AI-Driven Smart Home Automation: Enhancing Energy Efficiency, Security, and User Comfort

Ishwari Banjare

Assistant Professor, Department of BCA
Acharya institute of Graduate Studies, Bengaluru, Karnataka, India

Amrita Singh

Associate Professor, Department of Physics
Acharya institute of Graduate Studies, Bengaluru, Karnataka, India

Editorial history

Received: 09.03.2026
Accepted: 11.04.2026
Published Online: 08.05.2026

Cite this article

Banjare, I. & Singh, A. (2026). AI-Driven Smart Home Automation: Enhancing Energy Efficiency, Security, and User Comfort. *Journal of Advanced Research and Innovation, 2*(3), 6-12.

Abstract

This review paper presents the development of a smart home automation system designed to improve energy management, security, and user convenience. The system is built using a Raspberry Pi and Python, allowing users to remotely monitor and control household appliances, such as lights, fans, air conditioners, and TVs, through any web browser on the local network without the need for additional software.

The system works in two main stages. The first stage uses IoT devices and sensors—including temperature and humidity sensors (DHT11), gas sensors (MQ2), and ultrasonic distance sensors (HC-SR04)—to monitor the home environment and control appliances in real time. Data is transmitted via the Zigbee protocol to Arduino and Raspberry Pi microcontrollers, while relays safely manage high-voltage devices. A web and mobile interface allows users to easily interact with the system.

The second stage uses a linear regression model to analyze historical data, enabling the system to anticipate user behavior and automatically optimize energy use. Additionally, the system incorporates security features, including video monitoring, face detection, and recognition, with alerts sent securely via email and mobile notifications. Local processing and encrypted cloud storage protect user privacy.

This approach offers a practical, scalable, and cost-effective solution for smart home management, providing energy efficiency, personalized automation, and enhanced security, with potential for future improvements such as voice control and broader device integration.

Keywords: Smart Home, Home Automation, Smart Building, Artificial Inteligence, IoT (Internet of things)

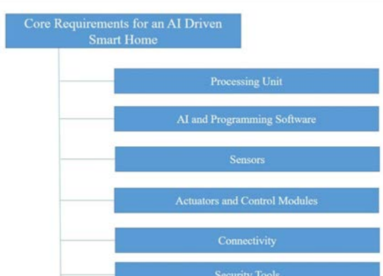

Figure Core Requirements for an AI Driven Smart Home

Introduction

The rapid growth of intelligent home automation systems has significantly transformed modern living environments, making homes more efficient, secure, and convenient. By integrating connected devices with data-driven technologies, smart homes can monitor surroundings, control appliances, and optimize energy usage with minimal human intervention. Unlike traditional automation systems that rely on fixed rules or manual adjustments, modern smart homes can learn from user behavior, identify daily patterns, and adapt to individual preferences. This adaptability creates a more personalized and seamless living experience. Wireless communication technologies such as Wi-Fi and Zigbee enable devices to interact and share information in real time. Users can remotely manage appliances through smartphones or web-based platforms, enhancing accessibility and control. However, true intelligence in smart homes goes beyond connectivity. Systems must analyze historical data, environmental conditions, and usage trends to make informed decisions automatically. Despite advancements, challenges such as inefficient energy use, limited interoperability, and cybersecurity risks remain. To overcome these issues, an improved framework has been developed using a Raspberry Pi platform with sensor-based monitoring and predictive control. By applying a linear regression model to analyze usage patterns, the system automates operations efficiently, strengthens security, and promotes sustainable energy management for modern households.[1]

The early twenty-first century witnessed rapid growth in internet connectivity, transforming communication, workplaces, and daily life. As networking technologies advanced, the Internet of Things (IoT) emerged, enabling physical devices to connect and exchange data seamlessly. Among its major applications, smart homes have gained significant importance. A smart home integrates interconnected devices that work together to provide automated, efficient, and user-friendly services. With continuous technological progress, users now expect greater comfort, energy efficiency, and intelligent interaction from home systems .The affordability of electronic components and widespread internet access have accelerated the adoption of home automation. Modern systems combine embedded computing platforms with wireless sensors and actuators to enable centralized monitoring and remote control. However, increased connectivity also raises concerns about data privacy and cybersecurity, as smart homes process sensitive personal information. Therefore, secure and privacy-focused system design has become essential. This research proposes an intelligent smart home security framework that integrates IoT infrastructure with advanced analytical techniques. The system uses motion sensors, a processing unit, and a camera module to enable real-time monitoring. When motion is detected, the camera captures footage, and computer vision algorithms analyze it for facial recognition. Authorized individuals are identified, while unknown persons trigger alerts. The system, implemented using OpenCV, supports customization, secure cloud access, and privacy protection, ensuring reliable and efficient home security.[2]

The Internet of Things (IoT) is a modern technological concept that enables physical devices to connect to the internet and communicate with each other. By integrating sensors, microprocessors, and communication modules into everyday objects, IoT allows devices to collect data, exchange information, and operate automatically with minimal human intervention. Today, IoT is widely used in areas such as smart cities, industrial automation, healthcare, and residential environments. The term was first introduced in 1999 by Kevin Ashton at the Massachusetts Institute of Technology during research on RFID technology, which later became the foundation for IoT development. Over the years, IoT has evolved to connect devices like lighting systems, refrigerators, thermostats, wearable devices, medical equipment, and security cameras through wireless networks. This advancement has played a key role in the growth of smart homes, allowing users to monitor and control appliances remotely for improved comfort and safety. Earlier home automation systems relied mainly on wired setups using platforms such as Arduino or Raspberry Pi, which were expensive and difficult to modify. The adoption of wireless technologies like Wi-Fi, Bluetooth, and Zigbee has improved flexibility and scalability. However, issues such as security risks and compatibility challenges still require careful system design and management.[3]

Literature Survey

The rapid advancement of intelligent home automation has significantly transformed modern living spaces, making homes smarter, safer, and more energy-efficient. With the growth of internet connectivity in the early twenty-first century, the Internet of Things (IoT) emerged as a powerful concept that connects physical devices to the internet, enabling them to communicate and operate automatically. By embedding sensors, processors, and communication modules into everyday appliances, IoT allows devices to collect data, exchange information, and function with minimal human involvement. This development has played a vital role in the evolution of smart homes. Modern smart home systems go beyond simple remote control. They integrate wireless technologies such as Wi-Fi, Bluetooth, and Zigbee to create interconnected networks of sensors and actuators. These systems continuously monitor environmental conditions and user activities, allowing appliances to adjust automatically for improved comfort, efficiency, and security. Unlike traditional rule-based automation, intelligent systems analyze historical usage patterns and adapt to user behavior, creating a personalized living experience. Despite these benefits, challenges such as cybersecurity risks, privacy concerns, and device compatibility issues remain. As smart homes process large amounts of sensitive data, strong encryption and secure system design are essential. To address these concerns, advanced frameworks combine sensor-based monitoring with predictive analytics and real-time surveillance. Using platforms like Raspberry Pi and computer vision tools such as OpenCV, modern systems enable motion detection, facial recognition, and remote monitoring. This integrated approach supports the development of secure, adaptable, and sustainable smart home environments for contemporary households.[1]

Early home automation systems primarily depended on wired setups using platforms such as Arduino or Raspberry Pi. Although suitable for newly built houses, these systems were costly and challenging to install in existing structures. The adoption of wireless technologies like Wi-Fi, Bluetooth, and Zigbee has significantly simplified deployment and improved system scalability. Despite these improvements, issues such as cybersecurity threats, device compatibility problems, scalability constraints, and installation expenses continue to pose challenges. To overcome these limitations, the proposed IoT-based system uses Zigbee-enabled distributed sensors integrated with a web-based control interface, ensuring greater flexibility, improved security, and reliable smart home management.[3]

Methodology -

Raspberry Pi in Smart Home Automation

The Raspberry Pi 3B+ serves as the central processing unit in the smart home system due to its compact size, affordability, and adequate performance. It manages real-time communication, stores usage data, runs predictive algorithms, and hosts a Flask web server, enabling secure local monitoring, automation, and easy integration of additional devices.[1]

Passive Infrared (PIR) Sensors for Motion Detection

PIR sensors play a key role in occupancy-based automation by detecting infrared radiation changes caused by human movement. When motion is sensed, they signal the Raspberry Pi to activate appliances, and turn them off after inactivity to save energy. They preserve privacy and, combined with machine learning, enable predictive, energy-efficient control.[1]

Relays for Smart Appliance Control

Relays act as electrically controlled switches that enable the low-voltage Raspberry Pi to operate high-voltage household appliances safely. In this system, 5V, 10A relay modules control devices such as lights, fans, and air conditioners through web or mobile interfaces. Enhanced designs may use solid-state relays and support voice or gesture control.[1]

Flask Server for Web-Based Automation

Flask offers a lightweight and efficient platform for deploying automation services on the Raspberry Pi. It provides a secure, user-friendly web interface for monitoring sensors and controlling appliances. Operating within a local network or via VPN, its low resource usage and modular structure support scalable smart home implementations.[1]

Face Detection Algorithms and Libraries

Face detection and recognition are vital for smart security systems. OpenCV supports real-time methods like Haar Cascade and LBP, though they are less accurate in complex settings. Advanced models such as MTCNN, RetinaFace, YOLOv8, MediaPipe, and CenterFace improve accuracy but require balancing speed, precision, and computational resources.[2]

Face Recognition Models

Traditional face recognition techniques such as Eigenfaces and Fisherfaces use dimensionality reduction and are computationally efficient, but they struggle with lighting and pose variations. LBPH improves lighting tolerance yet lacks scalability. Modern deep learning models like FaceNet, ArcFace, and Dlib offer higher accuracy, though they require greater computational resources.[2]

Security, Privacy, and Compliance in Smart Homes

Smart home systems are vulnerable to unauthorized access, data breaches, and device tampering. Security measures such as strong authentication and encryption standards including AES, RSA, TLS/SSL, and ECC protect communications. Blockchain enhances data integrity, while image masking preserves privacy. Compliance with ENISA and ETSI standards strengthens reliability and user trust.[2]

Proposed Smart Security Framework

The system features a compact edge-based design built around a Raspberry Pi, integrating a camera and PIR sensor for smart monitoring. The camera activates only upon motion detection to save energy. Video is processed locally using OpenCV and Dlib, then securely uploaded, with alerts sent via email and mobile notifications.[2]

IoT Integration Layer

The IoT layer consists of a PIR sensor and a Raspberry Pi High-Quality Camera featuring a 12.3 MP Sony IMX477 sensor, connected through the MIPI CSI interface for reliable data transfer. Operating on a client–server model, the system processes video locally and shares only filtered data externally to ensure privacy.[2]

Video Analysis and Face Recognition

Video processing is performed directly on the Raspberry Pi, including frame extraction, grayscale conversion, resizing, normalization, and Gaussian blurring. Face detection uses Haar Cascade and HOG methods, while Dlib generates 128-dimensional feature vectors. Euclidean distance determines identity, labeling known faces and triggering alerts for unknown individuals efficiently.[2]

Secure Notification and Data Handling

Processed files are securely uploaded to Google Drive using authenticated APIs. Email alerts are sent via SMTP with SSL encryption, while Pushbullet delivers instant mobile notifications. Recordings are shared through password-protected links, supported by two-factor authentication, time-limited access, and verification protocols like DKIM, SPF, and DMARC.[2]

Risk Assessment and Mitigation

Cloud storage enhances accessibility and remote monitoring but also creates risks such as unauthorized access and phishing attacks. Compliance with regulations like GDPR and HIPAA is essential when handling sensitive data. These risks can be minimized through strong authentication mechanisms, encrypted communication channels, and optional file encryption before uploading.[3]

Overall System Architecture

The system is structured into hardware and software components that operate collaboratively to ensure efficient functionality. It follows a three-layer IoT architecture consisting of the sensing layer for data collection, the processing layer for analysis and decision-making, and the visualization layer for user interaction and monitoring.[3]

Sensing Layer

The hardware setup includes sensors such as the DHT11 for temperature and humidity measurement, the MQ2 gas sensor for detecting smoke or gas leaks, and the HC-SR04 ultrasonic sensor for distance measurement, along with a servo motor for controlled movement. These components are connected to the Arduino or Raspberry Pi using jumper wires and powered through USB.[3]

Processing Layer

Microcontrollers are responsible for collecting and processing data received from various sensors in the system. Zigbee technology facilitates reliable wireless communication between devices, ensuring smooth data transmission. The processed information is then stored securely in Firebase, enabling real-time synchronization, remote monitoring, and efficient data management.[3]

Visualization Layer

An Android application developed using MIT App Inventor enables user interaction with the smart home system. The app includes login authentication, live sensor monitoring, and seamless Firebase integration. Firebase ensures secure data storage and real-time updates, while cloud integration provides remote access, centralized control, scalability, and reliable overall system performance.[3]

Block Chain for Security in Smart Home

The smart home automation system aims to ensure secure and reliable identification of IoT devices using blockchain technology. Blockchain offers decentralization, anonymity, and tamper resistance through SHA-256 hashing, encrypted data, timestamps, and block validation mechanisms, reducing reliance on centralized servers while enhancing security.[6]

Challenges of using AI in Smart Home

The implementation of Artificial Intelligence (AI) within smart home environments introduces numerous challenges that necessitate meticulous consideration to guarantee safety, reliability, and operational efficiency. Although AI enhances aspects of automation, convenience, and energy management, apprehensions pertaining to privacy, security, complexity, cost, and data integrity persist as significant obstacles. Smart home apparatuses perpetually gather personal data, including user preferences and daily routines, thereby amplifying the vulnerability to cyberattacks, as each interconnected device serves as a potential access point for cybercriminals. Consequently, robust encryption protocols, secure system architecture, and routine updates are imperative. Moreover, with the proliferation of integrated devices, the complexities associated with system configuration and management escalate, often necessitating a level of technical proficiency that may deter certain users. Elevated initial investment, ongoing maintenance costs, and potential increases in energy consumption additionally influence adoption rates, rendering affordability and energy efficiency critical factors. Additionally, AI systems are fundamentally reliant on precise and uninterrupted data; inadequate connectivity or substandard data quality can impair system efficacy, underscoring the necessity for dependable networks and robust data validation protocols.[5]

Future Vision

Integrating AI and biometrics will enable the creation of advanced biometric systems that will significantly improve the security of the Internet of Things and open new opportunities in various industries. These systems can use deep learning techniques to extract complex features from physiological and behavioral data to improve recognition accuracy and reliability. At the same time, explainable AI increases transparency by clarifying how decisions are made, builds user trust, reduces bias, and supports ethical deployment. Emerging trends such as TinyML allow machine learning models to run efficiently on resource-constrained IoT devices, and AutoML simplifies model development and optimization, expanding access to areas such as healthcare and smart infrastructure.

Biometric security is also evolving with continuous authentication and multimodal approaches that combine fingerprints, facial recognition and voice verification for enhanced protection without sacrificing usability. In IoT-based applications such as smart homes, smart cities, and healthcare monitoring, AI-based biometrics enhance personalized services and secure access control. Future developments will focus on encryption, federated learning, interoperability, and standardization to ensure secure, reliable, and scalable deployments.[4]

Result and Discussion

The implemented smart home automation system successfully integrates IoT devices, sensor-based monitoring, and predictive control using a Raspberry Pi 3B+ platform. Real-time communication through Wi-Fi and Zigbee ensures smooth coordination between connected appliances, while a Flask-based web interface enables secure remote access and control. PIR sensors automate lighting and fans based on motion detection, and relay modules manage high-voltage devices safely. Sensor calibration and filtering techniques minimize false triggers, enhancing operational stability.

A linear regression model analyzes historical usage patterns to predict user behavior and adjust appliances proactively, improving energy efficiency and personalization. Security features, including local video processing and facial recognition, generate alerts only for unknown individuals. Encrypted communication, authenticated access, and secure cloud synchronization further protect data. Despite hardware and internet limitations, the modular design ensures scalability and reliable performance.

Conclusion and Implication

In conclusion, the Raspberry Pi–based smart home automation system demonstrates how IoT integration, sensor monitoring, and predictive analytics can build an efficient, secure, and user-friendly environment. The system optimizes energy consumption through adaptive controls that learn user behavior, reducing waste while maintaining comfort. Security is strengthened through face recognition, encrypted communication, and two-factor authentication, ensuring data protection. Its modular and scalable design supports easy expansion and device integration. By combining edge processing with intelligent automation, the model addresses limitations of traditional systems and promotes sustainable, safe, and convenient smart living for residential and commercial applications.

References

1. Hakilo Sabit Artifical Intelligence-Based Smart Security System Using Internet of Things for Smart Home Applications Electronics 2025, 14(3), 608;https://doi.org/10.3390/electronics14030608
2. Muhammad Inam Ul Haq, Muhammad Sohail , Irsha Qureshi , Haji Muhammad Shoaib , RajibSaha, Muhammad Shaheer, Mohammed Duhis, ALI JOHN, Muhammad Shoaib, Shaping the Next Generation of AI-Integrated Smart Homes: Innovations in Intelligence, Security, Sustainability, and User Experience,Scholars Journal of Engineering and Technology https://doi.org/10.36347/sjet.2025.v13i08.004.
3. O. B. Akan, S. Andreev, and C. Dobre, "Internet of things and sensor Networks," IEEE Communications Magazine, vol. 57, no. 2, p. 40, 2019. https://doi.org/10.1109/mcom.2019.8647109
4. Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. Journal of Information Security and Applications, 82, 103748.
5. Elkhalik, W. A. (2023). AI-Driven Smart Homes: Challenges and Opportunities. Journal of Intelligent Systems & Internet of Things, 8(2).
6. R. Majeed, N. A. Abdullah, I. Ashraf, and Y. B. Zikria, "An intelligent, secure, and smart home automation system," Scientific Programming, vol. 2020, 14 pages, 2020. https://doi.org/10.1155/2020/4579291