Smart Home Control System Design using Internet of Things Based Energy Harvesting Technology

Lukman Medriavin Silalahi
Department of Electrical Engineering
Universitas Mercu Buana
Jakarta, Indonesia
lukman.medriavin@mercubuana.ac.id

Muhammad Rafi Indrawan
Department of Electrical Engineering
Universitas Mercu Buana
Jakarta, Indonesia
rafiindrawan.s3@gmail.com

Setiyo Budiyanto
Department of Electrical Engineering
Universitas Mercu Buana
Jakarta, Indonesia
sbudiyanto@mercubuana.ac.id

Dirman Hanafi
Instrumentation and Sensing Technology (INSeT) Research Group
Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia
Johor, Parit Raja, Malaysia
dirman@uthm.edu.my

Abdul Hamid
Industry Machining Tech Focus Group Faculty of Technical and Vocational Education
Universiti Tun Hussein Onn Malaysia
Johor, Parit Raja, Malaysia
abdulhamid@uthm.edu.my

Davit Ronaldo
Department of Electrical Engineering
Universitas Mercu Buana
Jakarta, Indonesia
davidronaldo2508@gmail.com

2024 IEEE 6th Symposium on Computers & Informatics (ISCI) | 979-8-3503-5385-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISCI62787.2024.10667797

Abstract*— The problem in this research discusses home security control systems and energy harvesting technology based on the internet of things. Harvesting energy is a technology in storing electrical energy temporarily, the process starts from capturing sunlight energy. The objective of this research is to provide security for homeowners by facilitating fingerprints and PIN (Personal Identification Numbers) in entering the house, then in the event of a power outage, it activates the function of energy harvesting technology. The method is to design and analyze a prototype that combines the Raspberry Pi and its supporting components. The contribution of this research is to reduce the risk of theft or the risk of house fires due to electricity and overcome problems if the house is in a power outage. The novelty of this research is that the energy harvesting technology built on the Raspberry Pi as the main control and its supporting devices runs well in charging backups from solar panels with a length of 2 hours depending on the intensity of the light received. Then the Blynk application has a real-time response in monitoring electrical appliances at home.

Keywords*— Doorlock, Fingerprint, Harvesting, Internet of Things, Raspberry Pi, Smarthome

I. INTRODUCTION

Smart Home [1]–[3] is a combined innovation of several automated systems, to provide a sense of security, comfort for users because it provides automatic monitoring and control facilities [4]–[7] among others, lights, windows, doors, temperature, etc. A smart home necessitates three components: an internal home network, intelligent control, and home automation accessible via wired or wireless gateways [8], [9].

IoT (Internet of Things) is a concept that allows connectivity and exchange of information data from devices and systems through the internet network. There are three functional requirements of comprehensive perception, namely, reliable transmission. intelligent processing, and IoT implementation processes [10].

Harvesting energy [11]–[13] is a method of development of PV (Photovoltaic) that carries out the harvesting process from external sources including solar sun, heat, and other electromagnetic waves that emit signals. PV effect is a phenomenon that occurs in a PV cell so that it can absorb light energy and convert it into electrical energy [14]–[16].

According to [17] revealed that the main concern for the problem of home security systems or office environments is the door lock security system that has loopholes to be hacked. As a result of raising security concerns, the design of a prototype fingerprint-based door lock system provides a way to run reliable system transaction logs and protect individual privacy rights.

Reference [18] underscores the necessity of security systems driven by automation. The study introduces a facial recognition method within the IoT realm, specifically for implementing automation in smart home devices. Consequently, the identified limitations and challenges serve as a robust basis for future investigations in the intersection of IoT, automation, and facial recognition [19].

Furthermore, reference [20], safety concerns within current home automation setups are discussed, advocating for the integration of logic-driven security algorithms [21], [22] to enhance home safety. These algorithms validate the authenticity of fire alarms by monitoring fluctuations in temperature, humidity, and carbon monoxide levels, while also offering protection against tampering. The experiment successfully deployed the suggested sensing algorithm.

As per references [23], [24], enhancing the user's lifestyle spans various domains like lighting, security, etc. Thus, the study introduces a smart home control mechanism utilizing a coordinator-based ZigBee network. The system's functionality entails smart interference control, managing interference stemming from coexisting IEEE 802.11x-based wireless local area networks and wireless sensor networks. Additionally, it includes a smart energy control system, integrating natural light with artificial sources and optimizing household appliance energy usage by regulating unnecessary energy consumption, alongside an intelligent management control system ensuring the efficiency of electronic equipment operation. The proposed smart home's performance was validated through computer simulations, demonstrating its immunity to interference and effectiveness in reducing energy consumption from household appliances employed in smart homes.

As per reference [25], discussions encompass smart city initiatives, smart living, and the burgeoning field of IoT. Within this context, the concept of "Smart Home" stands out, integrating automation and interactive technologies. The focus of this study lies in developing a "Smart Home Automation System," enabling users to employ voice commands for controlling household appliances and devices for various purposes. The system's goal is to adapt to users' voices and recognize commands, irrespective of individual speaker characteristics like accents. It aims to be cost-efficient, adaptable, and resilient. Consequently, the research proposes an evaluation of the performance of multifunctional miniature prototypes. Encouragingly, the experimental results indicate promise as the prototype can effectively convert an existing home into a smart one at a relatively low cost and with convenience.

From the literature review, this research objectives are:

1. Design a prototype that can monitor electronic devices in the house. As well as providing privacy security for owners to authenticate their fingerprints and PIN (Personal Identification Numbers).
2. Analysis precise python programming algorithms to measure and test the accuracy of fingerprint reading, PIN reading, and the IoT integrated electrical energy harvesting process.
3. Testing the function of energy harvesting technology during a power outage.

This is supported by the hypothesis that the use of electrical control security systems uses Blynk-based IoT as a remote control and can carry out the solar energy harvesting process. Therefore, this system was designed using Raspberry Pi as the main control with its supporting sensors. The design is expected to contribute to efforts to reduce the risk of theft or the risk of house fires, as well as overcome blackouts because this prototype will continue to operate using energy harvesting technology as a backup of electrical power.

II. METHOD

Figure 1 shows the block diagram system. This system design consists of Raspberry Pi, keypad, fingerprint, LCD, solenoid, reed switch, buzzer, lights, and solar panels. Starting from Raspberry as the main control, then requires a power source of 5V supplied by a series of power supplies and be through backups, namely from Harvesting.

Next, the user will be instructed to insert Fingerprint and Enter PIN to be able to open the door. The door will be able to be opened if the fingerprint and PIN entered match in the system. If there is an error, the user is still tolerated three times, if the error still repeats then an alarm will sound accompanied by an error indicator that will be displayed. As double security, the security code can be changed by the user himself. A keypad is used as a security PIN input where the number of passwords itself is 4 digits to be used as a password. This safety system uses a magnetic principle that is used as a door lock. The process of opening and closing the lock uses a solenoid, in the "ON" position the solenoid gets a voltage flow of 12V by the power supply. The process of opening and closing the solenoid is controlled using a relay. The process of using the prototype will be displayed information via LCD 20×4. So, this design can control some electrical appliances at home, for example, there are lights 1 to 4 that can be controlled through an application to anticipate an electrical short circuit if you forget to turn off electricity for a long time when not at home.

Figure 2 shows a flowchart of the proposed control system. there will be 3 modes, including: door lock system, electrical equipment, and energy harvesting.

1) 1st Mode: Door lock system

Figure 2(a) describes the process when the LCD displays "Please Insert Your Fingerprint" then insert your fingerprint that has been entered into the program to be able to access then compare fingerprints against the compatibility in the program. If the fingerprints do not match, then the LCD displays "Your Fingerprint is Incorrect" then paste your fingerprint back. If during 3-times attempts the identification is wrong, the LCD will display "Your Fingerprint is Wrong" then the Buzzer alarm is active. If your Fingerprint matches then to the next stage is please "Enter your PIN", then compare the compatibility of the PIN with the program that has been saved. If the PIN does not match, the LCD will display "Your PIN is Incorrect" then re-enter your PIN. If during 3-times attempts the PIN is wrong, the LCD will display your PIN Wrong 3-times and the active Buzzer sounds. If the fingerprint and PIN are correct, then to the next stage, the LCD will display "Open Door", then the Solenoid will open, the door will open.

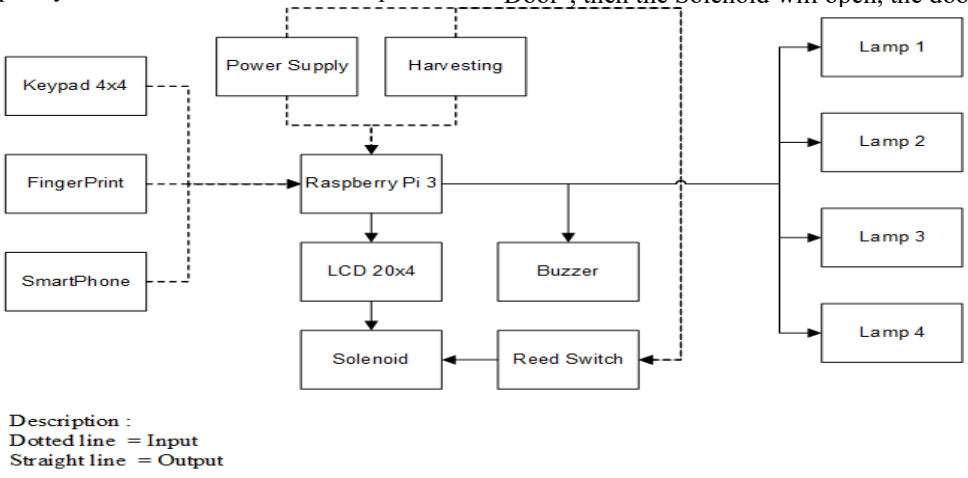

Fig. 1. Block diagram system

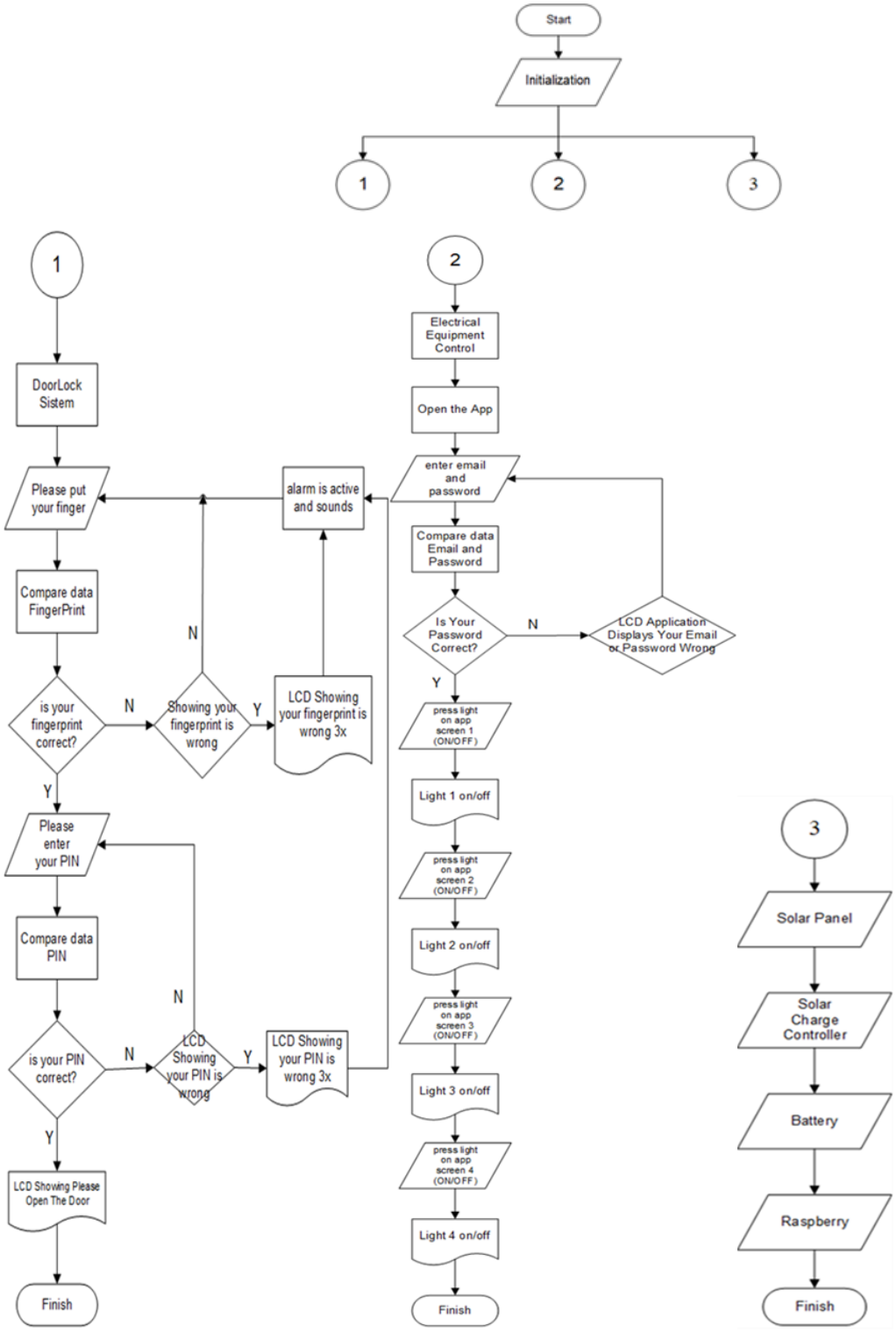

Fig. 2. Flowchart (a) Door lock system (b) Electrical system (c) Harvesting energy system

2) 2nd Mode: Electrical equipment control

Figure 2(b) explains the process of "Open Application". Input Email and Password that has been registered, then compare the email and password that has been created. If wrong, then LCD will display your wrong input data. If the data entered are correct, it will appear to the next display Bulbs 1 (ON/OFF), Bulbs 2 (ON/OFF), Bulbs 3 (ON/OFF), Bulbs 4 (ON/OFF). If bulbs 1-4 are pressed ON in the application, Lights 1-4 will light up, if lights 1-4 are pressed OFF in the application, Lights 1-4 will turn off.

3) 3rd Mode: Energy harvesting control

Figure 2(c) describes the process of connecting solar panels to solar charge controllers, then from the solar charge controller connected to the battery as a storage place for energy from solar panels. Then the battery is connected to the designed prototype.

III. RESULT AND DISCUSSION

After designing, then testing the entire series of prototypes. The stages of operation consist of:

1. Connect the power supply cable to the outlet, then the prototype will turn on. "Insert Fingerprint" and "Enter PIN" on the keypad correctly then after that the door opens.
2. If the "Fingerprint" and "PIN" are entered incorrectly 3 times, the buzzer will be ON.
3. IoT control is used in magicom, dispenser, washing machine, air conditioner, air conditioner, water machine using 4 lights as indicators by accessing the Blynk application.

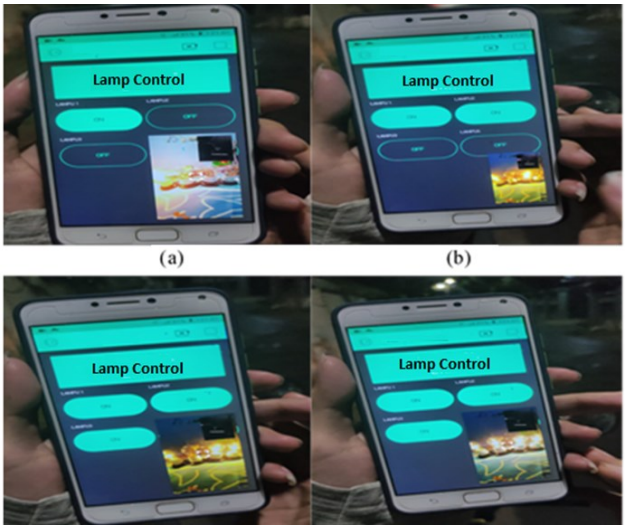

Fig. 3. (a) lights 1 On ; (b) lights 1-2 On ; (c) lights 1-3 On ; (d) lights 1-4 On

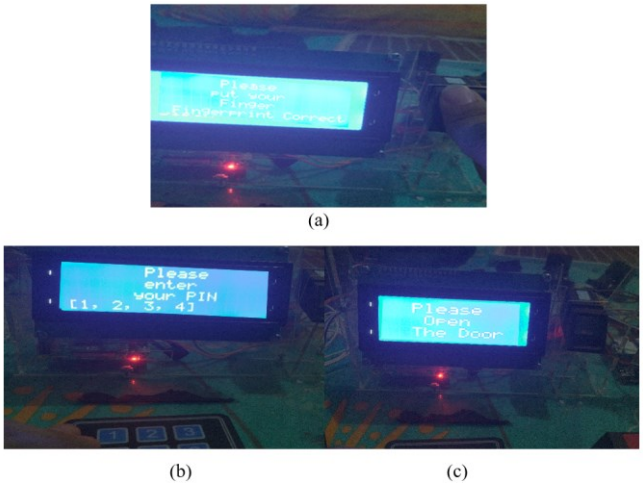

Fig. 4. (a) scan finger ; (b) input pin ; (c) information success

A. *Function testing*

Figure 4. shows the results of function testing on the Blynk application used by owners in monitoring or managing electronic equipment in the house. Table 1 shows an experiment to control home electrical appliances connected to the Blynk app using lights as indicators.

Table 1. Results of experimental control of electrical appliances

Electrical equipment experiments	Result
Bulb 1	Success
Bulb 2	Success
Bulb 3	Success
Bulb 4	Success

B. *Access testing using fingerprint and PIN*

Testing a pre-programmed fingerprint and entering a PIN as an owner. If the fingerprint has been pasted and entered the correct PIN. Table 2 shows the results of the PIN test. Table 3 shows the results of fingerprint testing. Table 4 shows the results of fingerprint testing with any condition. It can be analyzed that the user can access the door only with fingerprint conditions under normal circumstances, if the fingerprint is other than in normal circumstances, then the condition remains closed.

Table 2. PIN testing

PIN attempt	Result
1234	Success
123	Unsuccess
123*	Unsuccess
123#	Unsuccess
12345	Unsuccess

Table 3. Fingerprint test

Fingerprint test	Result
Thumb	Success
Fore finger	Success
Middle finger	Unsuccess
Ring finger	Unsuccess
Little finger	Unsuccess

Table 4. Fingerprint interference testing

Fingerprint interference testing	Result
Fingers with gloves	Undetected
Wet fingers	Unsuccess
Finger with plastic	Undetected
Finger with plaster	Unsuccess
Normal fingers	Success

C. *Charging testing using harvesting energy technology*

Energy harvesting technology that takes sunlight as backup power during power outages. Testing charging from solar panels to batteries with several parameters including:

1. The hour range of 06.00-10.00 is shown in figure 6.
2. The hour range of 10.00-14.00 is shown in figure 7.
3. The hour range of 14.00-18.00 is shown in figure 8.

It can be analyzed based on energy harvesting technology testing that the most ideal test is at 10.00-14.00 because at that time the maximum yield of sunlight is obtained as shown in table 5.

Table 5. Charging experiments

Time	Duration (Minutes)	Voltage (Volt)	Percentage (%)
06.00-10.00	240	11.9	89
10.00-14.00	197	12.5	100
14.00-18.00	171	11.9	89

Fig. 5. Battery charging at 06.00-10.00

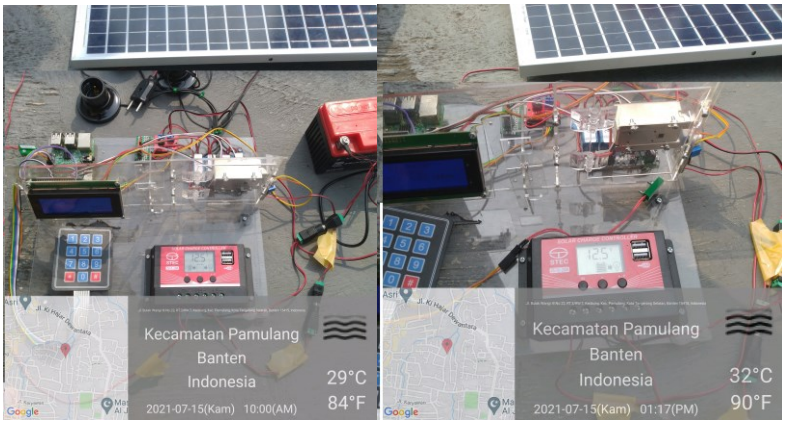

Fig. 6. Battery charging at 10.00-14.00

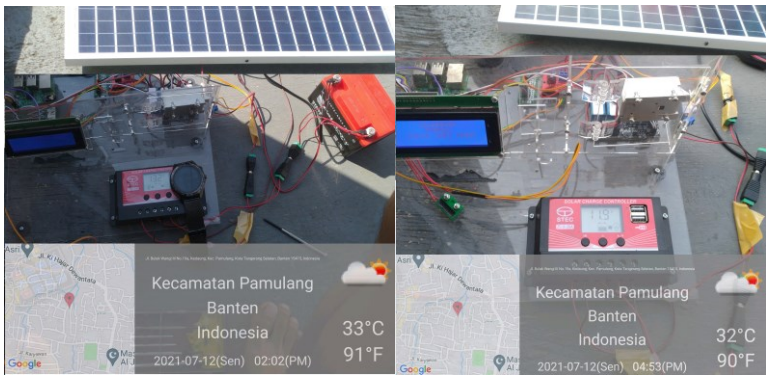

Fig. 7. Battery charging at 14.00-18.00

IV. CONCLUSIONS

The conclusions obtained are based on the results of documentation, testing and analysis of the entire system, namely on prototypes that have been designed to run according to the expected procedures correctly. Fingerprint will be active when the thumb or index finger is attached to the fingerprint sensor, fingerprints that can be used are fingerprints that have been stored in the program. The working process of the solenoid is that when the fingerprint and PIN entered correctly will give a voltage of "0" to the relay which later the relay will provide voltage to the solenoid. The Keypad module works as expected by pressing the 4 digit number correctly then the door will open. Harvesting energy has succeeded in becoming a temporary solution when there is a power outage with a charging period of 2 hours, this is adjusted to solar conditions. The Blynk application has succeeded in being a solution when homeowners want to monitor the condition of electrical appliances at home in conditions far from home or conditions not inside the house.

ACKNOWLEDGMENT

Thanks to Universiti Tun Hussein Onn Malaysia which has supported in foreign collaborative research and the second to Badan Riset dan Inovasi Nasional for their assistance. Hopefully there will be the novelty of joint research in further research.

REFERENCES

[1] S. Budiyanto *et al.*, "Design of control and monitoring tools for electricity use loads, and home security systems with internet of things system based on Arduino Mega 2560," *{IOP} Conf. Ser. Mater. Sci. Eng.*, vol. 909, no. 1, p. 12020, Dec. 2020, doi: 10.1088/1757-899x/909/1/012020.

[2] A. Bauchiero, G. Perboli, and M. Rosano, "Smart Home applied to historic buildings A real case study," in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, Jul. 2021, pp. 1273–1278. doi: 10.1109/COMPSAC51774.2021.00177.

[3] S. Budiyanto, L. Medriavin Silalahi, F. Artadima Silaban, U. Darusalam, S. Andryana, and I. M. Fajar Rahayu, "Optimization Of Sugeno Fuzzy Logic Based On Wireless Sensor Network In Forest Fire Monitoring System," in *2020 2nd International Conference on Industrial Electrical and Electronics (ICIEE)*, Oct. 2020, pp. 126–134. doi: 10.1109/ICIEE49813.2020.9277365.

[4] A. S. Ahmed, H. A. Marzog, and L. A. Abdul-Rahaim, "Design and implement of robotic arm and control of moving via IoT with Arduino ESP32," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 5, pp. 3924–3933, 2021, doi: 10.11591/ijece.v11i5.pp3924-3933.

[5] A. Yudidharma, N. Nathaniel, T. N. Gimli, S. Achmad, and A. Kurniawan, "A systematic literature review: Messaging protocols and electronic platforms used in the internet of things for the purpose of building smart homes," *Procedia Comput. Sci.*, vol. 216, pp. 194–203, 2023, doi: https://doi.org/10.1016/j.procs.2022.12.127.

[6] J. P. Juaneza, "The development of a disruption responsive smart room technology with attendance management system," *Int. Res. J. Sci. Technol. Educ. Manag.*, vol. 3, no. 1, May 2023, doi: 10.5281/zenodo.7777235.

[7] W. I. H. W. Izudi, S. B. Kutty, M. Kassim, and S. Saaidin, "Energy Saving of Electrical Appliances Through Mobile Application," in *2022 IEEE Symposium on Industrial Electronics & Applications (ISIEA)*, Jul. 2022, pp. 1–5. doi: 10.1109/ISIEA54517.2022.9873690.

[8] S. Budiyanto *et al.*, "The automatic and manual railroad door systems based on IoT," *Indones. J. Electr. Eng. Comput. Sci*, vol. 21, p. 1847, 2021.

[9] S. Budiyanto, F. A. Silaban, L. M. Silalahi, S. Kurniawan, and S. Andryana, "Design and monitoring body temperature and heart rate in humans based on WSN using star topology," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 22, no. 1, pp. 326–334, 2021.

[10] A. Yang, C. Zhang, Y. Chen, Y. Zhuansun, and H. Liu, "Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2521–2530, Apr. 2020, doi: 10.1109/JIOT.2019.2946214.

[11] Aznida Abu Bakar Sajak, Mohd Nabil Iqbal Ahmad, and Hassan Dao, "Green IoT Based on Tropical Weather: The Impact of Energy Harvesting in Wireless Sensor Network," *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 40, no. 1 SE-Articles, pp. 35–44, Feb. 2024, doi: 10.37934/araset.40.1.3544.

[12] M. E. Yuksel and H. Fidan, "Energy-aware system design for batteryless LPWAN devices in IoT applications," *Ad Hoc Networks*, vol. 122, p. 102625, 2021, doi: https://doi.org/10.1016/j.adhoc.2021.102625.

[13] C. A. M. Bernal *et al.*, "Localized Solar-Powered Resilient Communication System Using Wi-Fi Routers and Access Points with Integrated Smartphone Application through Raspberry Pi Chat Server," in *2019 IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)*, Nov. 2019, pp. 1–6. doi: 10.1109/HNICEM48295.2019.9073544.

[14] A. Z. Yonis, H. A. Dweig, and A. K. Tareed, "Comprehensive analysis of IEEE 802.11ah for Wireless Communication Networks," in *2021 IEEE Integrated STEM Education Conference (ISEC)*, Mar. 2021, pp. 28–31. doi: 10.1109/ISEC52395.2021.9763924.

[15] A. Z. Yonis, "Influence of low power consumption on IEEE 802.15.4 in wireless networks performance," *Bull. Electr. Eng. Informatics*, vol. 9, no. 1, pp. 205–211, 2020, doi: https://doi.org/10.11591/eei.v9i1.1678.

[16] A. Z. Yonis, "Performance analysis of IEEE 802.11 ac based WLAN in wireless communication systems," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 2, pp. 1131–1136, 2019, doi: 10.11591/ijece.v9i2.pp1131-1136.

[17] S. Budiyanto, L. M. Silalahi, I. U. Vistalina Simanjuntak, F. A. Silaban, G. Osman, and A. D. Rochendi, "Smart Door Lock Prototype Design at Internet of Things-Based Airport," in *2022 5th International Conference of Computer and Informatics Engineering (IC2IE)*, 2022, pp. 331–334. doi: 10.1109/IC2IE56416.2022.9970074.

[18] S. Fatima, N. A. Aslam, I. Tariq, and N. Ali, "Home Security and Automation Based on Internet of Things: A Comprehensive Review," *{IOP} Conf. Ser. Mater. Sci. Eng.*, vol. 899, no. 1, p. 12011, Jul. 2020, doi: 10.1088/1757-899x/899/1/012011.

[19] L. Medriavin Silalahi, I. Uli Vistalina Simanjuntak, F. Artadima Silaban, S. Budiyanto, Heryanto, and M. Ikhsan, "Integration of opencv raspberry pi 3b+ and camera sensor in access control of vehicle ignition key system," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 909, no. 1, p. 12002, 2020, doi: 10.1088/1757-899x/909/1/012002.

[20] P. Khanpara, K. Lavingia, R. Trivedi, S. Tanwar, A. Verma, and R. Sharma, "A context-aware internet of things-driven security scheme for smart homes," *Secur. Priv.*, vol. 6, no. 1, p. e269, 2023, doi: https://doi.org/10.1002/spy2.269.

[21] L. M. Silalahi, D. Jatikusumo, S. Budiyanto, F. A. Silaban, I. U. V. Simanjuntak, and A. D. Rochendi, "Internet of things implementation and analysis of fuzzy Tsukamoto in prototype irrigation of rice," *Int. J. Electr. Comput. Eng.*, vol. 12, no. 6, p. 6022, 2022.

[22] S. Budiyanto, L. M. Silalahi, D. Gunawan, and E. Y. T. Adesta, "An enhancement to the FLC-based baby incubator system using genetic algorithm," *J. INFOTEL*, vol. 15, no. 3, pp. 288–302, 2023, doi: https://doi.org/10.20895/infotel.v15i3.991.

[23] C. K. Rao, S. K. Sahoo, and F. F. Yanine, "A literature review on an IoT-based intelligent smart energy management systems for PV power generation," *Hybrid Adv.*, vol. 5, p. 100136, 2024, doi: https://doi.org/10.1016/j.hybadv.2023.100136.

[24] 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)*, Apr. 2023, pp. 1–4. doi: 10.1109/I2CT57861.2023.10126415.

[25] M. Albany, E. Alsahafi, I. Alruwili, and S. Elkhediri, "A review: Secure Internet of thing System for Smart Houses," *Procedia Comput. Sci.*, vol. 201, pp. 437–444, 2022, doi: https://doi.org/10.1016/j.procs.2022.03.057.