ISSN: 2581-1274


# Design and Construction of an Automatic Door System Based on Iris Detection Using Esp32-Cam and OpenCV Using the Rapid Application Development (RAD) Method

Nanda Angelika [a,1,*], Nurhasanah [a,2],

[a] *Faculty of Computer Science, Pamulang University, Sounth Tangerang 15417, Indonesia*
[1] *huwaeangelika@gmail.com*;* [2] *dosen01123@unpam.ac.id*
** corresponding author*

ARTICLE INFO

*Article history:*
Published
April 5, 2026

*Keywords:*
Automatic Door
Iris Recognition
OpenCV
Internet of Things
Flutter
Rapid Application Development
Security System

ABSTRACT

Conventional home security systems typically depend on mechanical keys and passive CCTV cameras, which do not offer active access control or real-time response. This study presents the design and implementation of an automatic door system that uses iris recognition for authentication, developed with an ESP32-S3 camera and OpenCV, and integrated into a Flutter-based mobile application. The system was created using the Rapid Application Development (RAD) method to ensure flexibility and fast iteration. The prototype includes biometric iris authentication, solenoid-based door locking, live video monitoring, alarm activation, and real-time notifications. Through black-box testing, the system achieved high recognition accuracy, maintained stable operation in low-light environments, and successfully prevented unauthorized access using photo or video spoofing. Additionally, users receive instant alerts for failed access attempts or suspicious motion. The results show that integrating iris biometrics with IoT technology significantly enhances both home security and user convenience. Compared to traditional locks and CCTV systems, this approach provides a more intelligent, responsive, and secure solution for modern smart homes, offering users greater safety, automation, and peace of mind.



## I. Introduction

Home security is a crucial aspect in protecting residents and valuable assets. However, burglary cases in Indonesia remain relatively high, especially when homeowners are away for work, travel, or other activities [1]. This condition indicates that many households still rely on manual security systems that are vulnerable to manipulation and unauthorized access [2]. Weak neighborhood supervision, the absence of dedicated security personnel, and the ease of breaking physical locks further contribute to this issue [3]. In addition, public awareness regarding the importance of modern security systems is still low, even though conventional keys can be easily duplicated or forcibly opened using simple tools [2].

Most households still use conventional locking mechanisms such as mechanical keys or padlocks, which are prone to being lost, stolen, or broken into [3]. Although modern solutions such as digital passwords and RFID cards have been introduced, these methods still present weaknesses—passwords can be forgotten, and access cards can be misplaced—making them less reliable for long-term security [2]. CCTV has also become a common alternative for monitoring residential areas [1]. However, CCTV only provides passive surveillance and does not prevent unauthorized individuals from physically opening the door if no active authentication system is implemented.

Biometric-based solutions, such as facial recognition or iris recognition, offer more secure authentication because the user's identity is verified through unique biological characteristics [2]. Among various biometric modalities, iris recognition provides higher accuracy and security due to the uniqueness and lifetime stability of iris patterns, which are difficult to forge [4]. The integration of biometric systems with Internet of Things (IoT) technology also enables real-time monitoring and remote door control through smartphones or applications such as Telegram, significantly enhancing convenience and security [5].

Previous studies have explored biometric technologies and the Rapid Application Development (RAD) method in different application contexts. Study [6] developed an Android-based attendance system using facial recognition, while [7] implemented the RAD method to develop a face-recognition-based attendance system using Amazon Rekognition. However, no existing research has integrated iris recognition using ESP32-CAM, IoT connectivity, and the RAD methodology for developing an automatic smart door system.

This research aims to fill that gap by developing an Automatic Door System Based on Iris Recognition using ESP32-CAM and OpenCV, designed with the Rapid Application Development (RAD) method. The system is intended to provide a more secure, accurate, and integrated biometric solution for home security, thereby offering enhanced safety and convenience for homeowners [8].

Despite the development of various home security technologies, most existing systems still rely on mechanical locks, passwords, RFID cards, or passive CCTV monitoring, which suffer from significant limitations such as key duplication, forgotten credentials, lost access cards, and the absence of active access control [9]. Although biometric approaches and the Rapid Application Development (RAD) method have been applied in previous studies, their implementation is generally limited to attendance systems or face recognition applications. To the best of the authors' knowledge, there is no prior study that integrates iris recognition using an ESP32-CAM platform, combined with Internet of Things (IoT) connectivity and the RAD methodology, specifically for an automatic smart door system. Therefore, the novelty of this research lies in the design and implementation of an integrated iris-based automatic door prototype that utilizes ESP32-CAM and OpenCV, developed through the RAD approach and connected to an IoT-based mobile application. This integration provides active biometric access control, real-time monitoring, and responsive security features, contributing a more secure and practical solution compared to conventional mechanical locks, RFID systems, and passive CCTV-based home security [10].

The objectives of this study are to design and implement an automatic door security system based on iris recognition that overcomes the limitations of conventional mechanical locks and passive CCTV systems [10]. The proposed system is built using an ESP32-CAM platform and OpenCV for iris-based authentication, integrated with Internet of Things (IoT) technology to enable real-time monitoring, access control, and notification services through a mobile application [8]. The system is evaluated through black-box testing under various scenarios, including registered and unregistered users, different lighting conditions, camera distance variations, and photo or video spoofing attempts. The scientific contributions of this research include the development of an integrated iris-based smart door prototype using the Rapid Application Development (RAD) method, a structured evaluation of its security and usability performance, and empirical evidence that iris biometrics combined with IoT can provide a more secure and responsive access control solution compared to conventional key-based, RFID, or passive CCTV home security systems [8][9].

## II. Method

### *A. Rapid Application Development (RAD)*

Rapid Application Development (RAD) is a software development methodology that emphasizes fast development cycles, prototyping, and continuous user feedback. Unlike traditional sequential models, RAD allows system components to be designed, implemented, tested, and refined iteratively, enabling rapid adaptation to functional and technical requirements. This approach is suitable for embedded and IoT-based systems where hardware–software integration and real-time performance evaluation are critical.

Previous studies have shown that RAD is effective for developing biometric-based systems due to its flexibility and rapid prototyping capabilities [7]. Therefore, this research adopts the RAD method to accelerate the development of an iris-based automatic door system while ensuring functionality, security, and usability.

The RAD stages implemented in this research are illustrated in Figure 1 and described as follows:

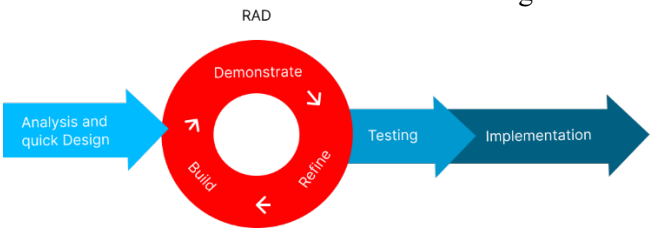


Fig 1. Rapid Application Development (RAD) Cycle

- Requirement Planning:

  Determining the required hardware components such as the ESP32-S3 with an OV5640 camera module, solenoid lock, vibration sensor, LED indicators, buzzer, power adapter, and prototype enclosure. The software components include Arduino IDE, OpenCV, Flutter, PHP, and MySQL.

- Quick Design:

  Developing the initial system design, including the iris detection workflow, automatic door control logic, alarm activation after three failed attempts, live CCTV monitoring, and the preliminary layout of the Flutter application interface.

- Build Prototype:

  Constructing the prototype by integrating the ESP32-S3 for iris detection and door control, adding security sensors, and developing a Flutter-based mobile application connected to the backend for door control, live CCTV streaming, alarm configuration, user management, and access logging.

- Testing & Iteration:

  Conducting tests to evaluate iris detection performance and system response time across all functional modules, followed by iterative improvements whenever discrepancies or unmet requirements are identified.

### *B. System Architecture and Hardware Design*

#### *1) System Architecture*

"The system consists of an ESP32-S3 microcontroller equipped with an OV5640 camera module as the main component for iris image acquisition and CCTV monitoring. The ESP32-S3 processes captured iris images using OpenCV-based image processing and authentication procedures, while also receiving distance data from the VL53L0X Time-of-Flight (ToF) sensor to detect user presence and reduce spoofing attempts. Based on the authentication results, the microcontroller controls actuators such as a solenoid door lock, buzzer, and indicator LEDs to manage door access and security alerts. The system is integrated with Flutter-based mobile application, which enables remote door control, real-time video monitoring, user management, and security notifications. The overall interaction between hardware components and the application is illustrated in Figure 2.

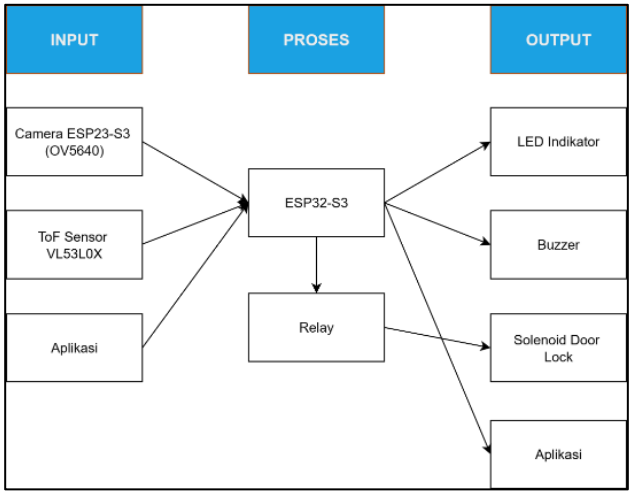


Fig 2. Block Diagram of the Proposed Automatic Door System

*2) Hardware Design*

The hardware design in this study utilizes an ESP32-S3 module equipped with an OV5640 camera as the main component. The camera captures the user's iris image and sends it directly to the ESP32-S3 for identity verification without requiring additional devices. This module also reads inputs from supporting sensors such as the ToF sensor for detecting the presence of a user in front of the door, and controls actuators such as the solenoid door lock and buzzer. The camera is supported by Near-Infrared (NIR) LED illumination to ensure optimal image quality even in low-light conditions. Verification results are then forwarded to the Android application, which functions as the user interface and monitoring center, allowing the system to operate efficiently with fast and reliable responses.

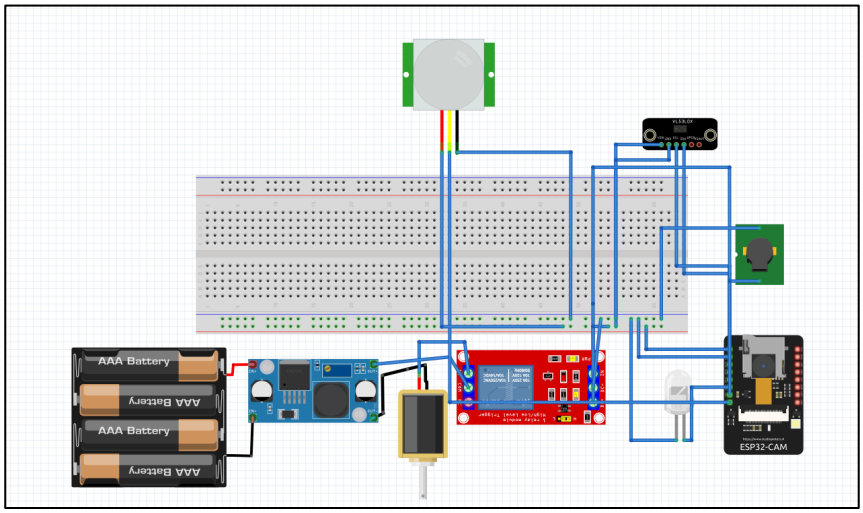


Fig 3. Hardware Design of the Automatic Door Prototype

## C. *Iris Recognition Algorithm*

The iris recognition algorithm in this study is implemented using OpenCV-based image processing on the ESP32-S3 platform. The algorithm is designed to provide reliable biometric authentication while maintaining computational efficiency suitable for embedded systems. The iris recognition process consists of sequential stages including eye detection, region of interest (ROI) extraction, iris circle detection, and iris segmentation.

*1) Eyes Detection*

The process begins with eye detection to identify the eye region from the captured facial image. This step ensures that further processing is focused only on the relevant eye area, reducing noise and computational load.

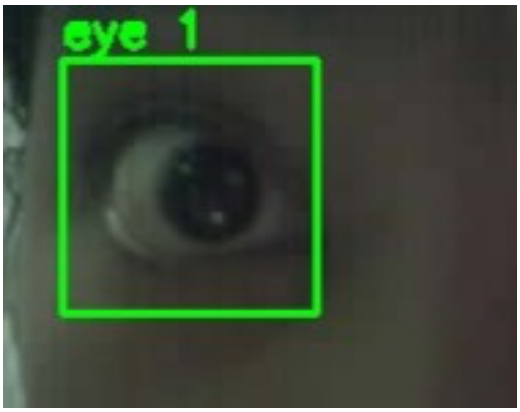


Fig 4. Eye Detection Result

*2) Region of Interest (ROI) Extraction*

After the eye is detected, a region of interest (ROI) is defined to isolate the iris area. The ROI limits the processing area to the eye region, enabling more accurate iris analysis and faster computation.


Fig 5. Region of Interest (ROI) Extraction

*3) Iris Circle Detection*

Iris circle detection is then performed to locate the circular boundary of the iris. This step separates the iris from surrounding regions such as the sclera and eyelids by identifying the iris radius and center point..

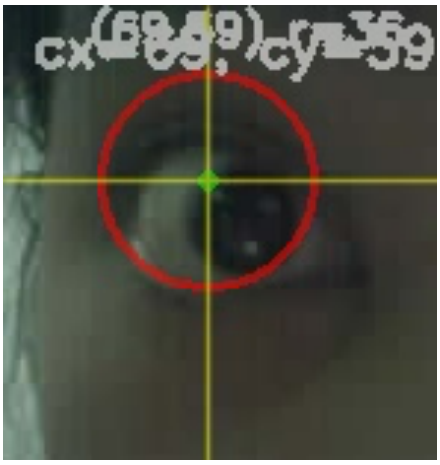


Fig 6. Iris Circle Detection

*4) Iris Segmentation*

The extracted iris region is segmented using thresholding techniques to distinguish iris patterns from the background. The resulting segmented image is used as the basis for feature extraction and authentication...

Fig 7. Iris Segmentation Result

*5) Texture Feature Extraction (Local Binary Pattern – LBP)*

After segmentation, texture features are extracted from the iris image using the Local Binary Pattern (LBP) method. LBP encodes local texture information into a feature vector that represents the unique characteristics of the iris. The extracted features are used for similarity comparison during the authentication process.*Results and Discussion*

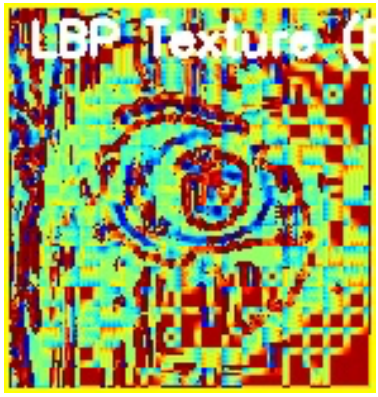


Fig 8. Texture Feature Extraction

## *D. Testing Scenario and Procedure*

System testing was conducted to ensure that all features of the ESP32-S3 based automatic door system with iris recognition operate according to the defined requirements. The testing method employed was Black Box Testing, which focuses on verifying system functionality by providing specific inputs and observing system responses without examining internal code structures.

Table 1. Table Black Box Testing Plan

| Test Class | Test Item | Test Type |
|---|---|---|
| **System Connection** | ESP32-S3 successfully connects to Wi-Fi | Black Box |
| | Flutter application can connect to the server/database | Black Box |

| Test Class | Test Item | Test Type |
|---|---|---|
| | Camera streaming runs smoothly without interruption under stable Wi-Fi — Black Box | Black Box |
| **Camera Monitoring & Live Stream** | Displays real-time video on the application | Black Box |
| | Live stream continues while the door is opened | Black Box |
| | Live stream stops automatically when the connection is lost | Black Box |
| **Iris Registration** | Saves new user iris images | Black Box |
| | Rejects already registered iris data (duplicate prevention) | Black Box |
| | Validates iris data before saving to the database | Black Box |
| **User Management** | Add a new user via the application | Black Box |
| | Delete a user from the database | Black Box |
| | Display the list of registered users | Black Box |
| **Iris Authentication (Normal Condition)** | User facing camera with registered iris → door opens | Black Box |
| **Iris Authentication (Abnormal Condition)** | Using an unregistered iris → door remains locked | Black Box |
| | Using an image/video of an eye → door remains locked | Black Box |
| | Authentication fails 3 times → buzzer activates & notification is sent | Black Box |
| **Physical Security – PIR Sensor** | PIR detects movement → buzzer activates & notification is sent | Black Box |

## III. Result and Discussion

### *A. Implementation Result*

The proposed automatic door security system based on iris recognition was successfully implemented as a functional prototype. The system integrates hardware components and software applications into a unified smart door solution. The implementation confirms that the designed architecture operates as intended and is capable of providing active biometric access control and real-time security monitoring.

The hardware implementation consists of an ESP32-S3 microcontroller equipped with an OV5640 camera module, distance and motion sensors, alarm components, and a solenoid door lock. All components were assembled into a single prototype enclosure and operated reliably during system execution. The hardware was able to capture iris images, detect user presence, and physically control door locking and unlocking mechanisms as designed, as shown in Figure 8.

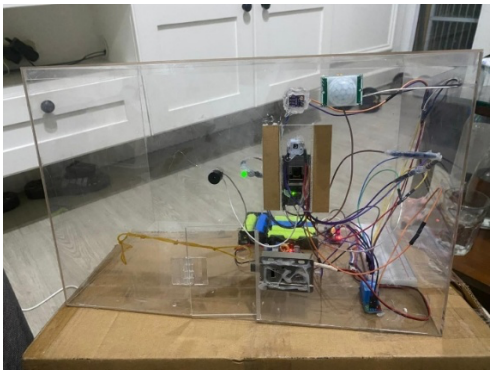

Fig 9. Implemented Automatic Door Prototype

A mobile application developed using Flutter was implemented as the main user interface for system interaction and monitoring. The application provides real-time camera streaming, user registration, access log visualization, and security notification features. Communication between the ESP32-S3 device and the application was successfully established, enabling remote door control and monitoring, as illustrated in Figure 9.

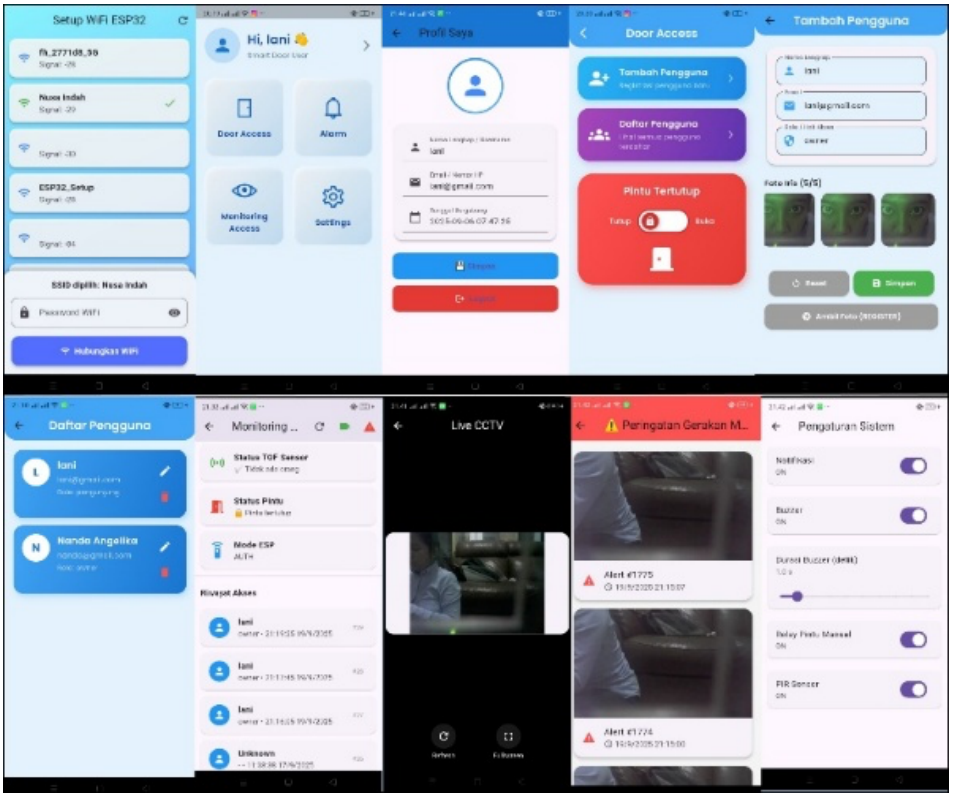


Fig 10. Flutter-Based Mobile Application Interface

The integrated system demonstrated synchronized operation between iris recognition, door control, and notification mechanisms. When a registered iris was detected, the system automatically unlocked the door and recorded the access event. In contrast, failed authentication attempts triggered alarms and real-time notifications sent to the mobile application. These results indicate that the implemented system functions cohesively and fulfills the operational requirements of a smart door security system.

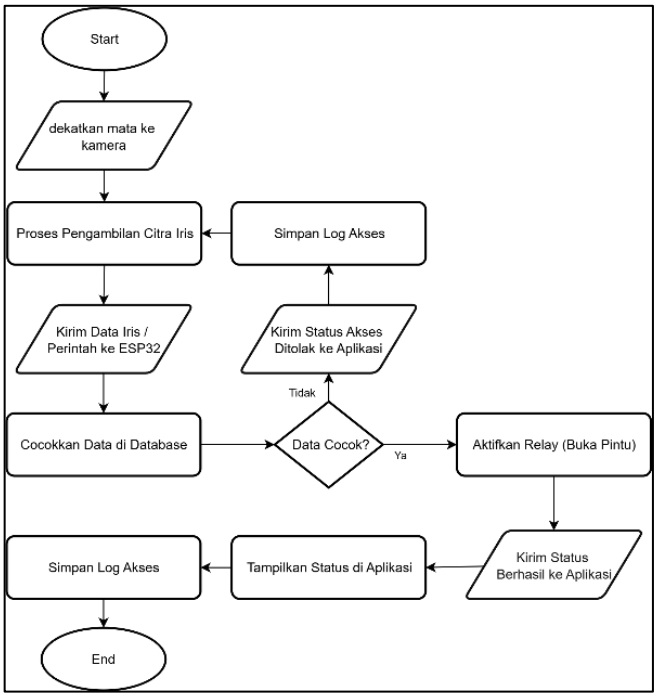


Fig 11. System Operation Flowchart of the Implemented Iris-Based Automatic Door

### *B. Iris Recognition Performance*

Iris recognition performance was evaluated to measure the system's ability to correctly authenticate registered users and reject unauthorized access attempts. The testing scenarios were derived from real system usage conditions, including registered and unregistered irises, normal access attempts, and spoofing attacks using eye photographs and videos. The evaluation focused on system response outcomes rather than internal algorithmic processes.

Table 2. Table Iris Recognition Performance Result

| Test Scenario | System Response |
|---|---|
| **Registered Iris** | Access granted |
| **Unregistered Iris** | Access denied |
| **Photo Spoofing** | Rejected |
| **Video Spoofing** | Rejected |
| **Three Consecutive Failures** | Alarm activated & notification sent |

The experimental results indicate that the system successfully distinguished between registered and unregistered iris patterns. Access was granted only when the input iris matched the stored biometric template, while unauthorized attempts were consistently rejected. This demonstrates that the implemented iris recognition mechanism functioned as intended under normal operating conditions.

Photo and video spoofing attempts were rejected by the system due to the distinctive texture characteristics of the human iris. Unlike printed images or digital displays, a real iris contains complex micro-patterns and natural texture variations that cannot be accurately replicated by flat

images or video playback. As a result, the extracted iris features from spoofing media did not satisfy the similarity threshold required for authentication.

Compared to conventional authentication approaches such as RFID cards or face recognition, iris-based authentication offers higher resistance to duplication and spoofing. RFID systems are vulnerable to card loss or cloning, while face recognition systems may be deceived by photographs or screen displays. In contrast, iris recognition relies on highly unique biometric textures, making unauthorized replication significantly more difficult and enhancing overall access security.

### *C. System Security and Usability Evaluation*

#### *1) Security Mechanism Evaluation*

The security mechanism of the proposed automatic door system was evaluated based on its response to failed authentication attempts and suspicious physical activity. The system is designed to activate an alarm mechanism after three consecutive unsuccessful iris authentication attempts. This feature aims to prevent brute-force access and unauthorized entry. During testing, when an unregistered iris, photo, or video was repeatedly used for authentication, the system consistently denied access. After three failed attempts, the buzzer was automatically activated, indicating a security breach attempt. This behavior demonstrates that the system is capable of enforcing access control rules and responding appropriately to abnormal conditions.

#### *2) Notification and Monitoring Response*

In addition to the local alarm, the system provides real-time notification capabilities to enhance user awareness. When a security event occurs, such as multiple authentication failures or motion detected by the PIR sensor, a notification is immediately sent to the user through the mobile application or Telegram service. The notification system enables users to receive alerts remotely, allowing timely responses even when they are not physically present near the door. Test results show that notifications were successfully delivered shortly after the event was triggered, indicating reliable communication between the ESP32-S3 device, server, and user interface.

#### *3) Usability Evaluation*

From a usability perspective, the system provides real-time monitoring through a live camera stream displayed in the Flutter-based mobile application. Users can observe the door area, monitor access attempts, and review system status without direct interaction with the hardware. The integration of live streaming, access logs, and notification alerts improves overall user experience by offering a centralized and intuitive control interface. Based on testing, the system was easy to operate and provided clear feedback for both successful and failed access attempts, demonstrating good usability for residential security applications.

Table 3. Table Black Box Testing Plan

| 5Test Scenario | Expected Result | Observed Result | Conclusion |
|---|---|---|---|
| **ESP32-S3 connected to Wi-Fi** | ESP32-S3 successfully connects to Wi-Fi | ESP32-S3 connected and obtained an IP Address | Passed |
| **Flutter application launched and logged in to server** | Application successfully connects to server/database | Application displayed the dashboard | Passed |
| **Camera streaming under stable Wi-Fi** | Video stream runs smoothly without interruption | Real-time video stream appears in Flutter app | Passed |

| 5Test Scenario | Expected Result | Observed Result | Conclusion |
|---|---|---|---|
| **Registering a new iris** | New iris data is saved to the database | New iris saved and can be used for authentication | Passed |
| **Adding a new user via the application** | New user data is stored in the database | New user displayed in the user list | Passed |
| **Deleting a user from the database** | User data is deleted | User removed from the list | Passed |
| **Eyes aligned with camera using registered iris** | Door unlocks automatically | Door unlocked and access log recorded | Passed |
| **Using an unregistered iris** | Door remains locked | System denied access | Passed |
| **Using an image or video of an eye** | Door remains locked | System denied access | Passed |
| **Three consecutive authentication failures** | Buzzer activates & notification sent | Buzzer triggered and notification received in the app | Passed |
| **PIR detects motion in front of the door** | Notification sent to Android device | System sent notification and stored capture & log | Passed |

### *D. Discussion*

The experimental results indicate that the proposed iris-based automatic door system is able to effectively address the limitations of conventional home security mechanisms. Unlike mechanical locks and RFID-based access systems, which are vulnerable to key duplication, loss, or unauthorized borrowing, the proposed system performs identity verification based on unique iris patterns that are inherently difficult to replicate. Furthermore, compared to passive CCTV systems that only provide post-event monitoring, the developed system implements active access control by preventing unauthorized users from opening the door in real time. The integration of iris recognition with IoT-based monitoring allows homeowners to receive immediate notifications and access logs, thereby enhancing situational awareness and overall security. These findings demonstrate that the proposed system offers a more proactive and secure solution than traditional mechanical locks, RFID cards, and passive CCTV-based home security systems.

Despite its effectiveness, the system still exhibits several limitations that should be considered. The accuracy of iris recognition is influenced by external factors such as insufficient lighting, improper head positioning, and unstable network connectivity, which may affect image quality and response time. Nevertheless, the combination of iris biometrics and IoT technology remains scientifically valid, as iris texture patterns are highly distinctive and stable over a person's lifetime, providing strong resistance against spoofing attempts using photos or videos. The experimental results support this claim, as the system successfully rejected photo and video-based attacks during testing. By integrating biometric authentication with real-time IoT communication, the proposed system not only enhances security but also improves usability through remote monitoring and instant notifications, making it a practical and scalable solution for smart home security applications.

## IV. Conclusion

Based on the design, implementation, and testing of the proposed system, several conclusions can be drawn as follows:

- The automatic door security system based on iris recognition was successfully designed and implemented using the ESP32-S3 platform, OpenCV-based image processing, and Internet of Things (IoT) integration, enabling active biometric access control and real-time monitoring.
- Experimental results show that the system is able to accurately authenticate registered users and deny access to unregistered users. The iris recognition mechanism successfully rejected photo and video spoofing attempts, indicating strong resistance against common biometric attacks.
- The system demonstrated reliable security responses, where three consecutive authentication failures triggered alarm activation and real-time notifications through the mobile application, while the PIR sensor effectively detected suspicious movement and sent alerts to users.
- The integration of iris biometrics with IoT technology provides significant advantages over conventional mechanical locks, RFID-based systems, and passive CCTV monitoring by offering higher security, real-time access control, and immediate user notifications.

**Recommendations:**

For future development, it is recommended to expand the testing scenarios by involving more users and diverse environmental conditions, improve liveness detection techniques to further enhance spoofing resistance, and integrate the system into a broader smart home ecosystem with more robust network performance evaluation.

## Acknowledgment

The author would like to express sincere gratitude to the academic supervisor from Universitas Pamulang for the valuable guidance, support, and constructive feedback throughout the completion of this research. The author also extends appreciation to the Faculty of Computer Science for providing the facilities and academic environment that supported the successful development of this independent study.

## References

[1] B. Sumboro, S. Sutariyani, dan R. I. Utomo, "Sistem Keamanan Rumah Berbasis Raspberry Pi dan Menggunakan Sensor PIR," *Go Infotech: Jurnal Ilmiah STMIK AUB*, vol. 26, no. 1, hlm. 96, Jun 2020, doi: 10.36309/goi.v26i1.127.

[2] A. Mude dan L. B. F. Mando, "Implementasi Keamanan Rumah Cerdas Menggunakan Internet of Things dan Biometric Sistem," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 1, hlm. 179–188, Nov 2021, doi: 10.30812/matrik.v21i1.1381.

[3] A. Rozaq, D. Irawan, dan Y. A. Surya, "Sistem Keamanan Rumah Menggunakan RFID dan Keypad Matrix Dengan One Time Pad Home Security Systems Using RFID and Keypad Matrix With One Time Pad," 2023. [Daring]. Tersedia pada: http://jurnalnasional.ump.ac.id/index.php/JRRE

[4] F. Alonso-Fernandez, P. Tome-Gonzalez, V. Ruiz-Albacete, dan J. Ortega-Garcia, "Iris Recognition Based on SIFT Features."

[5] N. Harun dan M. Shamian Zainal, "Development of Face Recognition Smart Door Lock System Using ESP32-CAM and Telegram Application As Media Control and Monitoring," *Progress in Engineering Application and Technology*, vol. 4, no. 2, hlm. 35–048, 2023, doi: 10.30880/peat.2023.04.02.004.

[6] I. Sumarsono dan K. Harefa, "LOGIC : Jurnal Ilmu Komputer dan Pendidikan PERANCANGAN SISTEM APLIKASI ABSENSI MENGGUNAKAN FACE RECOGNITION DAN LOKASI BERBASIS ANDROID PADA PT. TRANS CORP FOOD AND BEVERAGE." [Daring]. Tersedia pada: https://journal.mediapublikasi.id/index.php/logic

[7] M. Steeven, H. Pratiwi, and S. Lailiyah, "Penerapan Metode Rapid Application Development Untuk Perancangan Arsitektur Presensi Berbasis Pengenalan Wajah dengan Amazon Web Service (AWS) Pada STMIK Widya Cipta Dharma," 2025.

[8] A. Pratama, R. Nugroho, dan D. Setiawan, "Prototype of Smart Monitoring System Based on Internet of Things," Inotera: Jurnal Informatika dan Teknologi Rekayasa, 2024.

[9] R. Saputra dan A. Ramadhan, "ESP32-Based Smart Home Security System," Inotera: Jurnal Informatika dan Teknologi Rekayasa, vol. 3, no. 2, 2022.

[10] M. Hidayat, L. Kurniawan, dan S. Fadillah, "IoT-Based Home Security Monitoring System," Inotera: Jurnal Informatika dan Teknologi Rekayasa, vol. 2, no. 1, 2021.