JAITA

JOURNAL OF ADVANCED INDUSTRIAL TECHNOLOGY AND APPLICATION
e-ISSN: 2716-7097

Vol. 7 No. 1 (2026) 118-130
https://publisher.uthm.edu.my/ojs/index.php/jaita

An Integrated IoT-Based Smart Home System for Safety and Automation

Muhamad Amirul Hafeez Azhar[1], Zuhairiah Zainal Abidin[1]*, Saizalmursidi Md Mustam[1], Shaharil Mohd. Shah[1]

[1] *Advanced Telecommunication Research Center, (ATRC), Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, 86400 Batu Pahat, Johor, MALAYSIA*

*Corresponding Author: zuhairia@uthm.edu.my
DOI: https://doi.org/10.30880/jaita.2026.07.01.009

Article Info

Received: 10 October 2025
Accepted: 8 February 2026
Available online: 18 June 2026

Keywords

Internet of Things (IoT), ESP32-S3, facial recognition, gas detection, smart home, MIT app inventor

Abstract

This paper presents the design and implementation of a unified smart home system that combines facial recognition for access control, hazardous gas detection, and IoT-based appliance automation. The system employs an ESP32-S3 CAM microcontroller with a pre-trained DeepStack model for real-time facial identification, MQ-series gas sensors for gas detection, and a mobile application developed using MIT App Inventor for remote control of appliances. Google Sheets functions as a lightweight cloud backend for data logging and system monitoring. Experimental results confirmed the system's high reliability under various lighting conditions, sub-second switching latency for appliances, and reliable gas detection at multiple distances. The results demonstrate that the proposed system provides a scalable framework suitable for enhancing residential safety and convenience.

1. Introduction

Smart home technologies aim to improve residential safety and optimize energy usage. Although incidents such as gas leaks and break-ins are less common today, they still pose significant risks to homeowners [1]. For instance, Malaysia recorded multiple gas cylinder explosions between 2021 and 2023 [2], leading to property loss and fatalities. Home safety technologies can help prevent these accidents by detecting gas leaks. Recent studies have successfully demonstrated how IoT-enabled systems can also enhance both safety and home management. For example, Shawon et al. [3] developed a smart home danger alert framework that uses flame, motion, and gas sensors to issue early warnings to homeowners.

While many smart home systems focus either on security or automation, few address both concerns in a unified solution. This paper introduces an integrated smart home system that combines facial recognition-based access control, gas leak detection, and IoT-enabled appliance control, providing a comprehensive and user-friendly approach for enhancing home safety and convenience.

A simple security system can be made as a surveillance system. Rahiman and Manohar [4] demonstrated how an ESP32-based monitoring system can detect intrusions and send immediate notifications, offering an effective, low-cost solution for smart home surveillance. A secure and robust security system can provide peace of mind from any intruders. In terms of system vulnerabilities, Vardakis et al. [5] provided a comprehensive review of IoT-related security risks in smart homes, stressing the importance of encryption, secure authentication, and real-time monitoring to protect against unauthorized access and data breaches. However, as technologies continue to improve, the robbers, intruders and even hacker also utilize more advanced methods of breaking into houses. Recent advancements in smart home technology have emphasized not only the importance of automation and

This is an open access article under the CC BY-NC-SA 4.0 license.

convenience but also the critical need for robust safety and security features. Authentication remains a central challenge, with AlJanah et al. [6] highlighting the shift toward multilevel and interaction-based authentication models to secure access to smart environments. Face recognition has also become a popular method for non-intrusive authentication; Rahim et al. [7] implemented a logit-boosted convolutional neural network (CNN) model that accurately detects faces and anomalies in real-time to enhance smart home access control.

Smart home automation technologies, ranging from Wi-Fi-enabled cameras and smart locks to smart home appliances, have become more accessible and diverse. These systems typically support remote monitoring and control via smartphones, tablets, or voice assistants, significantly enhancing user convenience. While early methods use localized technologies like Bluetooth and Zigbee, modern IoT-based designs using micro web servers and mobile apps provide both flexibility and remote accessibility [8]. Additionally, Singh and Mishra showcased how ESP8266 units, when paired with cloud frameworks such as Blynk, allow users to remotely monitor and control devices [9]. Cloud-connected platforms are becoming increasingly central to smart home designs. For example, Etuk et al. [10], demonstrated a cloud connected IoT system that controls appliances and monitors environmental data for energy and safety management, while Thomas and Mathew demonstrate successful implementations of centralized control over appliances through integrated IoT platforms [11]. Security-focused system designs are increasingly incorporating cloud-enabled and context-aware architectures, such as the model proposed by Hassan and Eassa [12], which allows for real-time automation and adaptive control of home appliances. Recent advancements in smart home systems have focused on combining energy-efficient automation with responsive environmental monitoring. Patil et al. demonstrated how low-cost microcontroller platforms like Arduino and ESP8266 can be used to design systems that regulate lighting, climate, and safety sensors using IoT architectures [13]. Besides that, gesture-controlled interfaces, as explored by Pandey and Tiwari, offer intuitive and hygienic means to manage appliances without physical contact [14].

This paper presents a unified smart home system that integrates facial recognition for secure, contactless access control; gas detection for early hazard warning; and IoT-based appliance automation to improve convenience and reduce energy waste. The proposed approach emphasizes a seamless and secure user experience through biometric authentication and mobile control, offering a practical and scalable solution for modern smart home environments.

2. Related Work

Smart home technologies have evolved significantly, with many initiatives targeting specific domains such as security, automation, and safety. For instance, Verma et al. [15] introduced a flexible solution that leverages the ESP32-CAM, combining PIR-based motion detection with appliance control via the Blynk IoT platform. While practical for basic tasks, their setup relied on simple motion triggers and lacked advanced features such as biometric access or comprehensive hazard detection.

Karnatak et al. [16] focused on energy efficiency and secure entry, utilizing an Arduino Mega alongside a Global system for mobile communication (GSM) module that enforced password-based access. Even though their system included critical safety elements such as gas leak detection via an MQ2 sensor and temperature regulation with a digital humidity and temperature sensor, DHT11, its security relied heavily on manual codes and did not feature biometric authentication.

The authors in [17] employed a low-cost smart home automation by integrating NodeMCU ESP8266 with the Blynk cloud. Their system managed basic intrusion detection and flame alerts but was not designed with modularity or deeper system integration in mind.

Recently, facial recognition has emerged as a more intelligent substitute for traditional access methods. Kumar and Rekha [18], for example, achieved 97.5% recognition accuracy even under varying lighting conditions by applying OpenCV and Haar classifiers. However, their setup wasn't embedded within a larger smart home ecosystem.

Siddhartha et al. [19] and Anjum et al. [20] explored sensor integration, including Light Dependent Resistor (LDR), infra-red (IR) modules, and gas detectors, to handle both monitoring and access. Despite their promise, these systems typically lacked a cohesive framework that integrated security, safety, and automation into a unified design.

A novel route with gesture-based appliance control using an APDS9960 sensor and Arduino Uno was proposed by Urmee et al. [21]. The touch-free interface added convenience, but the absence of access control and hazard alerts limited its scope in terms of comprehensive home safety.

In summary, while existing research offers valuable progress in isolated aspects of smart home systems, there's still a significant need for a more integrated and affordable solution. This paper addresses that need by introducing a cohesive system that integrates biometric access, real-time hazard detection, and remote appliance control.

J. Adv. Ind. Technol. Appl. Vol. 7 No. 1 (2026) p. 118-130

3. Novelty and Comparison

This system uniquely integrates facial recognition, IoT appliance control, and gas detection using low-cost ESP32-S3 hardware. Unlike previous systems that separate safety from automation, this framework enables simultaneous monitoring and actuation. Table 1 compares this work with some recent implementations.

Table 1 *Comparison of related works and the proposed system*

Trait	[15]	[16]	[17]	[18]	Proposed System
Facial Recognition	No	No	No	Yes (OpenCV)	DeepStack
Gas Detection	No	Yes (MQ-2)	Flame Sensor	No	MQ-2, MQ-9, MQ-135
Internet of Things Appliance Control	Yes (Blynk)	Yes	Yes (Blynk)	No	Mobile App (HTTP)
Unified Integration	Partial	No	No	No	Yes
Custom Mobile Application	Yes (Blynk)	Not Mentioned	Yes (Blynk)	No	MIT App Inventor
Hardware	ESP32	Arduino Mega	NodeMCU	Raspberry Pi	ESP32-S3
Cloud	Yes (Blynk Cloud)	No	Yes (Blynk)	No	Google Sheets

4. Proposed System

The proposed system consists of two primary modules: the security door unit for access control and the controlling unit for home automation and hazard detection. Each unit is presented with its respective system design and operational flow.

4.1 Security Door Unit

The block diagram of the security door unit, shown in Fig. 1 illustrates the process of facial recognition-based access control. The operational process for facial recognition-based access control of the security door unit was depicted in Fig. 2. The facial recognition process employs a pre-trained DeepStack model deployed on a local server, which performs image verification in real time. The ESP32-S3 CAM captures a facial image and sends it to the DeepStack service for comparison with the stored dataset. If a match is detected, the microcontroller activates the relay module to unlock the door, ensuring secure and contactless user access. Alternatively, authorized users also can unlock the door remotely via the mobile application, providing a secondary access method through secure login authentication.

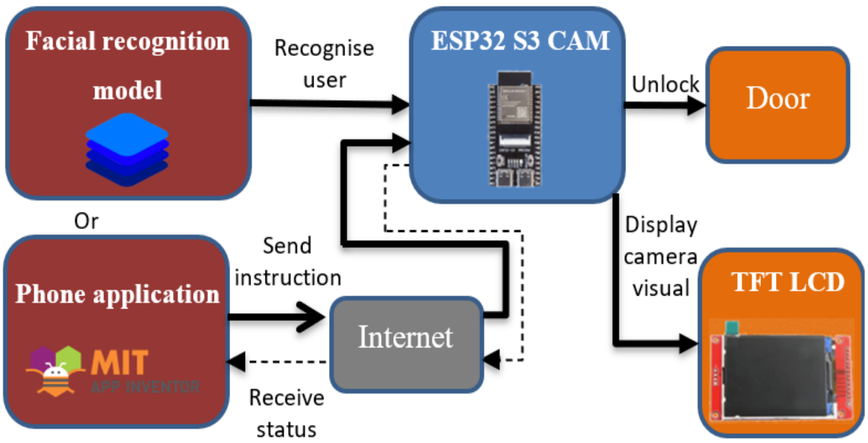


Fig. 1 *Block diagram of the security door unit*

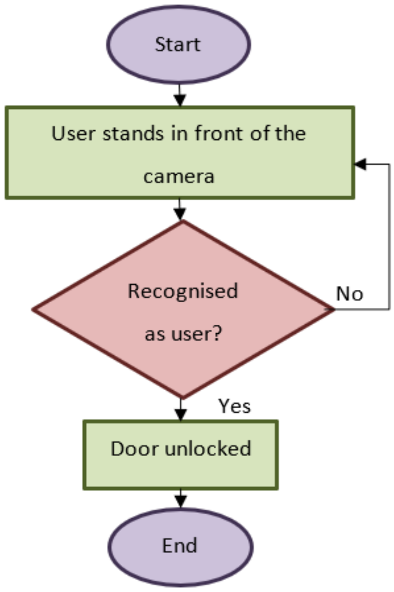


Fig. 2 *Flowchart of the security door unit*

4.2 Controlling Unit

The controlling unit, shown in Fig. 3, is designed to perform two primary functions: remote control of household appliances and detection of hazardous gases. An ESP32-S3 microcontroller serves as the central controller, interfacing with a 6-channel relay module to manage appliances such as lights and fans. The system incorporates MQ-2, MQ-9, and MQ-135 gas sensors to detect flammable or harmful gases in the environment.

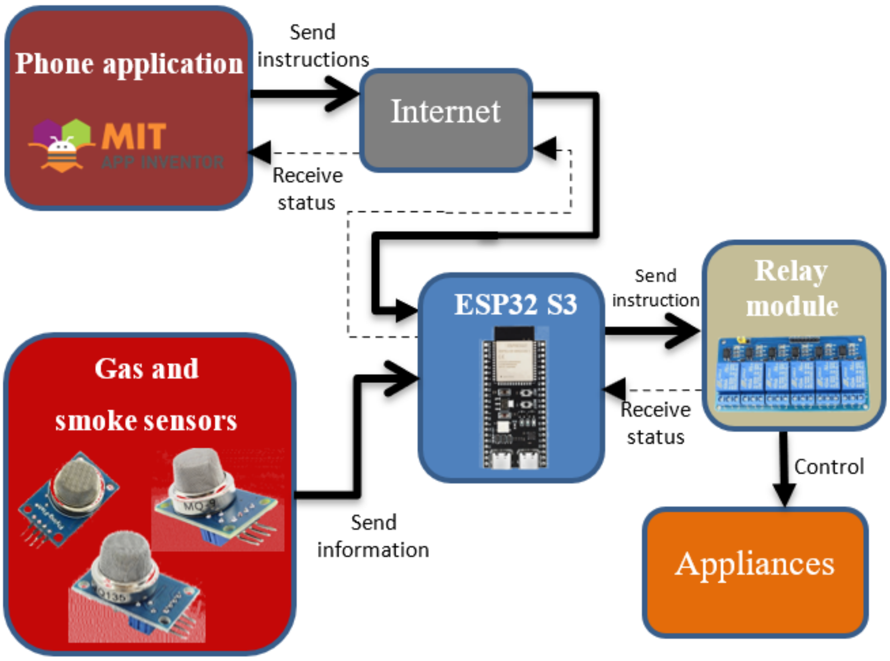


Fig. 3 *Block diagram of the controlling unit*

Fig. 4 shows the operational flow of the control unit, which begins with continuous monitoring of environmental gas concentrations using the connected sensors. Simultaneously, the ESP32-S3 remains ready to receive appliance control commands issued via the mobile application. Appliance switching is executed via the relay module, with real-time feedback communicated to the user through the mobile app interface. If the hazardous gas levels are detected, the system immediately activates a buzzer to provide an audible local alert and sends a notification to the mobile app.

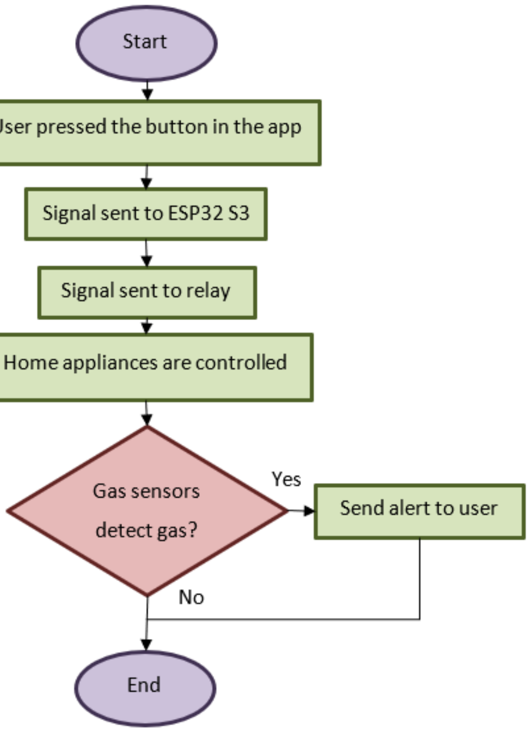


Fig. 4 *Flowchart of the controlling unit*

Fig. 5 shows the circuit diagram of the controlling unit utilizes an ESP32-S3 microcontroller to interface with both environmental sensors and appliance control hardware. MQ-2, MQ-9, and MQ-135 gas sensors are employed for flammable gas and air quality detection. For home automation, a 6-channel relay board is connected to household appliances, enabling the ESP32-S3 to switch devices on and off via user commands from the mobile application.

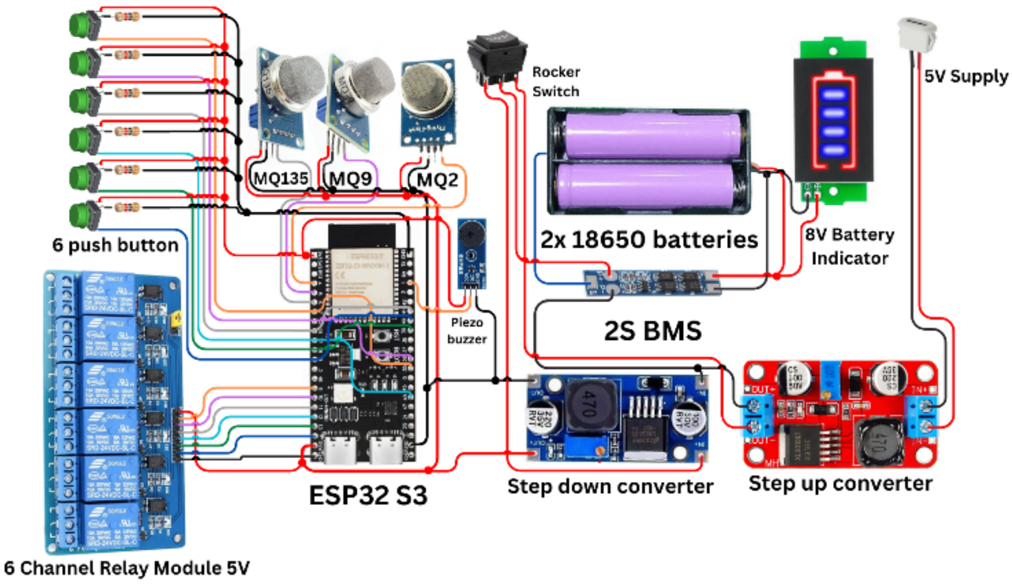


Fig. 5 *Circuit diagram of the controlling unit*

When a hazardous gas is detected, the ESP32 activates a piezoelectric buzzer to provide an immediate local alert. Appliance status and environmental readings are communicated wirelessly to the mobile application over the local network. The system is powered by a regulated 5 V supply derived from a standard 12 V DC adapter, which is stepped down via a buck converter to power the ESP32 and sensor modules.

By integrating these two modules, the system delivers both safety and automation within a single, locally processed IoT framework, ensuring seamless communication between sensing, decision-making, and actuation layers.

4.3 Software

The software implementation of the system consists of three main components: facial recognition processing, mobile application control, and cloud data management.

4.3.1 Facial Recognition Implementation

The ESP32-S3 CAM captures facial images and sends them to the DeepStack facial recognition server hosted on a local device via HTTP POST requests. The DeepStack model, running inside a Docker container (as illustrated in Fig. 6), processes the image and returns a JSON object containing the identification result and confidence score. The ESP32-S3 CAM will interpret the result to determine whether to trigger the relay for door unlocking. To initiate the capture process, a push button on the Security Door Unit was installed for allowing the ESP32 to conserve processing resources when idle.

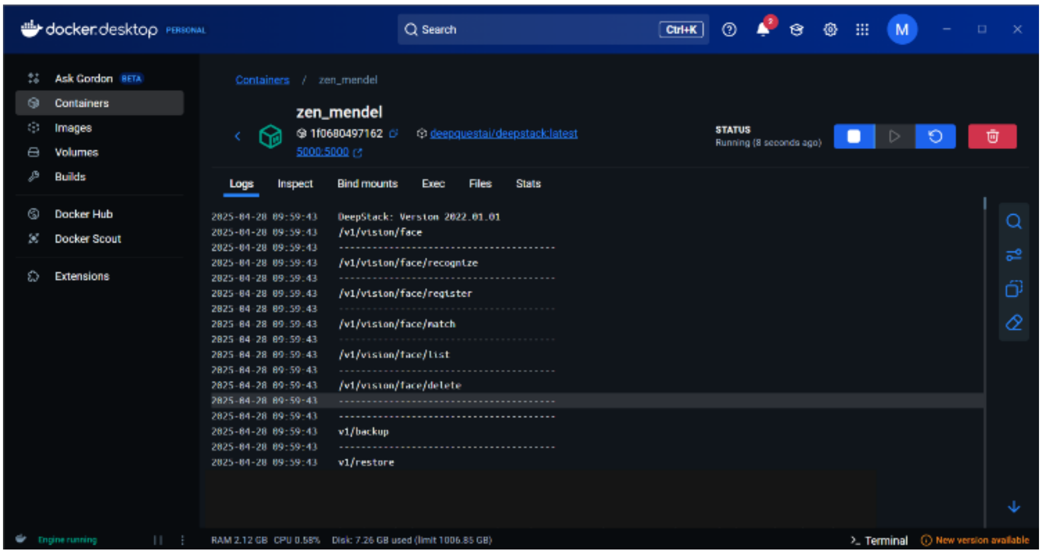


Fig. 6 *Docker desktop with DeepStack running*

4.3.2 Mobile Application Implementation

To give users easy control over their home appliances and the door lock system, a custom Android app was created using MIT App Inventor, as shown in Fig. 7. The app connects to ESP32-S3 microcontrollers via the local network, sending commands through HTTP GET requests. The app also delivers real-time updates, such as appliance status and gas leak alerts. To keep the system secure, a login feature restricts access to authorized users, working alongside the facial recognition system at the door to enhance overall security.

4.3.3 Cloud Integration

To store and synchronize appliance data and user settings, the system uses Google Sheets as a lightweight cloud backend. Communication between the MIT App Inventor application (as shown in Fig. 8) and the cloud is handled through Google Apps Script, which acts as a bridge between the app and the spreadsheet. The app sends HTTP POST requests containing user commands and system updates, which are written to specific cells within the sheet. Similarly, the app sends HTTP GET requests to retrieve appliance statuses and gas sensor readings, ensuring real-time synchronization between the local ESP32-S3 microcontroller and the cloud. This setup provides a simple yet effective cloud solution for real-time monitoring without the need for complex IoT platforms such as Firebase or AWS IoT.

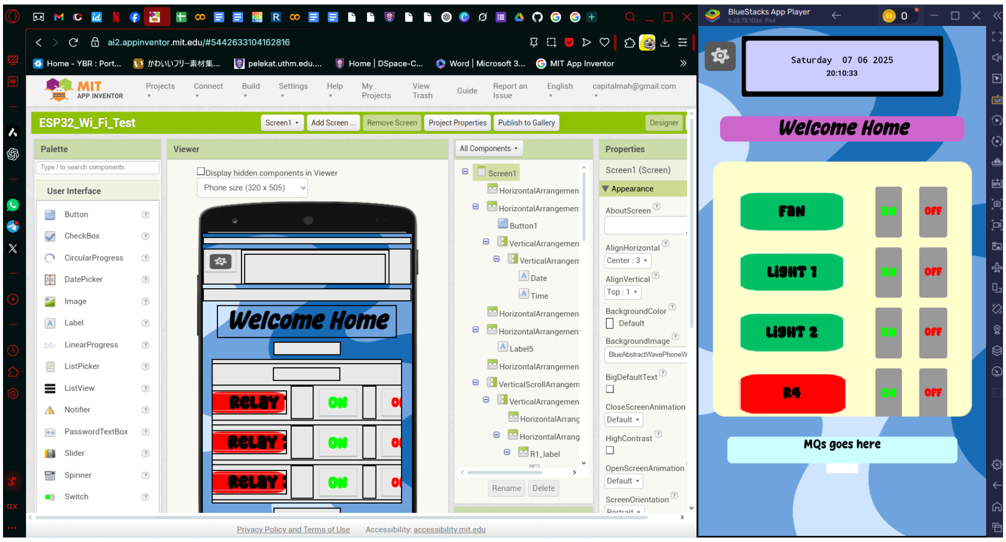
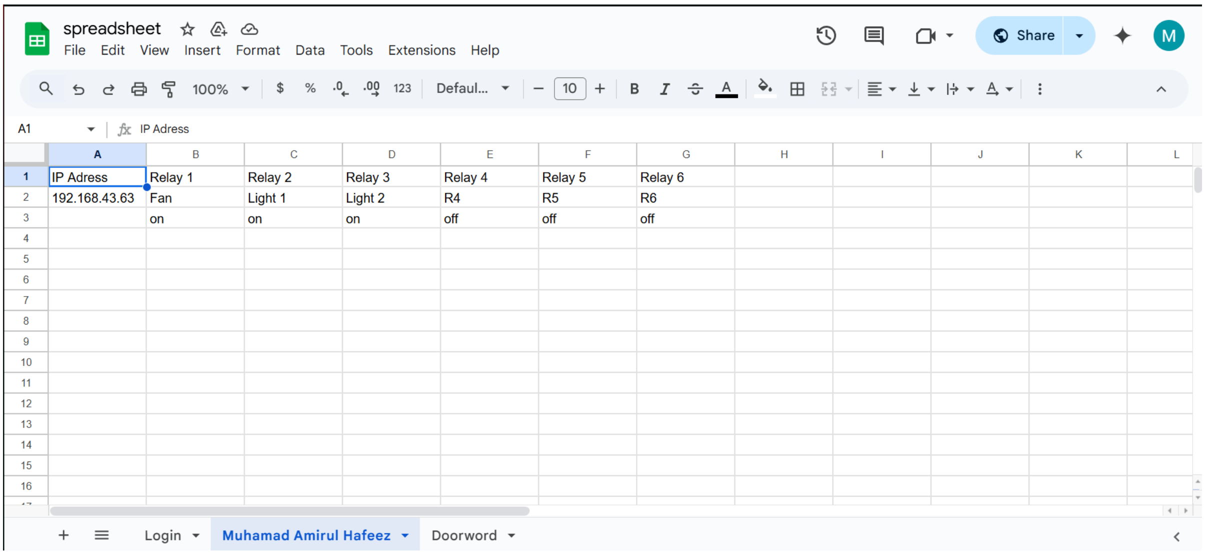


Fig. 7 *Development of the mobile application in MIT App Inventor*



IP Adress	Relay 1	Relay 2	Relay 3	Relay 4	Relay 5	Relay 6
192.168.43.63	Fan	Light 1	Light 2	R4	R5	R6
	on	on	on	off	off	off

Fig. 8 *The spreadsheet used within Google Sheets*

4.4 Experimental Setup

Each part of the system requires proper setup and different conditions to get satisfactory results.

4.4.1 Facial Recognition Setup

Facial recognition performance was verified in three different environments: indoors and outdoors (day and night). The tests were carried out by varying the user distances from the camera by 30 cm, 45 cm, 60 cm, and 75 cm. During the tests, the security door unit was placed at the same height as the user's face. For indoor testing, a 5 V, 3 W LED bulb was positioned above the unit to provide consistent illumination of the user's face, as shown in Fig. 9. For outdoor testing during the day, natural sunlight served as the illumination source, while the LED bulb was used again at night.

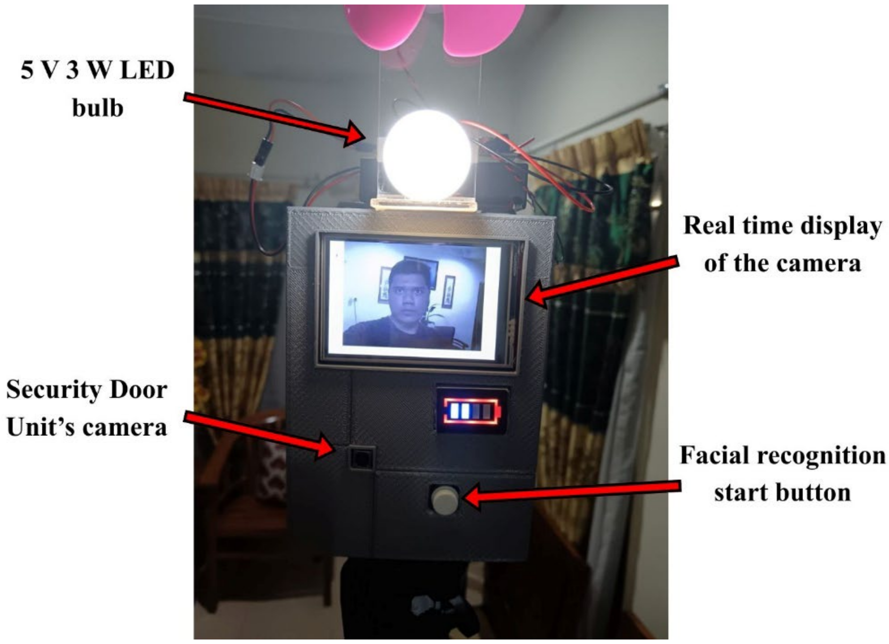


Fig. 9 *Setup of the security door unit for indoor testing*

The prediction value is the model's confidence, ranging from 0 to 1, that the input face matches a registered identity. The value was obtained by connecting the ESP32-S3 CAM module to the laptop running Arduino IDE and reading the serial monitor output. The serial monitor displays the successful recognition parameters, such as the user's name and the corresponding prediction value, as highlighted in Fig. 10.

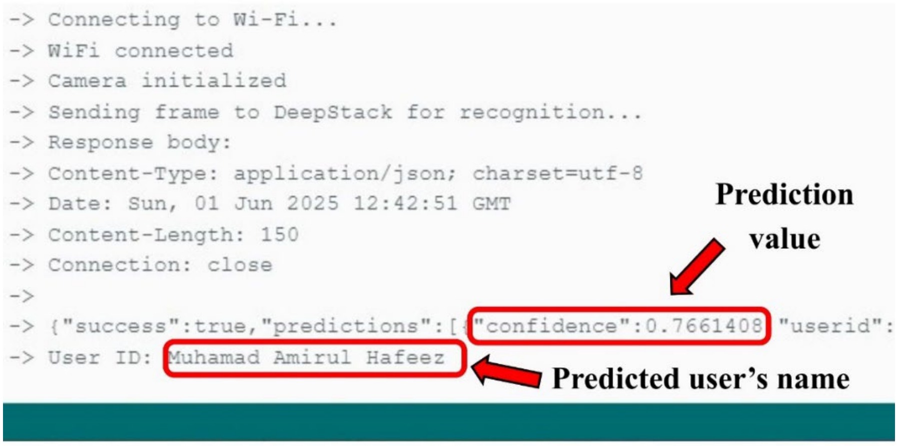


Fig. 10 *Prediction value through Arduino IDE*

Two metrics were used to measure the performance: the Success Rate (SR), calculated as shown in (1), and the Average Prediction (AP), defined in (2).

The Success Rate (SR) was calculated as:

$$\frac{Number\ of\ successful\ identifications}{Total\ number\ of\ recognition\ attempts} \times 100\% = success\ rate\ (\%) \tag{1}$$

while the Average Prediction (AP) was computed as:

$$\frac{Total\ predictions}{Total\ number\ of\ recognition\ attempts} = Average\ Prediction \tag{2}$$

4.4.2 Appliances Control Setup

The performance of the appliance control system was evaluated by measuring the average switching times for turning appliances on and off using two control methods: the mobile application and physical push buttons. The experimental setup is as illustrated in Fig. 11.

Three conditions were tested: controlling a fan, a light, and an unloaded relay (no appliance attached). 7.4V batteries were regulated to 5V and used as the supply for these devices, which served as appliances. The application was opened in a phone emulator for a clearer view of any changes.

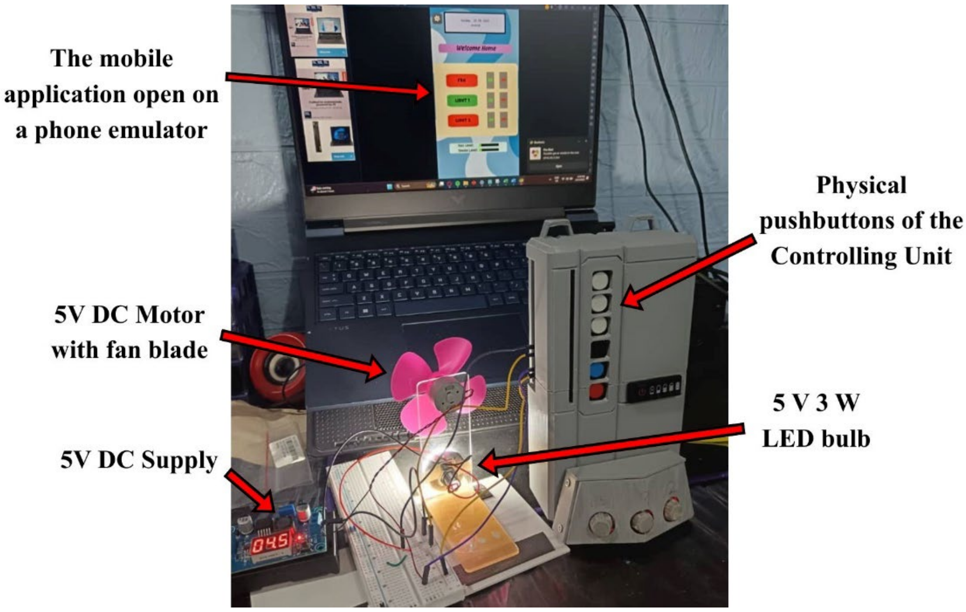


Fig. 11 *Setup of the controlling unit*

4.4.3 Gas Detection Setup

The gas detection performance of the system was evaluated by measuring the time taken for the gas sensors to detect hazardous gas at varying distances from the source. The tests were conducted using a butane gas source dispersed at distances of 20 cm, 40 cm, 60 cm, and 80 cm from the sensors, as illustrated in Fig. 12.

A plastic plate was used to mark where the gas should be dispersed and control its spread. The distance was measured using a small measuring tape capable of measuring up to 100cm. Detection time was recorded in milliseconds (ms) from the release of gas to the activation of the system's alert mechanism.

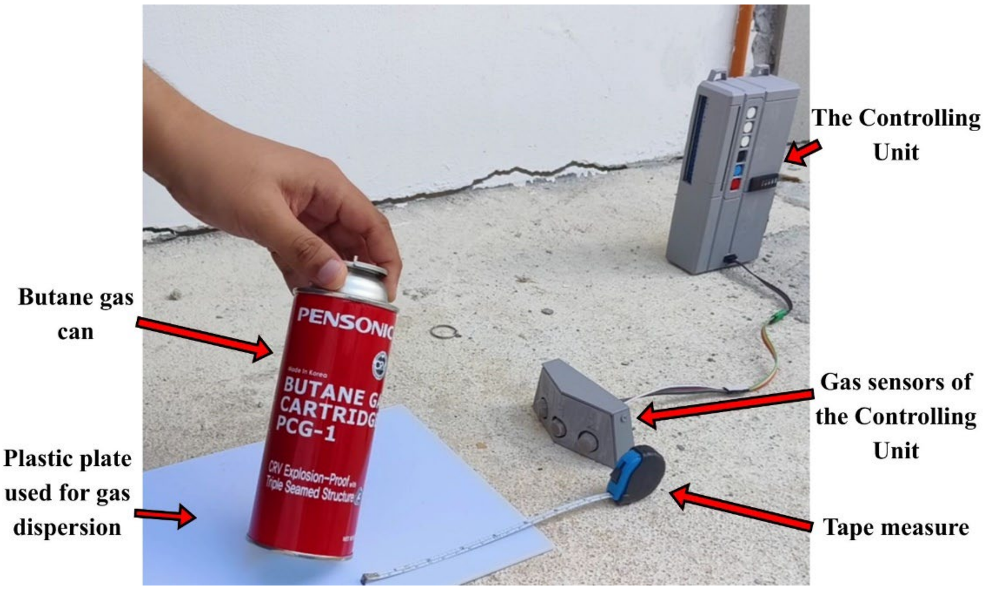


Fig. 12 *Setup of the gas sensors of the controlling unit*

5. Experimental Results

The performance in terms of its facial recognition, appliance control, and gas control, was evaluated under various previously established test setups.

5.1 Facial Recognition Performance

As shown in Table 2, the success rate (SR) consistently achieved 100% across all conditions and distances, indicating that the system reliably identified authorised users in every trial, regardless of environment or distance.

The highest average prediction (AP) was observed during indoor testing at 60 cm (0.78559) and daytime testing at 60 cm (0.7788), suggesting optimal recognition performance at moderate distances under favourable lighting conditions. Although AP values decreased slightly at 75 cm across all environments, recognition accuracy remained sufficient to maintain a 100% success rate. Night time testing produced slightly lower AP scores, with the lowest being 0.72705 at 75 cm, yet still achieved perfect recognition performance.

Table 2 *Results of facial recognition with different settings*

Distance (cm)	Indoor – Average Prediction (AP)	Indoor – Success Rate (SR) (%)	Day – Average Prediction (AP)	Day – Success Rate (SR) (%)	Night – Average Prediction (AP)	Night – Success Rate (SR) (%)
30	0.76383	100	0.78105	100	0.75582	100
45	0.78245	100	0.77643	100	0.75817	100
60	0.78559	100	0.7788	100	0.75698	100
75	0.74303	100	0.74597	100	0.72705	100

These results confirm that the proposed facial recognition system is robust across different environments and distances, making it suitable for secure access control in smart home applications.

5.2 Appliances Control Performance

According to Table 3, the results show that both mobile application and physical push-button control methods provide responsive appliance operation with switching times well below one second. However, the push-button control exhibited slightly shorter and more consistent response times, ranging from 274 ms to 378 ms, compared to 294 ms to 421 ms for the mobile application. This small difference is primarily due to the network transmission delay in the mobile control path. Despite this, both methods delivered stable and reliable performance suitable for practical home automation, confirming that the proposed IoT control architecture can support real-time actuation of household devices.

Table 3 *Average response time for appliance control using different methods*

Type of home appliance	Mobile application – On (ms)	Mobile application – Off (ms)	Push button – On (ms)	Push button – Off (ms)
Fan	369	367	362	274
Light	421	335	343	342
Unloaded	298	294	378	276

5.3 Gas Detection Performance

As detailed in Table 4 and Fig. 13, the results showed a clear correlation between distance and detection time. The system achieved the fastest average detection at 20 cm (1,813 ms), with detection time progressively increasing as the distance increased. The longest detection time was recorded at 80 cm (15,433 ms), reflecting the reduced gas concentration that reached the sensors at greater distances.

Table 4 *Results of gas detection with varying distances*

Distance (cm)	Attempt 1 (ms)	Attempt 2 (ms)	Attempt 3 (ms)	Average (ms)
20	1270	2100	2070	1813
40	6170	4270	2290	4243
60	9010	3020	6030	6020
80	21730	12010	7160	15433

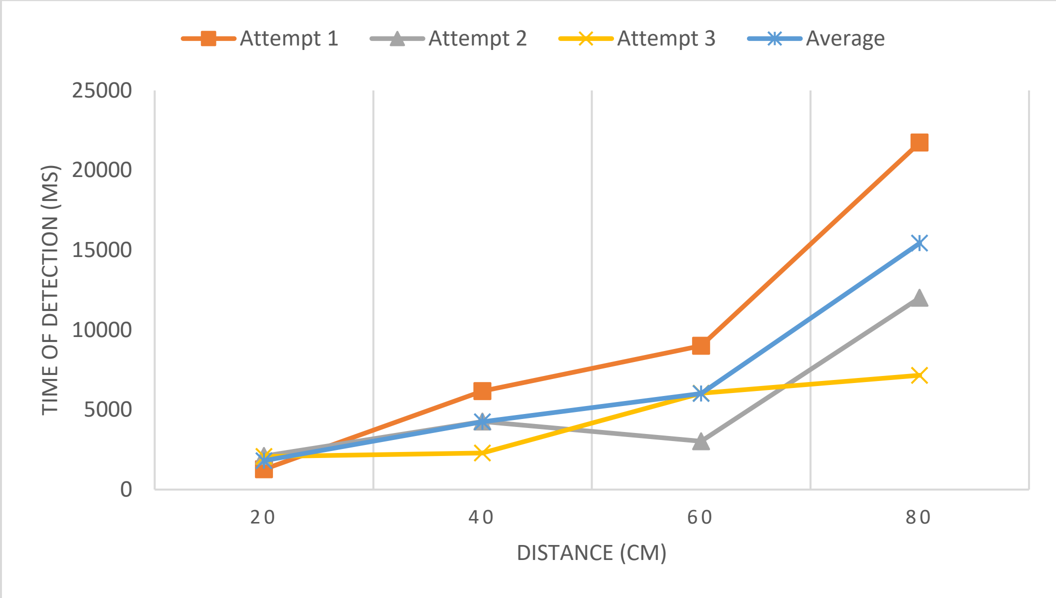


Fig. 13 *Graph of gas detection time versus distance*

Despite the increase in detection time with distance, the gas detection system consistently activated alarms for all test scenarios, confirming its reliability in detecting hazardous gases within close proximity. For larger or multi-room environments, the deployment of multiple sensors is recommended to ensure comprehensive coverage and faster detection across the entire area.

5.4 Complete System Setup

The fully assembled system is illustrated in Fig. 14, highlighting the integration of both the security door unit and the controlling unit. The security door unit, positioned on the left, consists of a door assembly equipped with a solenoid actuator, a TFT LCD, ESP32-S3 CAM, and a tactile push button for initiating facial recognition. Positioned adjacent to it, the Controlling Unit is paired with a house model, serving as a simulated residential environment to facilitate realistic evaluation of the system's operational performance under representative conditions.

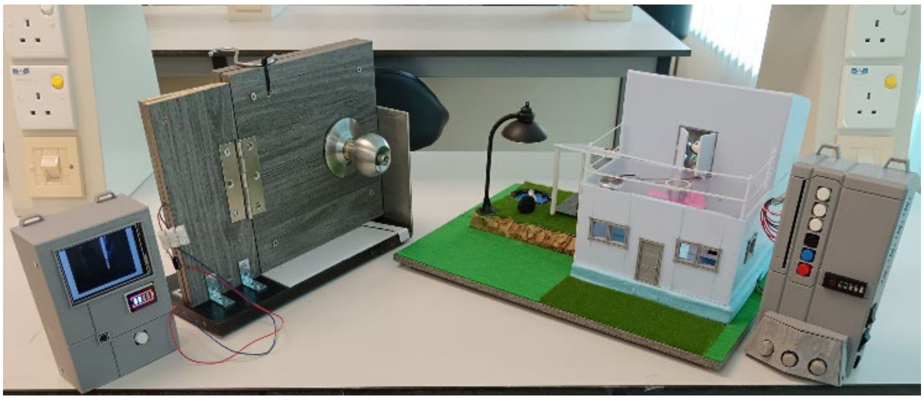


Fig. 14 *Fully assembled smart home safety and automation prototype system*

6. Conclusions

The proposed system successfully integrates facial recognition, gas detection, and IoT-based appliance control into a unified home framework. Experimental results demonstrated consistent and reliable performance across all modules. The facial recognition component achieved 100% recognition success under various distances and lighting conditions, ensuring secure and convenient access. The gas detection module effectively detected hazardous gases, such as butane, across different ranges, while the appliance control unit demonstrated sub-second switching latency during both mobile and manual operation.

The results validate the system's capability as a practical smart home platform for residential safety and automation. Future enhancements will focus on improving system scalability and security by integrating liveness detection to prevent spoofing attacks, adopting cloud-based IoT infrastructures for remote access beyond local networks, and deploying multiple sensor nodes for wider area coverage. Incorporating voice assistant compatibility could further enhance user interaction and accessibility.

Acknowledgement

The authors would also like to thank the Faculty of Electrical and Electronic Engineering at Universiti Tun Hussein Onn Malaysia for its support.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***Study conception and design****: Muhamad Amirul Hafeez Bin Azhar;* ***Data collection****: Muhamad Amirul Hafeez Bin Azhar;* ***Analysis and interpretation of results****: Muhamad Amirul Hafeez Bin Azhar;* ***Draft manuscript preparation****: Muhamad Amirul Hafeez Bin Azhar; Zuhairiah Zainal Abidin,* ***Validation of the research****: Zuhairiah Zainal Abidin, Saizalmursidi Md Mustam, Shaharil Mohd. Shah.*

References

[1] Jubit, N., Masron, T., & Marzuki, A. (2020). Spatial pattern of residential burglary: The case study of Kuching, Sarawak. Planning Malaysia, 18(13). https://doi.org/10.21837/pm.v18i13.785

[2] Abdul Kader, M. (2023, August 16). Letter: Improve safety standards for cooking gas cylinders. Malaysiakini. https://www.malaysiakini.com/letters/675922

[3] Shawon, N., Memo, M. P., Arafat, Y., Jannat, F., Uddin, M., & Hasan, M. (2023, December). IoT-based home monitoring and danger alert. In Proceedings of the 10th IEEE International Conference on Power Systems (ICPS) (pp. 1–5). https://doi.org/10.1109/ICPS60393.2023.10429027

[4] Rahiman, M. A., & Manohar, D. (2022). Smart home monitoring system using ESP32 and IoT. BSSS Journal of Computer, 13(1). https://doi.org/10.51767/jc1308

[5] Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of smart-home security using the Internet of Things. Electronics, 13(16), 3343. https://doi.org/10.3390/electronics13163343

[6] AlJanah, S., Zhang, N., & Tay, S. W. (2021). A survey on smart home authentication: Toward secure, multi-level and interaction-based identification. IEEE Access, 9, 130914–130927. https://doi.org/10.1109/ACCESS.2021.3114152

[7] Rahim, A., Zhong, Y., Ahmad, T., Ahmad, S., Pławiak, P., & Hammad, M. (2023). Enhancing smart home security: Anomaly detection and face recognition in smart home IoT devices using logit-boosted CNN models. Sensors, 23(15), 6979. https://doi.org/10.3390/s23156979

[8] Chaurasia, T., & Jain, P. K. (2020). A survey of control mechanisms for smart home systems. International Journal of Computer Applications, 175(9), 26–30. https://doi.org/10.5120/ijca2020920560

[9] Singh, S. K., & Mishra, V. (2020). IoT-based home automation system using ESP8266 and Blynk. International Journal of Scientific Research Engineering and Development, 3(5), 1114–1118.

[10] Etuk, U. E., Omenaru, G., Inyang, S. J., & Umoren, I. (2023). Towards sustainable smart living: Cloud-based IoT solutions for home automation. Journal of Information Systems and Informatics, 5(4), 1743–1763. https://doi.org/10.51519/journalisi.v5i4.621

[11] Thomas, L., & Mathew, D. (2020). Design and implementation of an IoT-based smart home system. In Proceedings of the 4th International Conference on Computing, Communications and Networking Technologies (ICCCNT) (pp. 1–5). https://doi.org/10.1109/ICCCNT49239.2020.9225539

[12] Hassan, S. A., & Eassa, A. M. (2022). A proposed architecture for smart home systems based on IoT, context-awareness, and cloud computing. International Journal of Advanced Computer Science and Applications, 13(6). https://doi.org/10.14569/IJACSA.2022.0130612

[13] Patil, S., Gaikwad, A., & Tarte, R. (2020). Home automation using Arduino and IoT. International Research Journal of Engineering and Technology, 7(5), 2316–2320.

[14] Pandey, A. R., & Tiwari, A. (2020). Gesture-based control of home appliances using Arduino. International Journal of Scientific & Technology Research, 9(3), 7160–7164.

[15] Verma, G., Pachauri, S., Kumar, A., Patel, D., Kumar, A., & Pandey, A. (2023). Smart home automation with smart security system over the cloud. In Proceedings of the 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1–7). https://doi.org/10.1109/ICCCNT56998.2023.10306548

[16] Karnatak, V., Mittal, S., Mishra, A. K., & Pandey, N. K. (2023). IoT-based energy-efficient smart home security. In Proceedings of the 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT) (pp. 1–6). https://doi.org/10.1109/CISCT57197.2023.10351475

[17] Mustafa, B., Iqbal, M. W., Saeed, M., Shafqat, A. R., Sajjad, H., & Naqvi, M. R. (2021). IoT-based low-cost smart home automation system. In Proceedings of the 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1–6). https://doi.org/10.1109/HORA52670.2021.9461276

[18] Kumar, A. S., & Rekha, R. (2023). Improving smart home safety with face recognition using machine learning. In Proceedings of the International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS) (pp. 478–482). https://doi.org/10.1109/ICISCoIS56541.2023.10100592

[19] Siddhartha, C. S., Kalyan, G. P., & Sravan, T. (2021). Facial recognition-based smart home access system using Raspberry Pi. International Journal of Engineering Trends and Technology, 69(4), 58–65. https://doi.org/10.14445/22315381/IJETT-V69I4P209

[20] Anjum, F., Gani, R., Isty, M. N., Ali, M. S., & Hasan, M. (2024). IoT-based smart home automation system: Ensuring safety for the elderly. In Proceedings of the 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT) (pp. 214–219). https://doi.org/10.1109/InCACCT61598.2024.10551092

[21] Urmee, R. A., Prome, N. S., & Ahmed, T. (2022). Hand gesture-based home automation system. In TENCON 2022: IEEE Region 10 Conference (pp. 1–5). https://doi.org/10.1109/TENCON55691.2022.9977647