IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

A Comprehensive Review on Smart Home Automation System Using IoT

Priyanka Singh[1], Aafiya Javed[2], Harshit Kumar Pandey[3], Ajisha Tyagi[4]
Assistant Professor, Department of Computer Science and Engineering (Internet of Things)[1]
Students, Department of Computer Science and Engineering (Internet of Things)[2-4]
Raj Kumar Goel Institute of Technology, Ghaziabad, India
spriyanka2605@gmail.com[1], aafiyajaved22@gmail.com[2], pandeyji6602@gmail.com[3], ajisha06tyagi@gmail.com[4]

Abstract: *Emerging technologies that utilize the Internet of Things (IoT) provide smart home automation systems that will allow users to remotely control and monitor their home appliances; thereby increasing user convenience as well as providing benefits related to energy conservation, comfort and enhanced security. This article reviews the current state of smart home control, as well as discusses working devices, techniques and their respective platforms that have been developed. Additionally, this article identifies the many trends in current research regarding smart home systems and highlights multiple areas in which further work must be completed in order to become scalable and affordable..*

Keywords: Internet of Things (IoT), Smart Home, Home Automation System, Wireless Communication System, Cloud computing, voice assistance, ESP8266, energy efficiency, remote monitoring, Smart devices

I. INTRODUCTION

The advancement of the Internet of Things (IoT) has completely changed how we live modernly by providing the opportunity for smart devices and sensors to communicate with each other. Smart Home Automation is where digital technologies are integrated to give users the ability to monitor, manage, and automate their home appliances from afar to make their lives more convenient. Increasing demand for intelligent systems developed by urbanization, lifestyle improvement, and wireless communication advancements has contributed to the rapid development of smart home technologies across the world.

Light, fans, door locks and security systems and other smart devices in the home are normally powered by microcontroller units (MCUs) like the ESP8266 and ESP32 and communicated through Wi-Fi, Bluetooth, and ZigBee among other IoT protocols. Users can manage their devices using a mobile app, a web dashboard or voice-controlled assistants such as Amazon Alexa and Google Assistant. Cloud services such as Blynk, Arduino IoT Cloud and Firebase provide data storage, remote connectivity and rules for automating devices within homes to make them more intelligent and responsive.

Many studies have examined the present system architecture; communications schemes; automation control measures and security improvements on the development of smart home environments. Nonetheless, there remain several issues concerning the reliability of technology; the ability of various types of IoT devices to communicate with one another; the risk of cyber-attacks and vulnerabilities in networks; the high cost associated with deploying IoT technology; and the lack of scalability of existing IoT automation solutions. Thus, a thorough review of the current landscape of smart home automation technology is necessary to identify gaps in our knowledge and to evaluate the current state of existing technologies to identify future research initiatives that will move smart home automation forward.

The objective of this article is to provide a comprehensive overview of current developments, to compare different currently available models, and to identify new and evolving approaches that are being developed that will create smart home automation solutions that are more efficient, secure, and cost-effective.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

II. LITERATURE REVIEW

The fast pace of development of the Internet of Things (IoT), cloud computing, wireless communication technologies, and artificial intelligence have played a significant role in the development of Smart Home Automation systems. These systems combine smart devices, sensors and communication networks so as to provide automated control, monitoring and management of appliances in the house. The main aims of smart home systems are to improve ease of use, increase protection and security, save energy as well as offer remote access using a mobile or web-based appliance. Smart home environments have been enhanced over the years by different researchers providing different architectures and implementation techniques to enhance the efficiency, reliability, scalability and intelligence of smart home environment.

Kumar et al. [1] designed and built an IoT-based Smart Home Automation system with the use of Node MCU and the Blynk mobile application in 2019. The system gave the ability to users to have electrical appliances controlled remotely by Wi-Fi. Their effort proved that they could monitor and control connected devices in real-time, which makes the system applicable to the real-life home automation application. Nevertheless, the system did not have high-end security features like encryption and authentication and was not meant to handle large scale implementation with a number of devices and users.

Sharma et al. [2] introduced more sophisticated smart home system, which is based on Raspberry Pi and Python, and combines camera surveillance and motion detection sensors. This system enhanced the automation intelligence and security of homes greatly in the sense that it allowed real-time monitoring and the creation of alerts. Although it was more functional, the implementation of the Raspberry Pi and other hardware components raised the total cost, and thus became less accessible to users with low budgets. In addition, system configuration and maintenance were also more complex than Simpler microcontroller-based solutions.

Ali et al. [3] proposed a voice-controlled smart home automation system to combine the MQTT communication protocol with Google Assistant in 2021. The strategy allowed such users to use voice commands to turn on and off home appliances and was therefore more convenient and accessible especially to the elderly and physically challenged. MQTT was also used to facilitate effective and low weight communications among devices. Nevertheless, the system was very sensitive to constant internet connection which restricted its functionality in places with a weak or unreliable internet connection.

Rahman et al. [4] created an inexpensive prototype of a smart home automation based on the Arduino and Bluetooth technology. This was system that gave priority to short range communication and was applicable in small home settings. Although it was simple and cost effective, the limitation was considerably large as it had a limited communication range, and could not be used to support remote access via the internet. In addition, the system was not scalable and had no advanced automation capabilities, which are critical to the new standards of smart home use.

More recently, in 2023, Patel et al. [5] introduced a smart home automation system, which is an intelligent system, using artificial intelligence and machine learning methods. The system used the behavior patterns of users with the aim of achieving maximum energy consumption and automated decision-making. It was shown that the system was more adaptive and intelligent as the experimental results showed better energy efficiency and predictive capabilities. Nevertheless, machine learning algorithms, along with their combination, made the computations more complex and demanded more processing power, which might not be appropriate when the low-power embedded system (e.g. ESP8266) is used.

Besides these works, there are recent works that have also examined the application of edge computing and hybrid architectures in minimizing latency and enhancing data privacy in smart home systems. Edge-based solutions store data locally rather than fully depending on the cloud server, thus improving the response time and reducing the reliance on an internet connection. Moreover, to mitigate the challenges that cybersecurity poses in regard to the IoT based systems, scholars have explored the application of secure communication protocols and encryption methodologies. Regardless of these improvements, a balance between cost, security, scalability and performance is a big challenge.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

All in all, the literature shows that there is a distinct shift away with simple remote-controlling systems to smarter and more adaptive and interrelated smart home systems. Although major positive changes have been observed with regards to increasing usability, energy emphasizing and automation potential, a number of shortcomings continue to exist such as security weaknesses, interoperability, expensive implementation, offline functionality, and scalability. These shortcomings indicate that there is a need to conduct additional research to create more effective, safer, and cheaper smart home automation system.

III. COMPARATIVE ANALYSIS

TABLE I: Comparison of Existing Smart Home Automation Solutions

Author / Year	Technology Used	Control Method	Strengths	Limitations
Patel et al., 2023	AI, ML, IoT	Prediction automation	Energy efficient, intelligent system	High computational cost
Rahman et al., 2022	Arduino, Bluetooth	Mobile (short-range)	Low cost, easy to implement	Limited range, no internet control
Ali et al., 2021	MQTT, Google Assistant	Voice commands	Hands-free, accessible	Internet dependent
Sharma et al., 2020	Raspberry Pi, Python, Sensors	Surveillance & monitoring	State-of-the-art, advanced features	Expensive, complex
Kumar et al., 2019	Node MCU, Blynk, Wi-Fi	Mobile app	Low price, real-time control	Low security, poor scalability

IV. METHODOLOGY

The first step in developing the Smart Home Automation System was to select a suitable microcontroller board, such as a Node MCU (ESP8266), Raspberry Pi, or Arduino, which will serve as the central control unit for the Smart Home Automation System. To acquire real time environmental data, an interface was provided between the Microcontroller Board and Sensors (e.g., Temperature Sensor, Motion Sensor, Light Sensor). The microcontroller board is also interfaced with actuators and relays to operate appliances (e.g., Lights, Fans, Door Locks) that are to be controlled by a user's instruction.

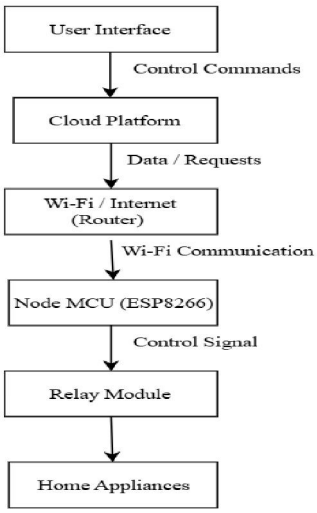

Fig. 1. Architecture of an IoT Based Smart Home Automation System

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

The microcontroller board is programmed using either Arduino IDE or Python to read data from the sensors and perform output actions based on the readings of the sensors. The communication module of the Smart Home Automation System connects the Mobile Application to the Smart Home Automation System using Wi-Fi or Bluetooth and is based on one of several available Communication Protocols (e.g., MQTT or HTTP). Information on the Smart Home Automation System is transmitted to a cloud server (e.g., Blynk, Firebase, Thing Speak) where it is available to view remotely and control using smartphone applications. The purpose of the mobile app is to allow users to control their home appliances remotely. The mobile app also allows users to monitor their appliances by receiving alerts for events or situations related to them and to automate the appliance's operation according to predetermined automation rules.

Users can use voice assistants, such as Google Voice and Amazon Alexa, to control an IoT-enabled appliance from a mobile app by connecting the IoT-enabled appliance to a cloud-based voice recognition API.

User authentication and encrypted communication will help ensure that the IoT device and mobile device communicate securely and prevent unauthorized access to the IoT device.

The performance of the IoT system and mobile application are evaluated through testing in a variety of conditions to confirm that they can meet user expectations in terms of response time, connectivity, and energy efficiency.

Following testing, the mobile application and IoT system will be improved and optimized so that they remain reliable, stable, and user-friendly.

V. TECHNOLOGY USED

There exist smart home automation systems that use many different kinds of technology to monitor and control the many different types of appliances in your home, thus providing enhanced comfort, security, and energy efficiency for you and your family. The core of these systems is based on the Internet of Things (IoT). The IoT integrates all the devices, sensors, actuators and Cloud Services together in such a way that they are able to function together. Microcontroller based hardware platforms such as the ESP8266, ESP32, Raspberry Pi and Arduino will often feature in such systems because they are affordable, flexible, and can handle real time data processing. Microcontrollers connect to electrical loads with relay modules and sensor networks and enable automatic decision making based on the properties of the environment in which they reside. Wireless communication technologies such as Wi-Fi, Bluetooth, ZigBee, Z-Wave, and LoRaWAN provide the various necessary ranges, energy-consumption profiles, and network topologies to connect devices to Cloud Servers for the purposes of controlling devices within a smart home.

In addition, Cloud computing platforms such as AWS IoT, Google Firebase, Blynk, ThingSpeak and Azure IoT Hub provide the ability to remotely connect to internet-connected devices; conduct data analysis on their activity patterns; synchronize with one another; and control them.

TABLE II: Technical Stack Overview

Category	Technology / Tools	Usage
Hardware	ESP8266, ESP32, Arduino	Primary appliance automation controller
Communication	Wi-Fi	Wireless data transfer
Cloud Platforms	Blynk, ThingSpeak	Remote control and data storage
Software Development	Arduino IDE, Python, C/C++	Back-end and firmware coding
Voice Assistants	Amazon Alexa, Google Assistant, Siri	Voice command automation

Based on this comparison, it is observed that current solutions do have issues such as a lack of security and scalability, a complicated and high-cost deployment procedure, and a need for a constant internet connection.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

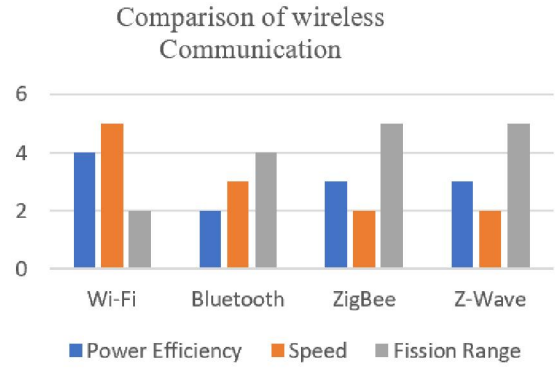

Fig. 2. Comparison chart of smart home automation wireless communication technologies.

VI. CONCLUSION

This review paper involved an in-depth study of Smart Home Automation systems that are built on the IoT technologies. Different available models were examined as Wi-Fi based, Bluetooth based, cloud based, and Voice controlled automation models. The review also indicated that the contemporary smart home systems enhance user convenience, energy efficiency, and security based on remote monitoring and intelligent control systems.

Comparative analysis of already existing works showed that although low-cost solutions are appropriate in the small-scale deployments, they have many limitations including short range, non-scaling, and insufficient security functions. More automated and predictive advanced AI-enabled and cloud-integrated systems, in turn, are more computer intensive and expensive to implement.

As per the findings, it is clear that a smart system of home ought to be efficient enough in cost, scale, security, and usability. The next generation smart home systems are supposed to be based on the combination of safe communication, smart decision-making, and interaction with other gadgets at the same time being affordable. The review would make an excellent starting point of researchers and developers who seek to develop stable, scalable, and user-friendly smart home automation systems.

Moreover, system responsiveness, data privacy, and reliability can be enhanced tremendously by the incorporation of newer technologies (e.g., edge computing, machine learning, and blockchain). The heterogeneity of IoT devices and their interoperability is also a significant issue and needs to be standardized into a common communication protocol to ensure compatibility.

REFERENCES

[1] A. Kumar, R. Singh, and P. Verma, "IoT-based smart home automation system using NodeMCU and Blynk," International Journal of Engineering Research and Technology (IJERT), vol. 8, no. 6, pp. 234–239, 2019.

[2] R. Sharma and S. Verma, "Smart home automation based on Raspberry Pi and Python," International Journal of Advanced Research in Computer Science, vol. 11, no. 3, pp. 45–50, 2020.

[3] M. Ali, T. Khan, and S. Ahmed, "Voice controlled smart house automation with Google Assistant and MQTT," in Proc. IEEE Int. Conf. on Smart Systems and Inventive Technology (ICSSIT), pp. 112–117, 2021.

[4] M. Rahman, A. Hossain, and K. Hasan, "Low cost Bluetooth-based smart home automation system," International Journal of Computer Applications, vol. 174, no. 25, pp. 10–15, 2022.

[5] D. Patel, N. Mehta, and R. Joshi, "Intelligent home automation for energy optimisation using AI," IEEE Access, vol. 11, pp. 45678–45686, 2023.

[6] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A literature review," Journal of Computer and Communications, vol. 3, no. 5, pp. 164–173, 2015.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys and Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.
[8] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[9] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over low-power wireless personal area networks (6LoWPAN)," IEEE Internet Computing, vol. 11, no. 6, pp. 26–34, 2007.
[10] K. Ashton, "That 'Internet of Things' thing," RFID Journal, vol. 22, pp. 97–114, 2009.
[11] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, protocols and applications," Journal of Electrical and Computer Engineering, vol. 2017, pp. 1–25, 2017.
[12] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
[13] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22–32, 2014.
[14] M. B. Yassein, M. Q. Shatnawi, S. Aljwarneh, and R. Al-Hatmi, "Internet of Things: Survey and open issues of MQTT protocol," in Proc. IEEE Int. Conf. on Engineering and MIS, pp. 1–6, 2017.
[15] M. Palattella et al., "Standardized protocol stack for the Internet of (Important) Things," IEEE Communications Surveys and Tutorials, vol. 15, no. 3, pp. 1389–1406, 2013.
[16] R. Piyare, "Internet of Things: Ubiquitous home control and monitoring system with Android based smart phone," International Journal of Internet of Things, vol. 2, no. 1, pp. 5–11, 2013.
[17] S. R. Kodali and C. Soratkal, "MQTT based home automation system using ESP8266," in Proc. IEEE Region 10 Conf. (TENCON), pp. 1–5, 2016.
[18] A. ElShafee and K. A. Hamed, "Design and implementation of a Wi-Fi based home automation system," World Academy of Science, Engineering and Technology, vol. 68, pp. 2177–2180, 2012.
[19] K. Gill, S. H. Yang, F. Yao, and X. Lu, "A ZigBee-based home automation system," IEEE Transactions on Consumer Electronics, vol. 55, no. 2, pp. 422–430, 2009.
[20] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
[21] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, vol. 38, pp. 8–27, 2018.
[22] A. Rghioui, J. L. Guerra, and A. Oumnad, "Internet of Things: Smart home automation and security challenges and solutions," Procedia Computer Science, vol. 134, pp. 630–636, 2018