JPPIPA 10(2) (2024)

Jurnal Penelitian Pendidikan IPA

Journal of Research in Science Education

http://jppipa.unram.ac.id/index.php/jppipa/index

IoT-based Facelook and Fingerprint Safe Security System

Josya Marvin Immanuel[1*], Ibrahim[1], Reni Rahmadewi[1], Yuliarman Saragih[1]

[1] Electrical Engineering Department, Engineering Faculty, Universitas Singaperbangsa Karawang, Karawang, Indonesia

Received: November 7, 2023
Revised: January 4, 2024
Accepted: February 25, 2024
Published: February 29, 2024

Corresponding Author:
Josya Marvin Immanuel
josyamarvin05@gmail.com

DOI: 10.29303/jppipa.v10i2.6832

Abstract: This research aims to develop an advanced safe security system by combining Facelook and Fingerprint technologies based on the Internet of Things (IoT). These technologies are expected to provide a higher level of security and facilitate access for safe owners. Subsequently, testing is carried out on the safe's opening mechanism after successful authentication via both the fingerprint sensor and the face recognition system. These trials encompass the evaluation of success rates, the speed of the opening mechanism, and the overall response time. Data from the testing phase is collected and analyzed to comprehensively assess the system's performance. The average notification delivery delay for the face recognition system was measured at 2.67 seconds with a standard deviation of 0.37. The notification delivery data revealed an average delay of 2.04 seconds with a standard deviation of 0.38 These findings collectively affirm the effectiveness of the integrated face recognition and fingerprint system in the proposed safe security setup

Keywords: Facelook; Fingerprint; Internet of Things

Introduction

Security is crucial in ensuring a system's continuity and integrity. In the realm of physical security, safes have long been a common solution to protect various valuable items, documents, and other assets (Javaid et al., 2023; Tariq et al., 2023). Safes are considered practical storage places, but they come with a high risk as they can be easily breached without the owner's knowledge. Therefore, an advanced security system is required in line with technological advancements (Shukla et al., 2022). However, with technological advancements, traditional safe security needs to be enhanced to meet modern security challenges (Kumar et al., 2019).

Previous research discussed safe security with password and fingerprint codes based on the AVR ATmega16 microcontroller (Wijaya et al., 2020). This study aims to construct a safe security system utilizing two types of protection, namely password and fingerprint codes. The ATmega16 serves as the central controller and data processor. The keypad functions as the input medium for passwords, the LCD serves as the display medium for information, transistors act as switching components, the solenoid serves as the safe door opener, and a 12V power supply comprises all the supporting components of the system circuit.

Facelook technology utilizes facial recognition as one form of authentication, while Fingerprint technology utilizes unique fingerprint identification. Both will be integrated with IoT systems to enable remote access and monitoring of safes via the internet. Consequently, safe owners can control and monitor the security of their safes remotely, enhancing convenience and efficiency in managing valuable assets. Through the combination of these technologies, it is anticipated that the proposed safe security system can offer better protection against hacking or theft attempts (Kaur et al., 2023; Li & Liu, 2021). Additionally, integration with IoT allows the system to continuously evolve and update automatically, keeping pace with the latest developments in information security.

ESP8266 is an Internet of Things (IoT) platform equipped with a 4MB flash, featuring 11 GPIO pins, where 10 of them can be utilized for Pulse Width Modulation (PWM), 1 ADC pin, 2 sets of UART, 2.4GHz WiFi. It supports WPA/WPA2 security (Revadiaz et al., 2022). NodeMCU can be programmed using the LUA

How to Cite:
Immanuel, J. M., Ibrahim, Rahmadewi, R., & Saragih, Y. (2024). IoT-based Facelook and Fingerprint Safe Security System. *Jurnal Penelitian Pendidikan IPA*, *10*(2), 500–505. https://doi.org/10.29303/jppipa.v10i2.6832

language or the C language through the Arduino IDE (Setyawan et al., 2022).

ESP32 CAM is a platform capable of real-time monitoring by incorporating a camera and a built-in wifi module (Hercog et al., 2023). Setting up the ESP32-Cam requires the use of FTDI USB to TTL, which will then be connected to the camera module and a personal computer or laptop.

The sensor employed for fingerprint detection utilizes an optical system, where detection is performed by reading the contours (variations in surface height) of fingerprints and the static electricity of the body (Tang et al., 2018). The output signal of this sensor is in the form of a TTL serial from pin 3 connected to Arduino. This fingerprint scanner module is equipped with a red LED on the lens, which will light up as an indicator when image capture is taking place (Yeh et al., 2023).

Method

The research methodology begins with a comprehensive literature review to gather information related to safe security, facial recognition technology (Facelook), fingerprint sensors, and the Internet of Things (IoT). Subsequently, the design of the safe security system, incorporating both technologies based on the literature, is developed, outlining the necessary hardware and software specifications. Once the system design is established, the next step involves the development of a prototype by the outlined plan. The flowchart of the system can be seen in Figure 1. The product is designed as seen in Figure 2.

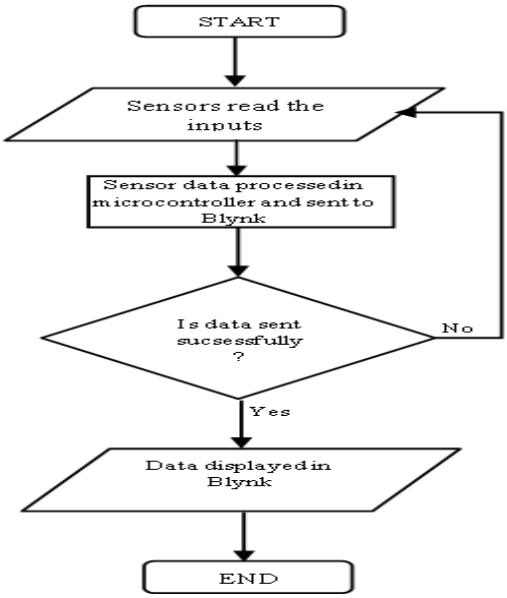

Figure 1. Flowchart System

In the testing phase, the initial focus is on the fingerprint sensor, where experiments are conducted to measure the success rate of fingerprint identification while analyzing the accuracy and speed of the sensor (Sarfraz, 2021). Following this, the face recognition system on the ESP32CAM module undergoes testing to evaluate its effectiveness in recognizing the owner's face, measuring the success rate of identification. Tests are conducted separately for each technology.

Subsequently, testing is carried out on the safe's opening mechanism after successful authentication via both the fingerprint sensor and the face recognition system. These trials encompass the evaluation of success rates, the speed of the opening mechanism, and the overall response time. Data from the testing phase is collected and analyzed to comprehensively assess the system's performance (Aldoseri et al., 2023; Setyawan et al., 2022).

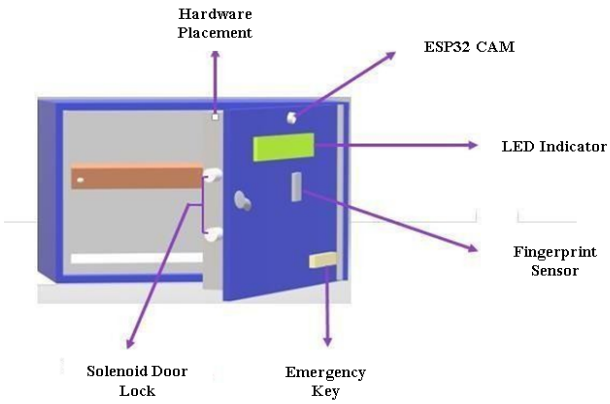

Figure 2. Product Design

The results of the data analysis are used to compare against established security standards (Chauhan & Shiaeles, 2023). The findings from the research are then validated to conclude whether the proposed safe security system can meet the desired security objectives. The research conclusion is presented along with recommendations for further development of the system.

Result and Discussion

Technological advances and ease of communication in this era cannot be separated from the role of the Internet of Things (IoT) (Atzori et al., 2017; Rejeb et al., 2022; Ullah et al., 2023). A concept that connects the digital world with human activities greatly facilitates human activities (Haleem et al., 2022; Hassani et al., 2021). The communication tools and technology that you use today are a combination of several systems connected to IoT (Bansal & Kumar, 2020; Fortino et al., 2020; Shafique et al., 2020). Internet of Things is a concept that is connected to devices as an internet-based communication medium (Radouan, 2021). With IoT, users can connect and communicate with each other to

carry out certain activities, search, process and send information automatically. When talking about IoT, this concept is almost similar to M2M (Machine-to-Machine) (Salama et al., 2023; Sudarmani et al., 2022). However, these two concepts actually have differences in terms of scale and scope of use.

M2M here refers to technology that allows communication between machines without involving human intervention (Leminen et al., 2020; Lokhande & Patil, 2021; Pradhan & Tun, 2022). In other words, M2M focuses more on the machine's working system to run a program (Amodu & Othman, 2018; Chakravarthi, 2021; Dwivedi, 2021). The easiest example to see is the operation of machines in a factory. In factories, machines run automatically and only communicate between machines (Nardo et al., 2020; Soori et al., 2023). So, they can manage the production process themselves without the need for human intervention. Basically, IoT operates by connecting various types of devices such as software or hardware to the internet network. There are 3 main components that play an important role in the IoT work process, namely sensors, gateways and cloud (Alahi et al., 2023). The sensors used in this concept can be movement sensors, light sensors, and other types of sensors (Aroganam et al., 2019; Siddique & Ogami, 2022).

The purpose of using this component is to collect data from physical objects connected to the internet network. After the sensor successfully collects the data, the gateway component functions to transmit the data to the connected cloud or internet. The gateway here can also process and perform automatic actions on existing data, such as turning off or turning on connected devices. Here, AI can help IoT to optimize device functions. Finally, the transmitted data is then sent to the cloud server. This cloud, which is connected to the internet, will also provide the services and applications needed to manage IoT. That way, users can directly give commands to a device to do something by accessing data from the cloud.

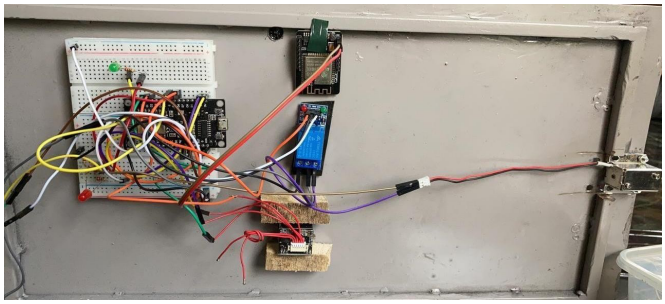

Figure 3. Sistem Wiring Implementation

The device that has been made has 2 main components, namely ESP8266 and ESP32-Cam (Babiuch & Postulka, 2021; Wicaksono & Rahmatya, 2020) ESP8266 functions as a communication component between the FPM10A sensor and the blynk application (Yulianto et al., 2022). ESP32-Cam functions as a communication component for capturing face images with the blynk application.

The performance of the face recognition using facelook and monitoring system on Blynk runs well with the test data that can be seen in Table 1.

Table 1. Facelook and Blynk Test

Sample	Notification Delay	Facelook Status	Notification Status
1	2.20	Success	Success
2	2.19	Success	Success
3	2.35	Success	Success
4	2.41	Success	Success
5	2.70	Success	Success
6	2.77	Success	Success
7	2.98	Success	Success
8	2.80	Success	Success
9	3.11	Success	Success
10	3.23	Success	Success

Based on the test results, it is found that the face recognition system runs well where from 10 samples obtained in the test it is found that all samples successfully recognize the registered face and successfully send notifications to the Blynk application. From the results in Table 1, it is found that the average value of the notification delivery delay is 2, 67 seconds with a deviation value represented by a standard deviation of 0.373. The performance of the Fingerprint sensor and monitoring system on Blynk runs well logically with the test data that can be seen in Table 2.

Table 2. Fingerprint and Blynk Test

Finger Name	Average Notification Delay	Fingerprint Status	Register Status
Right Thumb	2.73	Success	Registered
Right Index	1.78	Success	Registered
Right Middle	2.45	Success	Registered
Right Ring	1.97	Success	Registered
Right Little	2.21	Success	Registered
Left Thumb	-	Not Success	Not Registered
Left Index	-	Not Success	Not Registered

The test results in Table 2 show that the working logic of the fingerprint system is very good by only reading the results of fingerprints that have been registered. From the results of the notification delivery data, it is found that the average value of the notification delivery delay is 2, 04 seconds with a deviation value represented by a standard deviation of 0.377.

Conclusion

In conclusion, the research outcomes indicate a successful implementation of the face recognition system, as evidenced by its reliable performance in recognizing registered faces across all 10 test samples. Moreover, the system consistently achieved successful notifications sent to the Blynk application. The average notification delivery delay for the face recognition system was measured at 2.67 seconds with a standard deviation of 0.37 indicating a relatively consistent and prompt response. Similarly, the fingerprint system demonstrated robust functionality by accurately reading only registered fingerprints, showcasing its effective working logic. The notification delivery data revealed an average delay of 2.04 seconds with a standard deviation of 0.37 reinforcing the system's efficiency in providing timely notifications. These findings collectively affirm the effectiveness of the integrated face recognition and fingerprint system in the proposed safe security setup. The negligible delays observed in both systems contribute to a seamless user experience, highlighting the system's potential for real-world applications. However, further research and refinement may be necessary to address any potential challenges and enhance the system's overall performance.

Acknowledgments
Thank you to all parties involved in this research, I hope this research can be useful for the environment and further research.

Author Contributions
Conceptualization, J., I., R. R., Y. S.; methodology, J.; validation, I. and.; R. R. formal analysis, Y. S.; investigation, J and I.; resources, R. R. and. Y. S; data curation, J.: writing—original draft preparation, I. and R. R.; writing—review and editing, Y. S..: visualization, J. and I. All authors have read and agreed to the published version of the manuscript.

Funding
This research was independently funded by researchers.

Conflicts of Interest
The authors declare no conflict of interest.

References

Alahi, M. E. E., Sukkuea, A., Tina, F. W., Nag, A., Kurdthongmee, W., Suwannarat, K., & Mukhopadhyay, S. C. (2023). Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends. *Sensors*, *23*(11), 5206. https://doi.org/10.3390/s23115206

Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges. *Applied Sciences*, *13*(12), 7082. https://doi.org/10.3390/app13127082

Amodu, O. A., & Othman, M. (2018). Machine-to-Machine Communication: An Overview of Opportunities. *Computer Networks*, *145*, 255–276. https://doi.org/10.1016/j.comnet.2018.09.001

Aroganam, G., Manivannan, N., & Harrison, D. (2019). Review on Wearable Technology Sensors Used in Consumer Sport Applications. *Sensors*, *19*(9). https://doi.org/10.3390/s19091983

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, *56*, 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004

Babiuch, M., & Postulka, J. (2021). Smart Home Monitoring System Using ESP32 Microcontrollers. In F. P. G. Márquez (Ed.), *Internet of Things. IntechOpen*. https://doi.org/10.5772/intechopen.94589

Bansal, S., & Kumar, D. (2020). IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *International Journal of Wireless Information Networks*, *27*, 340–364. https://doi.org/10.1007/s10776-020-00483-7

Chakravarthi, V. S. (2021). *Internet of Things and M2M communication technologies*. Springer. https://doi.org/10.1007/978-3-030-79272-5

Chauhan, M., & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network*, *3*(3), 422–450. https://doi.org/10.3390/network3030018

Dwivedi, J. N. (2021). Internet of Things (IoT) and Machine to Machine (M2M) Communication Techniques for Cyber Crime Prediction. *Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications*, 31–55. https://doi.org/10.1002/9781119711629.ch2

Fortino, G., Savaglio, C., Spezzano, G., & Zhou, M. (2020). Internet of things as system of systems: A review of methodologies, frameworks, platforms, and tools. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *51*(1), 223–236. https://doi.org/10.1109/TSMC.2020.3042898

Haleem, A., Javaid, M., Qadri, M. A., & Suman, R. (2022). Understanding the role of digital technologies in education: A review. *Sustainable Operations and Computers*, *3*, 275–285. https://doi.org/10.1016/j.susoc.2022.05.004

Hassani, H., Huang, X., & Silva, E. (2021). The Human Digitalisation Journey: Technology First at the Expense of Humans? *Information*, *12*(7), 267. https://doi.org/10.3390/info12070267

Hercog, D., Lerher, T., Truntič, M., & Težak, O. (2023). Design and Implementation of ESP32-Based IoT Devices. *Sensors*, *23*(15), 6739. https://doi.org/10.3390/s23156739

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016. https://doi.org/10.1016/j.csa.2023.100016

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: A review. *Journal of Big Data*, *6*(1), 111. https://doi.org/10.1186/s40537-019-0268-2

Leminen, S., Rajahonka, M., Wendelin, R., & Westerlund, M. (2020). Industrial internet of things business models in the machine-to-machine context. *Industrial Marketing Management*, *84*, 298–311. https://doi.org/10.1016/j.indmarman.2019.08.008

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lokhande, M. P., & Patil, D. D. (2021). Secured energy efficient machine -to-machine communication for telerobotic system. *Informatics in Medicine Unlocked*, *26*, 100731. https://doi.org/10.1016/j.imu.2021.100731

Nardo, M., Forino, D., & Murino, T. (2020). The evolution of man–machine interaction: The role of human in Industry 4.0 paradigm. *Production & Manufacturing Research*, *8*(1), 20–34. https://doi.org/10.1080/21693277.2020.1737592

Pradhan, D., & Tun, H. M. (2022). Security Challenges: M2M Communication in IoT. *Journal of Electrical Engineering and Automation*, *4*(3), 187–199. Retrieved from https://shorturl.asia/pKLGO

Radouan, A. M. R. A. (2021). Internet of Things (IoT. *Journal of Data Analysis and Information Processing*, *09*(02), 77–101. https://doi.org/10.4236/jdaip.2021.92006

Rejeb, A., Suhaiza, Z., Rejeb, K., Seuring, S., & Treiblmaier, H. (2022). The Internet of Things and the circular economy: A systematic literature review and research agenda. *Journal of Cleaner Production*, *350*, 131439. https://doi.org/10.1016/j.jclepro.2022.131439

Revadiaz, E., Fatkhurrokhman, M., & Aribowo, D. (2022). Prototype Automated Manipulator Robot Menggunakan Mikrokontroler NodeMCU ESP8266 Berbasis Internet of Things (IoT. *JTEV (Jurnal Teknik Elektro Dan Vokasional*, *8*(2), 439. https://doi.org/10.24036/jtev.v8i2.117682

Salama, R., Altrjman, C., & Al-Turjman, F. (2023). An overview of the Internet of Things (IoT) and Machine to Machine (M2M) Communications. *NEU Journal for Artificial Intelligence and Internet of Things*, *2*(3). Retrieved from https://dergi.neu.edu.tr/index.php/aiit/article/view/728

Sarfraz, M. (2021). Introductory Chapter: On Fingerprint Recognition. In M. Sarfraz (Ed.), *Biometric Systems. IntechOpen*. https://doi.org/10.5772/intechopen.95630

Setyawan, R. A., Muttaqin, A., & Khulud, H. (2022). Aplikasi NODEMCU ESP8266 sebagai Pemantau Suhu dan Kelembaban Ruang Data Center. *Jurnal EECCIS (Electrics, Electronics, Communications, Controls, Informatics, Systems*, *15*(1), 23–28. https://doi.org/10.21776/jeeccis.v15i1.1554

Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *Ieee Access*, *8*, 23022–23040. https://doi.org/10.1109/ACCESS.2020.2970118

Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K., & Weldehawaryat, G. K. (2022). System security assurance: A systematic literature review. *Computer Science Review*, *45*, 100496. https://doi.org/10.1016/j.cosrev.2022.100496

Siddique, K., & Ogami, Y. (2022). Computational Study on Thermal Motion Sensors That Can Measure Acceleration and Rotation Simultaneously. *Sensors*, *22*(18), 6744. https://doi.org/10.3390/s22186744

Soori, M., Arezoo, B., & Dastres, R. (2023). Internet of things for smart factories in industry 4.0, a review. *Internet of Things and Cyber-Physical Systems*, *3*, 192–204. https://doi.org/10.1016/j.iotcps.2023.04.006

Sudarmani, R., Venusamy, K., Sivaraman, S., Jayaraman, P., Suriyan, K., & Alagarsamy, M. (2022). Machine to machine communication enabled internet of things: a review. *International Journal of Reconfigurable and Embedded Systems*, *11*(2), 126. Retrieved from https://shorturl.asia/vM79c

Tang, K., Liu, A., Wang, W., Li, P., & Chen, X. (2018). A Novel Fingerprint Sensing Technology Based on Electrostatic Imaging. *Sensors*, *18*(9), 3050. https://doi.org/10.3390/s18093050

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023).

A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117

Ullah, A., Anwar, S. M., Li, J., Nadeem, L., Mahmood, T., Rehman, A., & Saba, T. (2023). Smart cities: The role of Internet of Things and machine learning in realizing a data-centric smart environment. *Complex & Intelligent Systems*. https://doi.org/10.1007/s40747-023-01175-4

Wicaksono, M. F., & Rahmatya, M. D. (2020). Implementasi Arduino dan ESP32 CAM untuk Smart Home. *Jurnal Teknologi Dan Informasi*, *10*(1), 40–51. https://doi.org/10.34010/jati.v10i1.2836

Wijaya, N. H., Mujib, A. K., Santoso, A. B., & Supriyadi, K. (2020). Design and Development of Heart Rate Per Minutes Based on Atmega16 Microcontroller with Alarm Warning. *IOP Conference Series: Materials Science and Engineering*, *835*(1), 12053. https://doi.org/10.1088/1757-899X/835/1/012053

Yeh, C.-C., Huang, T.-W., Lin, Y.-R., & Su, G.-D. (2023). The Design and Fabrication of Large-Area Under-Screen Fingerprint Sensors with Optimized Aperture and Microlens Structures. *Sensors*, *23*(21), 8731. https://doi.org/10.3390/s23218731

Yulianto, Y., Juarto, B., Rachmawati, I. D. A., & Yulistiani, R. (2022). Safe-Deposit Box Using Fingerprint and Blynk. *Engineering, MAthematics and Computer Science (EMACS) Journal*, *4*(1), 1–4. https://doi.org/10.21512/emacsjournal.v4i1.8080