Raut Riya Prakas, 2026, 14:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Iot-Based Smart Home Automation: A Review Of Architectures, Microcontroller Platforms, Communication Protocols And Security

Raut Riya Prakash[1] Prof. M. R. Kumbhoje[2] Prof. M. C. Kolse[3] Prof. S. K. Said[4]
Department of Artificial Intelligence and Data Science
Jaihind College of Engineering
Pune, Maharashtra, India

Abstract—A smart greenhouse is an IoT-based automated agriculture system that maintains suitable conditions for plant growth while reducing water, energy and labour. Conventional greenhouses depend on continuous human monitoring and manual switching of pumps, fans and lights, which wastes resources and allows stress conditions to go unnoticed. This paper reviews AI- and IoT-enabled smart greenhouses. It examines sensing of temperature, humidity, soil moisture, light intensity and carbon dioxide; microcontroller platforms such as Arduino and ESP32 that drive irrigation pumps, exhaust fans, foggers and grow lights; and communication through Wi-Fi and MQTT to cloud dashboards and mobile applications for remote monitoring. Beyond fixed-threshold control, it reviews machine learning that predicts the greenhouse microclimate a few hours ahead, recurrent networks for time-series forecasting, and AI-based climate and irrigation strategies that have competed with expert growers. A five-layer architecture comprising sensing, edge control, connectivity, cloud intelligence and user application is proposed, along with research gaps, objectives, a comparison of control strategies and challenges such as sensor drift, power failures, energy cost and crop-specific tuning. The review concludes that predictive, AI-assisted control can make greenhouses more productive and resource-efficient than threshold-based automation alone.

Index Terms—Smart greenhouse, IoT, ESP32, climate control, soil moisture, LSTM forecasting, precision agriculture, controlled environment agriculture

I. INTRODUCTION

Imagine switching off a fan left running at home from the college campus, receiving an alert when motion is detected while the family is away, or having lights turn on automatically at dusk. Smart home automation makes such scenarios possible by connecting household devices to the internet and to each other.

Low-cost Wi-Fi microcontrollers such as the ESP8266 and ESP32 and open-source platforms have made home automation affordable for students and small households. Stojkoska and Trivodaliev [1] reviewed IoT for smart homes and identified challenges of interoperability, energy management and data handling, and Alaa *et al.* [2] classified smart home applications and technologies.

This paper reviews smart home automation architectures, platforms, protocols and security, and proposes a reference design.

II. BACKGROUND AND RELATED WORK

1. Smart Home Functions

Fig. 1 summarizes smart home functions: appliance control, environmental automation, security and surveillance, energy monitoring and assisted living.

© 2026Raut Riya Prakas, , This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

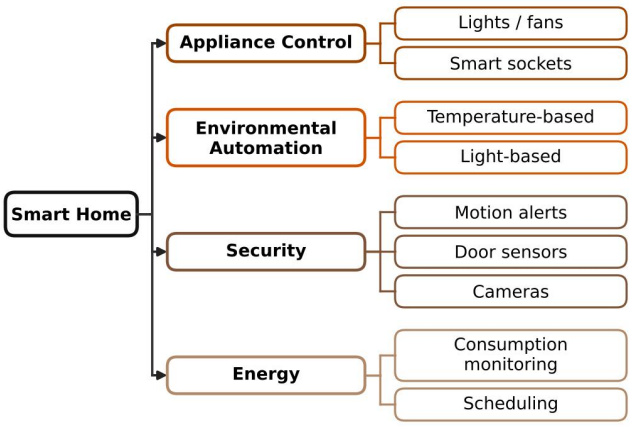


Fig. 1. Functions of IoT-based smart home automation.

2. Platforms And Protocols

Arduino boards provide easy prototyping, while ESP8266 and ESP32 add built-in Wi-Fi and, for ESP32, Bluetooth. MQTT [3] is a lightweight publish–subscribe protocol widely used between devices and cloud brokers. Bluetooth Low Energy [4] and Zigbee support low-power devices, and Matter [5] aims to make devices from different vendors work together.

3. Review Of Related Studies

Brush *et al.* [6] studied households that had installed home automation and found benefits in convenience and security, but also barriers of cost, inflexibility, poor manageability and difficulty achieving security. Stojkoska and Trivodaliev [1] proposed a holistic framework for IoT smart homes, including fog computing for local processing. Alaa *et al.* [2] systematically reviewed smart home applications and grouped them by purpose and technology.

Pirbhulal *et al.* [7] designed a secure IoT-based smart home system using a wireless sensor network with a lightweight encryption scheme suited to resource-constrained nodes. Fernandes *et al.* [8] analysed a popular smart home platform and found that over-privileged apps and insecure event handling could allow attackers to unlock doors or disable alarms. Zeng *et al.* [9] interviewed smart home users and found limited awareness of security and privacy risks.

Kolias *et al.* [10] described how the Mirai botnet compromised poorly secured IoT devices with default passwords, a warning for home devices. Al-Fuqaha *et al.* [11] reviewed IoT protocols relevant to home automation. Table I summarizes these works.

Ref.	Authors	Year	Technique Used	Merits	Demerits
[6]	Brush et al.	2011	Field study of home automation	Benefits and adoption barriers	Early-generation systems
[11]	Al-Fuqaha et al.	2015	IoT protocol survey	Protocol comparison	General IoT
[8]	Fernandes et al.	2016	Security analysis of smart home platform	Over-privilege attacks	Single platform
[1]	Stojkoska and Trivodaliev	2017	Review of IoT smart homes	Holistic framework with fog	Conceptual
[2]	Alaa et al.	2017	Review of smart home applications	Taxonomy of apps and tech	Review only
[7]	Pirbhulal et al.	2017	Secure WSN smart home	Lightweight encryption	Prototype scale
[9]	Zeng et al.	2017	User security and privacy study	Limited user awareness	Small interview sample
[10]	Kolias et al.	2017	Mirai botnet analysis	Default passwords exploited	Attack analysis

TABLE I Summary of Literature Survey

III. RESEARCH GAP AND OBJECTIVES

1. Identified Research Gaps

G1: Devices from different vendors often cannot interoperate.

G2: Many low-cost devices lack secure defaults and firmware updates.

G3: Cloud dependence makes automation fail when the internet is down.

G4: Users have limited understanding of privacy and security settings.

G5: Energy-saving potential is often not quantified.

2. Objectives Of The Review

To review smart home architectures and microcontroller platforms.

To compare communication technologies and protocols.

To examine security and privacy issues in smart homes.

To propose a secure, five-layer smart home automation architecture.

To identify challenges and future enhancements.

IV. DESIGN OF THE PROPOSED SYSTEM

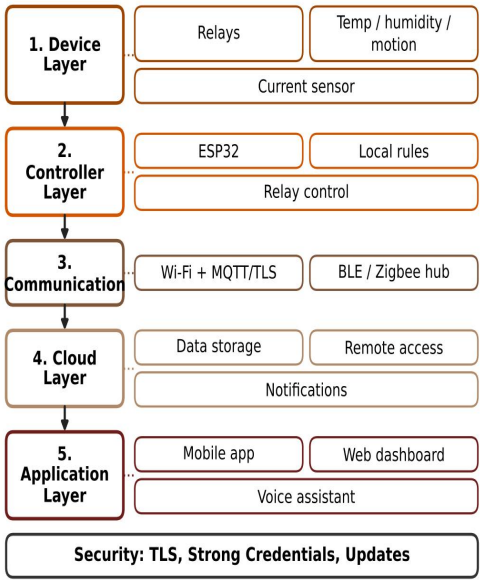


Fig. 2 shows the proposed architecture.

Fig. 2. Proposed five-layer IoT smart home automation architecture.

1. Device Layer

Relays control lights, fans and sockets; sensors measure temperature, humidity, motion, light and door status; a current sensor measures energy use.

2. Controller Layer

An ESP32 reads sensors, executes local rules (for example, turning on a fan when temperature exceeds a set value) and drives relays.

3. Communication Layer

The ESP32 connects through home Wi-Fi to an MQTT broker using TLS; low-power sensors may use BLE or Zigbee through a hub.

4. Cloud Layer

A cloud service stores data, provides remote access, sends notifications and can run learning-based routines that suggest schedules.

5. Application Layer

A mobile app and web dashboard allow monitoring, manual control, scheduling and alerts; voice assistants can be integrated.

6. Methodology

Fig. 3 describes the workflow. A simple rule controls a fan with hysteresis to avoid rapid switching:

$$Fan = ON \text{ if } T > T_set + \delta;\ OFF \text{ if } T < T_set - \delta \quad (1)$$

and energy consumption over a period is computed from measured power,

$$E = \Sigma P_t \cdot \Delta t \quad (2)$$

allowing users to see which appliances consume most.

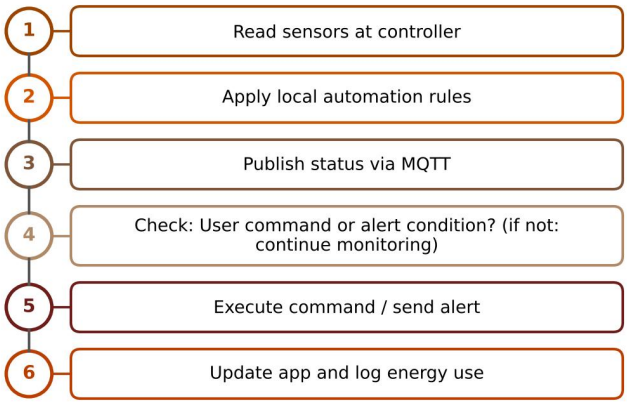


Fig. 3. Smart home automation workflow.

V. DISCUSSION AND COMPARISON

Table II compares communication technologies. Wi-Fi is convenient and fast but power-hungry, BLE suits battery devices nearby, Zigbee forms low-power meshes and Matter aims to unify devices across ecosystems.

Technology	Power	Range	Best Use
Wi-Fi	High	Home-wide	Mains-powered devices
Bluetooth LE	Very low	Short	Battery sensors, phone control
Zigbee	Low	Mesh, home-wide	Many low-power sensors
Matter (over Wi-Fi/Thread)	Low–Medium	Home-wide	Cross-vendor interoperability

TABLE II Comparison of Smart Home Communication Technologies

VI. CHALLENGES AND FUTURE DIRECTIONS

Table III summarizes challenges. Future directions include AI-based occupancy prediction for energy saving, local processing for privacy, integration with rooftop solar and batteries, and voice control in Indian languages.

Challenge	Mitigation
Interoperability	Matter and open protocols
Weak device security	Unique passwords; TLS; updates
Internet outages	Local rules on controller
Privacy	Local processing; minimal cloud data
Cost	Low-cost ESP32-based modules

TABLE III Challenges and Mitigation

VII. CONCLUSIONS

IoT-based smart home automation offers comfort, convenience, safety and energy savings at low cost using platforms such as Arduino and ESP32. The reviewed literature shows mature architectures and protocols but also persistent problems of interoperability and security. A layered design with local control, encrypted communication, secure defaults and a user-friendly app can create smart homes that are both convenient and safe.

1. Acknowledgment

The authors express their sincere gratitude to the Department of Artificial Intelligence and Data Science, Jaihind College of Engineering, Pune, for providing the facilities, guidance and encouragement needed to carry out this work. The authors also thank the faculty members and colleagues whose valuable suggestions helped improve the quality of this review.

REFERENCES

1. B. L. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," J. Clean. Prod., vol. 140, pp. 1454–1464, 2017.
2. M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, "A review of smart home applications based on Internet of Things," J. Netw. Comput. Appl., vol. 97, pp. 48–65, 2017.
3. OASIS, MQTT Version 5.0, OASIS Standard, Mar. 2019.
4. C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of Bluetooth Low Energy: An emerging low-power wireless technology," Sensors, vol. 12, no. 9, pp. 11734–11753, 2012.
5. Connectivity Standards Alliance, "Matter Specification, Version 1.0," CSA, 2022.
6. A. J. B. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon, "Home automation in the wild: Challenges and opportunities," in Proc. CHI, 2011, pp. 2115–2124.
7. S. Pirbhulal et al., "A novel secure IoT-based smart home automation system using a wireless sensor network," Sensors, vol. 17, no. 1, Art. no. 69, 2017.
8. E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in

Proc. IEEE Symp. Security Privacy, 2016, pp. 636–654.

9. E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes," in Proc. 13th Symp. Usable Privacy Security (SOUPS), 2017, pp. 65–80.
10. C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017.
11. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 2015.