Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Design and Implementation of a Prototype Smart Door Lock Integrating Face Recognition and Smart Doorbell for Residential Access Control

Farah Atriani
Hasanuddin University
Ida Laila
Hasanuddin University
Arifin Arifin
arifinpide@gmail.com

Hasanuddin University

Research Article

Keywords: Smart Door Lock, Face Recognition, Residential Access Control, Smart Doorbell, Edge Artificial Intelligence, Internet of Things

Posted Date: September 24th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10353667/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Design and Implementation of a Prototype Smart Door Lock Integrating Face Recognition and Smart Doorbell for Residential Access Control

Farah Atriani[1], Ida Laila[1], Arifin Arifin[1*]
[1]Department of Physics, Faculty of Mathematics and Natural Sciences,
Hasanuddin University, Indonesia

*Corresponding author(s). E-mail(s): arifinpide@gmail.com;
Contributing authors: atrianif21h@student.unhas.ac.id;
ida_laila@science.unhas.ac.id

Abstract

Conventional residential door security systems generally rely on physical keys and often lack integrated user authentication and remote access management. This study presents the design and implementation of a prototype smart door lock that integrates face recognition, a smart doorbell, and remote access control for residential access management. The proposed system employs YOLOv8n for face detection, FaceNet for facial feature extraction, and cosine similarity for identity verification, while Blynk and Supabase support remote monitoring, visitor notifications, image storage, and mobile-based access control. Experimental results show that the face detection model achieved a detection rate of 100% at distances up to 300 cm. Face recognition achieved an accuracy of 92.44%, with 100% precision and specificity, while the prototype successfully authenticated registered users with a success rate of 91.11% and rejected all unregistered users. Furthermore, visitor notifications and remote door unlocking were completed with average response times of 2.60 s and 0.90 s, respectively. These results demonstrate that the proposed prototype provides an effective and reliable solution for integrating face-based authentication, visitor management, and remote access control in residential environments.

Keywords: Smart Door Lock, Face Recognition, Residential Access Control, Smart Doorbell, Edge Artificial Intelligence, Internet of Things

1 Introduction

Residential environments have evolved from simple rule-based automation systems to smart homes that leverage Internet of Things (IoT) connectivity and, more recently,

to intelligent residential environments through the integration of Artificial Intelligence (AI). This evolution reflects a paradigm shift from systems that merely execute predefined commands to systems capable of providing adaptive services based on information acquired from both the surrounding environment and users. Consequently, modern residential systems are expected not only to automate household devices but also to deliver intelligent, efficient, and user-oriented services [1].

Home automation has been widely adopted to improve daily living by enhancing comfort, energy efficiency, safety, and security. Among these applications, residential security has received considerable attention because it is directly related to occupant protection and access management. Therefore, access control systems have become an essential component of home automation architectures, enabling monitoring, visitor management, and remote control of security devices to improve both residential security and user convenience [2].

Various authentication methods have been employed in door access control systems, ranging from knowledge-based authentication to hardware-based authentication using physical keys, access cards, or badges, as well as biometric authentication. Although conventional authentication methods remain widely used, they are susceptible to several limitations, including forgotten credentials, loss or theft of physical media, and credential forgery, all of which increase the risk of unauthorized access. Biometric authentication has therefore emerged as a promising alternative because it relies on unique physiological characteristics that are difficult to duplicate, providing a more reliable and secure authentication mechanism [3,4].

Among biometric technologies, face recognition has become one of the most widely adopted approaches because it enables contactless user identification using either images or video. Recent advances in deep learning have substantially improved face recognition accuracy, leading to its widespread application in surveillance, authentication, and access control systems. These advantages make face recognition a promising solution for developing intelligent, practical, and efficient residential security systems [5].

A modern face recognition system generally consists of three sequential stages: face detection, feature representation, and identity verification. During the verification process, facial features extracted from an input image are compared with reference features stored in a database to determine user identity. Accordingly, both feature extraction and identity matching play critical roles in determining overall recognition

performance. Considering the computational limitations of embedded edge devices, lightweight deep learning models are particularly attractive because they provide an effective balance between recognition accuracy and inference efficiency [6,7].

Previous studies have demonstrated the potential of IoT technologies and face recognition for improving residential access security. A biometric attendance system based on MTCNN and FaceNet achieved high face recognition accuracy for user authentication [8]. An IoT-based smart door lock system integrated visitor monitoring, remote door control, a smart doorbell, and automated security notifications through an ESP32-CAM platform [9]. Face detection using the YOLO algorithm has also been employed to replace RFID-based authentication in door security systems [10]. Furthermore, the IoT-MFaceNet framework combined MobileNetV2 and FaceNet to enable efficient face recognition on Raspberry Pi devices [11], while another Raspberry Pi-based smart door lock integrated face recognition with remote monitoring to improve access security [7].

Despite these advances, among the studies reviewed in this manuscript have focused on specific functionalities, such as biometric authentication, remote door control, or IoT-based monitoring, rather than integrating these capabilities into a unified residential security system. For example, although the IoT-based system in [9] supports remote access control, visitor monitoring, and smart doorbell functionality, it does not employ face recognition for user authentication. Conversely, face recognition-based systems primarily concentrate on user identification while providing limited support for visitor interaction and suspicious activity monitoring prior to access authorization. These limitations indicate the need for an integrated residential access control system that combines face recognition, IoT services, and intelligent visitor management within a single framework.

Motivated by these challenges, this study proposes the design and implementation of a Raspberry Pi-based AIoT smart door lock prototype that integrates face recognition with smart doorbell functionality for residential access control. The proposed system employs YOLOv8n for face detection, FaceNet for facial feature extraction, and cosine similarity for identity verification. In addition, a rule-based mechanism is incorporated to identify suspicious activities when visitors fail to press the doorbell within a predefined time interval, enabling automatic notifications to be delivered through the Blynk mobile application. By integrating biometric authentication, visitor monitoring, remote access authorization, and IoT connectivity into a unified

prototype, the proposed system provides a practical and low-cost AIoT solution for intelligent residential access control.

2 Methods

2.1 Systems Design

The proposed system consists of hardware, software, and cloud service modules integrated through a Raspberry Pi 4B, which serves as the central controller. The hardware module comprises a passive infrared (PIR) sensor, a Raspberry Pi Camera Module, a reed switch sensor, a push button, a solenoid door lock controlled via a relay module, a buzzer, and an I²C LCD. Sensor data are acquired through the Raspberry Pi General Purpose Input/Output (GPIO) interface, whereas facial images are captured through the Camera Serial Interface (CSI).

When motion is detected by the PIR sensor, the camera captures a facial image for identity verification. Based on the verification result, the Raspberry Pi determines the access decision. If the detected face matches a registered user, the relay module is activated to unlock the solenoid door lock. Otherwise, the door remains locked and the system switches to the smart doorbell mechanism, allowing the homeowner to authorize access remotely through a mobile application. The overall system architecture is illustrated in Fig. 1.

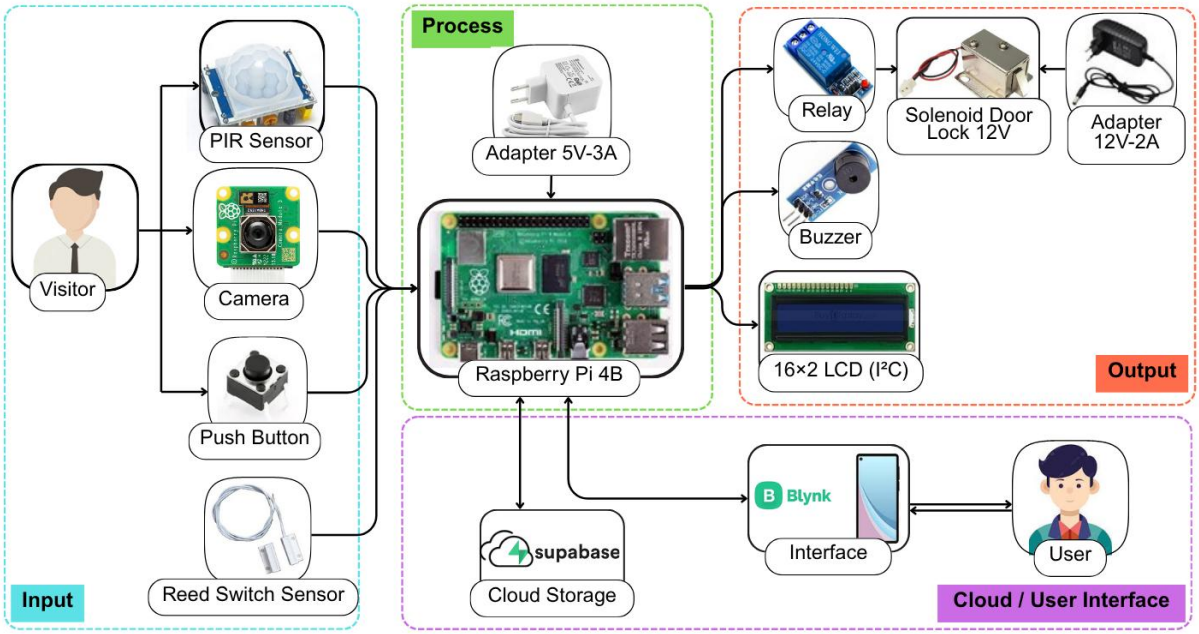


Fig. 1 Proposed system architecture

In addition to controlling the door access mechanism, the Raspberry Pi communicates with cloud services to support remote monitoring and access control.

The Blynk platform is used to exchange system status, door status, notifications, and remote door unlocking commands. Meanwhile, Supabase Storage stores images of unrecognized visitors and generates public URLs that are transmitted to the Blynk application for visualization through the Image Gallery widget. This integration enables homeowners to monitor system activities and respond to access requests in real time.

2.2 Operasional Workflow

The operational workflow describes the decision-making process for residential access control based on face verification results. The workflow begins when the PIR sensor detects motion in front of the door, triggering the camera to capture a facial image for identity verification. If the detected face matches a registered user, the door lock is automatically released. Otherwise, the LCD displays the message "Please Press the Doorbell", and the system waits for the visitor to press the doorbell button within 20 s.

If the doorbell button is pressed, a "Visitor" notification is sent to the homeowner through the Blynk application, and the system waits up to 30 s for a remote access authorization. When access is granted, the door lock is released; otherwise, the LCD displays "No Response" after the waiting period expires. If the visitor does not press the doorbell within 20 s, the system classifies the event as suspicious activity and automatically sends a "Suspicious Activity" notification to the homeowner. The operational workflow of the proposed system is illustrated in Fig. 2.

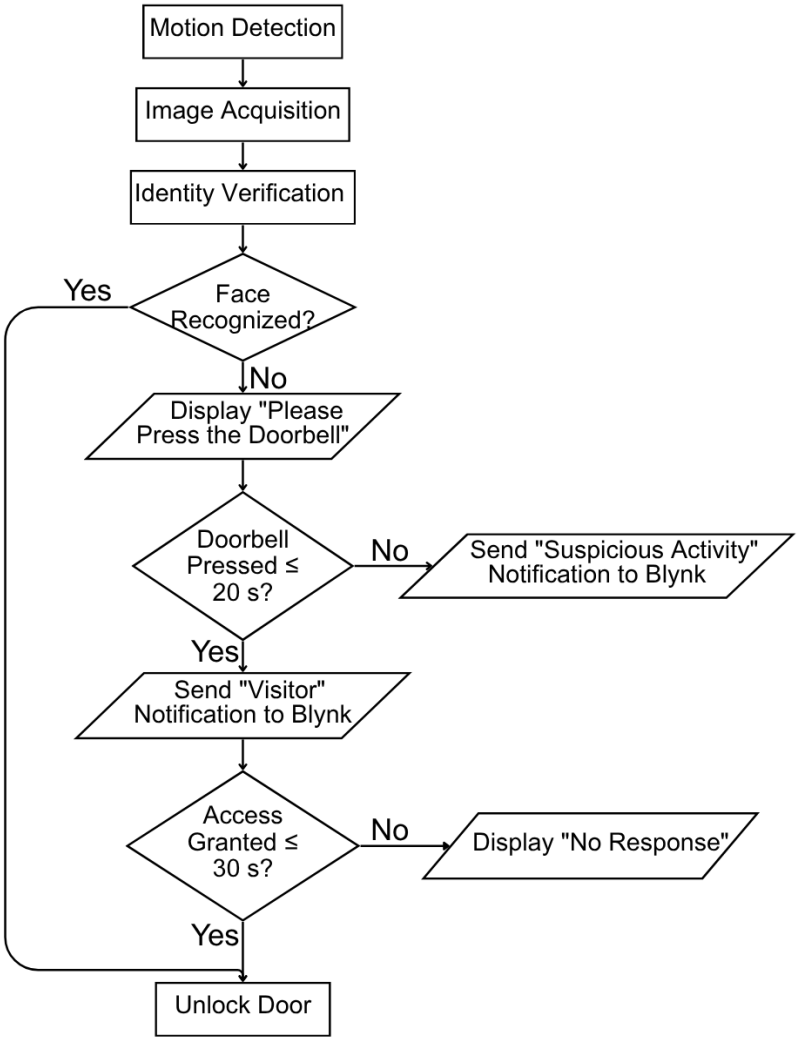


Fig. 2 Operational workflow of the proposed residential access control system

2.3 Face Recognition Module

The proposed face recognition module combines YOLOv8n for face detection and FaceNet for facial feature extraction. YOLOv8n was selected because of its lightweight architecture and fast inference speed, making it suitable for deployment on resource-constrained edge devices such as the Raspberry Pi. FaceNet was employed to generate a 512-dimensional face embedding that represents each facial identity for the subsequent verification process [12 – 14]. [13][14]

The YOLOv8n model was obtained through fine-tuning using the pretrained yolov8n.pt weights on the WIDER FACE dataset [15]. Before training, the dataset was preprocessed through auto-orientation, resizing to 640 × 640 pixels, conversion into the YOLO annotation format using Roboflow, and filtering based on bounding box size to reduce the dominance of images containing extremely small faces. The dataset was subsequently divided into training and validation subsets, as summarized in Table 1.

Table 1 Dataset distribution

Category	Number of Images	Percentage
Training Data	5,899	80.03%
Validation Data	1,472	19.97%
Total	**7,371**	**100%**

The model was trained in Google Colaboratory for 100 epochs with a batch size of 16 using lightweight data augmentation to improve generalization capability. The best-performing model on the validation set was automatically saved as best.pt and subsequently converted to the ONNX format (best.onnx) for deployment on the Raspberry Pi. Model performance was evaluated using Intersection over Union (IoU), precision, recall, mAP@50, and mAP@50–95. IoU measures the overlap between the predicted bounding box and the ground-truth annotation, whereas precision and recall evaluate the correctness and completeness of face detection based on the numbers of true positives (TP), false positives (FP), and false negatives (FN) [16]. These metrics are computed using Eqs. (1) - (3).

$$IoU = \frac{Area_{pred} \cap Area_{\mathrm{gt}}}{Area_{pred} \cup Area_{\mathrm{gt}}} \tag{1}$$

$$Precision = \frac{TP}{TP+FP} \tag{2}$$

$$Recall = \frac{TP}{TP+FN} \tag{3}$$

The face recognition workflow is illustrated in Fig. 3. First, YOLOv8n detects the facial region from the input image. The detected face is then cropped and resized before being processed by the TensorFlow Lite implementation of FaceNet to generate a 512-dimensional face embedding. The resulting embedding is compared with the reference embeddings stored in the face database using cosine similarity. A face is considered recognized when the cosine similarity exceeds the threshold determined through Receiver Operating Characteristic (ROC) analysis; otherwise, it is considered unrecognized [17]. Cosine similarity is calculated using Eq. (4).

$$\textit{Cosine similarity} = \frac{A.B}{\|A\|\|B\|} = \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2}\sqrt{\sum_{i=1}^{n} B_i^2}} \tag{4}$$

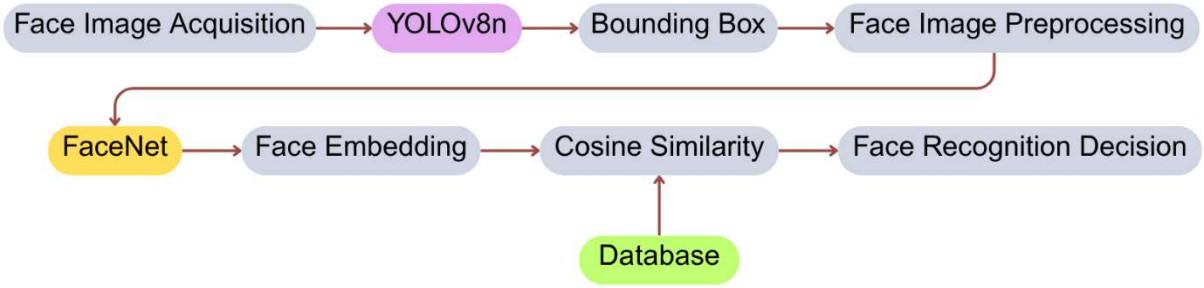


Fig. 3 Face recognition workflow

2.4 Face Database Construction

The face database was constructed from facial images acquired from registered users during the image acquisition stage. The selected reference images were subsequently augmented to increase facial representation under variations in orientation, illumination, contrast, sharpness, and image quality. The augmentation parameters used in this study are summarized in Table 2.

Table 2 Data augmentation parameters for face database construction

Augmentation Type	Value	Description
Rotation	-15°, -10°, -5°, 5°, 10°, 15°	Changes the face orientation
Brightness	1.2, 1.5, 1.8	Increases image brightness
Darkness	0.8, 0.6, 0.4	Decreases image brightness
Contrast	0.8, 1.3, 1.6	Adjusts image contrast
Sharpness	0.7, 1.5, 2.0	Enhances facial details
Gaussian Blur	1 dan 2	Applies image blurring
Horizontal Flip	Enabled	Performs horizontal mirroring

As illustrated in Fig. 4, each augmented image was first processed by YOLOv8n to detect the facial region. The detected face was then cropped and resized before being processed by FaceNet to generate a 512-dimensional face embedding representing the user's facial characteristics. Finally, the embeddings corresponding to each registered user were averaged to obtain a centroid, which served as the reference representation during the identity verification process.

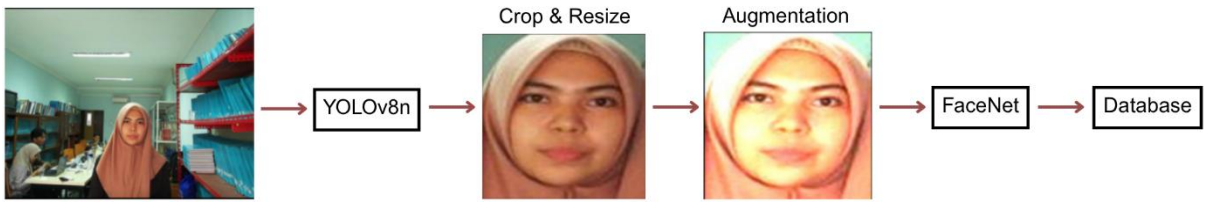


Fig. 4 Face database construction process

2.5 Dataset Acquisition

Dataset acquisition was conducted to collect facial images for face detection evaluation, face database construction, and face recognition evaluation. All images were captured using a Raspberry Pi Camera Module mounted at a fixed position and adjusted to approximately match the average height of the participants. Data acquisition was performed indoors under controlled illumination provided by room lighting supplemented with natural daylight from nearby windows.

For face detection evaluation, images were collected from 10 participants in a frontal pose at distances ranging from 50 cm to the maximum evaluation distance with 50 cm intervals. Ten images were acquired for each participant at every distance. For face recognition evaluation, the dataset consisted of 10 registered and 10 unregistered participants. Each participant was recorded in three facial poses, namely frontal, three-quarter right (¾ right), and three-quarter left (¾ left), with 10 images captured for each pose. Images of registered users were subsequently used to construct the face database following the procedure described in Section 2.4.

2.6 Recognition Threshold Determination

The recognition threshold was determined to establish the decision boundary for the face verification process. The threshold was obtained from the distribution of cosine similarity values between genuine (registered) and impostor (unregistered) face pairs. ROC analysis was employed to evaluate the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) over a range of threshold values [18]. TPR and FPR were calculated using Eq. (5) and (6).

$$TPR = \frac{TP}{TP+FN} \tag{5}$$

$$FPR = \frac{FP}{FP+TN} \tag{6}$$

The optimal threshold was selected using the Youden Index, which is defined in Eq. (7). Since specificity can be expressed as $1 - FPR$, the Youden Index can be reformulated as Eq. (8). The threshold corresponding to the maximum Youden Index was adopted as the operating threshold for all subsequent face recognition experiments [18].

$$J = Sensitivity + Specificity - 1 \tag{7}$$

$$J = TPR - FPR \tag{8}$$

2.7 User Interface Module Design

The user interface module was developed using the Blynk platform to provide system monitoring and control functionalities for the smart door lock through a smartphone. The interface consists of a mobile dashboard, Virtual Pins (VPins), and an event notification feature. Each VPin is associated with a specific widget on the dashboard to display system status, door status, visitor images, last access information, and receive door-opening commands from users. Guest images and suspicious activities are displayed through the Image Gallery widget using public URLs generated by Supabase Storage, while notifications are delivered to users through the event notification feature provided by the Blynk application. Through this interface, users can monitor system conditions and remotely authorize access via mobile devices. The VPin configuration implemented in the proposed system is presented in Table 3.

Table 3 VPin configuration and corresponding functions

VPin	Widget	Description
V0	Button	Provides access authorization to unlock the door
V1	Status / Label	Displays the system status
V2	LED	Indicates the door status
V3	Image Gallery	Displays guest images or suspicious activity images
V4	Status / Label	Displays information and timestamp of the latest access

2.8 System Evaluation

The proposed system was evaluated from three perspectives: face detection, face recognition, and overall system performance. Face detection performance was evaluated to assess the capability of the YOLOv8n model in detecting faces at different testing distances. A confidence threshold of 0.7 was applied to suppress low-confidence detections, ensuring that only reliable detection results were considered during the evaluation [19]. The detection performance was quantified using the Detection Rate (DR), defined as the ratio between the number of correctly detected faces and the total number of actual faces in the test dataset [20], as expressed in Eq. (9).

$$DR = \frac{Number\ of\ Correct\ Detections}{Total\ Number\ of\ Actual\ Faces} \tag{9}$$

Face recognition performance was evaluated using a confusion matrix consisting of true positive (TP), true negative (TN), false positive (FP), and false negative (FN). A

true positive represents a registered face that is correctly recognized, whereas a true negative represents an unregistered face that is correctly rejected. A false positive indicates an unregistered face that is incorrectly recognized as a registered user, while a false negative denotes a registered face that fails to be recognized. Based on these outcomes, the recognition performance was evaluated using accuracy, precision, recall, and F1-score, as defined in Eqs. (10) – (13) [20 – 22]. [21][23][22]

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{10}$$

$$Precision = \frac{TP}{TP+FP} \tag{11}$$

$$Recall = \frac{TP}{TP+FN} \tag{12}$$

$$F1-score = 2 \times \frac{precision \times recall}{precision+recall} \tag{13}$$

Overall system performance was evaluated by measuring the operational success of the proposed prototype, including automatic door unlocking for registered users, access rejection for unregistered users, smart doorbell operation, suspicious activity notification, and communication between the Raspberry Pi and the Blynk application. In addition to the success rate of each testing scenario, the system response time was measured to evaluate the operational performance and responsiveness of the proposed system.

The system response time was defined as the time interval between a triggering event and the corresponding system output. Depending on the evaluation scenario, response time was measured using a combination of automatic timestamp recording within the program and manual measurement using a stopwatch. The response time and the average response time were calculated using Eqs. (14) and (15), respectively. The response time measurement scenarios, including the observed trigger conditions and system outputs, are summarized in Table 4.

$$T_{response} = T_{output} - T_{trigger} \tag{14}$$

$$\bar{T} = \frac{\sum T_{response}}{n} \tag{15}$$

Table 4 Response time measurement scenario

Scenario	Trigger	Output
Recognized User	Motion detected	Solenoid lock activated

Unrecognized User	Motion detected	“Please press the doorbell” instruction displayed
Doorbell Operation	Doorbell button pressed	Notification sent
Access Granted	Access authorization button pressed on Blynk	Solenoid lock activated
No Response	Doorbell button pressed	Access denied after owner authorization timeout
Suspicious Activity	Unrecognized face detected and doorbell authorization timeout	Notification sent

3 Result and Discussion

3.1 Prototype Implementation

The proposed residential access control system was successfully implemented as a functional prototype integrating hardware, edge artificial intelligence, and Internet of Things (IoT) services. The prototype consists of a Raspberry Pi 4B as the central controller, a PIR sensor for motion detection, a camera module for facial image acquisition, a reed switch for door status monitoring, a push button serving as the smart doorbell trigger, a relay-controlled solenoid door lock, a buzzer as an audible indicator, and an I^2C LCD for displaying system messages. The prototype implementation is presented in Fig. 5.

The Raspberry Pi executes all AI processes locally, including face detection using YOLOv8n, feature extraction using FaceNet, and identity verification based on cosine similarity. In addition to controlling the door locking mechanism, the Raspberry Pi communicates with the Blynk platform for remote monitoring, visitor notifications, and access control, while Supabase Storage is used to store images of unrecognized visitors and provide image links for display within the Blynk application. The integration of these components enables the prototype to perform face authentication, smart doorbell operation, visitor monitoring, and remote access control within a unified residential access system.

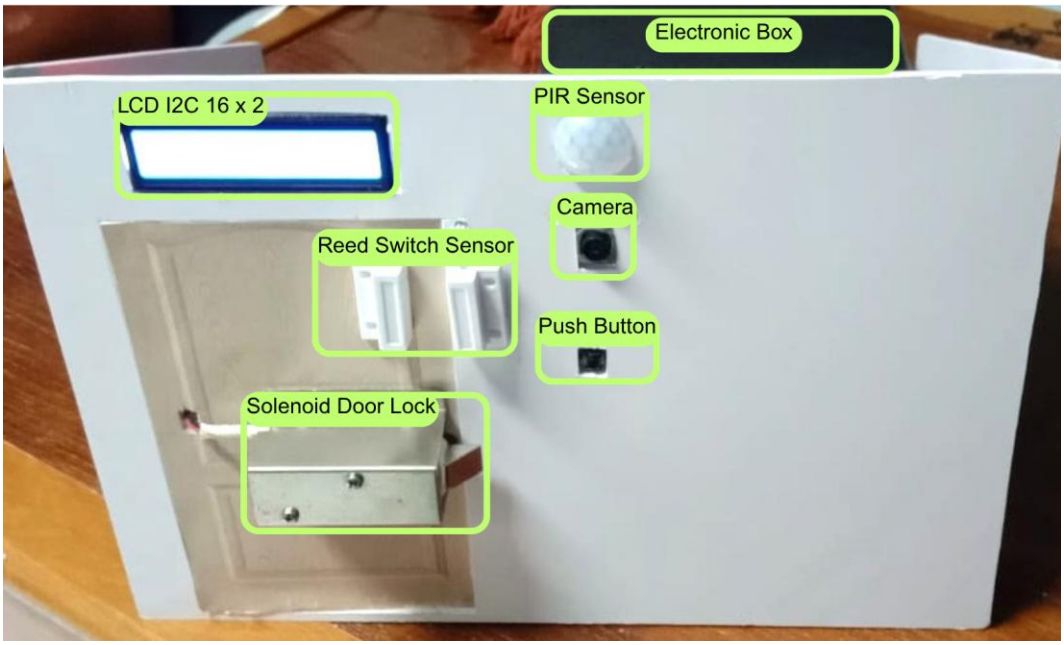


Fig. 5 Prototype implementation of the proposed residential access control system

3.2 YOLOv8n Detection Performance

The YOLOv8n model was trained for 100 epochs using the prepared face dataset. During training, the model performance was evaluated using mAP@50 and mAP@50–95, as illustrated in Fig. 6. The mAP@50 increased rapidly during the early training epochs and gradually converged after approximately 40 epochs, reaching 0.976 at the end of training. Meanwhile, mAP@50–95 exhibited a steady improvement throughout the training process and achieved 0.689 after 100 epochs. These results indicate that the model successfully converged and achieved satisfactory detection performance for subsequent deployment in the proposed system.

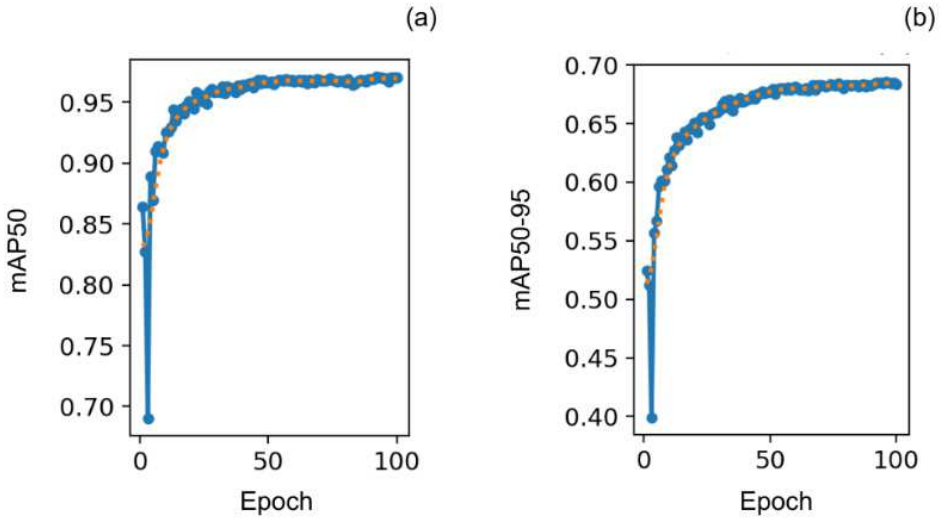


Fig. 6 YOLOv8n training performance: (a) mAP@50 and (b) mAP@50–95

The best-performing model on the validation dataset was automatically saved as best.pt and subsequently used throughout the experimental evaluation. A summary of the model performance is presented in Table 5. The trained model achieved a precision of 0.962, recall of 0.933, mAP@50 of 0.976, and mAP@50–95 of 0.689, demonstrating a high level of face detection performance.

Table 5 Performance metrics of the trained YOLOv8n model

Metrics	Value
Precision	0.962
Recall	0.933
mAP50	0.976
mAP50-95	0.689

3.3 Face Detection Evaluation

The face detection performance of the implemented system was evaluated at different camera-to-subject distances using a confidence threshold of 0.7. The results are presented in Fig. 7, showing that the system maintained a 100% detection rate over the distance range of 50–300 cm. Beyond 300 cm, the detection rate gradually decreased, reaching approximately 45% at 400 cm and 31% at 450 cm. These results indicate that the ability of the deployed YOLOv8n model to detect faces declined as the apparent facial size decreased with increasing acquisition distance.

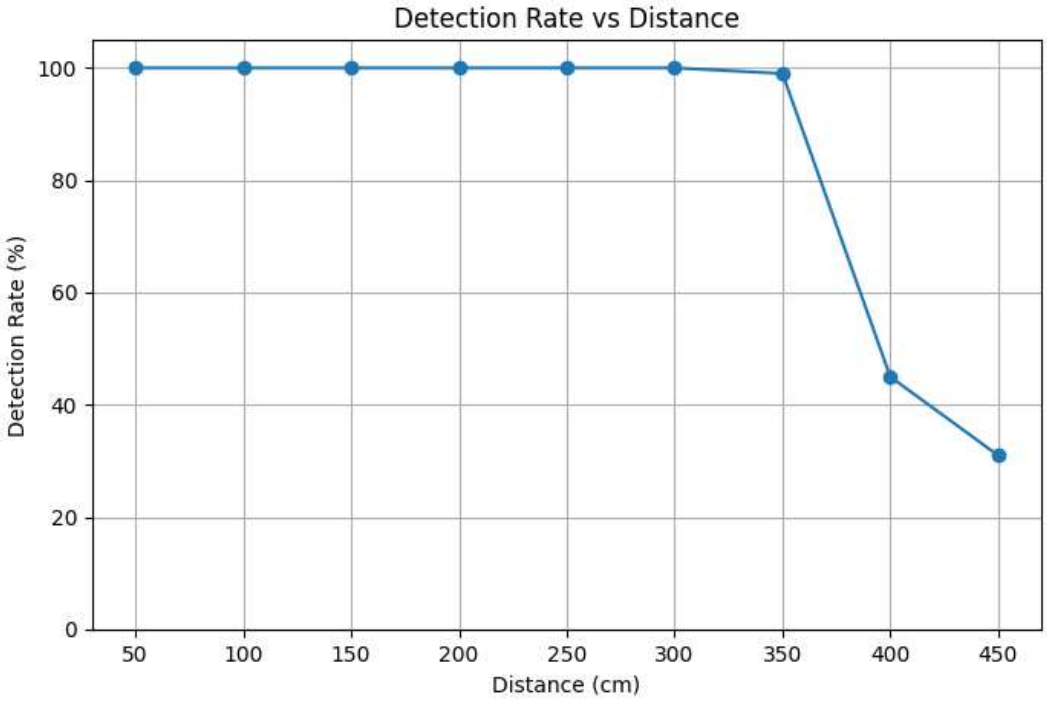


Fig. 7 Detection rate of the proposed face detection system at different acquisition distances

To further investigate the detector performance, the relationship between the acquisition distance and the confidence score was analyzed, as shown in Fig. 8. Linear regression produced the following relationship:

$$y = -0.000373x + 0.920 \quad (16)$$

with a coefficient of determination of $R^2 = 0.9737$, indicating a strong negative linear relationship between the acquisition distance and the confidence score. As the distance increased, the confidence score consistently decreased. Furthermore, the error bars became noticeably larger beyond 350 cm, suggesting greater variability in detection confidence when the facial region occupied fewer pixels in the captured image. Variations in facial characteristics among participants may also contribute to this increased variability.

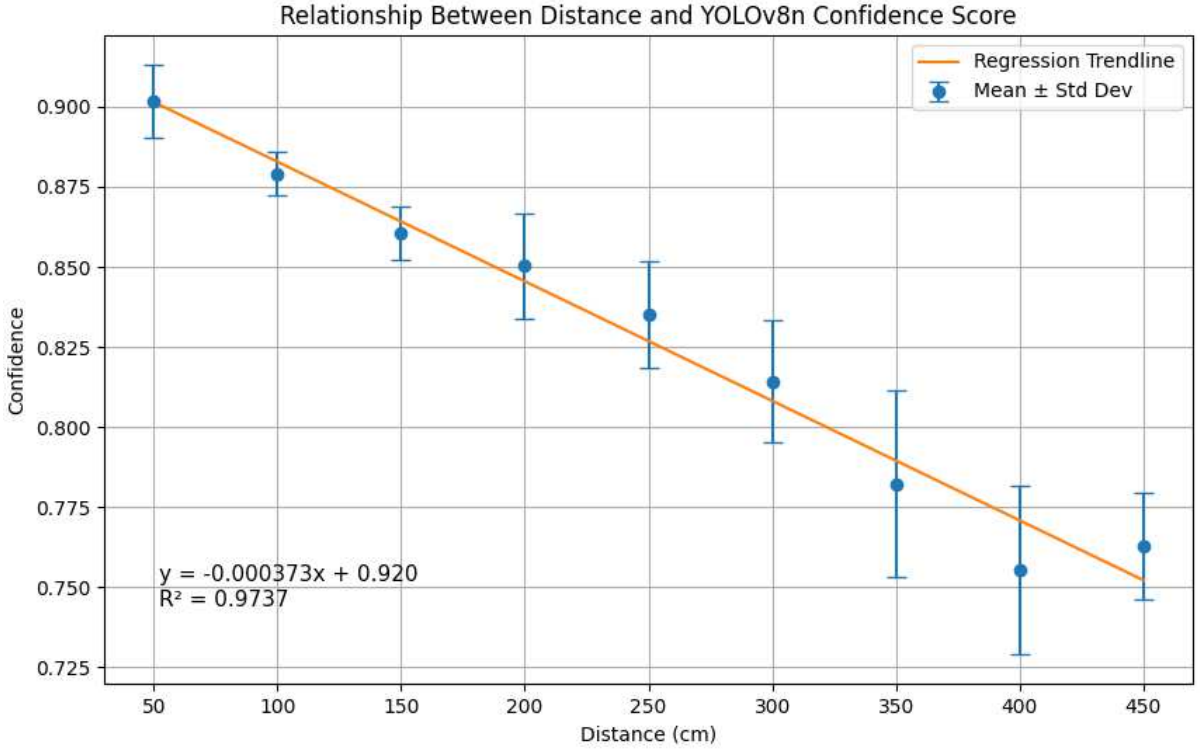


Fig. 8 Relationship between acquisition distance and the confidence score of the deployed YOLOv8n face detector

Representative face detection results at different acquisition distances are presented in Fig. 9. The system consistently detected faces with high confidence at distances between 50 cm and 250 cm. In contrast, missed detections began to appear at 400–450 cm, where one participant was no longer detected while another remained detectable. These observations indicate that face detection performance is influenced not only by the acquisition distance but also by facial characteristics and image quality. Based on these findings, the operational distance of the proposed system was

established at 50–150 cm, where face detection remained both accurate and stable. Within this operating range, facial images acquired at 100 cm were selected as the reference images for constructing the face database.



Fig. 9 Representative face detection results at different acquisition distances: (a)–(b) 50 cm, (c) 400 cm, and (d) 450 cm

3.4 Recognition Threshold Selection

The optimal threshold for face recognition was determined using ROC analysis. The threshold was selected by evaluating the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) over a range of cosine similarity thresholds. The ROC curve obtained from the evaluation is presented in Fig. 10.

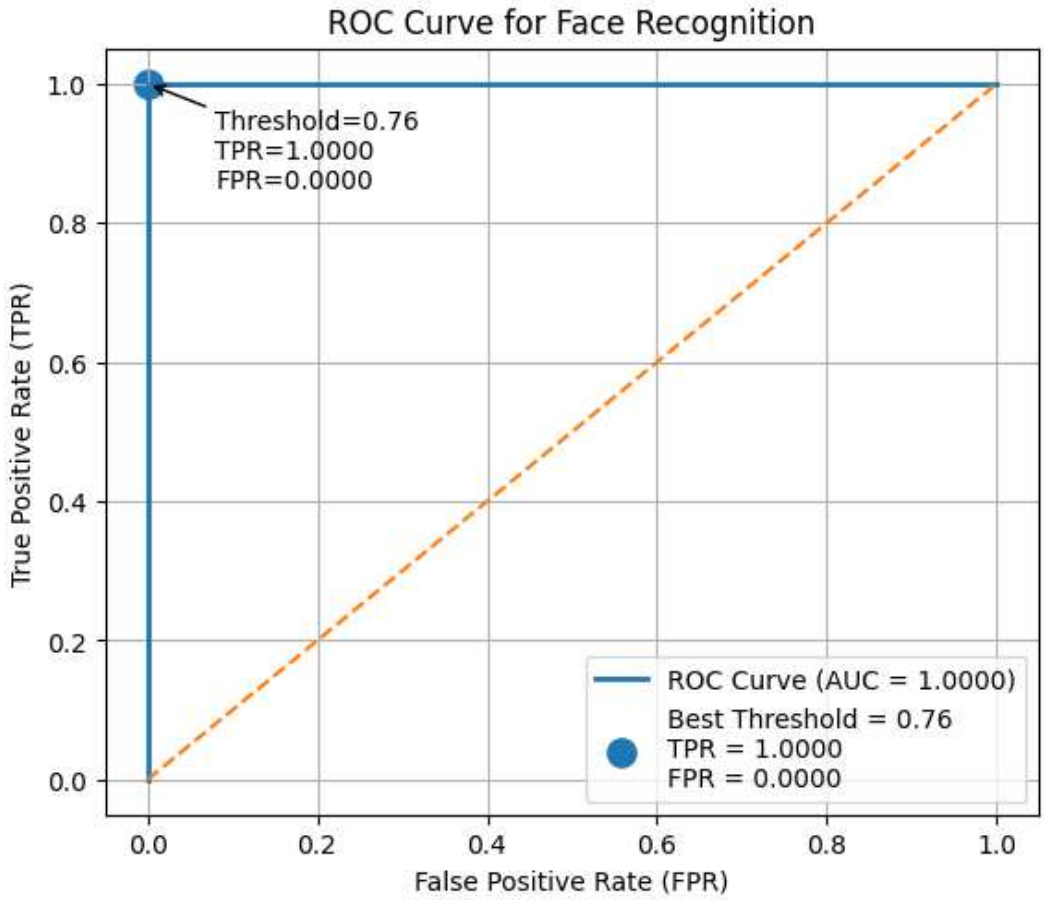


Fig. 10 ROC curve used for determining the optimal cosine similarity threshold

As shown in Fig. 10, the Area Under the Curve (AUC) reached 1.00, indicating excellent discriminative capability of the proposed face recognition system. Based on the ROC analysis, a cosine similarity threshold of 0.76 was selected as the optimal operating point because it provided the best balance between recognizing registered users and rejecting unregistered users. This threshold was subsequently applied throughout all face recognition experiments.

3.5 Face Recognition Performance

Face recognition was evaluated using 1,800 facial images, comprising 900 registered and 900 unregistered face images. To investigate the effect of the recognition threshold on system performance, experiments were conducted using threshold values ranging from 0.75 to 0.78, centered around the value obtained from the ROC analysis. The results are summarized in Table 6.

Table 6 Recognition results at different cosine similarity thresholds

Threshold	TP	FP	TN	FN
0.75	764	8	900	136
0.76	764	0	900	136

0.77	726	0	900	174
0.78	674	0	900	226

Based on Table 6, increasing the recognition threshold reduced the number of TP while increasing the number of FN, whereas the number of TN remained unchanged. At a threshold of 0.75, the system produced eight FP. These FP identifications were completely eliminated at a threshold of 0.76 without increasing the number of FN. Further increasing the threshold to 0.77 and 0.78 resulted in fewer correctly recognized registered users and a corresponding increase in FN. Therefore, a threshold of 0.76 was selected as the operational threshold because it provided the best balance between correctly recognizing registered users and rejecting unregistered users. The confusion matrix obtained at the selected threshold is presented in Fig. 11.

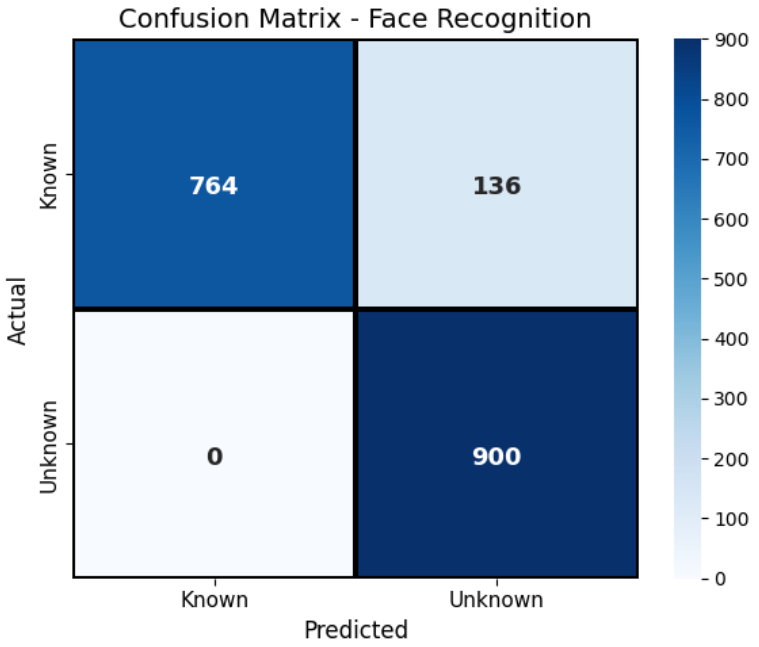


Fig. 11 Confusion matrix of the proposed face recognition system at the selected threshold

The confusion matrix shows that the proposed system correctly recognized 764 registered face samples and correctly rejected all 900 unregistered face samples without producing any false-positive identifications. However, 136 registered face samples failed to be recognized because their cosine similarity scores did not exceed the decision threshold. These results were subsequently used to calculate the evaluation metrics summarized in Table 7.

Table 7 Face recognition performance metrics

Metrics	Value (%)
Accuracy	92.44
Precision	100
Recall	84.89
Specificity	100
F1-Score	91.83

Based on Table 7, the proposed system achieved an accuracy of 92.44%, precision of 100%, recall of 84.89%, specificity of 100%, and an F1-score of 91.83%. The perfect precision and specificity indicate that all unregistered users were successfully rejected without producing any false-positive identifications. In contrast, the recall of 84.89% indicates that a proportion of the registered users could not be successfully recognized. Nevertheless, the F1-score demonstrates that the proposed system maintained a good balance between precision and recall. To further investigate the false-negative cases, additional experiments were conducted to evaluate the effects of acquisition distance and facial pose. The results are presented in Table 8.

Table 8 Recognition accuracy under different acquisition distances and facial poses

Distance (cm)	Accuracy by Facial Pose (%)		
	Frontal	Three-Quarter Left	Three-Quarter Right
50	99.5	97.5	99.0
100	97.0	91.5	94.5
150	86.0	87.0	80.0

As shown in Table 8, the face recognition accuracy gradually decreased as the acquisition distance increased. At 50 cm, all facial poses achieved recognition accuracies above 97%. At 100 cm, the recognition accuracy slightly decreased but remained above 90% for all poses. A more pronounced performance degradation was observed at 150 cm, particularly for the three-quarter right pose, where the recognition accuracy decreased to 80.0%. These findings indicate that increasing the acquisition distance reduces the amount of facial information captured by the camera, thereby affecting feature extraction and identity matching. Furthermore, non-frontal facial poses reduce the visibility of certain facial characteristics, which also contributes to

lower recognition performance. Representative recognition results for both registered and unregistered users are presented in Table 9.

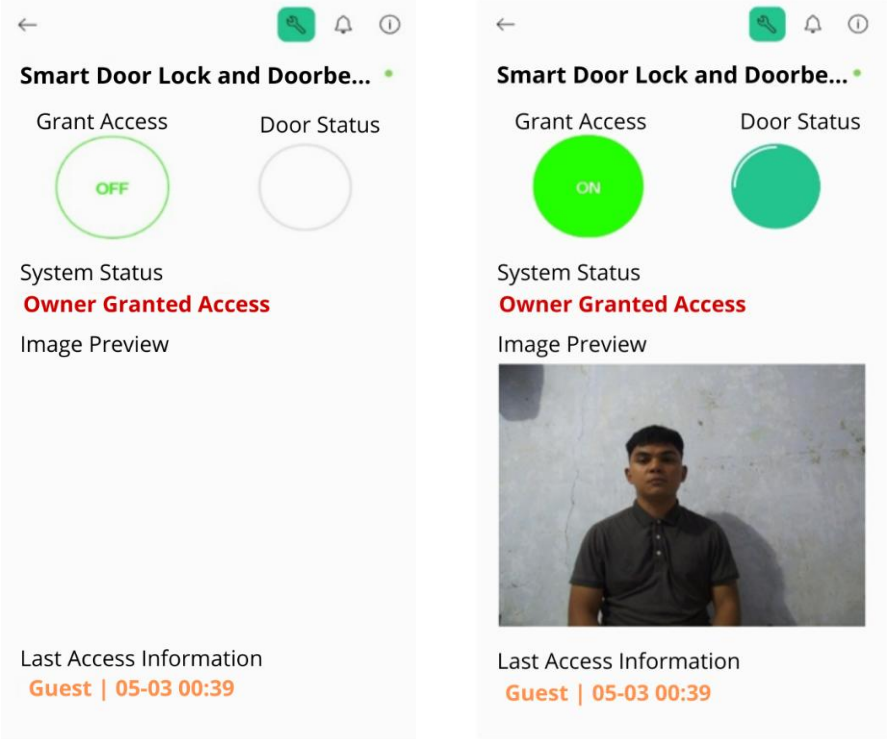
Table 9 Representative face recognition results for registered and unregistered users

Subject	Pose	Distance	
		50 cm	150 cm
Registered User	Frontal		
Registered User	Three-Quarter Left, Three-Quarter Right		
Unregistered User	Frontal		

The proposed face recognition system achieved an overall accuracy of 92.44%, while maintaining 100% precision and 100% specificity, indicating that all unregistered users were correctly rejected without producing any False Positive (FP) identifications. This accuracy is slightly lower than those reported in previous studies, which achieved 94.4% using a YOLO-based smart door lock system [10] and 95% using a face recognition system combining MTCNN and FaceNet [8]. The differences are likely attributable to variations in the dataset, the number of participants, image acquisition conditions, experimental configurations, and deployment platforms. Nevertheless, the absence of false-positive identifications demonstrates that the proposed system provides a high level of reliability in preventing unauthorized access. This characteristic is particularly important for residential access control systems because granting access to unauthorized users generally poses greater security risks than denying access to authorized users.

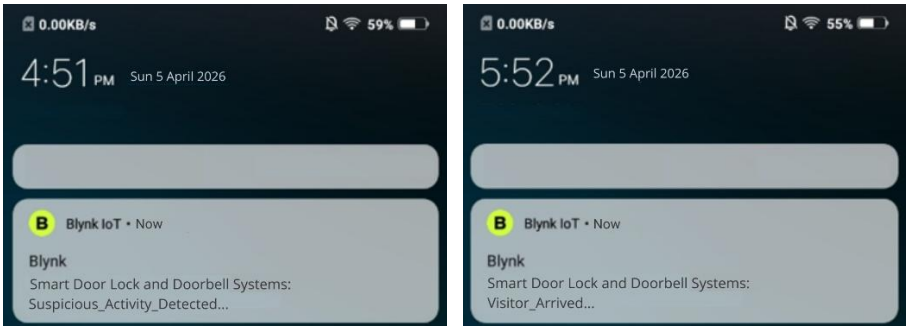
3.6 Blynk Implementation

The implementation of the Blynk user interface successfully supports real-time system monitoring and remote access control. The mobile dashboard displays the system status, door status, the most recent access information, and images of visitors or suspicious activities transmitted from the Raspberry Pi through the Supabase service. In addition, the homeowner can remotely grant door access through the dashboard after receiving a visitor notification. The implemented mobile dashboard is shown in Fig. 12, while examples of the notifications received by the homeowner for visitor and suspicious activity events are presented in Fig. 13.



(a) (b)

Fig. 12 Blynk interface: (a) developed mobile dashboard and (b) mobile dashboard during system operation after receiving an event trigger



(a) (b)

Fig. 13 Blynk notifications on a smartphone: (a) suspicious activity and (b) visitor notification

3.7 Door Access Control Performance

The face recognition-based door access system successfully granted access to registered users with success rates of 93.33%, 83.33%, and 96.66% at the three evaluated acquisition distances. In contrast, all unregistered users were correctly denied access at every testing distance, resulting in a 100% rejection rate. These results demonstrate that the proposed system effectively prevents unauthorized access by eliminating false acceptance of unregistered users. The experimental results are summarized in Table 10.

Table 10 Performance of the face recognition-based door access system

User Type	Decision	System Decision	Success Rate	Average Response Time (s)
Registered User	50 cm	Access Granted	93.33%	4.50
Registered User	100 cm	Access Granted	83.33%	4.48
Registered User	150 cm	Access Granted	96.66%	4.72
Unregistered User	50 cm	Access Denied	100%	4.39
Unregistered User	100 cm	Access Denied	100%	4.43
Unregistered User	150 cm	Access Denied	100%	4.32

Although the proposed system achieved a high access success rate at all evaluated distances, the performance at 100 cm was slightly lower than that at the other distances. This variation does not indicate a strictly linear relationship with acquisition distance and is likely attributable to differences in image quality during acquisition. Examination of the images automatically transmitted to the Blynk application during failed recognition events revealed that several images were captured while the subject's face was slightly tilted downward rather than directly facing the camera. Consequently, the extracted facial features became less representative, leading to unsuccessful identity matching.

The average system response time ranged from 4.32 s to 4.72 s across all experimental scenarios. The response times exhibited only minor variations with respect to acquisition distance and user type, indicating that changes in acquisition distance within the operating range had little effect on the overall processing time.

Therefore, the proposed system was able to complete user authentication and access control decisions in less than five seconds.

3.8 Smart Doorbell Performance

The smart doorbell system was evaluated to assess its capability to notify the homeowner and respond to decisions made through the Blynk application when an unregistered face was detected. Four experimental scenarios were considered, including visitor notification, remote access authorization, homeowner no-response, and suspicious activity detection. The results are summarized in Table 11.

Table 11 Performance of the smart doorbell system

Scenario	Notification	System Status	Owner Response	Solenoid Status	Average Response Time (s)
1	Sent	Visitor	N / A	Locked	2.60
2	N / A	Visitor	Access Granted	Unlocked	0.90
3	Sent	Visitor	No Response	Locked	33.30
4	Sent	Suspicious Activity	N / A	Locked	26.78

Based on Table 11, the proposed system successfully delivered visitor notifications to the Blynk application with an average response time of 2.60 s. After the homeowner granted remote access through the application, the solenoid door lock was successfully unlocked in every trial, with an average response time of 0.90 s. Conversely, when no response was received from the homeowner, the system maintained the door in the locked state until the predefined timeout elapsed, after which the access request was automatically terminated.

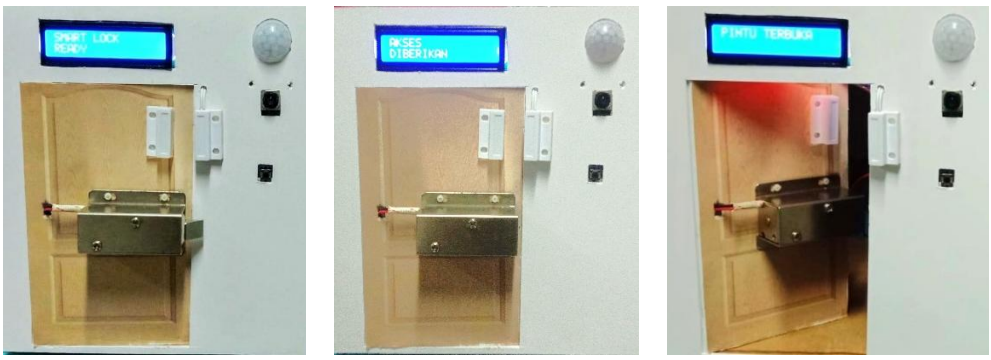
The proposed system also successfully detected situations in which visitors did not press the doorbell button within the specified time limit. Under this condition, the system status changed to Suspicious Activity, a notification was sent to the homeowner, and the solenoid door lock remained locked. These results demonstrate that the proposed system not only supports remote access authorization but also enhances residential security by monitoring potentially suspicious visitor behavior.

Compared with the previously reported IoT-based smart door lock system [9], the proposed system integrates face recognition as the primary identity verification

mechanism in addition to remote access control. Registered users are granted access automatically after successful facial authentication, whereas access requests from unregistered visitors remain under the homeowner's control through the Blynk application. This approach combines biometric authentication and remote access control within a single AIoT-based prototype.

3.9 Smart Door Lock Visualization

The implementation of the access control mechanism on the proposed door prototype is illustrated in Fig. 14. The figure shows three operating conditions: (a) the door in the locked state, (b) the solenoid door lock activated to unlock the door, and (c) the door after being opened by the user. These results confirm that the proposed system successfully controls the door locking mechanism according to the authentication outcome and the corresponding access decision.



(a) (b) (c)

Fig. 14 Operating conditions of the proposed smart door lock prototype: (a) door locked, (b) door unlocked, and (c) door opened

4 Conclusion

This study proposed an Internet of Things (IoT)-based smart door lock system that integrates facial recognition, a smart doorbell, and remote access control to support access control mechanisms in residential environments. The proposed system combines YOLOv8n as the face detection model, FaceNet for facial feature extraction, and cosine similarity as the identity verification method, with seamless integration into the Blynk and Supabase platforms.

The experimental results demonstrated that the system maintained a detection rate of 100% up to a distance of 300 cm, while facial recognition achieved optimal performance within an operational range of 50–150 cm. By applying a cosine similarity threshold of 0.76, the system achieved an accuracy of 92.44%, precision of 100%, recall of 84.89%, specificity of 100%, and an F1-score of 91.83%. Furthermore, the

system successfully granted access to registered users with a success rate of 91.11% while rejecting all unauthorized users. The integration with IoT platforms also enabled real-time system monitoring, notification delivery, and remote access authorization, with response times below five seconds across all primary testing scenarios.

The findings indicate that the integration of edge AI-based facial recognition with IoT services can support a reliable access control mechanism while providing monitoring capabilities and remote access management through mobile devices. Future developments may focus on evaluating system performance under more diverse operational conditions, including variations in illumination, weather conditions, and activity density around the entrance area. In addition, the integration of face anti-spoofing mechanisms, multimodal authentication, alarm systems, and backup power supplies could further enhance the security and reliability of the proposed system for real-world deployment.

Acknowledgements

The authors would like to thank the Department of Physics, Faculty of Mathematics and Natural Sciences, Hasanuddin University, and all parties who supported the system development and testing process.

Author's contributions

Farah Atriani contributed to system design, implementation, data collection, analysis, and manuscript preparation, while Arifin and Ida Laila contributed to supervision, methodological validation, manuscript review, and revision.

Funding

This research received no external funding from public, commercial, or not-for-profit organizations.

Availability of data and materials

The WIDER FACE dataset used in this study is publicly available from its official repository. The private face image dataset collected for system evaluation and testing is not publicly available due to privacy considerations. The source code supporting the findings of this study is available from the corresponding author upon reasonable request.

Declaration Competing interests

The authors declare that they have no competing interests.

Ethics approval and consent to participate

This study did not involve clinical intervention, and facial images used for system testing were obtained with consent from the individuals involved.

References

1. Abdelnaby KM, Al-Husainy MAF, Alhawarat MO, et al (2026) The Intelligent Home: A Systematic Review of Technological Pillars, Emerging Paradigms, and Future Directions. Symmetry (Basel) 18:718. https://doi.org/10.3390/sym18050718
2. Stolojescu-Crisan C, Crisan C, Butunoi BP (2022) Access control and surveillance in a smart home. High-Confidence Comput 2:100036. https://doi.org/10.1016/j.hcc.2021.100036
3. Loume GA, Abana AB, Tonye E, Kabiena Y (2022) Facial Recognition in the Opening of a Door using Deep Learning and a Cloud Service. Int J Intell Syst Appl Eng 10:40–45
4. Elmir Y, Abdelaziz A, Haidas M (2023) Design and Implementation of Embedded Biometric-Based Access Control System with Electronic Lock using Raspberry Pi. J Ilm Tek Elektro Komput dan Inform 9:429–443. https://doi.org/10.26555/jiteki.v9i2.26162
5. Jing Y, Lu X, Gao S (2023) 3D face recognition: A comprehensive survey in 2022. Comput Vis Media 9:657–685. https://doi.org/10.1007/s41095-022-0317-1
6. Lestriandoko NH, Veldhuis R, Spreeuwers L (2022) The contribution of different face parts to deep face recognition. Front Comput Sci 4:958629. https://doi.org/10.3389/fcomp.2022.958629
7. Elnozahy SSFA, Pari SC, Liang LC (2025) Raspberry Pi-Based Face Recognition Door Lock System. Internet of Things 6:31. https://doi.org/10.3390/iot6020031
8. Moulita Andiani F, Soewito B (2021) Face Recognition for Work Attendance using Multitask Convolutional Neural Network (MTCNN) and Pre-Trained FaceNet. ICIC Express Lett 15:57–65. https://doi.org/10.24507/icicel.15.01.57

9. Sonamoni JS, Sikdar R, Akib ASMAS, et al (2024) IoT-Based Smart Remote Door Lock and Monitoring System Using an Android Application †. Eng Proc 76:1–8. https://doi.org/10.3390/engproc2024076085
10. Putri H, Hadiyoso S, Fatoni SBP, et al (2025) Security System for Door Locks Using YOLO-Based Face Recognition. Int J Informatics Vis 9:224–230. https://doi.org/10.62527/joiv.9.1.2410
11. Mohammad AS, Jarullah TG, Al-Kaltakchi MTS, et al (2024) IoT-MFaceNet: Internet-of-Things-Based Face Recognition Using MobileNetV2 and FaceNet Deep-Learning Implementations on a Raspberry Pi-400. J Low Power Electron Appl 14:46. https://doi.org/10.3390/jlpea14030046
12. Afifah V, Erniwati S (2026) YOLOv8 for Object Detection : A Comprehensive Review of Advances , Techniques , and Applications. Int J Adv Comput Informatics 2:53–61. https://doi.org/10.71129/ijaci.v2i1.pp53-61
13. Essien UD, Ansa GO (2023) A Deep Learning-Based Face Recognition Attendance System. Glob J Eng Technol Adv 17:9–22. https://doi.org/10.30574/gjeta.2023.17.1.0165
14. Schroff F, Kalenichenko D, Philbin J (2015) FaceNet : A Unified Embedding for Face Recognition and Clustering. Proc IEEE Conf Comput Vis Pattern Recognit
15. Yang S, Luo P, Loy CC, Tang X (2016) WIDER FACE : A Face Detection Benchmark. IEEE Conf Comput Vis Pattern Recognit 5525–5533
16. Dewi C, Manongga D, Hendry, et al (2024) Deep Learning and YOLOv8 Utilized in an Accurate Face Mask Detection System. Big Data Cogn Comput 8:1–17. https://doi.org/10.3390/bdcc8010009
17. Aditama MF, Haryanti M (2023) Sistem Pengenalan dan Verifikasi Wajah Menggunakan Transfer Learning Berbasis Raspberry Pi. J Teknol Ind 12:30–39. https://doi.org/10.35968/jti.v12i1.1045
18. Hassanzad M, Tilaki KH (2024) Methods of Determining Optimal Cut - Point of Diagnostic Biomarkers with Application of Clinical Data in ROC Analysis : an Update Review. BMC Med Res Methodol 24:1–13. https://doi.org/10.1186/s12874-024-02198-2
19. Terampe GC, Pramudwiatmoko A (2025) Facial Recognition Performance Evaluation with YOLOv8, ArcFace, and SVM in a Contactless Employee Attendance System. J Ris Inform 8:108–120. https://doi.org/10.34288/jri.v8i1.465

20. Isong B, Ndouvhada S, Kgote O (2025) Empirical Analysis of Deep Learning Models for Real-time Face Detection on Resource-constrained Devices. IT J Res Dev 10:28–45. https://doi.org/10.25299/itjrd.2025.22402
21. Sugusa GC, Kavitha HS, Shirahatti S, Bangari SR (2021) Face Recognition System for Real Time Applications using SVM Combined with FaceNet and MTCNN. Int J Electr Technol 12:328–335. https://doi.org/10.34218/IJEET.12.6.2021.031
22. Muttaqin ANI, Luthfiarta A, Nugraha A, Salsabila PM (2025) Single-Image Face Recognition For Student Identification Using Facenet512 And Yolov8 In Academic Environtment With Limited Dataset. J Tek Inform 6:3018–3032. https://doi.org/10.52436/1.jutif.2025.6.5.3908
23. Adliansyah FN, Holilah, Krisdianto N (2025) Sistem Absensi Berbasis Face Recognition dengan Model Inception-Resnet. J Artif Intell Digit Bus 4:2111–2118. https://doi.org/10.31004/riggs.v4i4.3545