Volume XI Issue 2 Year 2026 | Page 463-474 | ISSN: 2527-9866
*Received:* ***02-03-2026*** | *Revised:* ***17-03-2026*** | *Accepted:* ***24-05-2026***

# Centralized Access Management for Vertical Housing Using Edge Computing and Deep Learning

**Zaky Wahyu Oktavianto[1], M. Udin Harun Al Rasyid[2], Setiawardhana[3]**
[1,2,3]Departement of Informatics and Computer Engineering, Politeknik Elektronika Negeri Surabaya, Surabaya City, Indonesia, 60111
*e-mail:* zakywwahyu7@pasca.student.pens.ac.id [1], udinharun@pens.ac.id [2], setia@pens.ac.id[3]
*Correspondence: *udinharun@pens.ac.id*

***Abstract:*** *The implementation of security systems in vertical housing, there is often a choice between high infrastructure costs from decentralized hardware and privacy risks from Cloud solutions. This study presents a prototype for a Centralized Access Management System utilizing Edge Computing (Intel NUC) as a local server to authenticate residents at various access points. The system uses Frigate NVR for lightweight real-time object detection and the ArcFace Deep Learning model for facial recognition. It processes all biometric data locally to protect privacy. We used a dataset of three registered subjects to test the experiment. The tests looked at how well the system worked at different distances (1 to 5 meters), in different lighting conditions (daylight and infrared), with different types of facial occlusions (medical masks), and with 2D spoofing attacks (print and digital media). Using a confusion matrix over 50 random test samples that included both authorized users and unknown intruders, the system got a Global Accuracy of 80.0%. The system also had a Genuine Acceptance Rate (GAR) of 86.6%. The system was very stable when it was 1 to 2 meters away, but it didn't work as well in extreme conditions. With an average CPU usage of 46.87% and physical control latency via the MQTT protocol of less than 0.2 seconds, resource efficiency was kept up. These results show that the proposed edge architecture can work as a responsive and computationally efficient prototype for smart apartment security. They also show that liveness detection needs to be improved in the future to reduce the risk of digital spoofing.*

***Keywords:*** *Edge Computing, Access Management, Deep Learning, ArcFace, Home Assistant.*

## 1. Introduction

The rapid urbanization and vertical expansion of modern cities have accelerated the adoption of smart building technologies, creating a pressing need for integrated residential security systems [1]. As vertical housing complexes and apartments become increasingly dense, the demand for efficient, automated, and secure access management continues to rise. Recent studies highlight that the implementation of Internet of Things (IoT) in smart homes has evolved beyond simple automation to encompass complex security protocols managed by intelligent virtual assistants [2]. In this context, Home Assistant platforms have gained prominence for their ability to orchestrate various sensors and actuators within a unified local network [3], [4]. However, as these systems become ubiquitous, the reliance on traditional access control methods, such as RFID cards or PIN codes, is increasingly viewed as inadequate due to their susceptibility to duplication and lack of biometric verification [5], [6]. Despite the advancements in smart security, a critical dichotomy remains between architectural efficiency and data privacy. Currently, a significant portion of commercial solutions relies heavily on centralized cloud-based architectures [7]. While cloud computing offers scalable resources, reports project that the exponential growth of data center workloads will inevitably exacerbate network latency issues, rendering real-time applications unstable [8]. More critically, the transmission of sensitive video feeds and biometric data to third-party cloud servers raises profound privacy concerns. Research indicates that cloud-based IoT environments are frequent

targets for cyberattacks, exposing residents to potential data breaches and unauthorized surveillance [9].

To mitigate these risks, the paradigm of Edge Computing has been proposed as a viable alternative, shifting data processing from remote servers to the edge of the network to ensure data sovereignty and reduce response times [10], [11], [12]. Previous research has attempted to implement this edge computing concept using low-power single-board computers [13], [14], [15]. For instance, several studies have developed facial recognition door locks utilizing Raspberry Pi and standard webcams [13]. While these implementations succeed in reducing infrastructure costs, they often exhibit significant performance limitations. Low-power devices struggle to maintain acceptable frame rates when executing complex recognition tasks, leading to sluggish user experiences.

Consequently, many of these systems resort to lightweight algorithms such as Haar Cascade or Local Binary Pattern Histograms (LBPH) to preserve performance [16], [17], [18]. However, comparative analyses demonstrate that these conventional methods suffer from high False Negative rates, particularly in suboptimal lighting conditions or when subjects are partially occluded by masks [17], [19]. Furthermore, systems relying solely on basic computer vision techniques often lack the robustness required to distinguish between genuine faces and spoofing attacks [20].

To address this sharply defined gap, the novelty of this research lies in proposing a centralized, hybrid Edge AI architecture deployed on a mid-range Edge Server (Intel NUC) rather than distributed low-power nodes. This architecture uniquely integrates a multi-stage processing pipeline: utilizing Frigate NVR as a lightweight first-line object detector to eliminate false motion alarms, followed by the ArcFace Deep Learning model for high-precision facial extraction, which outperforms earlier models in false positive reduction [21], [22]. This synergy bridges the gap by achieving Cloud-level AI precision entirely on-premise without hardware acceleration (GPU) dependency.

Therefore, to validate the proposed architecture this study establishes specific and measurable goals. The first goal is to design and implement a cloud-independent access management system that can process a continuous Full HD (1080p) video stream while keeping the server CPU load below 60%. Furthermore, the study aims to evaluate the Frigate-ArcFace pipeline's reliability by measuring global accuracy, the genuine acceptance rate (GAR), and the false acceptance rate (FAR) under different conditions. These conditions include distances from 1 to 5 meters, various lighting situations (daylight and infrared), and facial obstructions like masks. Finally, the research seeks to ensure the system's high responsiveness by achieving an end-to-end physical control latency of less than 0.5 seconds for door actuator activation using the MQTT protocol.

## 2. Literature Review

The Literature Review establishes the theoretical and empirical foundation for this study, focusing on the evolution of smart home security architectures from cloud-dependent models to edge computing solutions.

### A. Cloud-Based Security Systems

Early iterations of IoT security heavily relied on cloud computing to handle complex processing tasks. Studies by Verma et al. [7] and Lee [23] demonstrate that cloud architectures offer scalability and ease of integration for smart home devices. However, this centralized approach introduces critical vulnerabilities. Research by John [9] highlights that transmitting sensitive biometric video data to third-party servers exposes residents to significant privacy risks and

cyberattacks. Furthermore, reliance on external networks creates latency issues, which can render real-time access control unstable during network congestion [8].

### B. Low-Power Edge Computing

To mitigate cloud-related risks, recent research has shifted towards Edge Computing. Numerous studies have attempted to implement facial recognition on low-cost single-board computers (SBC) like the Raspberry Pi [13], [15], [24]. While these solutions address data sovereignty, the hardware limitations often necessitate the use of lightweight algorithms such as Haar Cascade or Local Binary Pattern Histograms (LBPH) [16], [19]. Comparative analyses indicate that these conventional algorithms suffer from high False Negative rates, particularly in suboptimal lighting or when faces are partially occluded by masks [17], [20].

### C. Deep Learning and Centralized Edge

State-of-the-art Deep Learning models, such as ArcFace, utilize additive angular margin loss to significantly outperform earlier models like FaceNet in discrimination accuracy [21], [22]. However, these models are computationally intensive and unsuitable for standard low-power edge nodes. This study proposes a "Centralized Edge" architecture using an Intel NUC to bridge this gap, enabling the use of robust Deep Learning locally without the performance bottlenecks of Raspberry Pi or the privacy risks of the Cloud. The position of this study relative to existing research is detailed in Table I.

**Table 1** Comparison of Existing Research and Proposed System

| Reference | Platform / Hardware | Method / Algorithm | Key Limitations (Research Gap) |
|---|---|---|---|
| Begum et al. [13] | Raspberry Pi (Low-Power Edge) | Basic Face Recognition | Limited computational power resulting in low frame rates and slow response times. |
| Sharma et al. [16] | Single Board Computer | Haar Cascade & LBPH | High False Negative rate in low-light conditions; struggles with facial occlusion (masks). |
| John et al. [9] | Cloud Server | Cloud-based AI Analysis | High latency due to network dependence; significant data privacy risks (data leaves premise). |
| Proposed System | Intel NUC (Centralized Edge) | ArcFace + Frigate NVR | High accuracy with Deep Learning; low latency; preserves privacy (local processing). |

## 3.Methods

This section describes the system architecture, hardware specifications, and Deep Learning algorithms used to achieve the research objectives.

### A. Data Description

The primary data used in this study consists of high-resolution real-time video streams captured by a Tapo C220 IP Camera with a 2K resolution (2560 × 1440 pixels). To ensure privacy compliance, the system utilizes a strict local processing policy. Instead of storing raw video footage which consumes significant storage and poses privacy risks, the system extracts 512-dimensional facial feature vectors from the video frames using the ArcFace algorithm. The dataset used for training and testing was collected directly from three authorized subjects representing the apartment residents. The data acquisition procedure for the training (registration) phase involved capturing more than 20 facial images per subject from various angles and lighting conditions to build a robust local database. For the experimental testing phase, a validation subset of 50 randomized test samples was systematically composed. This testing composition included 30 samples of authorized residents to evaluate True Positives and

False Negatives, and 20 samples of unknown individuals and 2D spoofing media to evaluate True Negatives and False Positives.

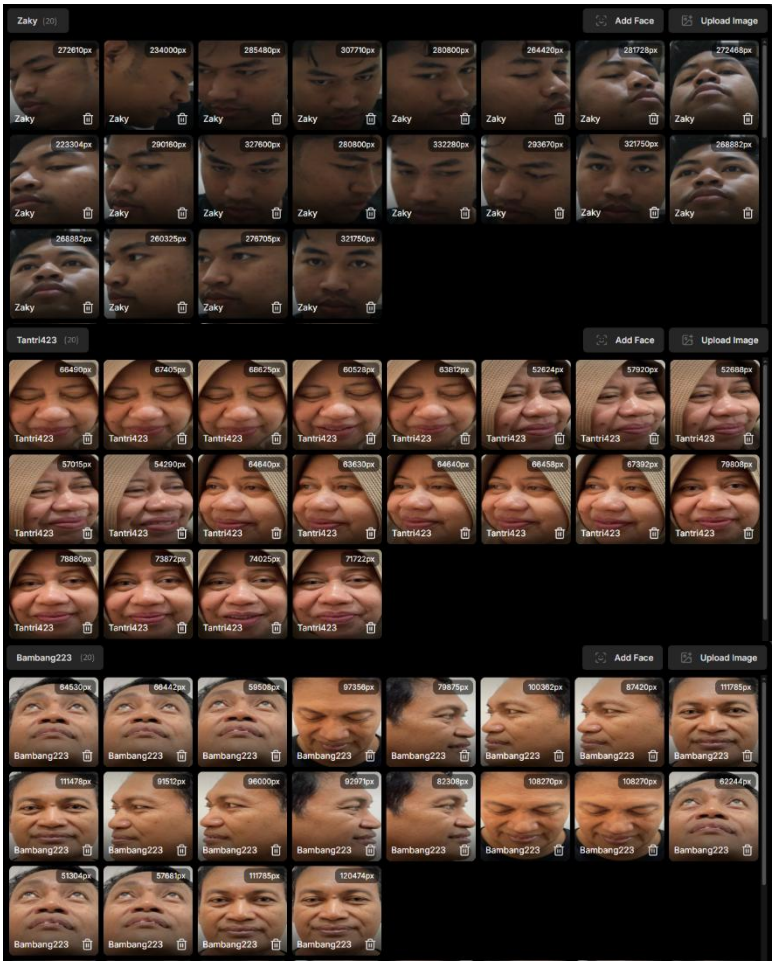


**Figure 1.** (a) the face of the first person (b) the face of the second person (c) the face of the third person

## B. Research Location

The proposed Centralized Access Management System was tested in a simulated vertical housing environment designed to replicate the architectural constraints of a modern smart apartment complex. To acknowledge the practical limitations of a full-scale deployment in a real vertical housing building, the experimental validation was rigorously conducted as a Proof of Concept (PoC). The full hardware deployment was physically implemented exclusively at the primary access node (Lobby). Meanwhile, the secondary access points (Gym Area and Swimming Pool Area) were logically simulated via software to evaluate the server's scalability and concurrent network load. This controlled environment allowed for rigorous testing of the system's response to varying distances (1 to 5 meters) and lighting conditions (daylight vs. infrared night vision) to evaluate the robustness of the edge computing architecture.

## C. Research Methods and Evaluation

The research methodology is divided into three main components: Hardware Architecture, Intelligent Detection Pipeline, and Face Recognition Algorithm.

### 1. System Architecture and Hardware Design

The hardware infrastructure is categorized into the Perception Layer and the Processing Layer. For the central processing unit, the system utilizes an Intel NUC 12 Pro Kit (NUC12WSH) equipped with an Intel Core i7-1260P processor (12 Cores, 16 Threads) and 8GB of DDR4 RAM. This high-performance specification was selected to handle the computational load of real-time video decoding and deep learning inference, addressing the performance bottlenecks often found in low-power edge devices like the Raspberry Pi. On the Perception Layer, the system deploys distributed sensor nodes built upon the ESP8266 microcontroller (NodeMCU V2). Each node integrates a PIR HC-SR501 sensor for motion detection, an MC-38 magnetic switch for door status monitoring, and a 12V Solenoid Lock for physical access control. The communications framework relies on a dual-protocol approach to ensure stability. The Real-Time Streaming Protocol (RTSP) is employed for high-bandwidth video transmission from the camera to the server, while the Message Queuing Telemetry Transport (MQTT) protocol handles lightweight control signals and sensor status updates with minimal latency.

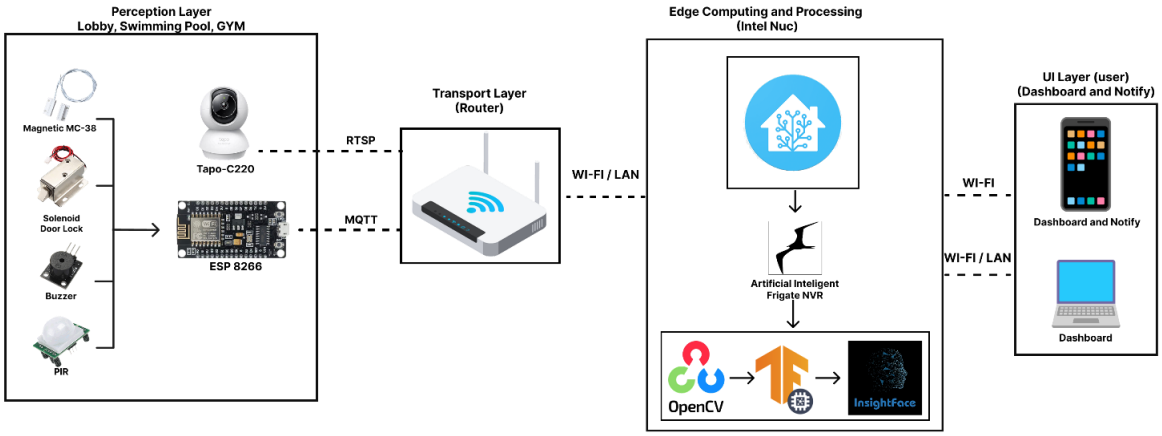


**Figure 2.** Block Diagram of the Proposed Centralized Edge Computing Architecture

### 2. Intelligent Detection Pipeline

The core intelligence of the system is orchestrated by the Home Assistant Operating System (HAOS), which manages a multi-stage detection pipeline. The process initiates with Frigate NVR utilizing OpenCV to detect motion and filter out static frames, significantly reducing unnecessary processing. Upon detecting motion, a TensorFlow Lite model analyzes the region of interest. If a "Person" class is identified with a predefined confidence threshold, the frame is passed to the facial recognition stack. This efficient filtering ensures that the heavy deep learning model is only triggered when a human subject is present. This logic flow is shown in Figure 2.

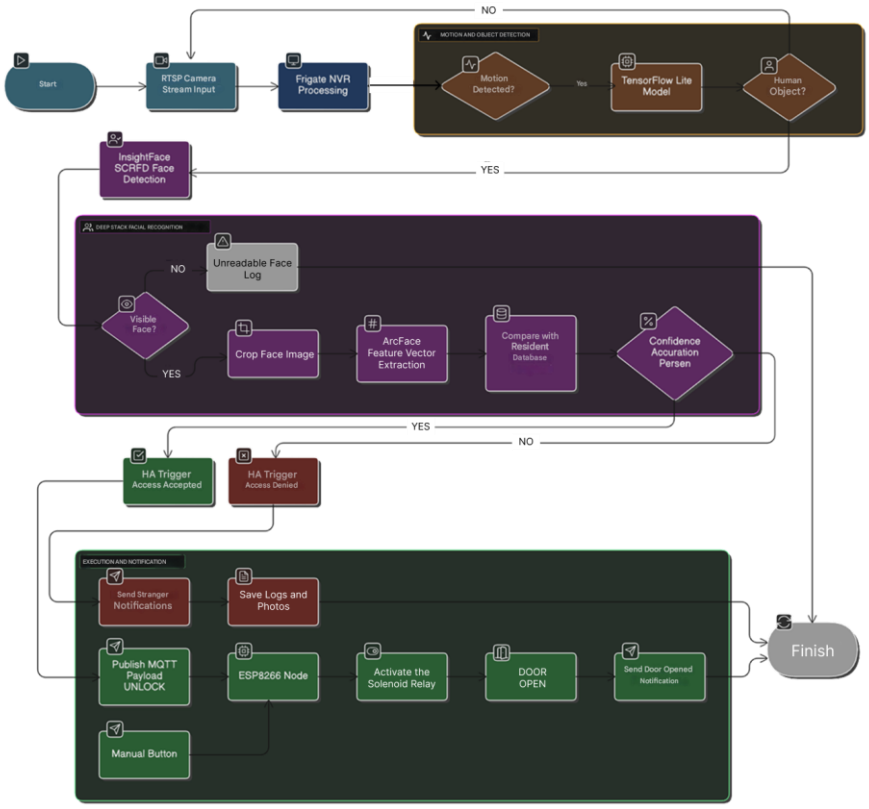


**Figure 3.** Flowchart of the Intelligent Detection and Recognition Pipeline

## 3. Deep Learning Algorithms

For biometric verification, the system employs the ArcFace Deep Learning model. ArcFace is chosen for its ability to maximize the discrimination between different identities by mapping facial features onto a hypersphere. Unlike traditional softmax loss, ArcFace introduces an additive angular margin penalty ($m$) to enforce higher intra-class compactness. The objective function is mathematically defined as:

$$L = -\frac{1}{N}\sum_{i=1}^{N} \log \frac{e^{s(\cos(\theta_{yi}+m))}}{e^{s(\cos(\theta_{yi}+m))}+\sum_{j\neq yi} e^{s\cos\theta_j}} \quad (1)$$

Where $N$ is the batch size, $s$ is the scaling factor, and $\theta_{yi}$ is the angle between the feature vector and the weight vector of the ground truth class $yi$. After extracting the 512-dimensional feature vectors, the system determines the identity match by calculating the Cosine Similarity ($S$) between the captured vector $A$ and the registered database vector $B$:

$$S(A,B) = \frac{A\,.\,B}{||A||\,||B||} = \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2}\sqrt{\sum_{i=1}^{n} B_i^2}} \quad (2)$$

The system sets a matching threshold of 0.70. This specific value was optimized based on an empirical trade-off analysis between security and convenience. A threshold below 0.60 proved too lenient, significantly increasing the False Acceptance Rate (FAR). Conversely, a threshold above 0.80 was too strict, leading to a high False Rejection Rate (FRR) where authorized residents were frequently denied access due to minor environmental changes. Thus, 0.70 was established as the optimal equilibrium (sweet spot) for the system. If the score $S_{A,B} > 0.70$, the system authenticates the user and triggers the solenoid lock mechanism via MQTT.

### 4. Evaluation Metrics and Statistical Performance

The quantitative evaluation adopts a Binary Classification methodology based on the Confusion Matrix. The overall System Accuracy is calculated to measure the ratio of correctly predicted observations to the total observations, formulated as:

$$Global\ Accuracy = \frac{TP + TN}{TP + TN + FP + FN}\ x\ 100\% \quad (3)$$

Furthermore, to assess the security reliability and user convenience, we calculate the Genuine Acceptance Rate (GAR) which represents the system's ability to correctly verify authorized residents, the False Acceptance Rate (FAR) which indicates the risk of unauthorized access, and the False Rejection Rate (FRR) which measures the frequency of the system wrongly denying an authorized resident. These metrics are defined as:

$$GAR = \frac{TP}{TP+FN}, FAR = \frac{FP}{FP+TN}, FRR = \frac{FN}{TP+FN} \quad (4)$$

Where $TP$ denotes True Positives, $TN$ True Negatives, $FP$ False Positives, and $FN$ False Negatives. Additionally, system responsiveness is measured by the end-to-end latency from facial capture to door unlocking to ensure real-time performance.

## 4. Results and Discussion

### A. Edge Computing Performance

A crucial metric in edge computing deployments is the balance between responsiveness and resource efficiency. The evaluation of the edge server measured both latency and computational load during the continuous processing of a video stream. As summarized in Table II, the local processing approach utilizing the Intel NUC significantly minimized latency compared to cloud-dependent solutions found in the literature. The response time of physical sensors to actuate the solenoid lock via the MQTT protocol was recorded at just 0.20 seconds, while the total end-to-end recognition time averaged 1.50 seconds. This performance confirms that the system is capable of ensuring near real-time access control, eliminating the latency jitter typically associated with cloud-based API calls.

Simultaneously, operational stability was analyzed across different video resolutions to determine the optimal configuration for the edge server. A comparative test was conducted using SD, HD, FHD, and 2K resolutions at a fixed distance. The results indicate a clear trade-off: while 2K resolution offers the highest accuracy (94%), it demands a significant CPU load of 54.0%. In contrast, the FHD (1920x1080) resolution achieves a comparable accuracy of 91% but with a more efficient CPU usage of 48.8% and a stable processing speed of 10.2 detections per second. Consequently, FHD was selected as the operational standard, providing the best balance between recognition precision and system longevity.

**Table 2.** Edge Computing Performance Metrics

| Metric Category | Performance Parameter | Average Value | Operational Interpretation |
|---|---|---|---|
| System Responsiveness | Sensor Actuation Latency (MQTT) | 0.20 s | Near real-time response for physical locking mechanism. |
| | End-to-End Recognition Time | 1.50 s | Total processing time from face capture to door unlock. |
| Resource Efficiency | CPU Utilization (Intel NUC) | 48.8% | Processing 1080p video stream with object detection active. |
| | Processing Frame Rate | 5.1 FPS | Optimized stability for Frigate NVR event detection. |

The trade-off analysis between accuracy, CPU load, and speed is further visualized in Figure 3.

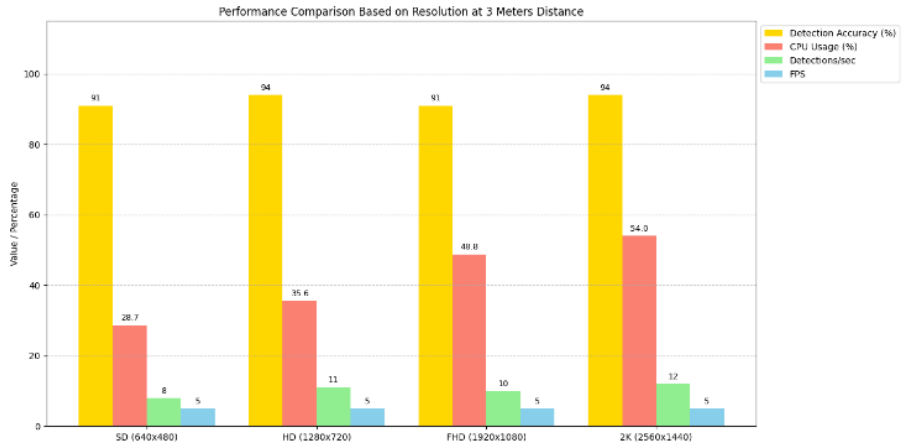


**Figure 4.** Performance trade-off analysis (Accuracy vs. CPU Load vs. Speed) across various video resolutions.

## B. Deep Learning Model Evaluation and Accuracy Analysis

The reliability of the facial recognition system was validated through a series of rigorous quantitative tests to measure the performance of the Deep Learning algorithm benchmarked against state-of-the-art models in unconstrained environments. This evaluation utilized a binary classification method based on a confusion matrix. To optimize the system for a residential security context, an empirical analysis of the False Acceptance Rate (FAR) and False Rejection Rate (FRR) was conducted. Based on this analysis, a matching threshold was configured at an optimal point that prioritizes perimeter security, significantly minimizing the risk of unauthorized access while maintaining convenient access for registered occupants.

The summary of the model performance at this specific configuration is detailed in Table III. The system achieved a Global Accuracy of 80.0% with a Precision of 81.2%. This high precision score confirms the system's reliability in verifying positive identities, ensuring that the unlocking mechanism is triggered only by legitimate occupants. Furthermore, to balance strict security with user convenience, the system recorded a Genuine Acceptance Rate (GAR) of 86.6%. This metric indicates that the vast majority of authorized residents are successfully recognized in a single scan without experiencing repeated rejections. Despite the inherent trade-offs in accuracy caused by real-time video compression, these figures represent optimal performance for implementation on resource-constrained edge devices.

**Table 3.** Model Performance Metrics Evaluation Results

| Evaluation Parameters | Percentage Value | Operational Interpretation |
|---|---|---|
| Global Accuracy | 80.0% | The overall success rate of the system in real-time conditions. |
| Precision | 81.2% | The system's confidence level that a recognized face is valid. |
| Recall (GAR) | 86.6% | The system's chance of recognizing a legitimate occupant in a single scan. |
| F1-Score | 83.9% | Harmonious balance between safety (Precision) and comfort (GAR). |
| FAR | 30.0% | Indicates the risk of unauthorized access, primarily showing the system's vulnerability to 2D digital spoofing attacks. |

| | | |
|---|---|---|
| FRR | 13.4% | Measures the frequency of authorized residents being wrongly denied access, reflecting the system's convenience trade-off. |

## C. Robustness Analysis and Environmental Limitations

A more in-depth analysis was conducted to test the stability of facial feature extraction over varying object distances from the camera (1 to 5 meters). As illustrated in Figure 4, the system demonstrated excellent performance (100% accuracy) at close distances (1–2 meters), where facial resolution remains optimal. A significant finding is the model's robustness at an extreme distance of 5 meters, where accuracy remains high at 89%. This demonstrates that the resulting facial embedding vector remains robust despite the decrease in facial pixel resolution due to distance, a key characteristic of the implemented Deep Learning architecture.

However, although the proposed architecture has proven reliable under standard lighting conditions, testing under extreme environmental conditions revealed significant operational limitations. In-depth analysis was performed on two key nuisance variables: infrared illumination and partial facial occlusion. In the night vision scenario, the system maintained an average global accuracy of 91.5%. However, granular analysis revealed a critical anomaly at a distance of 3 meters, where accuracy dropped drastically to 60%. This drop indicates a domain mismatch between the model's RGB-based training data and the monochromatic infrared input. The loss of color texture information, combined with the effects of light reflection at this specific distance, causes facial features to become flat, making it difficult for the algorithm to accurately distinguish facial contours.

A more fundamental challenge was found in the facial occlusion scenario. When the subject wore a medical mask, accuracy remained at 90% at a close distance of 1 meter, but experienced a linear degradation until it reached a critical point of 50% at a distance of 5 meters. This failure confirms that the facial recognition algorithm relies heavily on intact geometric structures, particularly the nose and mouth areas, to generate unique embedding vectors. When this area is occluded and pixel resolution decreases due to distance, the model is forced to rely solely on periocular features that have lower variance, significantly increasing the risk of misclassification.

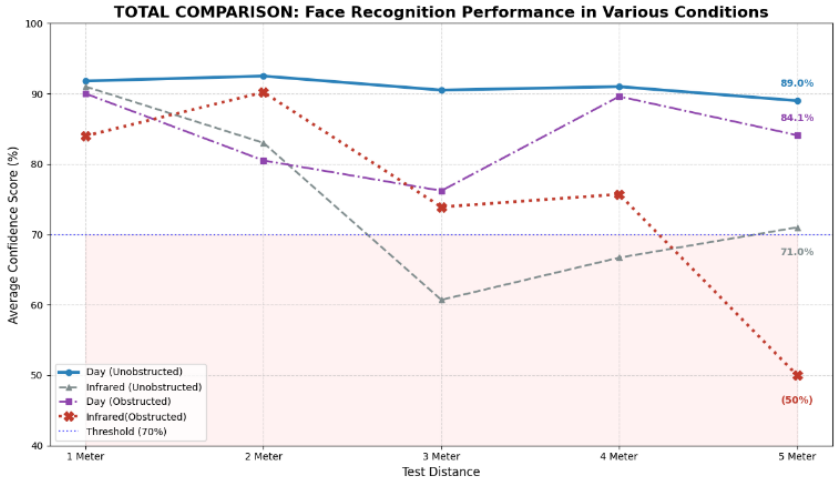


**Figure 5.** Comparison of Face Recognition Performance in Various Conditions

## 5. Conclusions

This study presents an initial validation of a prototype for a centralized access management system based on an Edge Computing architecture. By integrating the Home Assistant platform with a Deep Learning model on an Intel NUC server, the system explores the feasibility of

eliminating reliance on external cloud services. The experimental results demonstrate that the prototype achieves near real-time performance, with a sensor actuation latency of 0.20 seconds and a total recognition processing time of 1.50 seconds. Furthermore, the localized processing approach proved to be computationally efficient, maintaining an average CPU utilization of 48.8%, which indicates the potential viability of deploying computer vision tasks on mid-range edge hardware.

In terms of biometric evaluation, the system achieved a Global Accuracy of 80.0%, alongside a Precision of 81.2% and a Genuine Acceptance Rate (GAR) of 86.6%. While these metrics reflect a promising baseline for residential security under optimal conditions, it is important to emphasize that this work represents a prototype-level study. Significant operational boundaries were identified under extreme environmental conditions. Although the system maintained an 89.0% accuracy at a 5-meter distance in daylight, performance decreased substantially in challenging scenarios, dropping to 60% accuracy under infrared night vision and 50% when subjects were occluded by medical masks. Furthermore, the recorded False Acceptance Rate (FAR) of 30.0% indicates a notable vulnerability to 2D digital spoofing attacks. These limitations highlight the constraints of relying solely on RGB-based models in handling spectral domain mismatches and structural facial loss. Consequently, to transition this prototype into a fully robust system, future work must focus on integrating multi-modal sensors (e.g., thermal or depth cameras), employing specialized datasets for infrared/occluded conditions, and implementing active liveness detection.

**Acknowledgements**

The authors would like to express their sincere gratitude to the Department of Informatics and Computer Engineering, Politeknik Elektronika Negeri Surabaya, for providing the laboratory facilities and technical support required to conduct this research. We also extend our appreciation to the thesis advisors for their valuable guidance, constructive feedback, and supervision throughout the development of this system.

## References

[1] P. Thakur, S. Goel, and E. Puthooran, "Edge AI Enabled IoT Framework for Secure Smart Home Infrastructure," *Procedia Comput. Sci.*, vol. 235, pp. 3369–3378, 2024, doi: 10.1016/j.procs.2024.04.317.

[2] T. M. N. Vamsi, B. Suchitra, S. Kumar, K. V. V. Varma, and K. N. S. H. Kumar, "An IoT based Smart Home with Virtual Assistant," *2021 6th Int. Conf. Converg. Technol. I2CT 2021*, pp. 4–7, 2021, doi: 10.1109/I2CT51068.2021.9417883.

[3] I. Irvawansyah, U. Muhammad, M. Ihsan, A. Renanda, and K. Kurnia, "Prototype Teknologi Home Assistant Berbasis Internet of Things (IoT)," *Joule (Journal Electr. Eng.*, vol. 4, no. 1, pp. 16–21, 2023, doi: 10.61141/joule.v4i1.376.

[4] A. Tri, A. Hidayat, M. U. Harun, A. Rasyid, I. U. Nadhori, and Y. E. Wahyudi, "Journal of Advanced Vocational Information and Communication Technology Smart Home Implementation with Home Assistant Platform in Modern Housing," vol. 0437, pp. 38–52, 2026.

[5] N. Gupta, P. Sharma, V. Deep, and V. K. Shukla, "Automated Attendance System Using OpenCV," *ICRITO 2020 - IEEE 8th Int. Conf. Reliab. Infocom Technol. Optim. (Trends Futur. Dir.*, pp. 1226–1230, 2020, doi: 10.1109/ICRITO48877.2020.9197936.

[6] M. Z. Abdillah, M. U. H. Al Rasyid, and R. Sigit, "Implementation of Face Recognition Using Deep Metric Learning for Automatic Door Openers," *2024 Int. Electron. Symp. Shap. Futur. Soc. 5.0 Beyond, IES 2024 - Proceeding*, vol. 10, no. January, pp. 675–680, 2024, doi: 10.1109/IES63037.2024.10665820.

[7] G. Verma, S. Pachauri, A. Kumar, D. Patel, A. Kumar, and A. Pandey, "Smart Home Automation with Smart Security System over the Cloud," *2023 14th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2023*, pp. 1–7, 2023, doi: 10.1109/ICCCNT56998.2023.10306548.

[8] T. Barnett Jr. and A. Sumit, "Cisco Global Cloud Index 2015–2020," *Cisco Knowl. Netw. Sess.*, no. November 2016, 2016, [Online]. Available: https://www.cisco.com/c/dam/m/en_us/service-provider/ciscoknowledgenetwork/files/622_11_15-16-Cisco_GCI_CKN_2015-2020_AMER_EMEAR_NOV2016.pdf?dtid=osscdc000283

[9] A. John, "Security of Smart Homes in Cloud-Based IOT Environment," vol. 14, no. 04, 2025.

[10] S. Hamdan, M. Ayyash, and S. Almajali, "Edge-computing architectures for internet of things applications: A survey," *Sensors (Switzerland)*, vol. 20, no. 22, pp. 1–52, 2020, doi: 10.3390/s20226441.

[11] E. Al-Masri *et al.*, "Investigating Messaging Protocols for the Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 94880–94911, 2020, doi: 10.1109/ACCESS.2020.2993363.

[12] I. Sittón-Candanedo, R. S. Alonso, S. Rodríguez-González, J. A. García Coria, and F. De La Prieta, "Edge Computing Architectures in Industry 4.0: A General Survey and Comparison," *Adv. Intell. Syst. Comput.*, vol. 950, pp. 121–131, 2020, doi: 10.1007/978-3-030-20055-8_12.

[13] H. Muneera Begum, S. Jayasri, M. Kavya Dharshini, L. C. Govindapillai, and R. Jane Cynthia Juliet, "Face Recognition Door Lock System Using Raspberry Pi," *8th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2022*, pp. 1645–1648, 2022, doi: 10.1109/ICACCS54159.2022.9785217.

[14] X. Huang and X. Cao, "Face Detection and Tracking Using Raspberry Pi based on Haar Cascade Classifier," *Proc. - 2022 37th Youth Acad. Annu. Conf. Chinese Assoc. Autom. YAC 2022*, pp. 505–509, 2022, doi: 10.1109/YAC57282.2022.10023612.

[15] Z. Sharif, L. T. Jung, M. Ayaz, M. Yahya, and D. Khan, "Smart Home Automation by Internet-of-Things Edge Computing Platform," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 4, pp. 474–484, 2022, doi: 10.14569/IJACSA.2022.0130455.

[16] A. Sharma, K. Shah, and S. Verma, "Face Recognition using Haar Cascade and Local Binary Pattern Histogram in OpenCV," *Proc. IEEE Int. Conf. Image Inf. Process.*, vol. 2021-Novem, pp. 298–303, 2021, doi: 10.1109/ICIIP53038.2021.9702579.

[17] D. A. Wangean, S. Setyawan, F. I. Maulana, G. Pangestu, and C. Huda, "Development of Real-Time Face Recognition for Smart Door Lock Security System using Haar Cascade and OpenCV LBPH Face Recognizer," *ICCoSITE 2023 - Int. Conf. Comput. Sci. Inf. Technol. Eng. Digit. Transform. Strateg. Facing VUCA TUNA Era*, pp. 506–510, 2023, doi: 10.1109/ICCoSITE57641.2023.10127753.

[18] M. Gupta, K. Bisht, A. Sharma, and D. Upadhyay, "HaarCascade and LBPH Algorithms in Face Recognition Analysis," *2023 World Conf. Commun. Comput. WCONF 2023*, pp. 1–4, 2023, doi: 10.1109/WCONF58270.2023.10235019.

[19] Y. Fan *et al.*, "Low-FaceNet: Face Recognition-Driven Low-Light Image Enhancement," *IEEE Trans. Instrum. Meas.*, vol. 73, pp. 1–13, 2024, doi: 10.1109/TIM.2024.3372230.

[20] M. A. Azhari Halim, M. F. I. Othman, A. Z. Z. Abidin, E. Hamid, N. Harum, and W. M. Shah, "Face Recognition-based Door Locking System with Two-Factor Authentication Using OpenCV," *2021 6th Int. Conf. Informatics Comput. ICIC 2021*, 2021, doi: 10.1109/ICIC54025.2021.9632928.

[21] R. C. Juwanda, F. A. Alunjati, U. Elviani, and F. Hidayat, "Comparative Analysis of FaceNet

and ArcFace in Minimizing False Positives for Enhanced Access Control Security," *11th Int. Conf. ICT Smart Soc. Integr. Data Artif. Intell. a Resilient Sustain. Futur. Living, ICISS 2024 - Proceeding*, pp. 1–6, 2024, doi: 10.1109/ICISS62896.2024.10750931.

[22] A. Firmansyah, T. F. Kusumasari, and E. N. Alam, "Comparison of Face Recognition Accuracy of ArcFace, Facenet and Facenet512 Models on Deepface Framework," *ICCoSITE 2023 - Int. Conf. Comput. Sci. Inf. Technol. Eng. Digit. Transform. Strateg. Facing VUCA TUNA Era*, pp. 535–539, 2023, doi: 10.1109/ICCoSITE57641.2023.10127799.

[23] M. Lee, "Design for Visitor Authentication Based on Face Recognition Technology Using CCTV," *IEEE Access*, vol. 10, no. November, pp. 124604–124618, 2022, doi: 10.1109/ACCESS.2022.3223374.

[24] A. Ben Thabet and N. Ben Amor, "Enhanced smart doorbell system based on face recognition," *16th Int. Conf. Sci. Tech. Autom. Control Comput. Eng. STA 2015*, pp. 373–377, 2016, doi: 10.1109/STA.2015.7505106.