Fingerprint based smart door lock system using Arduino and smartphone application

Tole Sutikno[1,2,3], Moh Ainur Faqih Ubaidillah[2], Watra Arsadiando[3], Hendril Satrian Purnama[3]
[1]Master Program of Electrical Engineering, Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Department Electrical Engineering, Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[3]Embedded System and Power Electronics Research Group, Yogyakarta, Indonesia

ABSTRACT

In 2023, crime cases in Indonesia will reach 105,133. Cases of theft with aggravation dominate the majority of cases. Everyone is concerned about safety, but doors are typically opened and closed using physical keys. This is vulnerable to being tampered with with fake keys, which can lead to house break-ins and theft. In this research, we propose a fingerprint-based wireless door lock design using Arduino and a smartphone. We offer this solution as a preventive measure to reduce the high rate of theft in homes or other buildings. The devices used are Arduino UNO R3, fingerprint sensor, HC-05 Bluetooth module, buzzer, and door lock solenoid. The results of the fingerprint-based wireless door lock using Arduino and a smartphone can function well, with an average response time of 1.20 seconds. Furthermore, testing the HC-05 Bluetooth when sending signals to a smartphone shows that it can read data accurately with an average response time of 1.54 seconds.

Corresponding Author:

Tole Sutikno
Master Program of Electrical Engineering, Faculty of Industrial Technology
Universitas Ahmad Dahlan
Southern Ringroad, Kragilan, Tamanan, Banguntapan, Bantul, Special Region of Yogyakarta 55191, Indonesia
Email: tole@te.uad.ac.id

1. INTRODUCTION

Crime cases in Indonesia in 2023 will increase by 30.7% from 2022, with a total of 105,133 cases. According to data from the National Police of the Republic of Indonesia, 30,019 cases of aggravated theft make up the majority of these cases [1]. One of the crimes of cheating is theft in the house or yard by damaging and uncovering it to enter the house and cause a criminal case. The National Police of the Republic of Indonesia urges everyone to always be alert and to always provide a proper security system for their homes.

When talking about home security systems, doors are the most important part of a building because they are the main access to go in or out. For this reason, a proper security system is needed on the door to prevent theft [2]. Currently, the only doors available on the market have physical keys to securely open or close the door of a building. However, physical keys are vulnerable to being tampered with with fake keys, which can lead to house break-ins and theft. [3], [4]. With rapidly developing technology, people are looking for devices to ensure safety and comfort in their homes. There are currently several types of security device technology, such as facial recognition [5]–[7], fingerprint [3], [4], [8]–[10], finger geometry (finger size and position), iris recognition, vein recognition, retina scan, and voice recognition [2], [3], [6], [7], [9]–[18].

Smart door locks using biometrics have the advantage of higher security. In a smart home, the security system is a very important part [19]–[24]. Fingerprint recognition is one of the most secure systems because a person's fingerprint is never coordinated with anyone else's [24]–[26]. So, someone's access to the door lock can be limited. This makes fingerprints the new automatic ID for every person [26]–[29]. With this idea, a plan and model of a fingerprint-based door lock framework will be presented in this paper. This study proposes security device technology using a fingerprint sensor as the main access to unlock. Furthermore, in certain conditions, an alternative to unlocking the door remotely is to use an application on a smartphone with Bluetooth HC-05 as a wireless data transmitter.

2.   METHODS

This research focuses on security aspects in the context of using fingerprint sensors and smartphones to control home door locking. Through the use of this technology, data will be sent wirelessly via the HC-05 Bluetooth module to smartphone applications designed using the MIT App Inventor platform [30]–[38]. The process of recognizing and extracting fingerprint data for the smart door lock device being developed can be seen in Figure 1.

The expected result is the ability to unlock home doors automatically using a fingerprint sensor and hardware that is connected to a smartphone. In this research, there are several stages involving various research materials and resources. This sub-chapter includes hardware design, software development, and the preparation of wiring diagrams. The hardware design process begins with creating block diagrams and flowchart diagrams to plan the steps to be taken. The next step is to create a system schematic circuit design by combining all device components into a single, integrated, and controllable system.

2.1. System configuration

Figure 2(a) shows the block diagram system and becomes a reference for how the system works. Arduino UNO acts as the brain of the system and manages data from fingerprints and smartphones. The Arduino is then connected to various output components, including LEDs, buzzers, and relays. The relay functions as a link between the Arduino and the door lock solenoid. The fingerprint-based wireless door lock system is implemented using Arduino hardware and smartphone software. In this figure, the main steps and components of this system are shown sequentially, making it possible to understand clearly and in detail how the system can operate. The flow diagram starts with system initialization, where the system will wait for input data from the fingerprint or Bluetooth sensor. When Bluetooth sends data in the form of an interger 1, the LED, buzzer, and solenoid connected to the relay will light up for 5 seconds, then turn off while waiting for the data to be input again. Likewise with fingerprints, if the finger detected by the sensor is registered, then the LED, buzzer, and solenoid connected to the relay will turn on for 5 seconds, then turn off, and the door lock solenoid will close automatically until you wait for fingerprint data again to open it. If the attached fingerprint is not registered, the buzzer will flash three times, indicating that the attached fingerprint is not registered. This process is shown in Figure 2(b). The implemented hardware schematic diagram is shown in Figure 2(c).
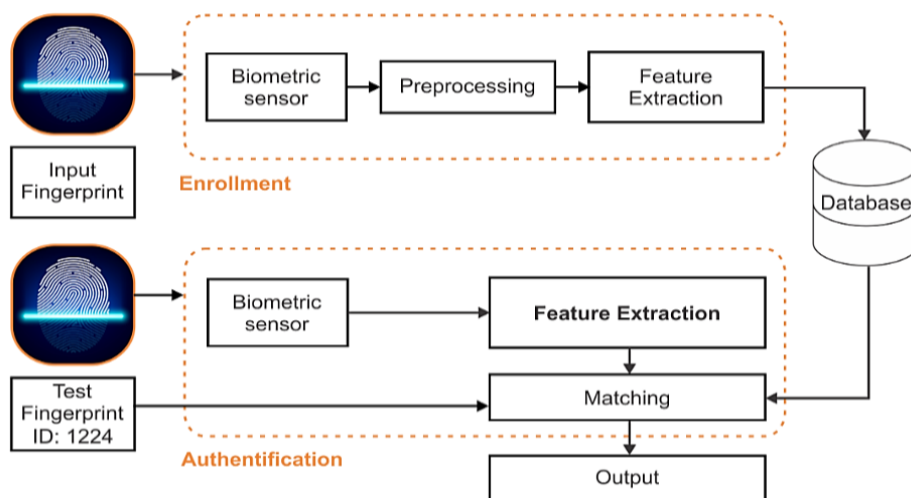

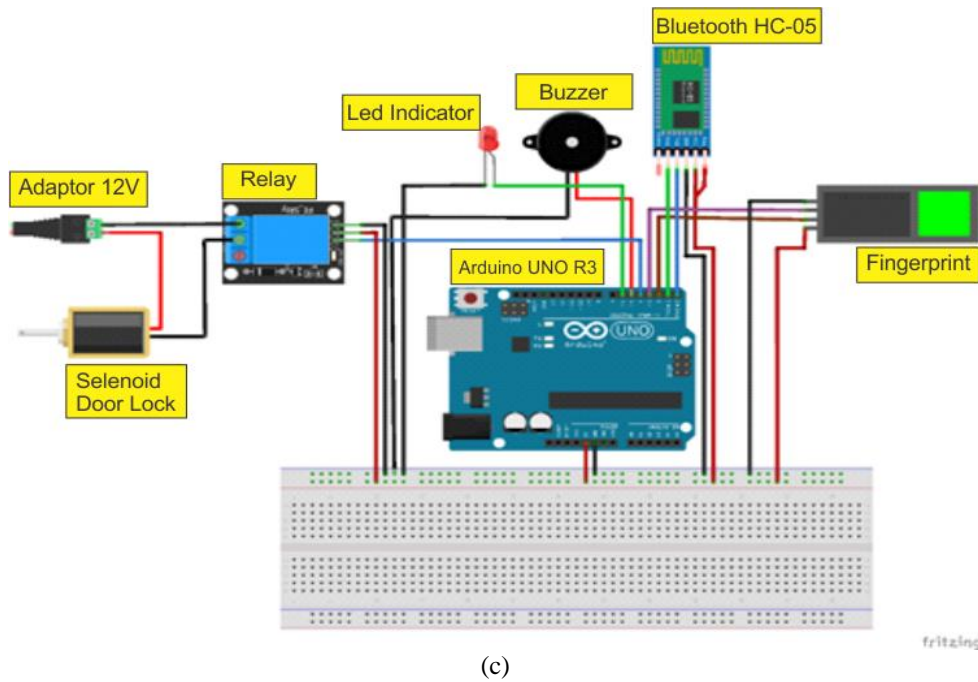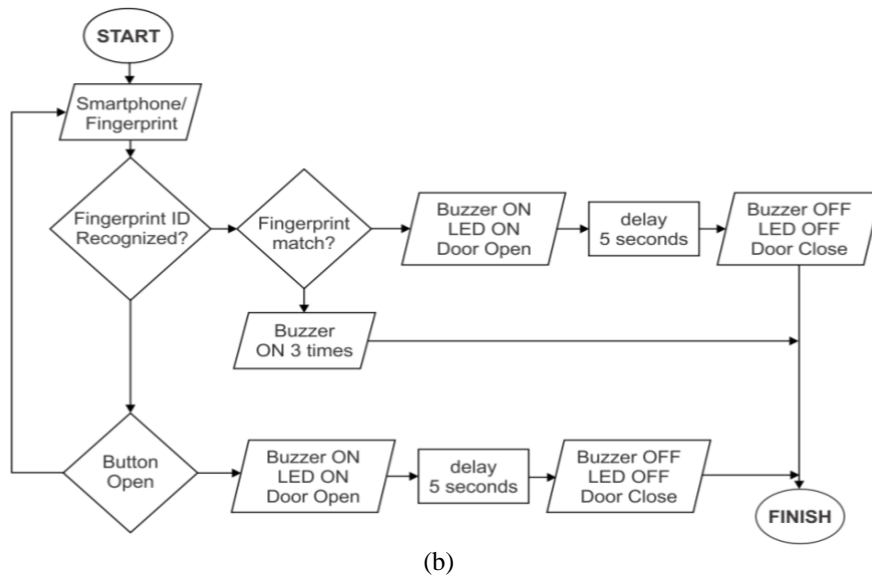Figure 1. The process of extracting features from the finger surface and storing them in a database.
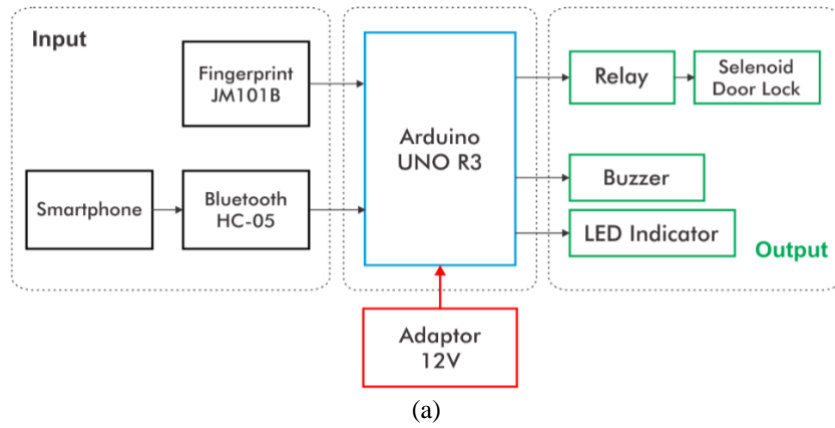
(a)

(b)

(c)

Figure 2. Hardware design: (a) Block diagram, (b) Flowchart, (c) Schematic circuit

3. RESULTS AND DISCUSSION

In this research, a smart door lock device has been successfully designed using fingerprint sensor technology and remote control with a smartphone. Figure 3 shows a photograph of the developed device prototype. In this research, tests were carried out on the device to determine its success in responding to and recognizing fingerprints registered on the system and testing the remote control using a smartphone application that had been designed using the HC-05 Bluetooth module [31]–[39] as the signal transmitter.

3.1. The test of fingerprint sensor

This test aims to find out whether the fingerprint sensor is connected and whether the fingerprint sensor is working according to its function. The first time the device is turned on, the fingerprint sensor has not yet saved the fingerprint ID, so when you attach the fingerprint, it will read on the serial monitor that it did not find a match. The fingerprint sensor can store fingerprints ranging from 1 to 127. The storage process begins by typing the numbers 1–127 to save the fingerprint. After that, the sensor will wait for the fingerprint that will be registered or that you want to save to be attached to the sensor. When the fingerprint has been obtained, the program will ask you to stick the same finger again for authentication purposes, and the fingerprint will be registered or stored in the number that was typed earlier.

3.2. Bluetooth testing

In this research, mobile applications are built using a website-based compiler developed by MIT. Application creation begins by entering or logging in to the website https://appinventor.mit.edu and clicking "Create Apps." This data delivery test uses an application that has been created using the MIT App Inventor platform [31], [39]. This test is carried out by opening the Bluetooth settings on the smartphone and connecting it to the HC-05 Bluetooth module [31]–[39].

Figure 4 shows the appearance of the application after the Bluetooth button is pressed, and after selecting Bluetooth, which was previously connected to the smartphone, the connectivity information indicator next to the open button becomes connected, indicating that the application and the Bluetooth module are connected. This shows that applications created using MIT App Inventor can send data. It can be seen that when the open button is pressed, the Blueetooth HC-05 will receive and open the door. The data sent by the application when the open button is pressed can be used as conditioning to activate the relay so that the door lock solenoid can open.

3.3. System testing

Placing a registered finger on the fingerprint sensor and timing how long it takes for the relay to activate in order to open the doorlock solenoid serve as the test's inputs. It can be seen that the response time required for the system to open the doorlock solenoid varies. This can be caused by the finger being attached incorrectly, so the finger must be placed in the right position so that the sensor can read the fingerprint correctly and the system can immediately open the doorlock solenoid.

The test results are carried out using a smartphone application created using the MIT App Inventor platform. Firstly, press the open button on the application after a Bluetooth connection with the connected device, then calculate the time needed for the system to respond and activate the relay so that it opens the door lock solenoid. Testing is also carried out by measuring the distance between the smartphone and the system in order to find out the ideal distance for this system to work. So, in testing the response time of smartphone applications with this system, it can be concluded that distance is one of the factors that influences the response time it takes for the system to receive data from the smartphone and respond, thereby opening the doorlock solenoid. The results of this test also show that at a distance of 15 meters, the system is no longer able to respond to or receive data sent by the application, so the system does not open the solenoid door lock.

The data in Table 1 shows the results of testing the entire system on the fingerprint sensor. It can be seen in the table that the fastest time required for the system to open the doorlock solenoid immediately after the registered finger is attached is 1.08 seconds, and the longest time is 1.28 seconds. So, in this test, the average time needed for the system to read fingerprints and open the doorlock solenoid was 1.20 seconds.

Based on Table 2, it can be seen that the fastest time in this test was at a distance of 2 meters with a time of 1.02 seconds, and the longest time for the system to respond to open the doorlock solenoid was at a distance of 14 meters with a time of 3.35 seconds. From the existing response time data, it was found that the average time required for the system to respond to data sent by the application on the smartphone was 1.54 seconds.
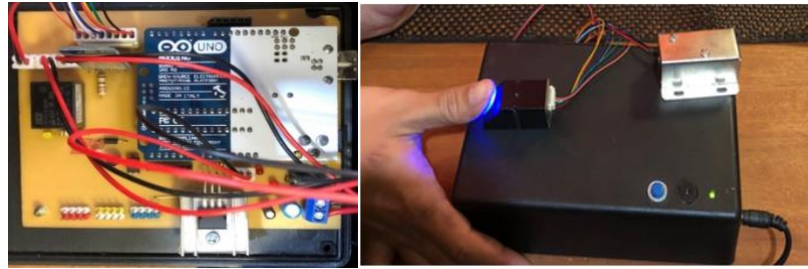
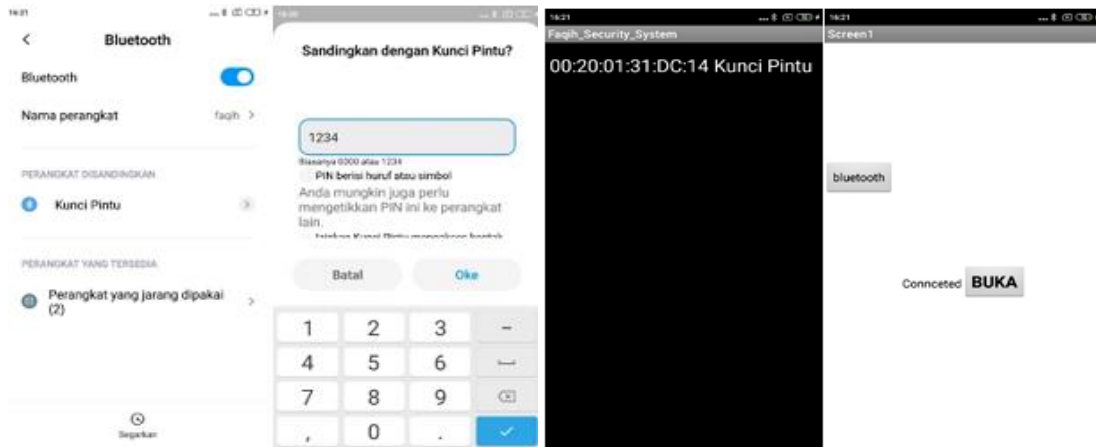Figure 3. Photograph of hardware and fingerprint sensor testing

Figure 4. Testing data transmission from smartphone to HC-05 module

Table 1. Testing data results of fingerprint sensor response time to door locks

Test No.	ID Fingerprint	Time Respons (s)	Selenoid Condition
1	1	1.1	Open
2	2	1.22	Open
3	3	1.23	Open
4	4	1.28	Open
5	5	1.19	Open
6	6	1.08	Open
7	7	1.21	Open
8	8	1.17	Open
9	9	1.27	Open
10	10	1.25	Open
Average		1.20	

Table 2. Results of Bluetooth application response time to door locks

Distance (m)	Respon Time (s)	Bluetooth HC-05	Selenoid Condition
1	1.08	ON	Open
2	1.02	ON	Open
3	1.3	ON	Open
4	1.33	ON	Open
5	1.56	ON	Open
6	1.37	ON	Open
7	1.86	ON	Open
8	1.2	ON	Open
9	1.12	ON	Open
10	1.39	ON	Open
11	1.56	ON	Open
12	2.02	ON	Open
13	1.52	ON	Open
14	3.35	ON	Open
15	-	OFF	Close
Average	1.54		

4.   CONCLUSION

Following the stages of design, system development, and trial implementation, a wireless door lock device utilizing fingerprint technology was successfully created. The device is powered by an Arduino and can be connected to a smartphone. This study has successfully designed and implemented an automatic door lock system that incorporates a fingerprint sensor as an input component. The system has undergone verification testing ten times, demonstrating the reliability of the fingerprint sensor. The door lock solenoid operates with a 100% accuracy rate. During a separate trial, the smartphone transmitted data to the HC-05 Bluetooth module, enabling the module to accurately retrieve the data from the smartphone within a maximum range of 14 meters. The average response time for this process was 1.54 seconds.

ACKNOWLEDGEMENTS

REFERENCES

[1] Pusiknas Bareskrim Polri, "Crime data (in *Indonesian: Data kejahatan*)," *Polri*. 2021, Accessed: Aug. 18, 2023. [Online]. Available: https://pusiknas.polri.go.id/data_kejahatan.
[2] M. A. Khan *et al.*, "Prototype model of an IoT-based digital and smart door locking system with enhanced security," 2022, doi: 10.1109/MACS56771.2022.10023385.
[3] S. Jeong, "Design on novel door lock using minimizing physical exposure and fingerprint recognition technology," *Int. J. Informatics Vis.*, 2022, doi: 10.30630/joiv.6.1.858.
[4] Y. Guo, C. Xiong, Y. Wang, S. Wu, L. Luo, and Q. Fu, "Design and fabrication of QN9080DK based Bluetooth 5.0 fingerprint lock controller," *J. Phys. Conf. Ser.*, vol. 2173, no. 1, p. 12066, Jan. 2022, doi: 10.1088/1742-6596/2173/1/012066.
[5] A. Siswanto, A. Efendi, and E. A. Kadir, "Biometric face authentication system for secure smart office environments," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 32, no. 2, pp. 1134–1141, 2023, doi: 10.11591/ijeecs.v32.i2.pp1134-1141.
[6] S. Yedulapuram, R. Arabelli, K. Mahender, and C. Sidhardha, "Automatic door lock system by face recognition," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 981, no. 3, 2020, doi: 10.1088/1757-899X/981/3/032036.
[7] S. Roy, M. Nasir Uddin, M. Jahidul Kabir, and M. Zahirul Haque, "Design and implementation of the smart door lock system with face recognition method using the Linux platform Raspberry Pi," *IJCSN-International J. Comput. Sci. Netw.*, vol. 7, no. 6, 2018.
[8] H. Alnabhi*, Y. Al-naamani, M. Al-madhehagi, and M. Alhamzi, "Enhanced security methods of door locking based fingerprint," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 3, pp. 1173–1178, Jan. 2020, doi: 10.35940/ijitee.B7855.019320.
[9] M. A. Kader, Y. Haider, R. Karim, S. Islam, and M. M. Uddin, "Design and implementation of a digital calling bell with door lock security system using fingerprint," *2016 Int. Conf. Innov. Sci. Eng. Technol. ICISET 2016*, pp. 5–9, 2017, doi: 10.1109/ICISET.2016.7856484.
[10] A. N. Mas Erwan, M. N. H. Muzaffar Alfian, and M. S. Mohamad Adenan, "Smart door lock," *Int. J. Recent Technol. Appl. Sci.*, vol. 3, no. 1, pp. 1–15, 2021, doi: 10.36079/lamintang.ijortas-0301.194.
[11] I. Ha, "Security and usability improvement on a digital door lock system based on internet of things," *Int. J. Secur. its Appl.*, vol. 9, no. 8, pp. 45–54, 2015, doi: 10.14257/ijsia.2015.9.8.05.
[12] Y. T. Park, P. Sthapit, and J. Y. Pyun, "Smart digital door lock for the home automation," *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, no. August, 2009, doi: 10.1109/TENCON.2009.5396038.
[13] T. Adiono, S. Fuada, S. F. Anindya, I. G. Purwanda, and M. Y. Fathany, "IoT-enabled door lock system," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 5, pp. 445–449, 2019, doi: 10.14569/ijacsa.2019.0100556.
[14] K. Gupta, N. Jiwani, M. H. U. Sharif, M. A. Mohammed, and N. Afreen, "Smart door locking system using IoT," *2022 Int. Conf. Adv. Comput. Commun. Mater. ICACCM 2022*, no. May, pp. 3090–3094, 2022, doi: 10.1109/ICACCM56405.2022.10009534.
[15] T. Malche and P. Maheshwary, "Internet of things (IoT) for building smart home system," *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, no. February, pp. 65–70, 2017, doi: 10.1109/I-SMAC.2017.8058258.
[16] N. N. Kumbhar, "Smart door locking system using wireless communication technology," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. V, no. VIII, pp. 507–512, 2017, doi: 10.22214/ijraset.2017.8070.
[17] N. Krishnamoorthy and N. S. Asif, "IoT based smart door locks," *Natl. Conf. Innov. Res. Trends Comput. Sci. Technol.*, vol. 4, no. 3, pp. 151–154, 2018.
[18] G. Sowmya, G. Divya Jyothi, N. Shirisha, K. Navya, and B. Padmaja, "Iot based smart door lock system," *Int. J. Eng. Technol.*, vol. 7, no. 3.6 Special Issue 6, pp. 223–225, 2018, doi: 10.22214/ijraset.2023.49470.
[19] M. D. Tobi and V. N. van Harling, "Study of PLTMH development planning in Sasnek village Sawiat district, South Sorong regency West Papua province," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2. pp. 678–687, 2020, doi: 10.11591/ijeecs.v18.i2.pp678-687.
[20] T. Alam, A. A. Salem, A. O. Alsharif, and A. M. Alhejaili, "Smart home automation towards the development of smart cities," *Comput. Sci. Inf. Technol.*, vol. 1, no. 1, pp. 17–25, 2020, doi: 10.11591/csit.v1i1.p17-25.
[21] T. S. Gunawan *et al.*, "Prototype design of smart home system using internet of things," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 7, no. 1, pp. 107–115, 2017, doi: 10.11591/ijeecs.v7.i1.pp107-115.
[22] T. S. Gunawan, I. R. H. Yaldi, M. Kartiwi, and H. Mansor, "Performance evaluation of smart home system using internet of things," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 1, pp. 400–411, 2018, doi: 10.11591/ijece.v8i1.pp400-411.
[23] M. K. Al-Gburi and L. A. Abdul-Rahaim, "Secure smart home automation and monitoring system using internet of things," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 28, no. 1, pp. 269–276, 2022, doi: 10.11591/ijeecs.v28.i1.pp269-276.
[24] N. A. Al-Shareefi, S. A. Abbas, M. S. Alkhazraji, and A. A. R. Sakran, "Towards secure smart cities: design and implementation of smart home digital communication system," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 1, pp. 271–277, 2021, doi: 10.11591/ijeecs.v21.i1.pp271-277.
[25] M. J. Mahammad, Y. Al Mashhadany, and A. M. Eyada, "Real time model of a lock gate system upon fingerprint with microcontroller," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 1, pp. 37 – 43, 2021, doi: 10.11591/ijeecs.v21.i1.pp37-43.

[26] A. Mishra and S. Dehuri, "Real-time online fingerprint image classification using adaptive hybrid techniques," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 5, p. 4372, Oct. 2019, doi: 10.11591/ijece.v9i5.pp4372-4381.

[27] S. R. and R. B., "Implementation of AES using biometric," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 5, p. 4266, Oct. 2019, doi: 10.11591/ijece.v9i5.pp4266-4276.

[28] A. A., S. T. E., and O. A., "Web based fingerprint roll call attendance management system," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 5, p. 4364, Oct. 2019, doi: 10.11591/ijece.v9i5.pp4364-4371.

[29] A. M. Ali and A. K. Farhan, "A novel multi-biometric technique for verification of secure e-document," *Int. J. Electr. Comput. Eng.*, vol. 14, no. 1, p. 662, Feb. 2024, doi: 10.11591/ijece.v14i1.pp662-671.

[30] A. Mishra and S. Dehuri, "Real-time online fingerprint image classification using adaptive hybrid techniques," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 5, pp. 4372–4381, 2019, doi: 10.11591/ijece.v9i5.

[31] W. B. A. Samad, M. A. Bin Othman, N. B. M. Safri, and M. A. B. A. Razak, "Portable cardiac self-stress test device development based on metabolic equivalent (MET)," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 15, no. 3, pp. 1223 – 1231, 2019, doi: 10.11591/ijeecs.v15.i3.pp1223-1231.

[32] Y. M. Hussain *et al.*, "Smartphone's off grid communication network by using Arduino microcontroller and microstrip antenna," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 19, no. 4, pp. 1100 – 1106, 2021, doi: 10.12928/TELKOMNIKA.v19i4.15949.

[33] H. R. Fajrin, B. S. Adi, H. Purwoko, and I. P. Sari, "Telemedicine-equipped android interface-based heart rate monitoring," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, pp. 1332 – 1340, 2021, doi: 10.11591/ijeecs.v21.i3.pp1332-1340.

[34] C. F. Soon, B. H. Teng, K. S. Tee, S. L. Jong, M. Morsin, and N. A. Rahman, "Bluetooth embedded digital ammeter with Android app data logging," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, no. 3, pp. 1400 – 1407, 2020, doi: 10.11591/ijeecs.v18.i3.pp1400-1407.

[35] J. K. Abed, "Smart monitoring system of DC to DC converter for photovoltaic application," *Int. J. Power Electron. Drive Syst.*, vol. 9, no. 2, pp. 722 – 729, 2018, doi: 10.11591/ijpeds.v9.i2.pp722-729.

[36] M. Murad, O. Bayat, and H. M. Marhoon, "Design and implementation of a smart home system with two levels of security based on IoT technology," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 1, pp. 546 – 557, 2021, doi: 10.11591/ijeecs.v21.i1.pp546-557.

[37] N. M. Hussien, Y. M. Mohialden, M. M. Akawee, and M. A. Mohammed, "The software requirements process for designing a microcontroller-based voice-controlled system," *Bull. Electr. Eng. Informatics*, vol. 12, no. 1, pp. 539 – 543, 2023, doi: 10.11591/eei.v12i1.4407.

[38] E. D. Widianto, G. N. Huda, and O. D. Nurhayati, "Portable spirometer using pressure-volume method with Bluetooth integration to Android smartphone," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 4, pp. 3977 – 3986, 2023, doi: 10.11591/ijece.v13i4.pp3977-3986.

[39] N. A. J. Salih, I. J. Hasan, and N. I. Abdulkhaleq, "Design and implementation of a smart monitoring system for water quality of fish farms," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 14, no. 1, pp. 44 – 50, 2019, doi: 10.11591/ijeecs.v14.i1.pp44-50.

BIOGRAPHIES OF AUTHORS

Tole Sutikno 🆔 Ⓖ SC Ⓒ is a professor in Electrical Engineering Department at the Universitas Ahmad Dahlan (UAD), Yogyakarta, Indonesia. He received his B.Eng., M.Eng. and Ph.D. degrees in Electrical Engineering from Universitas Diponegoro, Universitas Gadjah Mada and Universiti Teknologi Malaysia, in 1999, 2004 and 2016, respectively. He has been a Professor in UAD, Yogyakarta, Indonesia since 2023. He is among the top 2% of researchers named by Stanford University and Elsevier BV as the most influential scientists in the world for 2021–present. He is currently an Editor-in-Chief of the TELKOMNIKA and the Head of the Embedded Systems and Power Electronics Research Group (ESPERG). His research interests include the field of digital design, industrial applications, industrial electronics, industrial informatics, power electronics, motor drives, renewable energy, FPGA applications, embedded system, artificial intelligence, intelligent control, information technology and digital library. He can be contacted at email: tole@te.uad.ac.id.

Moh Ainur Faqih Ubaidillah 🆔 Ⓖ SC Ⓒ received his B.Eng. in Electrical Engineering from Universitas Ahmad Dahlan, Indonesia, in 2023. His research interests include robotics and Internet of Things. He can be contacted at email: moh1800022115@webmail.uad.ac.id.

Watra Arsadiando received B. Eng. in electrical engineering from Universitas Ahmad Dahlan, Indonesia, in 2017. He is a member of the Embedded Systems & Power Electronics Research Group (ESPERG). His current research interests include renewable energy, robotics, and digital control system. He can be contacted at email: watra24arsadiando@gmail.com or watra@journal.uad.ac.id.

Hendril Satrian Purnama received his B.Eng. degree in Electrical Engineering from Universitas Ahmad Dahlan, Yogyakarta, Indonesia in 2017. After receiving his degree, he became a member of the Embedded Systems and Power Electronics Research Group (ESPERG), and worked there as a researcher. In addition, he is also active as assistant editor in several international journals in the field of electrical engineering, computer and informatics. His research interests include power electronics, renewable energy technology, robotics and the Internet of Things. He can be contacted at email: lfriyan220@gmail.com.