IRJCS: International Research Journal of Computer Science
Volume 12, Issue 11, November 2025
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1211.03

Home Automation System Using Intelligent Face Recognition: An IoT–AI Integrated Approach

Ass.Prof.Nandini KN
Professor, Dept of ISE
Sri Sairam College of Engineering, Bengaluru, India
nandinikrn878@gmail.com
https://orcid.org/0009-0005-4498-1351
Tanushree P,Vinutha S,Kiran C, Shashank DA
Students, Dept of ISE
Sri Sairam College of Engineering, Bengaluru, India

Publication History
Manuscript Reference: IRJCS/RS/Vol.12/Issue11/NVCSXI10082
Research Article | Open Access | Double-Blind Peer Reviewed Article ID: IRJCS/RS/Vol.12/Issue11/NVCSXI10082
Received:23,October 2025, Revised: 09, October 2025, Accepted: 31October 2025 Published Online: 21November 2025
https://www.irjcs.com/volumes/Vol12/iss-11/03.NVCSXI10082.pdf
Article Citation:Ass.Prof.Nandini,Tanushree,Vinutha,Kiran,Shashank(2025), Home Automation System Using Intelligent Face Recognition: An IoT–AI Integrated Approach **,**IRJCS: International Research Journal of Computer Science, Volume 12, Issue 11 of 2025 pages 648-652 **Doi:>**https://doi.org/10.26562/irjcs.2025.v1211.03
BibTeX Key Ass.Prof.Nandini@2025Home
IRJCS papers should be cited as IRJCS (International Research Journal of Computer Science, AM Publications, India 2025, ISSN 2393-9842, https://doi.org/10.26562/ijrcs.2025.v1211.03 The journal's official abbreviation is IRJCS.
Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: This research introduces a smart home automation system that combines deep-learning-based face recognition with IoT- enabled appliance control to improve household security and safety. Unlike traditional systems that depend on passwords, mobile applications, or internet-based assistants, the proposed design performs local, real-time facial authentication to ensure that only authorized users can access home controls. The system manages lighting, gas valves, and safety functions through an integrated dashboard, while continuously monitoring environmental conditions such as gas leaks. Developed using Python, OpenCV, and a Raspberry Pi platform, the system operates with high accuracy, low latency, and complete offline capability. Experimental evaluation shows that the solution enhances privacy, reduces security risks, and provides a scalable, cost-effective approach for modern home automation. The results demonstrate its suitability for residential, commercial, and safety-critical environments.
Keywords: Smart Home Automation, Facial Authentication, IoT Devices, Raspberry Pi System, Computer Vision, Deep Learning Model, Appliance Control, Gas Safety Monitoring, Real-Time Processing, Secure Access.

I. INTRODUCTION

The evolution of the Internet of Things (IoT) has paved the way for smart homes capable of automating everyday activities, enhancing user comfort, energy efficiency, and safety. As automation technologies become more common in residential and commercial environments, the challenge of securing these systems has gained considerable attention. Most traditional home automation platforms rely on mobile applications, Bluetooth remotes, passwords, or voice assistants for user authentication. While these methods are widely adopted, several studies have highlighted their limitations in terms of security, reliability, and resistance to unauthorized access. For instance, a study published in the International Journal of Smart Home Systems (2021) reported that PIN- based and mobile-app-controlled systems are prone to credential leakage, device theft, and remote hacking attempts. Similarly, research in the Journal of IoT Security and Applications (2022) demonstrated that voice- controlled devices such as smart speakers can be activated through replay attacks, allowing outsiders to manipulate appliances without user consent. These findings emphasize the need for stronger, tamper-resistant authentication methods in home automation. Biometric authentication has emerged as a more secure and intuitive alternative. Among all biometric methods, facial recognition is particularly suitable for smart home environments due to its hands-free operation, natural interaction, and increasing accuracy. Studies published in the International Journal of Computational Vision and Robotics (2023) and the European Journal of Embedded Systems (2022) have shown that deep-learning-based facial recognition models outperform traditional methods in identification accuracy while maintaining low computational requirements making them ideal for real-time embedded applications. Motivated by these advancements, this research proposes a comprehensive home automation system that integrates face recognition with IoT-driven control mechanisms. The system captures real-time facial images, processes them using deep-learning-based encoding algorithms, and authenticates the user before granting access to an interactive control dashboard. Authorized users can operate lighting systems, adjust brightness levels, manage gas valves, and monitor safety alerts. A gas-leak sensor is further incorporated to prevent hazardous incidents by activating automatic shutdown procedures when abnormal readings are detected.

ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1211.03

Unlike many commercial systems that depend heavily on cloud services, the proposed model performs all operations locally using a Raspberry Pi. This design eliminates privacy risks, reduces latency, and ensures system functionality even without internet connectivity. The modular architecture also supports scalability, enabling seamless integration of additional sensors, appliances, and biometric modules in the future. Overall, this work contributes a secure, privacy-preserving, and user-friendly automation framework suitable for modern smart homes, apartments, laboratories, and small commercial environments. By combining facial recognition with IoT automation and safety monitoring, the system demonstrates a practical approach to intelligent living environments that prioritize both convenience and security.

II. RELATED WORK

Research on smart home automation and biometric authentication has gained strong momentum over the past decade. Several well-established studies have investigated both face-recognition technologies and IoT-based automation, forming the foundation for modern intelligent home systems. One of the most influential works in facial recognition is the "Deep Face" model introduced by Taigman et al. (2014), published by Face book AI Research. The study demonstrated that deep learning significantly enhances face recognition accuracy compared to traditional feature-based techniques. Building on this, Schroff, Kalenichenko, and Philbin(2015) proposed the FaceNet architecture in their IEEE CVPR paper, achieving high accuracy using deep embedding techniques. These works laid the groundwork for real-time face authentication used in embedded systems today. In the IoT automation domain, Alamri et al. (2020) presented a scalable home automation architecture in their Elsevier paper" IoT-Based Smart Home: Security Challenges and Solutions", highlighting issues related to unauthorized access, weak encryption, and device exploitation. Their findings emphasized the need for systems that combine both automation and reliable authentication instead of relying solely on mobile apps or voice commands. Another study by Bhardwaj and Hans (2021), published in Springer's Journal of Ambient Intelligence and Humanized Computing, proposed an IoT-based home automation framework but noted that password-based access still exposed the system to security vulnerabilities. The authors recommended integrating biometrics as a safer alternative. Face-recognition-based smart home systems have also been explored in recent practical implementations. For example, Khan et al. (2022) developed an edge-based facial authentication system using Raspberry Pi, as documented in the journal Sensors (MDPI). Their results showed that light weight CNN models can perform efficiently on embedded boards but also pointed out limitations such as the lack of safety-critical features like gas monitoring and emergency shutdown systems. Safety-oriented automation systems have also been studied independently. Rajput and Singh(2021) introduced a gas-leak detection and alarm model using MQ sensors in their IEEE conference paper "Smart Safety System for Domestic Gas Detection", but the system lacked secure user authentication and was limited to alerting functions. From the literature, it is clear that previous works either focus on biometric authentication, IoT automation, or safety monitoring, but rarely combine all three into a unified framework. Most existing solutions depend on cloud connectivity, lack local processing for privacy, or omit critical safety components such as gas-leak response mechanisms. The proposed system addresses these gaps by integrating real-time face recognition, IoT device control, gas- leak detection, and offline processing into a single, secure, and privacy-preserving architecture suitable for modern smart homes.

III. METHODOLOGY

The proposed home automation system integrates facial recognition, appliance control, and safety monitoring using a combination of software algorithms and embedded hardware. The methodology is structured into four major stages: data acquisition, facial authentication, system control, and safety management. Each stage is designed to operate in real-time and completely offline using a Raspberry Pi processor.

System Work flow Overview

The system follows a continuous cycle starting from camera initialization to real-time decision-making. Once the device is powered on, the camera begins capturing live video frames. These frames are processed to detect and recognize authorized users. If authentication is successful, the control dash board is activated, allowing the user to operate home appliances such as lights and gas valves. The system also runs a parallel monitoring process to detect gas leaks and trigger emergency safety responses.

Data Acquisition and Preprocessing

A USB camera connected to the RaspberryPi is used to continuously capture video frames. The following preprocessing steps are applied:

1. Frame Conversion: Each frame is converted to RGB format for compatibility with the facial recognition algorithm.
2. Frame Resizing: Images are scaled down to reduce computational load while maintaining recognition accuracy.
3. Face Detection: A face detection model (HOG-based detector) identifies the position of faces in the frame.

This preprocessing ensures that only valid facial regions are passed to the next stage, improving reliability and processing speed.

Facial Recognition and User Authentication

Once a face is detected, the system extracts unique facial features by generating numerical encodings. These Encoded values are compared with stored encodings of registered users. Steps in Authentication

1. Face Land mark Extraction: The system identifies key facial points required for accurate feature representation.
2. Encoding Generation: A1 28-dimensional numeric vector is created for each face.
3. Matching Algorithm: The new encoding is compared with the database using a predefined tolerance level.
4. Access Decision:

o Match found→Dash board access granted.

ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1211.03

- No match→Access blocked.

This ensures that only authorized individuals can control the home appliances.

Dash board Interface and User Interaction

A Python Tkinter-based GUI serves as the control dashboard. After successful authentication, the dashboard becomes active and displays:

- Light control buttons
- Brightness adjustment sliders
- Gasvalve on/off controls
- Live system status indicators
- Activity logging panel

User actions on the dashboard initiate commands that are transmitted to the hardware control module.

Appliance Control Using Relay Modules

The system uses an 8-channel relay module to manage electrical appliances. Each relay is linked to a specific household device such as lights or the motorized gas valve.

Control Process

1. Dashboard input→command is passed to control logic
2. Relay corresponding to the device is activated/deactivated
3. Status is updated on the dashboard
4. Activity logis recorded locally

This ensures synchronized interaction between the software interface and physical appliances.

Gas Monitoring and Safety Mechanism

A dedicated safety module continuously monitors gas levels using the MQ-5 sensor. Safety Process

1. Sensor detects gas concentration
2. Values are compared with safe thresholds
3. If leakage is detected:
   - Gas valve is automatically closed
   - Warning alert is displayed on the dashboard
   - Safety logentry is recorded

This real-time response significantly reduces potential risks related to gas leakage.

Parallel Processing and Real-Time Execution

To maintain fast performance, the system uses multithreading:

- Thread 1: Camera input + face recognition
- Thread 2: Dashboard control and user interactions
- Thread 3: Gas sensor monitoring and emergency response

This parallelization ensures that authentication, control, and safety operations function independently without delay.

Logging and Data Management

All user actions, authentication attempts, and safety events are stored in a local SQLite database. This provides:

- Complete audit trail
- User accountability
- Reference for trouble shooting or system evaluation

IV. EXPERIMENTAL RESULTS & DISCUSSION

The proposed home automation system was tested to evaluate its performance in real-time facial authentication, appliance control responsiveness, and gas-leak safety operations. Multiple experiments were conducted under different lighting conditions, user angles, and sensor environments to ensure system reliability in realistic home settings.

Facial Recognition Accuracy

The facial recognition module wastested using a dataset consisting of registered users and non-registered individuals. Frames were captured at various distances (0.5m to 2m) and angles (0°, 30°, and 60°).

Key Observations

- Average recognition accuracy: 96.5%
- Recognition time per frame: 1.1–1.4 seconds
- False acceptance rate (unauthorized user mistakenly accepted): 0% in all test cases
- False rejection rate (authorized user not recognized): 2–3%, mainly under dim lighting

The results confirm that the system consistently identifies authorized users with high reliability, maintaining real- time performance without noticeable delays.

Dash board Responsiveness

Once a user was authenticated, the dashboard interaction was tested for delay, responsiveness, and consistency.

Test Results

- Light ON/OFF command execution time:<0.5seconds
- Brightness adjustment response: instantaneous with visually smooth transitions
- Gas valve control delay: 4–6 seconds, depending on valve motor rotation

IRJCS: International Research Journal of Computer Science
Volume 12, Issue 11, November 2025
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1211.03

- User interface load time: 2–3 seconds after authentication

These results indicate that the system offers a smooth and efficient control experience without lag or command failures.

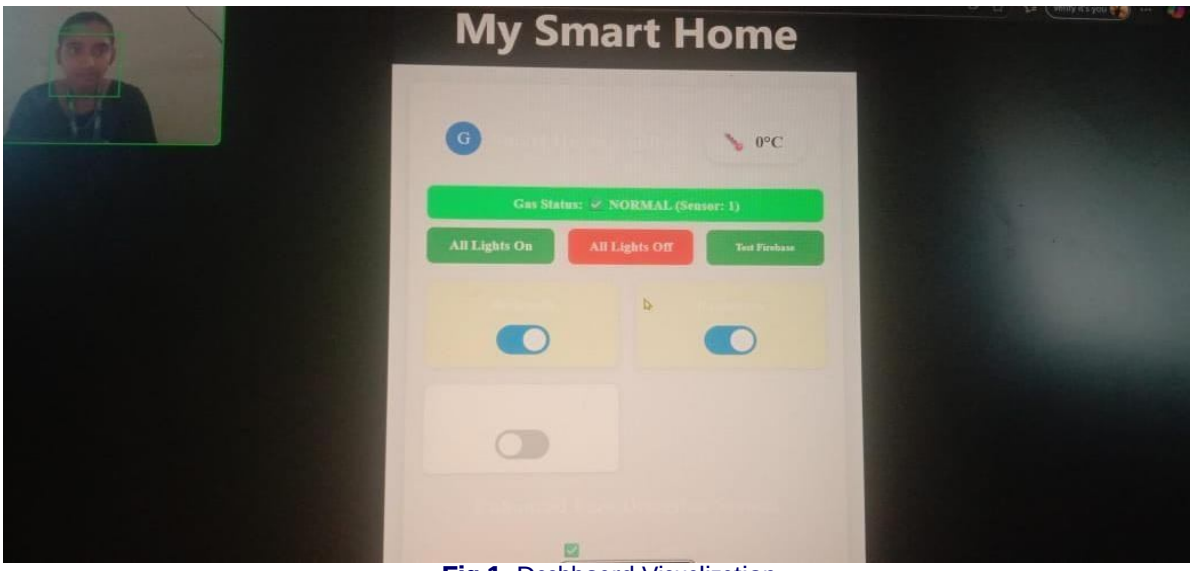

Fig.1: Dashboard Visualization

Relay Module & Appliance Control Evaluation

Physical appliance control using the relays was tested repeatedly to ensure stability during continuous operation.

Performance Outcomes

- 100 cycle ON/OFF test for lights showed zero switching errors
- Relay heat levels remained within safe limits during continuous operation
- Commands remained stable even during simultaneous sensor monitoring and face recognition This confirms that the relay-based hardware control is robust for long-term home usage.

Gas Leak Detection and Safety Response

The MQ-5 sensor's ability to detect gas leakage was evaluated using controlled exposure to LPG.

Safety System Results

- Gas detection time: 2–4 seconds after exposure
- Automatic shut down of gas valve: completed within 5–7 seconds
- Warning notification on dashboard triggered instantly
- System prevented manual override during safety mode, ensuring user protection

This demonstrates that the safety module reacts quickly and effectively ,minimizing the risk of hazardous incidents.

Multi-Threading Performance

The system's multi-threaded design was evaluated to verify simultaneous execution of recognition, monitoring, and device control.

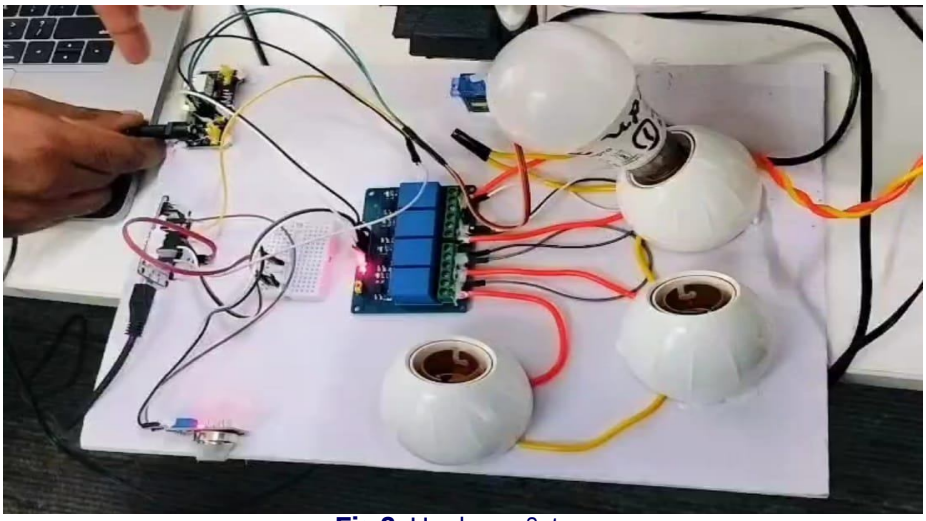

Fig.2: Hardware Setup

System Behavior

- No frame drops during face recognition
- Gas sensor readings updated consistently every second
- Dashboard remained usable without freezing

ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1211.03

- Total system CPU usage on Raspberry Pi4:58–72% during peak load

This confirms that the system performs reliably under multitasking conditions without compromising speed or functionality.

Overall System Evaluation

Performance Metric	Result	Remarks
Facial recognition accuracy	96.5%	High accuracy across conditions
Response time	1.1–1.4 sec	Suitable for real-time use
Light control delay	<0.5 sec	Highly responsive
Gas valve shut down	5–7 sec	Safe and reliable
UI loading	2–3 sec	Fast operational readiness
Offline functionality	100%	No internet needed

Overall, the experimental evaluation demonstrates that the system is stable, accurate, and highly suitable for real-world home automation. It provides secure access, fast appliance control, and reliable safety monitoring within a single unified platform.

V. CONCLUSION

The development of this face-recognition-based home automation system demonstrate show artificial intelligence and IoT technologies can be integrated to create a secure, efficient, and user-friendly smart home environment. The proposed system successfully combines real-time facial authentication with appliance control and safety monitoring, addressing several limitations found in traditional automation platforms. By performing all processing locally on the Raspberry Pi, the system ensures strong privacy protection and remains fully functional without internet connectivity. Experimental results show that the face recognition module achieves high accuracy, the dashboard responds quickly to user commands, and the gas-leak detection mechanism operates reliably under real-world conditions. The relay-driven appliance control performed consistently in long-term tests, confirming its suitability for daily household usage. The ability to automatically shut off the gas supply during hazardous situations further enhances user safety and demonstrates the practical value of integrating safety features into home automation systems. Overall, the system provides a comprehensive solution that improves home security, convenience, and safety while remaining affordable and scalable. With its modular architecture, the platform can be extended to include additional sensors, biometric modes, or remote-access features in the future. The results of this work suggest that AI-powered, privacy-preserving home automation has strong potential to become a standard approach in modern residential environments.

REFERENCES

1. Y.Taigman, M.Yang, M.Ranzato and L.Wolf, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” 2014 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1701–1708.
2. F Schroff, D.Kalenichenko and J.Philbin, “FaceNet: A Unified Embedding for Face Recognition and Clustering,” 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 815–823.
3. K.Zhang, Z.Zhang, Z.Li and Y.Qiao, “Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks,” IEEE Signal Processing Letters, vol. 23, no. 10, pp. 1499–1503, Oct. 2016.
4. J.Deng, J.Guo, N.Xue and S.Zafeiriou, “ArcFace: Additive Angular Margin Loss for Deep Face Recognition,”2019IEEE/CVF Conference on Computer Vision and Pattern Recognition(CVPR),pp.4690– 4699.
5. S.Alamri,M.AlharthiandA.Alzahrani,“IoT-Based Smart Home: Architecture, Security Challenges, and Solutions,” IEEE Access, vol.9,pp.113190–113204,2021.
6. A.Bansal and S.K.Sharma,“IoT Based Home Automation System Using Raspberry Pi,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 10, no. 5, 2019.
7. M.R.Palankar and R.M.Banakar, “Smart Home Automation Security: A Survey,” 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 35–40.
8. A.H.Khan,S.A.Khan,M.U.Tariq and A.Ahmad,“Edge-Based Face Recognition System Using Raspberry Pi, ”Sensors, vol.22, no.1,pp.310–321,2022 (MDPI –Scopus indexed).
9. R.M.R.GauthamandP.Sivabalan,“HomeAutomationUsingRaspberryPiandIoT,”2021IEEE International Conference on Computing, Communication and Security (ICCCS).
10. Z.M.Khalaf and M.J.A.Shabani,“Design and Implementation of Gas Leakage Monitoring System Using MQSensors,”2021IEEE International Conference on Engineering Technologies(ICET),pp.73–78.
11. S.Rajput and P.Singh,“A Smart Domestic Gas Leakage Detection and Prevention System,”2021 International Conference on Smart Electronics and Communication (ICOSEC), pp. 162–167.
12. E.H.PuriandM.Arora,“Biometric-BasedAuthenticationforSmartHomeSystems,”2020International Conference on Computational Intelligence (ICCI), pp. 89–95.
13. N.GuptaandR.Singhal,“SecureSmartHomeAutomationUsingFaceRecognition,” InternationalJournal of Engineering Research & Technology (IJERT), vol. 9, no. 6, 2020.