sensor for identity verification, and servo for the drive mechanism. In addition, jumper cables are also used to connect between components, NodeMCU ESP2866 for Wi-Fi connectivity, and LCD to display information to the user. All these components work together to create an efficient and integrated system.

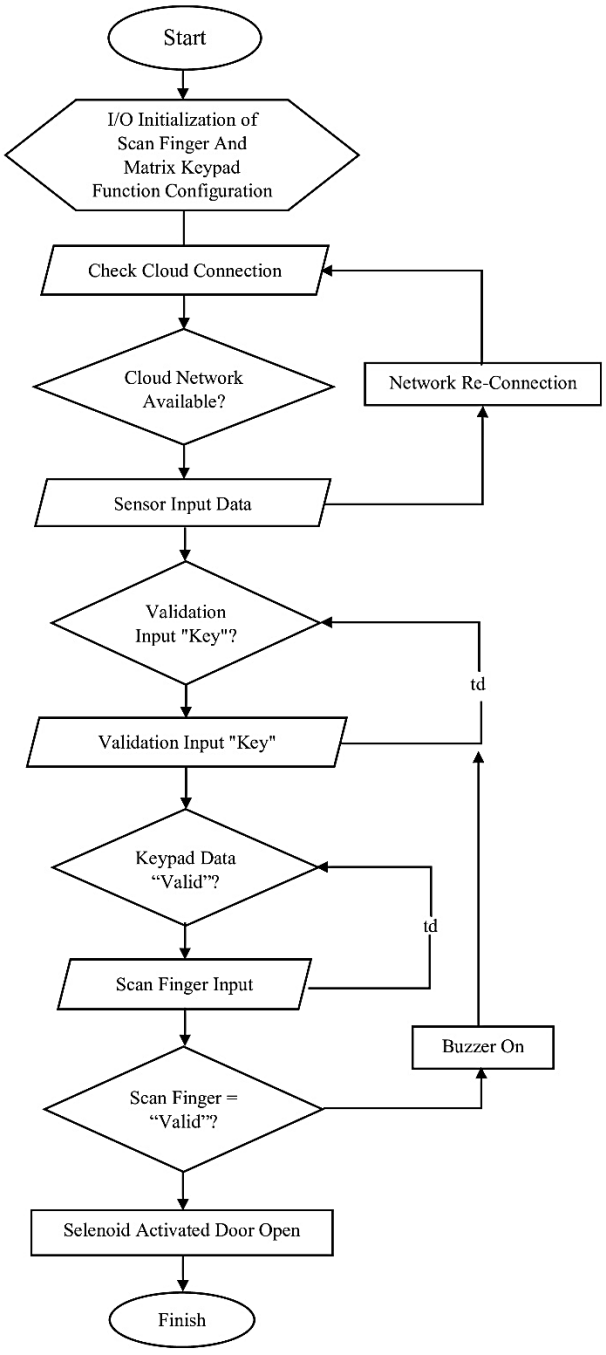

Figure 3. Software System Block Diagram

3.3.2 Software Used

The hardware used in this software design includes Arduino IDE and MIT App Inventor. Arduino IDE is used to write and upload code to the microcontroller, while MIT App Inventor is used to design an Android-based application that serves as the user interface to interact with the hardware. These two tools work together to support the development and implementation of the overall system.

5. Method development

The data that has been collected will then be developed to see the data that has been obtained in the monitoring response results on the designed tool design. Then the data is analyzed in order to get the results of the study on research to be combined with other data results. IoT is emerging as an important issue on the Internet. The physical world, or things, will require various types of sensors connected to the internet through technological infrastructure and networks, such as Radio Frequency Identification (RFID) tags, RFID frequency sensors, wireless sensors, web-based time tracking services, and the Internet of Things, which is

essentially a cyber-physical network. Real-time data will automatically be generated by connected devices and sensors in scenarios such as a large number of things with sensors/actuators connected to the internet. All IoT activities are intended to collect accurate mental data in an efficient way however, the most important task is to analyze and convert mental data into more valuable information.

3. RESULTS AND ANALYSIS

At this stage, there are several steps taken to put the finished toolkit into practice. This phase begins by utilizing the anticipated data to provide support and resources to achieve the desired level of growth.

3.1. Design

The results of this experiment are divided into two categories, namely hardware experiments and software experiments. The results of the previous hardware method resulted in a smart door lock, while the results of the previous software method resulted in an android smartphone application that functions as a control panel when the user wants to make a door. When a tool is geared, the purpose of this equipment inspection process is to ensure that, when examined in detail, each component can function at its best according to the agreed needs.

3.1.1. Hardware Design

This hardware design uses smart door controller tools such as Arduino Uno, LCD, Servo Motor, Jumper Cable, Power Suply, Adapter, Fingerprint and 4x4 Keypad. In this hardware design, it is placed in a miniature house that has been made, so that the design is made in such a way according to functions and uses. The following is an image of the results of the hardware design. Hardware can be shown in the figure 4, figure 5 and figure 6.

Figure 4. Front View of Miniature House

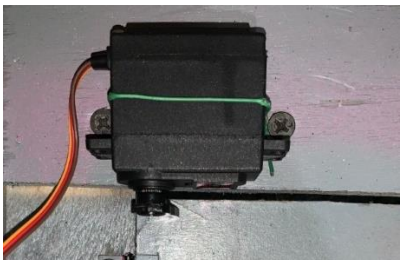

Figure 5. View of the Servo Located Behind the Door

Figure 6. Arduino UNO Display and Jumper Cable

Figure 1 above is a view from the front of the miniature house made as much as possible by the author. On the right side of the picture there is a placement of tools, namely LCD, keypad, and fingerprint. Figure 2 above shows the placement of the servo behind the door according to its function, namely as a controller when

the door is open and closed. Figure 3 above shows the Arduino UNO display and jumper cables under the miniature house, the reason for laying it down is so that the miniature jumper cables do not look messy.

3.1.2. Software Design

The results of this software design produce a programming in the Arduino IDE which is used to process keypad and fingerprint scanning data based on the protocol of each device and produce an application as a control tool to open the door. This application is made through MIT App Inventor which will be displayed on a smartphone (android) which will be directly connected to the internet network. Then, the keypad uses column and row scanning methods while the fingerprint uses serial data communication.

3.2. Testing Results Using Keypad and Fingerprint

The result of this work is the combination of hardware components, such as the keypad and sliding door in this smart lock, which provides a robust and flexible security system. The keypad provides flexibility with easy-to-read entries and PINs, while Fingerprint technology offers unique biometric fingerprint detection and enhanced security. By using these methods, smart lock doors can provide better user management, easier access, and better security.

Table 1. Test Results on Keypad and Fingerprint

Test	Password Code	Fingerprint	LCD Display	Servo
1	1234	right thumb	*Correct*	Open
2	1313	Right middle finger	*Correct*	Open
3	0808	Right middle finger	*Invalid Code*	Not Open
4	4321	Right index finger	*Invalid Code*	Not Open
5	0000	Right index finger	*Correct*	Open

Table 1 can be concluded that in this 5-time experiment some were successful and some were unsuccessful. The success of this experiment is because the PIN password and fingerprint that was tried were correct and the unsuccessful experiment was due to the entry of the wrong PIN password and fingerprint.

3.3. Test Results on Smartphone (Android)

To ensure the function of the application when remotely, that is, when the user is not at home or wants to provide access to open the door temporarily to guests or work, the smartphone application for the smart lock door is carried out. Securing the use of the smartphone to create the door ensures that only people who have the appropriate capabilities can create the door. Finally, the ease of use of this Android smartphone menu item allows users to navigate and interact more easily. Thereafter, any application can successfully connect to the smart lock door via an internet connection without the need for a wired or wireless connection. The application created consists of several display menus with several features tailored to the usage function which can be seen in the figure 7.

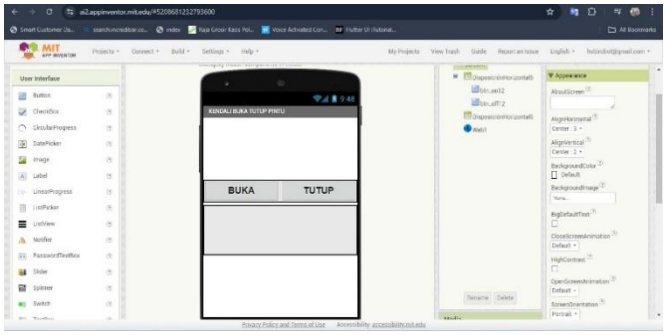

Figure 7. Display on the Smartphone Menu

In Table 2, application testing is successfully used with a menu display that functions as created. The command to open is by clicking the “OPEN” button while the command to close is by clicking the “CLOSE” button. Application testing on smartphones for smart lock doors is carried out to ensure the application functions can work properly or not. The security of using this smartphone is limited to users who are given access to have an application that has been designed on a registered smartphone. After that, an application can be successfully connected to a smart lock door via an internet connection without the need for a cable or wireless connection. The following table 2 is a look at the experiment using a smartphone (android).

Table 2. Experiment using a smartphone

Command	Result Description
OPEN	WORKS
CLOSE	WORKS

4. DISCUSSION

This research designs an IoT-based smart door lock that improves security and convenience with access features via smartphone, PIN, or fingerprint sensor. The system uses MIT App Inventor to control the device through smartphone, PIN, and fingerprint applications. The design process involves component selection, system design, programming, Android application development, and tool testing to ensure performance as expected. The difference from previous researchers is that this research focuses on the optical scan method in fingerprint biometric identification and the data communication protocol used in the applied sensor scanner interface. The advantages at the time of testing this tool are that the door can be opened when the tester forgets the pin password that has been made before and can open the door by using andoid, and vice versa. In testing the tools that have been carried out, there are still some shortcomings, so the authors suggest that fo.

5. CONCLUSION

Based on the results of the tool testing and the problem formulation listed on the previous page, it can be concluded "The fingerprint application process uses an optical scanning method based on finger scanning, which is based on the light penetration effect observed in the fingerprint optical sensor. As a result, a digital signature can be generated on a uniquely identified fingerprint. There is a communication method that uses a fingerprint sensor and an Arduino Uno as a data collection unit that uses serial data communication. Furthermore, at the time of keypad access, the data scanning process is performed using the column and row scanning method on the matrix keypad array. In this case, a 4x4 keypad is used. The data obtained through keypad input is a parallel set of eight PINs, consisting of four column entries and four row entries. On the menu screen of the pre-developed application, the "OPEN" button will notify the user when the door will be opened, and the "CLOSE" button will notify the user when the door will be closed."

6. ACKNOWLEDGEMENTS

In testing the tools that have been carried out, there are still some shortcomings, so the authors suggest for further research "Can be added detection through voice or face recognition so that access to open the door can be more easily used".

REFERENCES

[1] Mariza Wijayanti, "Prototype Smart Home Dengan Nodemcu Esp8266 Berbasis IoT," *J. Ilm. Tek.*, vol. 1, no. 2, pp. 101–107, 2022, doi: 10.56127/juit.v1i2.169.

[2] H. Yalandra and P. Jaya, "Rancang Bangun Pengaman Pintu Personal Room Menggunakan Sensor Sidik Jari Berbasis Arduino," *Voteteknika (Vocational Tek. Elektron. dan Inform.*, vol. 7, no. 2, p. 118, 2019, doi: 10.24036/voteteknika.v7i2.104347.

[3] M. L. Hakim and I. Yunianto, "System Smart Door Lock Pada Ruang Lab Komputer Sma Muhammdiyah 9 Kota Bekasi Berbasis Arduino Nano," *Jupiter J. Comput. Inf. Technol.*, vol. 4, no. 1, pp. 38–47, 2023, doi: 10.53990/cist.v4i1.253.

[4] D. Setiadi and M. N. Abdul Muhaemin, "Penerapan Internet Of Things (Iot) Pada Sistem Monitoring Irigasi (Smart Irigasi)," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 3, no. 2, p. 95, 2018, doi: 10.32897/infotronik.2018.3.2.108.

[5] W. Adhiwibowo, A. M. Hirzan, and M. S. Suprayogi, "Peningkatan Keamanan Data End-To-End Smart Door Menggunakan Advanced Encryption Standard," J. ELTIKOM, vol. 6, no. 2, pp. 186–194, 2022, doi: 10.31961/eltikom.v6i2.574.

[6] K. Y. Sun, Y. Pernando, and M. I. Safari, "Perancangan Sistem IoT pada *Smart Door Lock* Menggunakan Aplikasi *BLYNK*," *JUTSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 1, no. 3, pp. 289–296, 2021, doi: 10.33330/jutsi.v1i3.1360.

[7] M. I. Mahali, "*Smart Door Locks Based on Internet of Things Concept with mobile Backend as a Service*," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 1, no. 3, pp. 171–181, 2017, doi: 10.21831/elinvo.v1i3.14260.

[8] A. Unique, "済無*No Title No Title No Title*," no. 0, pp. 1–23, 2016.

[9] R. F. Christianti and D. Supriyadi, "4-*Article Text*-16-2-10-20160919," vol. 5, no. 2, pp. 17–23, 2013.

[10] J. M. Santoso and A. R. Iskandar, "Rancang Bangun Aplikasi Jurnal Dan Absensi Pada *Study* Center Di Wilayah Cengkareng Barat Berbasis Android," *eJournal Mhs. Akad. Telkom Jakarta*, vol. 2, no. 1, pp. 50–56, 2020, [*Online*]. *Available*: *http://ejournal.akademitelkom.ac.id/emit/index.php/eMit/article/view/39/26*

[11] J. Kuswanto and F. Radiansah, "Media Pembelajaran Berbasis Android Pada Mata Pelajaran Sistem Operasi Jaringan Kelas XI," *J. Media Infotama*, vol. 14, no. 1, 2018, doi: 10.37676/jmi.v14i1.467.

[12] D. Setiadi and M. N. Abdul Muhaemin, "Penerapan *Internet Of Things* (Iot) Pada Sistem Monitoring Irigasi (*SMART IRIGASI*)," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 3, no. 2, p. 95, 2018, doi:

10.32897/infotronik.2018.3.2.108.
[13] D. Aryani, D. Iskandar, and F. Indriyani, "Perancangan Smart Door Lock Menggunakan Voice Recognition Berbasis Rapberry Pi 3," J. CERITA, vol. 4,
no. 2, pp. 180–189, 2018, doi: 10.33050/cerita.v4i2.641.
[14] T. Lonika and S. Hariyanto, "Simulasi Smart Door Lock Berbasis QR Code Menggunakan Arduino Uno pada Penyewaan Apartemen Online," vol. 1, pp. 9– 15, 2019.
[15] N. Z. Ulinnuha, "Rancang Bangun Smart Key Menggunakan Nfc (Near Field Communication) Guna Meningkatkan Sistem Keamanan Sepeda Motor," pp. 52–57, 2020.
[16] Kaleb Yefune Sun, Yonky Pernando, M Ibnu Safari, "Perancangan Sistem Iot Pada Smart Door Lock Menggunakan Aplikasi Blynk," Vol. 1 No. 3October 2021, hlm. 289 – 296.
[17] Sofyan, A. A., Puspitorini, P., & Baehaki, D. (2017). Sistem Keamanan Pengendali Pintu Otomatis Berbasis Radio Frequency Identification (RFID) Dengan Arduino Uno R3. Jurnal Sisfotek Global, 7(1).
[18] Wahyudi, R., Soesanto, O., & Muliadi, M. (2016). Rancang Bangun Aplikasi Pengenalan Pola Sidik Jari. Klik-Kumpulan Jurnal Ilmu Komputer, 2(1), 74-83.
[19] Rurungan, J., Nugraha, D. W., & Anshori, Y. (2014). Sistem Pengaman Pintu Otomatis Menggunakan Radio Frequency Identification (RFID) Tag Card Dan Personal Identification Number (PIN) Berbasis Mikrokontroler AVR Atmega 128. Mektrik, 1(1).
Sofyan, A. A., Puspitorini,
[20] Arafat ,"Sistem Pengamanan Pintu Rumah Berbasis Internet Of Things (IoT) Dengan ESP8266 ".Technologia, 2016

BIBLIOGRAPHY OF AUTHORS

Wulan Trihandini, born in Lubuklinggau on March 12, 2002. Currently the author is a final semester student at the Telecommunication Engineering Study Program, Department of Electrical Engineering, Politeknik Negeri Sriwijaya.

Ir. Jon Endri, M.T currently the author is a lecturer at the Telecommunication Engineering Study Program, Department of Electrical Engineering, Politeknik Negeri Sriwijaya. The author graduated from S1 Sriwijaya University in 1987 and continued his Masters education at one of the universities in Indonesia. The author has several publications, one of which is entitled Designing an IoT-Based Server Room Temperature and Humidity Regulator in 2019.

Dr. Irma Salamah, S.T., M.T.I, currently the author is a lecturer at the Telecommunication Engineering Study Program, Electrical Engineering Department, Politeknik Negeri Sriwijaya. The author graduated from S1 Sriwijaya University in 2002, then continued his Masters at the University of Indonesia in 2011, and continued his Doctoral Program at Persada Indonesia Yai University in 2023. The author has several published works, one of which is entitled Design For A Remote Smart Home Monitor Using the Internet of Thinge (IoT) in 2022.