International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 3 (2026)



ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

IoT-Based Smart Home Automation and Intelligent Security System Using Deep Learning

CH.RAKESH [1], Dr. E. HARIKRISHNA [2]

[1]M.Tech Scholar, Dept of ECE, Kakatiya University Campus, Warangal, Telangana, India.

[2] Associate Professor, Kakatiya University Campus, Warangal, Telangana, India

rakeshchittimalla2000@gmail.com[1] , hari_etta@yahoo.co.in[2]

ABSTRACT

The proposed "IoT-Based Smart Home Automation and Security System Using IoT and Deep Learning" integrates smart appliance control and intelligent security into a single system. NodeMCU, Firebase, a mobile application, IR sensor, camera, OpenCV, and CNN are used to provide manual and automatic control of lights and fan while monitoring the home environment. In Manual Mode, appliances can be controlled through the mobile application, whereas Automated Mode uses the IR sensor to detect human presence and automatically operate the appliances. The camera-based security module uses OpenCV for image processing and a CNN model for person recognition. When an unauthorized or unrecognized person is detected, the system activates a buzzer and generates an alert. This integrated approach improves convenience, supports efficient appliance usage, and provides an additional layer of intelligent home security.

Keywords: IoT, Smart Home Automation, NodeMCU, Firebase, Mobile Application, IR Sensor, Deep Learning, CNN, OpenCV, Image Processing, Face Recognition, Home Security.

1. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has enabled the development of intelligent environments in which physical devices, sensors, controllers, and cloud platforms can communicate and operate with limited human intervention. Smart home automation is one of the important applications of IoT, providing remote appliance control, automated operation, energy management, and improved residential convenience. Conventional home automation systems commonly focus on appliance switching or basic sensor-based control, while security functions are often implemented as independent systems. Integrating automation and intelligent security within a common architecture can provide a more comprehensive solution for residential environments.

This paper proposes an IoT-based smart home automation and security system that combines NodeMCU, Firebase cloud communication, a mobile application, an infrared (IR) sensor, and deep-learning-based image recognition. The NodeMCU functions as the primary embedded controller and communicates with the mobile application through Firebase. The proposed system supports Manual and Automated operating modes for controlling household lights and a fan. In Manual Mode, appliance commands are generated by the user through the mobile application and transmitted to the controller through the cloud. In Automated Mode, the IR sensor provides occupancy information to the controller, enabling automatic operation of the connected appliances according to the detected presence condition.

To enhance residential security, the proposed system incorporates a camera-based image-processing module implemented using Python and OpenCV. Captured video frames are processed to identify relevant facial regions, which are subsequently analyzed using a Convolutional Neural Network (CNN). The deep-learning model is configured to recognize authorized persons from the available reference data. When an unrecognized or unauthorized person is detected, the system initiates an alert mechanism using a buzzer and notification functionality. The combination of IoT-based automation with computer-vision-assisted person recognition provides both appliance management and security monitoring within a unified framework.

The proposed approach demonstrates the integration of embedded systems, cloud computing, mobile communication, computer vision, and deep learning for smart residential applications. Unlike basic automation systems that rely only on manual control or simple presence detection, the proposed architecture incorporates both occupancy-based appliance control and identity-oriented security monitoring. The system is designed as a modular platform in which additional sensors, appliances, notification services, energy-monitoring mechanisms, and improved deep-learning models can be incorporated. The resulting framework provides a practical basis for developing connected, responsive, and intelligent smart home environments.

OBJECTIVES

The primary objective of this work is to develop an integrated IoT-based smart home automation and security system that enables reliable appliance control and intelligent residential monitoring. The proposed system aims to use NodeMCU and Firebase for cloud-based communication between the controller and mobile application, providing Manual and Automated modes for controlling lights and fan. The Automated Mode is intended to utilize an IR sensor for detecting human presence and controlling appliances accordingly, thereby reducing unnecessary operation. In parallel, the system aims to incorporate a camera-based security mechanism using Python, OpenCV, and a Convolutional Neural Network (CNN) for image processing and authorized-person recognition. The system is designed to generate an alert and activate a buzzer when an unauthorized or unrecognized person is detected. Overall, the objective is to integrate IoT, sensor-based automation, cloud communication,

computer vision, and deep learning into a unified and scalable smart home framework.

EXISTING SYSTEM

Conventional smart home systems primarily provide basic appliance control through physical switches, remote-control interfaces, or simple IoT-based applications. Some systems use sensors such as IR or motion sensors to detect occupancy and automatically operate appliances, but they generally focus on presence detection rather than identifying the person. Security solutions are often implemented separately using conventional surveillance cameras, alarms, or manual monitoring. Such systems may therefore require multiple independent components and do not provide an integrated mechanism for appliance automation and intelligent person recognition. Basic sensor-based systems can also be affected by sensor placement and detection conditions, while conventional camera-based monitoring may depend on continuous human observation. These limitations indicate the need for a unified system capable of combining automated appliance control with intelligent security analysis.

PROPOSED SYSTEM

The proposed system integrates IoT-based home automation with deep-learning-based security within a unified architecture. NodeMCU is used as the primary controller, while Firebase provides cloud-based communication between the controller and mobile application. The system supports Manual Mode, in which the user remotely controls the lights and fan through the mobile application, and Automated Mode, in which an IR sensor detects human presence and enables automatic appliance control. For security monitoring, a camera captures the monitored environment and transfers image frames to a Python-based processing module. OpenCV performs image acquisition, preprocessing, and face-region detection, while a Convolutional Neural Network (CNN) is employed for person recognition using authorized reference data. When an unauthorized or unrecognized person is detected, the system activates a buzzer and generates an alert. This integrated architecture combines IoT connectivity, sensor-based automation, computer vision, and deep learning to provide a scalable smart home automation and security framework.

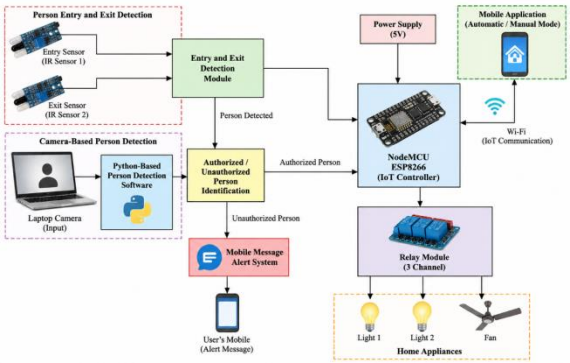


Fig. Block Diagram of Proposed Smart Home Automation System

2. LITERATURE SURVEY

1. Luigi Atzori, Antonio Iera, and Giacomo Morabito investigated the fundamental concepts, enabling technologies, and applications of the Internet of Things. Their study explained how sensing, communication, identification, and intelligent processing can be combined to connect physical objects with network services.

The work provides a theoretical foundation for developing IoT-based smart environments and connected home applications.

2. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami proposed a cloud-centric vision for IoT and discussed the integration of sensors, actuators, communication networks, and cloud computing. Their work emphasized the importance of cloud platforms for collecting and processing data from distributed IoT devices. This approach is relevant to the proposed system, where Firebase is used for communication between the mobile application and NodeMCU.

3 A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash reviewed IoT enabling technologies, communication protocols, and application areas. Their study highlighted the importance of selecting suitable communication technologies and protocols for reliable IoT deployment. The work supports the communication and connectivity aspects required for smart home automation systems.

4 Antonio Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi studied IoT technologies for smart-city applications, including heterogeneous devices, communication technologies, architectures, and services. Their research demonstrated the importance of integrating different types of connected devices into a common IoT infrastructure. These concepts are applicable to smart home systems that combine controllers, sensors, appliances, and cloud services.

5.Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac presented a broad survey of IoT technologies, applications, security issues, and research challenges. Their work emphasized identification, sensing, actuation, interoperability, and security as important aspects of IoT systems. These findings are relevant to the proposed architecture, which combines sensing, appliance control, cloud connectivity, and security monitoring.

6.Alex Krizhevsky, Ilya Sutskever, and Geoffrey Hinton demonstrated the effectiveness of deep convolutional neural networks for large-scale image classification. Their research showed that CNN architectures can automatically learn hierarchical visual features from image data and perform image classification effectively. This work provides an important foundation for the CNN-based person recognition component used in the proposed security system.

7.Yann LeCun, Yoshua Bengio, and Geoffrey Hinton reviewed the development and applications of deep learning and explained how multiple processing layers can learn increasingly complex representations from data. Their work highlighted the significant role of deep convolutional networks in image and video processing. This research supports the use of deep learning for intelligent visual security applications.

8.Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun introduced a residual learning framework for training deeper neural networks. Their work demonstrated that residual connections can facilitate the optimization of deep architectures and improve image-recognition performance. The study is relevant to the future enhancement of the proposed security module through more advanced deep-learning architectures.

9.Joseph Redmon, Santosh Divvala, Ross Girshick, and Ali Farhadi proposed YOLO, a real-time object-detection approach that processes an image through a unified neural network. Their research demonstrated the potential of deep-learning models for fast visual detection. The work is relevant to smart security applications where real-time camera analysis and rapid detection of persons or objects are required.

10.M. Zorzi, A. Gluhak, S. Lange, and A. Bassi examined the evolution of IoT communication from conventional intranet-based systems toward a broader Internet of Things environment. Their work discussed wireless connectivity and mobility-related aspects required for interconnected devices. These concepts are relevant to developing connected smart home systems in which embedded controllers communicate with cloud and mobile platforms.

3 .METHODOLOGY

The proposed system is designed as an integrated IoT and deep-learning-based platform for smart home automation and security monitoring. The overall methodology consists of hardware interfacing, cloud communication, appliance control, occupancy detection, image processing, and person recognition. NodeMCU is used as the primary controller and is connected to the required sensors and switching circuit. Firebase Cloud provides real-time data communication between the NodeMCU and the mobile application through an internet connection. The mobile application provides Manual and Automated operating modes for controlling the lights and fan. In Manual Mode, the user's ON/OFF commands are transmitted to Firebase and received by NodeMCU, which operates the connected appliances through the switching circuit.

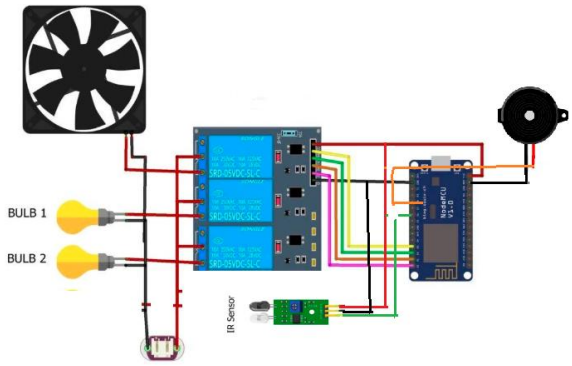
In Automated Mode, an IR sensor is interfaced with NodeMCU to detect the presence of a person in the monitored area. The sensor output is continuously monitored by the controller, and the programmed logic determines the required appliance condition. When a person is detected, the system can activate the lights and fan, while the

appliances can be switched OFF when the area becomes unoccupied according to the configured conditions. This sensor-based operation reduces the need for continuous manual control and can help avoid unnecessary appliance operation. The system can also be extended with additional sensors for environmental and energy monitoring.

For security monitoring, a camera is connected to a Python-based processing module. The captured video frames are acquired and processed using OpenCV. Image preprocessing and face-region detection are performed before providing the relevant image information to the deep-learning model. A Convolutional Neural Network (CNN) is used to learn visual characteristics from authorized-person reference data and classify the detected person. The recognition result is then used to determine whether the detected person is authorized or unrecognized. If an unrecognized person is detected, the security mechanism activates a buzzer and generates an alert for the user.

The final stage of the methodology integrates the automation and security modules into a common system architecture. Sensor data, appliance-control commands, and security events are processed according to predefined program logic. The complete system is tested under different operating conditions, including Manual Mode, Automated Mode, person detection, authorized-person recognition, and unauthorized-person detection. Parameters such as sensor response, appliance switching, cloud communication, image-processing performance, recognition response, and alert generation are observed during testing. This methodology provides a structured approach for implementing an IoT-enabled smart home system with deep-learning-assisted security functionality.

CIRCUIT DIAGRAM:



.

4.TECHNOLOGIES IOT:

The Internet of Things (IoT) is a gadget of interrelated registering gadgets, mechanical and virtual machines, items, creatures or individuals which may be outfitted with

specific identifiers (UIDs) and the cappotential to switch insights over a local area with out expecting human-to-human or human-to-pc connection.

FIREBASE:

Firebase's most memorable item turned into the Firebase Real-time Database, an API that synchronizes programming measurements all through iOS, Android, and Web gadgets, and shops it on Firebase's cloud. The item helps programming program developers in building constant, cooperative applications.

NODEMCU:

NodeMCU is a low-expense open inventory IoT stage. It at first covered firmware which runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and equipment which changed into principally based absolutely at the ESP-12 module. Afterward, help for the ESP32 32-cycle MCU changed into added.



WORKING OF THE SYSTEM

The proposed IoT-based smart home automation and security system operates through the integration of NodeMCU, Firebase Cloud, a mobile application, an IR sensor, a camera, and a deep-learning-based security module. When the system is powered ON, the NodeMCU initializes the connected components and establishes a Wi-Fi connection. After successful internet connectivity, the controller communicates with Firebase Cloud, which acts as an intermediate platform between the NodeMCU and the mobile application. The user can select either Manual Mode or Automated Mode through the mobile application depending on the required method of appliance control.

In Manual Mode, the user sends ON or OFF commands for the lights and fan through the mobile application. These commands are stored or updated in the Firebase database and are retrieved by the NodeMCU through the internet. The controller processes the received values and generates appropriate control signals for the connected switching circuit. The switching circuit then operates the lights and fan according to the user's command. This allows the appliances to be controlled remotely without directly operating the physical switches.

In Automated Mode, the IR sensor is used to detect the presence of a person within the monitored area. The sensor continuously provides its detection status to the NodeMCU. When a person is detected, the controller processes the sensor signal and activates the connected switching circuit to turn ON the lights and fan. When the monitored area becomes unoccupied, the programmed control logic can switch OFF the appliances. This automatic operation minimizes unnecessary appliance usage and reduces the requirement for continuous manual intervention.

The security operation is performed simultaneously through the camera and Python-based image-processing module. The camera captures images or video frames from the monitored area and transfers them to the Python application. OpenCV is used for camera interfacing, frame acquisition, preprocessing, and detection of the relevant facial region. The processed image is supplied to the CNN-based deep-learning model, which analyzes the visual features and compares the detected person with the configured authorized-person information. If the person is recognized as authorized, the system continues normal monitoring. If the person is unknown or unauthorized, the security module activates the buzzer and generates an alert to notify the user.

Thus, the complete system combines remote IoT-based appliance control, IR-based automatic operation, and camera-based intelligent security in a unified framework. Firebase enables communication between the mobile application and NodeMCU, while Python, OpenCV, and CNN provide the intelligent security functionality. The combined operation provides a practical approach for improving home convenience, reducing unnecessary appliance operation, and supporting real-time security monitoring.

RESULTES:

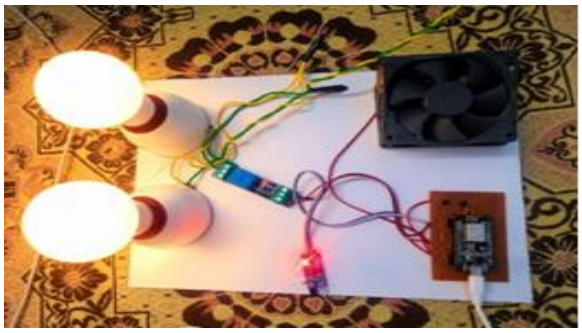


Fig.1 : Working Proto type of the Smart Home Automation System

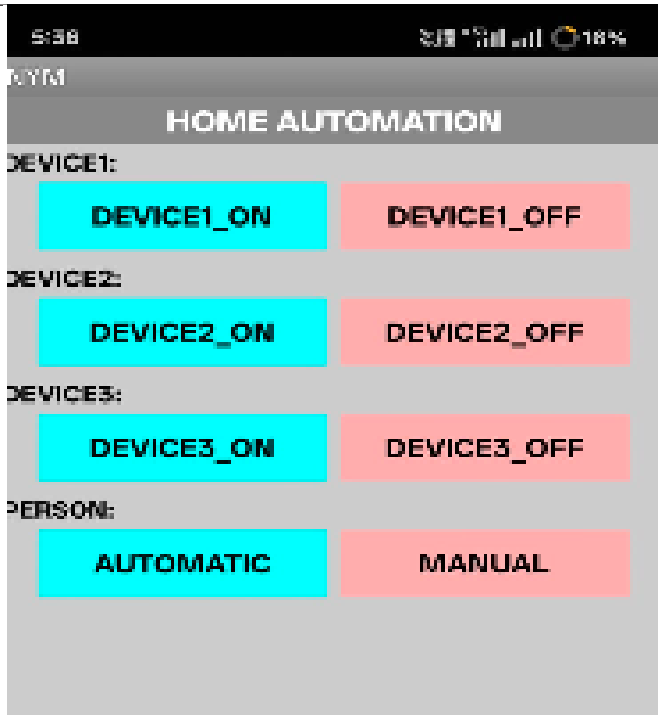


Fig :MOBIE APP DESIGN

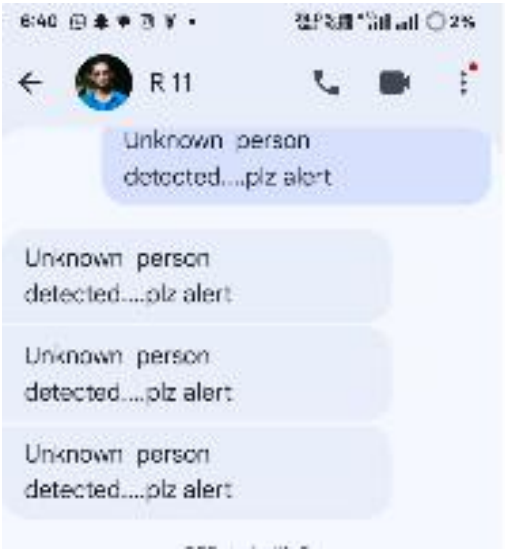


Fig MESSAGE ALERT

5. CONCLUSION

The proposed IoT-Based Smart Home Automation and Security System provides an integrated solution for appliance

automation and intelligent security monitoring. NodeMCU and Firebase enable remote control of lights and fan through a mobile application, while the IR sensor supports automatic appliance operation based on human presence. The security module combines a camera, Python, OpenCV, and CNN-based deep learning to identify authorized or unrecognized persons. When an unauthorized person is detected, the system can activate a buzzer and generate an alert. The integration of IoT, sensor-based automation, computer vision, and deep learning demonstrates a practical approach for developing a connected and intelligent home environment.

FUTURE SCOPE:

The future scope of the system includes integration of additional sensors for temperature, gas, smoke, door, energy, and environmental monitoring. The security module can be enhanced using larger datasets and advanced deep-learning models to improve recognition under different lighting and environmental conditions. Real-time mobile notifications, cloud-based event storage, voice-controlled appliances, energy-consumption monitoring, and edge-based image processing can also be incorporated. These enhancements can improve the scalability, reliability, security, and intelligence of the proposed smart home platform

REFERENCES

1. Atzori, L., Iera, A., & Morabito, G. (2010). "The Internet of Things: A Survey." Computer Networks, Vol. 54, No. 15, pp. 2787–2805.
2. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions." Future Generation Computer Systems, Vol. 29, No. 7, pp. 1645–1660.
3. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications." IEEE Communications Surveys & Tutorials, Vol. 17, No. 4, pp. 2347–2376.
4. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). "Internet of Things for Smart Cities." IEEE Internet of Things Journal, Vol. 1, No. 1, pp. 22–32.
5. Evans, D. (2011). "The Internet of Things: How the Next Evolution of

the Internet Is Changing Everything." Cisco Internet Business Solutions Group.

6. Borgia, E. (2014). "The Internet of Things Vision: Key Features, Applications and Open Issues." Computer Communications, Vol. 54, pp. 1–31.
7. Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). "ImageNet Classification with Deep Convolutional Neural Networks." Advances in Neural Information Processing.
8. LeCun, Y., Bengio, Y., & Hinton, G. (2015). "Deep Learning." Nature, Vol. 521, pp. 436–444.
9. Bradski, G. (2000). "The OpenCV Library." Dr. Dobb's Journal of Software Tools, Vol. 25, No. 11, pp. 120–125.
10. Szeliski, R. (2022). Computer Vision: Algorithms and Applications. 2nd Edition, Springer.
11. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach. 4th Edition, Pearson.
12. Monk, S. (2016). Programming Arduino: Getting Started with Sketches. 2nd Edition, McGraw-Hill Education.
13. Margolis, M., Jepson, B., & Weldin, N. R. (2020). Arduino Cookbook: Recipes to Begin, Expand, and Enhance Your Projects. 3rd Edition, O'Reilly Media.
14. Monk, S. (2018). Programming the ESP32. McGraw-Hill Education.
15. Bahga, A., & Madisetti, V. (2014). Internet of Things: A Hands-On Approach. Universities Press.