Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 3, May 2026, Page 128-135
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i3.9681

IoT-Based Smart Dorm Key System Using Voice Password and Fingerprint Authentication for Dormitory Access Control

DTM Faiq Zariaqwila, Rita Purnamasari*, Efri Suhartono

Indonesia School of Electrical Engineering, Telkom University, Bandung, Indonesia
Email: [1]faiqaqwila@student.telkomuniversity.ac.id, [2,*]ritapurnamasari@telkomuniversity.ac.id,
[3]esuhartono@telkomuniversity.ac.id
Correspondence Author Email: ritapurnamasari@telkomuniversity.ac.id
Submitted: 16/04/2026; Accepted: 31/05/2026; Published: 31/05/2026

Abstract–The Internet of Things (IoT) has become an important technology in the development of modern access control systems. This study presents the design and implementation of an IoT-based Smart Dorm Key system employing a two-factor authentication mechanism using voice password verification and fingerprint authentication to improve dormitory access security. The proposed system is designed for Telkom University dormitories and enables real-time access control, monitoring, and access log synchronization through internet connectivity. The system utilizes an ESP32 microcontroller as the main controller integrated with an AS608 fingerprint sensor, solenoid door lock, no-touch sensor, LCD display, and buzzer to support authentication and door operation. Voice password verification is performed through a mobile application as the first authentication layer before fingerprint verification is conducted as the second layer. Experimental results show that the fingerprint sensor achieved 100% accuracy under normal conditions, while its performance decreased under wet and dirty finger conditions with accuracy values of 8% and 11%, respectively. The no-touch sensor operated reliably with a maximum detection distance of 10.5 cm. The results indicate that the proposed system is capable of implementing layered authentication and real-time monitoring, although further improvement is required to enhance performance under non-ideal conditions.

Keywords: Internet of Things; ESP32; Smart Dorm Key; Fingerprint Authentication; Two-Factor Authentication

1. INTRODUCTION

Telkom University dormitories still use traditional security systems in the form of manual keys and handwritten logbooks, which are vulnerable to manipulation, prone to human error, and considered inefficient for monitoring access activities [1]. Such conventional mechanisms provide limited control and traceability, thereby reducing the effectiveness of security management within the dormitory environment. This condition creates opportunities for the application of Internet of Things (IoT) technology to enhance the safety and access control of dormitory residents. In the Smart Dorm Key system, IoT functions as an integrated framework that connects hardware components responsible for door authentication with software applications used by residents and administrators for verification and monitoring purposes.

The implementation of IoT in the Smart Dorm Key system focuses on the integration of an ESP32 microcontroller, a fingerprint sensor, and voice verification as the primary authentication components. These components are connected through a Wi-Fi network and linked to a server and Firebase database, enabling real-time data exchange, processing, and storage of access information [2]. The proposed system supports multi-layer authentication mechanisms, automatic access log recording, and synchronized door control, ensuring seamless coordination between hardware devices and software applications.

Several related studies have explored IoT-based door security systems using different authentication methods, yet most of them still rely on a single or environment-dependent authentication approach. Anam implemented an IoT-based door security system utilizing a Raspberry Pi 4 combined with face recognition and an ultrasonic sensor to enhance access validation and intrusion detection capabilities [3]. Although this approach improves monitoring, facial recognition performance remains dependent on lighting conditions, camera positioning, and user visibility. Other studies have developed ESP32-based door security systems employing sound sensor-based authentication mechanisms as alternative biometric approaches [4], while IoT-based smart door lock systems using ESP32-CAM and facial recognition with Android integration have also been proposed [5]. However, both sound- and camera-based systems may experience reliability issues caused by environmental noise, hardware limitations, or privacy concerns.

Fingerprint-based biometric access control systems have also been implemented to improve physical security in various environments, demonstrating reliable authentication performance under controlled conditions [6]. Nevertheless, fingerprint-only systems remain susceptible to authentication failure due to improper finger placement, dirty fingers, or sensor degradation. Furthermore, contactless door lock systems utilizing voice authentication have been developed and evaluated as alternative biometric access control methods [7][8]. Despite offering hands-free operation, voice-based systems are sensitive to background noise and voice variation, which may affect verification consistency. These limitations indicate that single-authentication approaches often involve trade-offs between usability, robustness, and environmental adaptability. However, limited studies have explored the integration of fingerprint and voice verification within an IoT-based smart lock system specifically designed for dormitory environments.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 3, May 2026, Page 128-135
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i3.9681

Based on these findings, integrating fingerprint and voice verification offers a complementary layered authentication approach, where each method compensates for the limitations of the other. Fingerprint authentication provides stable identity verification independent of lighting conditions, while voice verification serves as an additional access layer without requiring physical tokens or camera systems. In addition to authentication design, security and privacy remain critical challenges in IoT-based systems due to their distributed architecture and internet connectivity, which expose connected devices to potential cyber threats, unauthorized access, and data leakage risks [9]. Therefore, secure communication and proper access management are important considerations in the implementation of IoT-based dormitory security systems.

The development of the Smart Dorm Key system also requires an understanding of several supporting technologies used to build a secure and user-friendly IoT-based access control system. The Internet of Things enables the interconnection of physical devices with digital systems, allowing real-time communication, monitoring, and control through internet connectivity [10]. IoT systems generally consist of three layers, namely the perception layer, network layer, and application layer [10], and have been widely studied as a framework for intelligent services in smart homes and security systems [11]. In this study, IoT serves as the communication backbone between the ESP32 microcontroller, Firebase server, and Android application, enabling real-time access logging and centralized monitoring [2].

In addition, the Arduino IDE serves as the primary development environment for programming and configuring the system. The Arduino IDE provides a simple and intuitive interface that supports embedded system development, debugging, and integration with various sensors and network modules [12]. Its accessibility and extensive library support have led to widespread adoption in IoT prototyping and development [13]. In the Smart Dorm Key project, the Arduino IDE is utilized to program the ESP32 microcontroller and manage communication between hardware and software components. The ESP32 is widely used in IoT-based electronic systems due to its integrated Wi-Fi and Bluetooth capabilities. In the Smart Dorm Key system, the ESP32 functions as the central controller that manages authentication logic, hardware communication, and actuator control. Its dual-core processor enables multitasking, allowing simultaneous handling of sensor input, network communication, and system responses [14]. Furthermore, IoT-based embedded systems are designed to support scalability and interoperability, making them suitable for smart environments such as dormitories and smart homes [15].

The AS608 fingerprint sensor is a commonly used biometric module in microcontroller-based security systems. This sensor captures fingerprint images, extracts unique features, and stores fingerprint templates internally, reducing the computational load on the microcontroller [16]. Fingerprint biometric authentication has been demonstrated as a reliable access control method under ideal conditions and is commonly used in multi-factor security systems [17]. To improve usability, the system also incorporates a no-touch sensor, which enables users to unlock the door from inside the room without physical contact by placing their hand within a specified detection range [18]. This feature is intended to enhance hygiene and user convenience. Additionally, a solenoid door lock is employed as the physical locking mechanism. The solenoid operates using electromagnetic principles, in which electrical current generates a magnetic field that moves the locking pin to control door lock status [19][20].

Based on the identified limitations in previous studies and the supporting theoretical foundations discussed above, this study proposes an IoT-based Smart Dorm Key system integrating ESP32, fingerprint authentication, and voice verification to address operational and security requirements in dormitory access control systems.

2. RESEARCH METHODOLOGY

The methodology of this research focuses on the design and implementation of an IoT-based Smart Dorm Lock system. As part of a smart dormitory security system that employs machine learning for two-factor verification, IoT plays a crucial role in managing entry and exit access control.

2.1 System Architecture

The design of the Smart Dorm Key system operates by integrating two main functions: a mobile application as the user interface for initial voice verification and an IoT-based system utilizing an ESP32 microcontroller as the main control unit. The ESP32 serves as the central controller that connects and manages all hardware components used in the system.

As illustrated in Figure 1, the system architecture diagram shows the workflow of the Smart Dorm Key system, describing the interaction between the mobile application, IoT components, and hardware devices during the access control process.

The process begins when the user initiates the access procedure by inputting a registered voice code through the mobile application. This mobile application functions as the initial authentication interface and captures the user's voice input for verification. The captured voice data is then processed and compared with the stored voice template in the system. If the voice input does not match the registered data, the authentication

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 3, May 2026, Page 128-135
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i3.9681

process is terminated, and the user is required to repeat the voice verification step. If the voice verification is successful, the authentication result is transmitted to the ESP32 microcontroller via an internet connection. Upon receiving a valid voice authentication signal, the ESP32 activates the next verification stage by prompting the user to perform fingerprint authentication. The user is then required to place their finger on the fingerprint sensor to scan their fingerprint data.

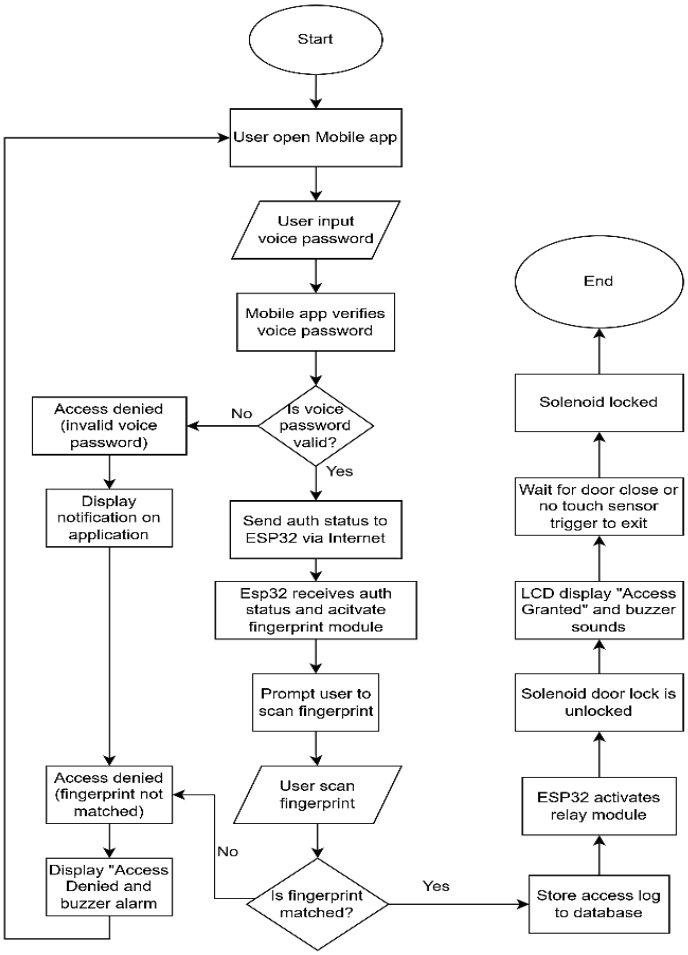

Figure 1. Smart Dorm Key System Flowchart

The scanned fingerprint is verified by comparing it with the fingerprint data stored in the system. If the fingerprint does not match the registered data, the system will deny access and request the user to repeat the fingerprint verification process. However, if both the voice and fingerprint verifications are successfully validated, the authentication results are transmitted to the database and recorded automatically as an access log.

Once the verification process is completed successfully, the ESP32 sends a control signal to the solenoid door lock to unlock the door. The solenoid door lock is then activated, allowing the user to enter the dormitory. After the access process is completed, the system returns to its initial standby state and is ready for the next authentication cycle.

2.2 System Implementation

The implementation phase in this study presents the realization of the IoT devices based on the previously designed system architecture. This process aims to ensure that all IoT hardware components are properly connected and operate optimally in accordance with the system design.

Based on Figure 2, the system design begins with a 12 V adapter that serves as the primary power supply for the Smart Dorm Key system. The output from the adapter is connected to a DC step-down converter to regulate and stabilize the voltage levels required by each hardware component. This voltage regulation is essential to ensure reliable operation and to prevent damage to sensitive electronic components. The ESP32 microcontroller acts as the central processing and control unit of the system. It is interfaced with an AS608 fingerprint sensor, which is responsible for capturing and verifying the user's fingerprint data during the authentication process. The ESP32 is also connected to a relay module that functions as an electrical switch to control the solenoid door lock. When valid authentication is confirmed, the ESP32 activates the relay to supply power to the solenoid, thereby unlocking the door.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 3, May 2026, Page 128-135
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i3.9681

In addition to access control components, the system integrates a buzzer that provides audible feedback to the user, indicating authentication status such as successful access or access denial. A push button is included as a manual input component for system interaction and operational control. Furthermore, a 16×2 LCD display is utilized to present system information, status messages, and user instructions in real time, enhancing user interaction and usability. To support exit access from inside the room, the system incorporates a no-touch infrared sensor. This sensor allows users to unlock the door without physical contact by placing their hand within the sensor's detection range, thereby improving convenience and hygiene. All components are electrically interconnected through the ESP32, enabling synchronized communication and coordinated operation between hardware modules within the Smart Dorm Key system.

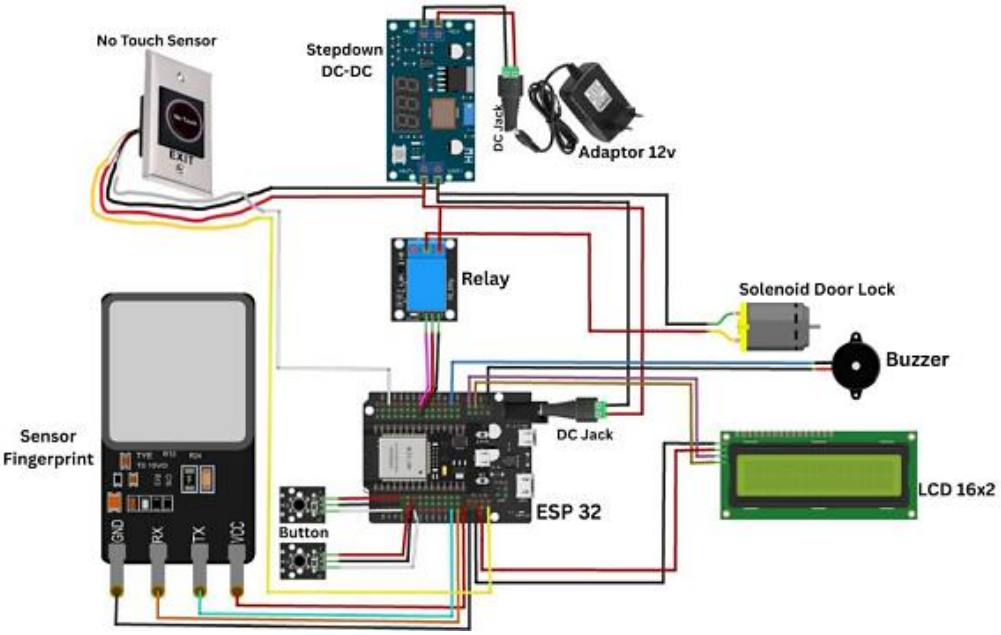

Figure 2. Smart Dorm Key Wiring Diagram

3. RESULT AND DISCUSSION

The Smart Dorm Key system was implemented and evaluated to assess the performance of its primary hardware components under different operating conditions. Testing in this study focused on the fingerprint sensor and no-touch sensor as the main hardware modules integrated within the proposed system. Experimental results indicate that while the fingerprint sensor performed well under normal conditions, its performance decreased significantly under wet and dirty finger conditions, demonstrating limitations in practical real-world usage. These findings suggest that the current system implementation is functional under controlled conditions but still requires further improvement to achieve more reliable operation in diverse user environments.

3.1 Fingerprint Sensor Testing

Fingerprint sensor testing was conducted to evaluate the reliability and accuracy of the AS608 fingerprint sensor as one of the primary authentication components in the Smart Dorm Key system. The testing involved three participants, namely Hazbi, Trisucipto, and Faiq, who acted as registered users in the system. Each participant performed multiple fingerprint authentication attempts to ensure consistency and repeatability of the results. The testing procedure consisted of three experimental trials. In the first trial, five different fingers from the right hand of each participant were used. The second trial involved five different fingers from the left hand of each participant. The third trial was conducted using five randomly selected fingers from each participant.

The fingerprint sensor was evaluated under three different conditions: normal finger condition, dirty finger condition, and wet finger condition.

3.1.1 Normal Finger Condition

The fingerprint sensor was first tested under normal finger conditions to evaluate its performance in an ideal environment. In this condition, participants performed fingerprint verification using clean and dry fingers. The results of this testing are presented in Table 1.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 3, May 2026, Page 128-135
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i3.9681

Table 1. Fingerprint Test Under Normal Condition

Name	Test 1 Successful	Test 1 Failed	Test 2 Successful	Test 2 Failed	Test 3 Successful	Test 3 Failed
Hazbi	✓		✓		✓	
Hazbi	✓		✓		✓	
Hazbi	✓		✓		✓	
Hazbi	✓		✓		✓	
Hazbi	✓		✓		✓	
Trisucipto	✓		✓		✓	
Trisucipto	✓		✓		✓	
Trisucipto	✓		✓		✓	
Trisucipto	✓		✓		✓	
Trisucipto	✓		✓		✓	
Faiq	✓		✓		✓	
Faiq	✓		✓		✓	
Faiq	✓		✓		✓	
Faiq	✓		✓		✓	
Faiq	✓		✓		✓	
Successfully captured fingerprints					45	
Failed captured fingerprints					0	
Fingerprint sensor accuracy (%)					100%	

Table 1 shows the fingerprint verification results for all participants under normal conditions. Based on the recorded data, all fingerprint attempts were successfully detected and verified by the AS608 sensor. A total of 45 fingerprint verification attempts were conducted, and all attempts were recorded as successful. Therefore, the fingerprint sensor achieved an accuracy of 100% under normal conditions. These results indicate that the AS608 fingerprint sensor performs reliably when no external disturbances affect the finger surface.

3.1.2 Wet Finger Condition

To evaluate sensor performance under non-ideal conditions, fingerprint testing was conducted using wet or moist fingers. This condition was designed to simulate real-world situations where users may attempt access with wet hands. The experimental procedure followed the same structure as the normal condition testing. The results of the wet finger condition test are presented in Table 2.

Table 2. Fingerprint Test Under Wet Condition

Name	Test 1 Successful	Test 1 Failed	Test 2 Successful	Test 2 Failed	Test 3 Successful	Test 3 Failed
Hazbi		✓		✓		✓
Hazbi		✓		✓		✓
Hazbi		✓		✓		✓
Hazbi		✓		✓		✓
Hazbi		✓		✓		✓
Trisucipto	✓			✓		✓
Trisucipto		✓		✓		✓
Trisucipto		✓	✓			✓
Trisucipto		✓		✓		✓
Trisucipto		✓		✓		✓
Faiq		✓		✓		✓
Faiq	✓			✓		✓
Faiq		✓		✓		✓
Faiq		✓	✓			✓
Faiq		✓		✓		✓
Successfully captured fingerprints					4	
Failed captured fingerprints					41	
Fingerprint sensor accuracy (%)					8%	

As shown in Table 2, a significant reduction in successful fingerprint detection was observed. Out of 45 fingerprint verification attempts, only 4 attempts were successfully detected, while the remaining attempts failed.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 3, May 2026, Page 128-135
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i3.9681

Based on these results, the fingerprint sensor achieved an accuracy of 8% under wet finger conditions. The data indicate a substantial decrease in sensor performance compared to normal conditions.
This result indicates that moisture on the finger surface severely affects the sensor's ability to capture and match fingerprint patterns. The reduced accuracy highlights a critical limitation of the fingerprint sensor when operating under non-ideal environmental conditions.

3.1.3 Dirty Finger Condition

Fingerprint testing under dirty finger conditions was performed to assess the impact of contaminants such as dust or dirt on sensor performance. Participants performed fingerprint authentication using fingers that were intentionally exposed to dust and debris. The testing procedure remained consistent with the previous conditions. The results of this test are summarized in Table 3.

Table 3. Fingerprint Test Under Dirty Condition

Name	Test 1 Successful	Test 1 Failed	Test 2 Successful	Test 2 Failed	Test 3 Successful	Test 3 Failed
Hazbi		✓		✓		✓
Hazbi	✓			✓		✓
Hazbi		✓		✓		✓
Hazbi		✓	✓			✓
Hazbi		✓		✓		✓
Trisucipto		✓		✓		✓
Trisucipto		✓	✓			✓
Trisucipto		✓		✓		✓
Trisucipto		✓		✓		✓
Trisucipto		✓		✓		✓
Faiq		✓		✓		✓
Faiq	✓			✓		✓
Faiq		✓		✓		✓
Faiq		✓	✓		✓	
Faiq		✓		✓		✓
Successfully captured fingerprints					5	
Failed captured fingerprints					40	
Fingerprint sensor accuracy (%)					11%	

According to the data presented in Table 3, the fingerprint sensor successfully detected only a small number of fingerprint attempts. Out of a total of 45 attempts, only 5 attempts were successfully verified, while the remaining attempts failed. As a result, the fingerprint sensor achieved an accuracy of 11% under dirty finger conditions. These results demonstrate a considerable decline in fingerprint recognition performance when finger cleanliness is compromised. These findings demonstrate that the fingerprint sensor's performance is highly sensitive to finger cleanliness, which may impact its reliability in practical, real-world usage scenarios.

3.2 No-Touch Sensor Testing

The no-touch sensor was tested to evaluate its effectiveness as an exit access mechanism from inside the dormitory room. This sensor allows users to open the door without physical contact, enhancing hygiene and ease of use. The testing focused on determining the maximum detection distance at which the sensor could reliably detect a user's hand. The experiment was conducted by placing a hand at various distances from the sensor, and each distance was tested three times to ensure consistency. The results of this testing are presented in Table 4.

Table 4. No-Touch Sensor Maximum Detection Distance Test

Distance	Test 1 Detected	Test 1 Not Detected	Test 2 Detected	Test 2 Not Detected	Test 3 Detected	Test 3 Not Detected
Distance 2 cm	✓		✓		✓	
Distance 4 cm	✓		✓		✓	
Distance 6 cm	✓		✓		✓	
Distance 8 cm	✓		✓		✓	
Distance 10 cm	✓		✓		✓	
Distance 10.5 cm	✓		✓		✓	
Distance 11 cm		X		X		X

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 3, May 2026, Page 128-135
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i3.9681

Based on the data shown in Table 4, the no-touch sensor was able to detect a hand reliably at distances ranging from 0 cm to 10.5 cm. At distances beyond 10.5 cm, the sensor failed to respond to the presence of an object. These results indicate that the effective operational range of the no-touch sensor is up to 10.5 cm, which is sufficient for practical exit access usage.

3.3 Discussion

The results demonstrate that the Smart Dorm Key system is capable of implementing a two-factor authentication mechanism by combining voice recognition and fingerprint verification in an IoT-based access control environment. The requirement for users to complete voice authentication through a mobile application before proceeding to fingerprint scanning enhances system security by introducing layered authorization. This approach ensures that access is granted only when both authentication stages are successfully verified, reducing the likelihood of unauthorized access.

The fingerprint sensor showed excellent performance under normal conditions, achieving a perfect accuracy rate. This result confirms that the AS608 fingerprint sensor is reliable when used in ideal environments. However, the significant decrease in accuracy observed under wet and dirty finger conditions highlights an important limitation of the sensor. Moisture and contaminants on the finger surface interfere with the sensor's ability to capture clear fingerprint patterns, leading to a substantial reduction in recognition accuracy. This limitation presents a challenge for real-world implementation, particularly in dormitory environments where users may not always have clean and dry fingers.

Despite these limitations, the integration of fingerprint authentication with voice recognition helps mitigate security risks by ensuring that access is not solely dependent on a single biometric factor. This multi-factor authentication approach is aligned with security best practices in IoT systems, which recommend layered authentication mechanisms to enhance protection against unauthorized access [9]. The system's IoT architecture enables real-time communication between the mobile application, ESP32 microcontroller, and database, allowing authentication results and access logs to be processed and stored efficiently. This real-time connectivity enhances system responsiveness and supports centralized monitoring.

In contrast, the no-touch sensor demonstrated stable and reliable performance during exit access testing, with an effective detection range that meets practical usage requirements. This feature provides a practical and hygienic solution for door access from inside the room, particularly in shared dormitory environments. The reliable operation of the no-touch sensor complements the overall system functionality and improves user convenience without compromising security.

The results indicate that while the Smart Dorm Key system performs effectively under ideal conditions, further optimization is required to ensure reliability under diverse environmental conditions. Enhancements in fingerprint sensing technology or the integration of alternative backup authentication methods would improve system robustness and usability. With continued development, the Smart Dorm Key system has strong potential to serve as a secure and adaptive IoT-based access control solution for dormitories and similar facilities.

4. CONCLUSIONS

This study designed and implemented an IoT-based Smart Dorm Key system utilizing two-factor authentication through voice password verification and fingerprint authentication, integrating an ESP32 microcontroller, mobile application, fingerprint sensor, solenoid door lock, no-touch sensor, and Firebase database to support real-time access control and monitoring in a dormitory environment. Experimental results showed that the AS608 fingerprint sensor achieved 100% successful authentication under normal conditions, indicating effective operation in ideal environments; however, its performance decreased significantly under wet and dirty finger conditions, with accuracy dropping to 8% and 11%, respectively, demonstrating that the fingerprint authentication mechanism is highly sensitive to environmental and user conditions. This limitation may affect accessibility and convenience in practical dormitory use, where users may not always have clean and dry fingers. Meanwhile, the no-touch sensor functioned effectively as an exit mechanism with a maximum detection distance of 10.5 cm, supporting practical and contactless door operation. Overall, the proposed system demonstrates the feasibility of integrating IoT devices and sequential authentication workflows for dormitory access management under controlled conditions, although further improvements such as sensor optimization or additional backup authentication methods are necessary to improve system reliability and usability for real-world implementation.

REFERENCES

[1] Telkom University, "*Asrama*," [Online]. Available: https://telkomuniversity.ac.id/asrama/. Accessed: Jul. 11, 2025.

[2] G. T. Le, N. M. Tran, and T. V. Tran, "IoT System for Monitoring a Large-Area Environment Sensors and Control Actuators Using Real-Time Firebase Database," *Intelligent Human Computer Interaction (IHCI 2020)*, Lecture Notes in Computer Science, vol. 12616, Springer, 2021, pp. 3–20, doi: 10.1007/978-3-030-68452-5_1.

[3] N. Anam, R. Purnamasari, and E. Suhartono, "*Integrasi perangkat keras dan realisasi sistem kunci pintar berbasis Raspberry Pi 4*," e-Proceeding of Engineering, vol. 11, no. 6, pp. 6494–6497, Dec. 2024. [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/24991

ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 3, May 2026, Page 128-135
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i3.9681

[4] D. Gultom and M. F. Susanto, "*Studi aplikasi smartlock pada pintu rumah dengan Arduino berbasis IoT dengan sensor suara*," in Proc. 11th Industrial Research Workshop and National Seminar, Bandung, Indonesia, 2020, pp. 239–245. [Online]. Available: https://jurnal.polban.ac.id/proceeding/article/view/2001

[5] Bhavishya Reddy K., Likitha G., N. Usha, and Syed Jahangir Badashah, "Automatic Door Access Control System Based on Facial Recognition Using ESP32-CAM," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 10, no. 5, May 2022, doi: 10.22214/ijraset.2022.43310

[6] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," *Symmetry*, vol. 11, no. 2, p. 141, Jan. 2019, doi: 10.3390/sym11020141.

[7] A. O. D. Adekola, A. Akinsanya, A. Olufowobi, O. Babajide, O. M. Somefun, and A. Oduroye, "Voice Recognition Door Access Control System," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 21, no. 5, ser. I, pp. 01–12, Sep.–Oct. 2019, doi: 10.9790/0661-2105010112.

[8] G. Chandu Preethi, B. Syam Sundar, K. Thorani Nyshidha, K. Krishna, and C. H. Viswanathasarma, "Smart Door Unlocking System Using Voice Authentication," *International Journal of Research Publication and Reviews*, vol. 6, no. 4, pp. 7384–7392, Apr. 2025, doi: 10.55248/gengpi.6.0425.14185.

[9] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, Aalborg, Denmark, May 2014, pp. 1–8, doi: 10.1109/PRISMS.2014.6970594.

[10] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015, doi: 10.1109/COMST.2015.2444095.

[11] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," *Journal of Computer and Communications*, vol. 3, no. 5, pp. 164–173, May 2015, doi: 10.4236/jcc.2015.35021.

[12] Arduino Indonesia, "Software Arduino IDE," [Online]. Available: https://www.arduinoindonesia.id/2018/07/software-arduino-ide.html. Accessed: Aug. 8, 2025.

[13] M. Banzi and M. Shiloh, *Getting Started with Arduino*, 3rd ed, Sebastopol, CA: Maker Media, 2014.

[14] Espressif Systems, "ESP32 series specifications," [Online]. Available: https://www.espressif.com/en/products/socs/esp32/specifications. Accessed: Aug. 8, 2025.

[15] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi:10.1016/j.comnet.2010.05.010.

[16] M. Shojaei, "Interfacing AS608 optical fingerprint sensor module with Arduino," [Online]. Available: https://electropeak.com/learn/interfacing-fpm10a-as608-optical-fingerprint-reader-sensor-module-with-arduino/. Accessed: Aug. 8, 2025.

[17] E. Esekhaigbe and E. O. Okoduwa, "Design and implementation of a fingerprint-based biometric access control system," *Journal of Advances in Science and Engineering*, vol. 7, no. 1, pp. 18–23, Jul. 2022, doi: 10.37121/jase.v7i1.183.

[18] ASSA ABLOY, "No-touch exit sensor – Access without the touch," [Online]. Available: https://www.assaabloy.com/za/en/stories/news/no-touch-exit-sensor---access-without-the-touch. Accessed: Aug. 8, 2025.

[19] H. Guntoro, Y. Somantri, and E. Haritman, "*Rancang bangun magnetic door lock menggunakan keypad dan solenoid berbasis mikrokontroler Arduino Uno*," ELECTRANS, vol. 12, no. 1, pp. 39–48, Mar. 2013. [Online]. Available: https://ejournal.upi.edu/index.php/electrans/article/view/1866

[20] D. Nagajyothi and P. Siddaiah, "Speech recognition using convolutional neural networks," Int. J. Eng. Technol., vol. 7, no. 4.6, pp. 133–137, 2018, doi: 10.14419/ijet.v7i4.6.20449