

Manuscript ID:  
IJRSEAS-2025-020520



Quick Response Code:



Website: <https://eesrd.us>



Creative Commons  
(CC BY-NC-SA 4.0)

DOI: 10.5281/zenodo.18594848

DOI Link:  
<https://doi.org/10.5281/zenodo.18594848>

Volume: 2

Issue: 5

Pp. 106-113

Month: October

Year: 2025

E-ISSN: 3066-0637

Submitted: 10 Sept. 2025

Revised: 15 Sept. 2025

Accepted: 10 Oct. 2025

Published: 31 Oct. 2025

Address for correspondence:

S.S. Watpade  
Ph.D Scholar, Department of  
Electronics, M. G. V. L.V. H. Arts,  
Science and Commerce College,  
Panchavati, Nashik, Affiliated to  
Savitribai Phule Pune University,  
Pune, Maharashtra, India  
Email: [sagarwatpade5@gmail.com](mailto:sagarwatpade5@gmail.com)

How to cite this article:

Watpade, S. S., Dandgavhal, H. N.,  
Shinde, U. P., Hawale, C. T.,  
Wankade, S. A., & Patil, A. B.  
(2025). Research on the Current  
Technology, Challenges and  
Limitations of IoT Based Smart  
Home. International Journal of  
Research Studies on Environment,  
Earth, and Allied Sciences, 2(5),  
106–113.  
<https://doi.org/10.5281/zenodo.18594848>

## Research on the Current Technology, Challenges and Limitations of IoT Based Smart Home

S. S. Watpade<sup>1</sup>, H. N. Dandgavhal<sup>2</sup>, Dr. U. P. Shinde<sup>3</sup>, C.T. Hawale<sup>4</sup>,  
Dr. S. A. Wankade<sup>5</sup>, Dr. A. B. Patil<sup>6</sup>

<sup>1,2</sup>. Ph.D Scholar, Department of Electronics, M. G. V. L.V. H. Arts, Science and Commerce College, Panchavati, Nashik, Affiliated to Savitribai Phule Pune University, Pune, Maharashtra, India

<sup>3</sup>Professor, M. J. M. Arts, Commerce and Science College Karan Jali Tal. Peth, Dist. Nashik, Maharashtra, Affiliated to SPPU, Pune, Maharashtra, India

<sup>4,5</sup> Assistant Professor, K T H M College, Nashik, Maharashtra, Affiliated to Savitribai Phule Pune University, Pune, Maharashtra, India

<sup>6</sup>Associate Professor, Department of Electronics, M. G. V. L.V. H Arts, Science and Commerce College, Panchavati, Nashik, Affiliated to SPPU, Pune, Maharashtra, India

### Abstract

The concept of smart homes has emerged as a transformative approach to modern living, leveraging the Internet of Things (IoT) to enable interconnected, intelligent, and energy-efficient environments. A smart home integrates sensors, actuators, and controllers with cloud and edge computing platforms to provide automation, safety, comfort, and energy optimization. Despite technological progress, IoT-based smart home systems face critical challenges, including high setup costs, limited interoperability, network dependency, and cybersecurity threats. This review presents an in-depth analysis of current technologies, architectures, and communication protocols used in smart homes. It also explores artificial intelligence (AI), machine learning (ML), and renewable energy integration as potential enablers for sustainable and secure home automation. The paper concludes with insights on future research directions for developing affordable, efficient, and privacy-aware smart home systems.

**Keywords:** IoT, Smart Home, IoT Applications, Single Board Computers, Home Automation.

### Introduction

The last ten years have seen sudden changes in the digital technologies and wireless communication that brought a revolution to how human beings interact with their living conditions. Internet of Things (IoT) facilitates the communication and exchange of data among ordinary everyday objects, including lights, thermostats, doors, and appliances, with the use of an embedded sensor and microcontroller [1]. These technologies together form a smart house, a smart system that can learn how to behave, and can control the things going on at home and automate the process [2], [3] when incorporated into the domestic environments. The IoT-driven smart home systems have a number of benefits such as remote access, greater safety, convenience, energy savings, and resource optimization [4]. As an illustration, intelligent lights can be set to regulate their intensity and the temperature of their colors depending on the occupancy and daylight level and smart thermostats can be set to turn on and off heating and cooling systems depending on the prevailing environmental conditions at a particular time [5]. The systems usually use the connections of clouds and interfaces of smartphones, which enable their users to track and manage the household equipment wherever they are in the world [6]. Machine Learning (ML) and Artificial Intelligence (AI) have also revolutionized smart home automation since it brings data-driven smartness. Predictive models have the ability to recognize behavioral patterns, the preferences of users and make independent decision to save energy and improve comfort [7], [8].

As an example, ML methods can identify anomalies in energy consumption, predict energy needs in the future, and even fire warnings related to possible system failures or breaches of the security system [9]. The IoT and AI integration is resulting in what researchers refer to as the Cognitive Home a self-adaptive environment that is proactive towards human needs [10]. The massive potential of the IoT-based smart homes is not as great as it is, and there are no worries about its large-scale implementation. The inhomogeneity of devices and communication standards can create rather often the problem of interoperability across products produced by various manufacturers [11].

Moreover, a well-built and strong network infrastructure is necessary because any disruption in the connectivity, however, small, may affect automation procedures within a smart home [12]. Cybersecurity and data privacy are also significant issues, as IoT devices produce huge volumes of personal and behavioral data which can be used without being properly handled [13]. Research reveals that a high percentage of commercial IoT appliances are released into the market with poor or obsolete security, which makes them more susceptible to unauthorized access and information theft [14].

Moreover, installation and maintenance expenses are also still a major obstacle to adoption especially in the developing world [15]. Premium smart home solutions are highly functional, but such products are usually costly in proprietary hardware and software. As a result, there has been an increasing desire to develop cost-effective and scalable and interoperable IoT-based systems that may enable automation to be accessible to the average household [16].

Sustainability is also a necessary issue of smart home research. Renewable energy sources, e.g. solar photovoltaic (PV) systems, and energy-efficient IoT devices can help cut carbon footprints and reliance on traditional power grids significantly [17]. Besides, Green IoT is aimed at making the electronic parts low-power and recyclable, as well as environmentally friendly [18].

In solving these challenges, recent studies are changing to edge and fog computing systems where the computing workload is divided between local devices and cloud servers. This mixed solution lowers the latency, maximizes the security of data, and minimizes the bandwidth usage [19]. Besides, the decentralized system used to authenticate devices with the help of blockchain technology and biometric-based access control can enhance system integrity and users' privacy [20].

Thus, the purpose of the paper is to conduct a general review of existing technologies, framework, challenges, and limitations of IoT-based smart homes. It discusses new tendencies, including AI addition, edge computing, and optimization of renewable energy and accentuates the necessity of low-cost and secure solutions related to the next generation of smart living environments.

### **Modern technologies and architecture**

The IoT-based smart home systems are composed of a number of integrated layers, which include perception, network, middleware, and application layers that can facilitate the seamless collection of data, communication, analysis, and intelligent decision-making [21]. All the layers are important in making sure that the interconnected devices work best, share information effectively, and automate processes to operate reliably in a smart environment.

### **Hardware Components**

The perception layer is the base of smart home architecture as it is made up of hardware devices that perceive and communicate with the environment [22]. This layer comprises several environment sensors, including temperature, humidity, gas, motion, light and proximity, sensors which constantly monitor the environment information. Actuators then use this information to take physical actions like turning on lights, opening windows or even regulating the room temperature. Raspberry Pi, Beagle Bone Black and Arduino Mega are single-board computer models that are most often used because of their processing power, small size, and affordability [23].

Those platforms are able to perform automation on-premise and also assist in integration with cloud services to have real-time control. More recently, systems based on microcontrollers, including ESP8266 and ESP32, are increasingly popular due to its inbuilt Wi-Fi modules and low power consumption, which allows it to communicate seamlessly with IoT networks [24].

In order to be even more efficient, scientists consider energy-gathering sensors that are able to act independently by transforming solar, kinetic, or thermal energy into electricity and hence less maintenance needs and more sustainability [25]. Also, the use of hardware security modules (HSMs) and trusted platform modules (TPMs) boosts data integrity and device authentication in the IoT system [26].

### **Communication Technologies**

The IoT-based smart home systems rely on wireless communication to provide connection between sensors and actuators as well as to the cloud services. Various communication protocols are available with different distance, data and power requirements.

Short-range communication is usually referenced to Bluetooth and ZigBee where a low-power consumption and mesh network are provided with the option of communicating multiple nodes efficiently [27]. ZigBee, which is founded on the IEEE 802.15.4 standard is specifically applicable in-home automation because of its reliability and scalability.

Wi-Fi is also one of the most popular technologies used as a medium of communication in the medium to long-range due to the high rate of data transmission and their extensive coverage. But it is relatively high-energy-consuming, which is why it is not so appropriate to low-power sensors [28]. The new Wi-Fi 6 (IEEE 802.11ax) standard ensures that most of these concerns are overcome by offering such features as Target Wake Time (TWT) and a better performance of the network with multiple users, which makes it more suited to the IoT context [29].

Lora WAN and NB-IoT have become effective in long-range low-power communication. Lora WAN is able to communicate the information with a distance of several kilometers and very little power consumption, which is suitable in remote supervision utilization [30]. In the meantime, NB-IoT is highly covered and secure communication in cellular networks, which is used in applications like smart metering, intrusion detection, and appliance monitoring [31].

The introduction of 5G networks has enabled IoT based smart houses to be ultra-low latency, highly reliable, and responsive in real-time [32]. 5G massive machine-type communication (m MTC) feature has created the possibility of having a large number of smart devices to be operational at the same time, which is the main enabler of the next-generation smart home automation.

In order to maximize the performance, researchers are working on the hybrid communication models, where several technologies (e.g., Wi-Fi with high bandwidth and LoRa with long-range coverage) are used and balanced in a manner that makes them fast and effective, or rather reliable [33].

### **Software and Platforms**

The middleware in IoT-based smart homes helps in controlling and smart management of the devices, as well as communication. It mediates the disparity between the physical devices and to the user service over middleware and cloud services [34].

AWS IoT core, Google Cloud IoT, and Microsoft Azure IoT Hub are cloud computing platforms available to provide infrastructure to register devices, store data, perform analytics, and visualize data in real-time. The platforms are very scalable and can be integrated with AI tools to provide sophisticated automation [35].

Nevertheless, complete reliance on cloud computing creates a latency and privacy risk. Edge computing and fog computing architectures are being embraced to overcome this. In such architectures, data processing is also done nearer to the source (on gateways or local nodes), and hence the response time is reduced significantly and bandwidth usage over the network is minimized [36]. Fog computing also expands the abilities of the cloud by establishing mini-data centers that are distributed between the edge and the cloud, thus enhancing the abilities of the cloud in terms of scalability and fault tolerance [37].

Lightweight communication protocols like MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) have been established as a standard in the industry in terms of IoT environment, mainly at the application layer [38]. The publish/subscribe concept of MQTT can guarantee effective message transmission in the case of unreliable networks, whereas the RESTful architecture of CoAP enables the use of constraints devices with low overhead.

Secondly, there is a growing popularity of open-source devices such as Home Assistant, Open HAB, and Domoticz since they provide the opportunity to incorporate multi-brand devices into a single dashboard. Such structures also increase the security by localizing data and less self-reliance on the external server.

### **New technologies and the use of new applications**

The transformation of smart houses based on IoT has transcended the easy automation and integration of devices. Artificial Intelligence (AI), Machine Learning (ML), Blockchain, Edge/Fog Computing, and Renewable Energy Integration are the new technologies that are being integrated to ensure smart homes are more adaptive, efficient, secure, and sustainable [40]. These technologies facilitate smart decision making, decentralized data processing, and energy optimization and can turn the traditional home automation into a self-educating, context-driven ecosystem.

#### **1. Smart Homes and Artificial Intelligence, and Machine Learning**

The role of AI and ML is very important in the automation of the process of decision making in IoT ecosystems. Through high volumes of data generated by sensors and devices, AI algorithms learn patterns of behavior, predict system failures, and give control enhancements, which do not require human intervention [41].

As an example, smart thermostats employ the supervised learning algorithms to forecast occupancy and dynamically adjust the temperature to save energy [42]. On the same note, the surveillance systems powered by AI can identify abnormal behaviors and issue security warnings in real time [43]. Activity recognition, energy prediction, and personalized automation is being performed by the use of deep learning and reinforcement learning techniques [44].

Research demonstrates that by combining ML and IoT, they can deliver significant improvements in efficiency by improving resource distribution and detecting anomalies [45]. Also, Natural Language Processing (NLP) enables direct communication between computers and people with the help of voice recognition via assistant applications like Amazon Alexa, Google Assistant, and Apple Siri [46].

With the implementation of the Edge AI (the direct deployment of AI models on local IoT devices), the reliance on cloud services decreased and privacy increased. Edge AI will provide real-time analytics, reduce latency, and improve response time of time-sensitive applications because data are processed locally [47].

#### **2. Blockchain to Secure and Decentralized Communication.**

The main concern in IoT-based systems of smart homes is security and privacy because the number of gadgets sharing sensitive information is very high. Conventional centralized systems are prone to single points of failure and data attacks. To deal with such concerns, the blockchain technology offers a decentralized and tamper-proof authentication, access control and data integrity mechanism [48].

The distributed ledger of blockchain secures the fact that all the transactions to be made between devices are properly checked and documented without third-party verification [49]. This allows clear management of device identities and traceability of data in intelligent home networks. Actions that can be automated through smart contracts, which are self-executing code written into the blockchain, include giving a device access or setting up the firmware when certain conditions are satisfied [50].

Recent studies indicate the usefulness of blockchain in preventing DDoS and spoofing attacks in Internet of Things. IOTA and Hyperledger Fabric have been adapted into lightweight blockchain models that are compatible with low-power IoT devices, and they are both scalable and secure [51].

3. **Renewable Energy and Smart Grid Technologies.**

The adoption of renewable sources of energy into smart homes is in tandem with the international trend of using renewable energy. IoT systems have the capability to measure and manage the production, storage, and use of solar panel and wind turbines or energy storage-based renewable energy [52].

IoT smart meters and sensors study power consumption trends, balance the distribution of loads, and optimally at what time to store or feed energy into the grid maximizing efficiency and minimizing the electricity bills [53]. Smart grids build upon these abilities by allowing two-way communication between utilities and homes, which will allow homes to be part of a demand-response program and provide grid resilience.

Combining IoT with solar-based energy control also facilitates electrification of the rural areas and economical access to energy. Smart homes powered by renewable energies are more sustainable and independent with energy-harvesting sensors and low-power communications.

4. **Healthcare and Ambient Assisted Living (AAL) Applications.**

Ambient Assisted Living (AAL) paradigms are employing IoT-based smart homes to monitor healthcare and elder-care. Embedded devices and wearable sensors constantly record vital signs such as heart rate, temperature, oxygen saturation, and blood pressure and send the information to be tracked remotely and intervened upon early [54]. Anomaly detection based on AI has the capability of detecting emergencies (falls, arrhythmias) and automatically notify the caregiver or medical services [55]. The COVID-19 pandemic boosted the usage of telemedicine characteristics integrated into smart homes, which highlight their importance in the interest of the common good health [56]. Context-aware systems also contribute to the emotional and mental well-being by adjusting the environmental stimuli (lighting, sound, temperature) to user requirements [57].

5. **Decentralized control using E. Edge and Fog computing.**

Conventional IoT services that are cloud-based are associated with constraints in latency, bandwidth, and privacy. With edge computing, computation is brought nearer to the devices, on the gateway and on local nodes, allowing quicker decision making and switching smaller loads to the cloud [58]. The idea of fog computing goes further and disperses the workloads to multiple local nodes and mini data centers, enhancing scalability and fault tolerance [59]. Empirical analysis notes that there are substantial latency and network transmission cost reduction in the case of deployed smart home using hybrid edge/fog/cloud architectures [60].

6. **The Future of IoT-based Smart Homes.**

The IoT based smart homes of the next generation will be context and self-adaptable and energy-positive and able to learn out of human behavior and out of the environment. The intersection of Edge AI, security based on blockchains and renewable energy management will allow houses to act independently in smart cities systems [61].

The new technologies like, 6G networks, quantum-resistant cryptography, and green computing are going to enhance the resilience of the systems, guaranteeing users with the high-speed connection, integrity of data, and sustainability. The future houses will comfortably combine the AI-based predictive functions, optimization of energy and human-oriented design and it will be a significant milestone to achieving the vision of a safe, sustainable and intelligent living environment of everyone.

### **Challenges and Limitations**

Although there have been tremendous advancements in the smart home technologies through IoT, a number of challenges still limit the full-scale implementation of the technologies and its sustainability in the long term. These issues emerge on the basis of technical, economic, environmental, and ethical factors that have to be met in a bid to have a secure, scalable, and intelligent smart home ecosystem.

### **Security and Privacy Concerns**

The most important problems in smart home systems based on IoT are security and privacy. Smart devices are actively gathering, relaying and processing sensitive information, including user patterns, health data and location data. Loss of such data to unauthorized people may lead to identity theft or invasion of surveillance [13]. The variety of IoT hardware/software/communication standards can frequently result in an irregular security setup, exposing networks to cybercrime [55].

Vulnerabilities include weak encryption schemes, out of date firmware, and hard coded credentials. Even more, the single points of failure that are presented by centralized cloud-based architectures risk data breach on a large scale [54]. The latest developments, including distributed authentication based on blockchain and homomorphic encryption, have been suggested as part of the measures to increase data confidentiality and security. Nevertheless, the implementation of these techniques in resource-constrained IoT devices is still a problem because of computational and energy constraints [57].

New methods such as federated learning enable training of data models on a local level across many devices without transferring raw data, which improves privacy and efficiency [51]. However, the challenge of maintaining a trade-off between privacy protection, computational efficiency and user experience remains a research problem.

## Interoperability and Standardization

One of the serious issues with the implementation of smart homes is that there is no interoperability between the devices of various manufacturers. Vendor communication standards and disconnected ecosystems frustrate consolidation and growth [61]. This fragmentation adds to the maintenance expenses, lowers flexibility and does not allow users to mix devices of various vendors.

Open-source communication platforms, like the MQTT, CoAP, and Open Connectivity Foundation (OCF) are structured to permit interoperability. But practical implementation is as yet restrained due to the lack of universal ontologies and universal APIs in which to exchange data [52]. To address these problems, scholars are placing a focus on development of coherent semantic models that determine common meaning among devices and platforms, so that devices can interoperate successfully in various smart home environments [61].

## Large Deployment and Maintenance Expenses

Though the components of the IoT like sensors and microcontrollers are increasingly becoming affordable, the cost of installing an initial smart home system is still very expensive. The costs in specialized configuration, tailored code, and periodic upgrades of the system raise the financial strain [60]. Implementation of the IoT solutions into older houses is especially difficult, since not all buildings have an electrical and data infrastructure built-in.

Also, the constant work of the IoT devices consumes more energy, which neutralizes potential energy savings in case it is not effectively addressed [53]. Reliance on batteries can be minimised by the utilisation of self-powered and energy-harvesting sensors, which require power sources relying on solar or kinetic energy [21]. Nevertheless, the technologies remain in their prototype form, which restricts their wide use.

## Dependence upon Latency, Interconnection, and Network

Smart homes are based on the idea of real-time connection. Failure of network connections or excessive delays may affect automation programs and safety, particularly with automation systems such as healthcare monitoring and residential security [43]. Dependency on cloud computing in the decision-making process brings about extra delays in communication [47].

The architecture of edge and fog computing has been developed to reduce the latency through the processing of data near the source. Despite enhancing responsiveness, there are still problems in various issues of resource allocation and device coordination issues over heterogeneous networks [37]. The 6G networks to come will focus on these constraints and overcome them by means of ultra-reliable low-latency communication (URLLC), higher data-rates, and massive machine-type connectivity [59].

## Environmental and Ethical Considerations

The rising quantity of IoT devices helps in the growing amount of electronic waste (e-waste) and escalating energy consumption. A large number of IoT parts used in low-cost devices have short operational life and are not very recyclable, further contributing to the destruction of the environment [17]. Meanwhile, the Green IoT methodology encourages greener design with energy efficient protocols, recyclable material and sustainable manufacture [53].

On the ethical level, permanent surveillance by IoT sensors creates the issues of privacy and consent. The users are not always aware of how their data is collected and processed. This is further complicated by AI-driven automation which makes decisions autonomously which do not necessarily reflect the intentions of the user [57]. The next generation policies therefore should guarantee transparency, informed consent, and right of ownership of the data to the user in the smart home settings.

## Conclusion and Future Work

Smart homes are transforming the modern way of life through the incorporation of interconnected devices, artificial intelligence, and cloud computing into the daily life settings. Such systems are energy efficient, secure, comfortable and automated providing a glimpse of adaptive and sustainable living [31]. Nonetheless, data security, interoperability, cost, connectivity, and ethical design are still problematic issues that inhibit adoption, especially in developing economies.

Further studies are needed to come up with secure-by-design systems that integrate blockchain authentication with lightweight-based encryption to ensure the integrity of the devices [54]. Smart automation will be made possible with privacy-sensitive AI systems, including federated and distributed learning, which will protect personal data [51]. Equally, context-sensitive AI models should compromise on both personalization and ethical decision-making, so that there is responsible automation within homes [46].

Technologically, convergence between 6G networks and Edge AI will provide near zero latency, high throughput, and distributed intelligence and allow real-time decision-making [59]. The key to developing carbon-neutral homes will be integration of solar-powered IoT devices and smart grid technologies to minimize footprints on the environment [58].

Standardization is also of equal concern and this is one of the main requirements of large-scale adoption. International interoperability standards in the IoT ecosystems will guarantee interoperability among devices, enhance data consistency and decrease fragmentation [61]. To achieve standard policies on cybersecurity, data management, and device certification, it will be necessary to have a multi-stakeholder approach between academia, industry, and regulatory authorities.

Recapping, smart homes using IoT have developed into a luxury system to a necessity in the future smart cities. Overcoming the issues of security, sustainability, and interoperability will open the path to intelligent homes that are autonomous and energy-positive and ethical and ultimately leading to a sustainable digital society.

#### Acknowledgments

The author is thankful to Research Centre, Department of Electronic Science, M.G.V.'s Loknete Vyankatrao Hiray Arts, Science and Commerce College, Panchavati, Nashik, Maharashtra, India-422003 and Savitribai Phule Pune University, Pune.

#### Financial support and sponsorship

Nil.

#### Conflicts of interest

The authors declare that there are no conflicts of interest regarding the Publication of this paper.

#### Reference:

1. R. Piyare, "Internet of Things: Ubiquitous home control and monitoring architecture," *International Journal of Internet of Things*, vol. 2, no. 1, pp. 5–11, 2013.
2. 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.
3. 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 & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
4. N. Patel and K. Patel, "IoT-based low-cost and intelligent smart home automation system," *Int. J. Eng. Res. & Technol. (IJERT)*, vol. 5, no. 5, pp. 180–184, 2016.
5. M. Burhan, R. Rehman, B. Khan, and B. Kim, "IoT elements, layered architectures, and security issues: A comprehensive survey," *Sensors*, vol. 18, no. 9, p. 2796, 2018.
6. S. Jabbar, A. Hanif, M. Sher, and M. Naseer, "Smart home automation using IoT and its low-cost implementation," *International Journal of Computer Applications*, vol. 179, no. 45, pp. 25–30, 2018.
7. M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, 2016.
8. M. Islam, S. Rahman, and A. Rahman, "Edge AI for intelligent IoT: Trends and challenges," *IEEE Access*, vol. 9, pp. 90525–90544, 2021.
9. L. Zhang, Z. Chen, and F. Li, "AI-based fault detection in IoT smart homes," *Sensors*, vol. 22, no. 7, p. 2649, 2022.
10. P. Srivastava and S. Agarwal, "IoT-based smart home using sensors and automation," *Int. J. Innovative Res. in Comp. & Comm. Eng. (IJRCCE)*, vol. 6, no. 3, pp. 2450–2456, 2018.
11. S. Gabhane, P. S. Rakhunde, and M. S. Rane, "Standardization challenges in Internet of Things (IoT): A review," *IJSRCSEIT*, vol. 6, no. 2, pp. 245–250, 2020.
12. C. Gomez, M. M. Uusitalo, J. D. C. Garcia, and K. Norrman, "From 802.11 to 802.11ax: Wi-Fi evolution for IoT applications," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1973–2008, 2020.
13. M. H. Alsharif, R. Nordin, and M. Ismail, "Security and privacy in smart homes: IoT technologies," *IEEE Access*, vol. 9, pp. 150307–150327, 2021.
14. A. W. Malik and H. Ali, "Integration of renewable energy sources in smart homes," *IEEE Transactions on Sustainable Energy*, vol. 12, no. 2, pp. 1001–1012, 2021.
15. B. Li and J. Yu, "Research on the architecture of Internet of Things," in *Proc. Int. Conf. on Advances in Energy Engineering (ICAEE)*, Beijing, China, 2011, pp. 69–72.
16. D. Sah, "IoT-based home automation using Raspberry Pi," *Int. J. Research in IT & Computer Communication (IJRITCC)*, vol. 9, no. 4, pp. 224–230, 2021.
17. K. Singh, V. Yadav, and P. Jain, "Green IoT for sustainable smart homes," *IEEE Access*, vol. 10, pp. 65321–65340, 2022.
18. 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.
19. L. Da Xu, W. He, and S. Li, "Edge computing for IoT applications: A comprehensive review," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6505–6520, 2022.
20. S. Li, L. Xu, and S. Zhao, "A blockchain-based IoT security framework," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5849–5858, 2021.
21. M. S. Hossain and G. Muhammad, "Energy harvesting for self-powered IoT: Recent advances and challenges," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4681–4698, 2021.
22. A. Ghosh, S. Paul, and S. Biswas, "Hardware-assisted security in IoT: Architectures and challenges," *IEEE Access*, vol. 9, pp. 42241–42257, 2021.
23. R. Khan, S. Khan, and A. Zaidi, "ZigBee-based wireless sensor network for smart home applications," *Sensors*, vol. 21, no. 5, p. 1789, 2021.
24. P. Sharma and R. Kaur, "Comparison of Bluetooth and ZigBee technologies for IoT," *Int. J. Computer Science and Information Technologies (IJCSIT)*, vol. 7, no. 3, pp. 1202–1206, 2016.

25. S. K. Sharma and X. Wang, "Toward massive machine-type communications in ultra-dense cellular IoT networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2312–2334, 2018.
26. D. Harwahu, I. Supeno, and A. Kusnadi, "NB-IoT for smart city and home automation: Performance analysis," *IEEE Access*, vol. 8, pp. 2169–3536, 2020.
27. Y. Zhang, J. Wang, and T. Yang, "Hybrid communication architectures for IoT-based smart homes," *IEEE Access*, vol. 10, pp. 13528–13541, 2022.
28. A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.
29. N. Kaur and A. Sharma, "Fog computing-based IoT framework for smart home automation," *J. Network & Computer Applications*, vol. 190, p. 103140, 2021.
30. P. Thota and S. Kim, "Implementation and comparison of MQTT and CoAP protocols for IoT," *Int. J. Computer Applications (IJCA)*, vol. 113, no. 1, pp. 6–10, 2015.
31. H. Rahman, S. Rahim, and M. Tariq, "Intelligent decision-making for IoT-based smart home automation," *IEEE Access*, vol. 9, pp. 110452–110463, 2021.
32. T. Nguyen and Y. Kim, "Machine learning approaches for energy-efficient smart homes," *IEEE Sensors Journal*, vol. 21, no. 12, pp. 13985–13996, 2021.
33. J. Lin, W. Yu, and N. Zhang, "AI-based surveillance and activity recognition in smart homes," *Sensors*, vol. 20, no. 23, p. 6900, 2020.
34. S. V. Kumar, R. Gupta, and L. Singh, "Deep reinforcement learning for home energy management systems," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4302–4312, 2021.
35. [35] M. Rahman, A. Hossain, and M. Alam, "AI and machine learning integration in IoT for smart living," *Int. J. Advanced Computer Science & Applications*, vol. 12, no. 9, pp. 90–98, 2021.
36. [36] A. W. Malik and M. A. Khan, "Integration of voice-controlled assistants in IoT smart environments," *IEEE Access*, vol. 10, pp. 68491–68503, 2022.
37. A. Yassine, H. Rahimi, and S. Shirmohammadi, "Edge computing for smart homes: A survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1234–1256, 2021.
38. A. Moinet, B. Darties, and J. Baril, "Blockchain for the Internet of Things: State of the art and future trends," *Future Generation Computer Systems*, vol. 92, pp. 366–380, 2019.
39. M. Singh and S. Kim, "Blockchain-enabled smart contracts for IoT-based smart home automation," *IEEE Access*, vol. 8, pp. 11732–11743, 2020.
40. R. Sharma, D. K. Singh, and P. K. Yadav, "Blockchain and AI-enabled security for smart IoT ecosystems," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 1843–1855, 2022.
41. S. A. Qureshi and M. A. Qureshi, "IoT-enabled energy optimization for residential smart grids," *IEEE Access*, vol. 9, pp. 65812–65823, 2021.
42. D. Kim and Y. Park, "Smart grid integration in IoT-based home automation systems," *IEEE Access*, vol. 10, pp. 25123–25133, 2022.
43. M. Alam, S. Ali, and T. Alzahrani, "IoT-based remote patient monitoring in smart homes," *Sensors*, vol. 21, no. 9, p. 3119, 2021.
44. J. Liu, H. Zhou, and Y. Chen, "AI-driven anomaly detection for healthcare IoT systems," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8027–8038, 2021.
45. A. Hussain and M. Khan, "IoT-enabled healthcare and telemedicine for pandemic management," *IEEE Access*, vol. 9, pp. 96016–96029, 2021.
46. S. Kumar and L. Jain, "Context-aware smart homes for emotional well-being," *IEEE Access*, vol. 10, pp. 44452–44464, 2022.
47. M. Chiang and T. Zhang, "Fog and edge computing: Emerging architecture for IoT," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 530–540, 2018.
48. N. Kaur and A. Sharma, "Fog computing-based IoT framework for smart home automation," *J. Network & Computer Applications*, vol. 190, p. 103140, 2021.
49. Y. Zhang, J. Wang, and T. Yang, "Hybrid communication and computing models for smart homes," *IEEE Access*, vol. 10, pp. 13528–13541, 2022.
50. P. Jain and S. Kumar, "6G-enabled intelligent IoT networks for future smart homes," *IEEE Internet of Things Magazine*, vol. 6, no. 1, pp. 25–36, 2023.
51. S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A literature review," *J. Computer and Communications*, vol. 3, no. 5, pp. 164–173, 2015.
52. L. Da Xu, S. Li, and S. Zhao, "5G Internet of Things: A survey," *J. Industrial Information Integration*, vol. 10, pp. 1–9, 2018.
53. P. Thota and S. Kim, "Implementation and comparison of MQTT and CoAP protocols for IoT," *Int. J. Computer Applications (IJCA)*, vol. 113, no. 1, pp. 6–10, 2015.
54. M. Alam, S. Ali, and T. Alzahrani, "IoT-based remote patient monitoring in smart homes," *Sensors*, vol. 21, no. 9, p. 3119, 2021.
55. J. Liu, H. Zhou, and Y. Chen, "AI-driven anomaly detection for healthcare IoT systems," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8027–8038, 2021.
56. A. Hussain and M. Khan, "IoT-enabled healthcare and telemedicine for pandemic management," *IEEE Access*, vol. 9, pp. 96016–96029, 2021.

57. S. Kumar and L. Jain, "Context-aware smart homes for emotional well-being," *IEEE Access*, vol. 10, pp. 44452–44464, 2022.
58. A. Yassine, H. Rahimi, and S. Shirmohammadi, "Edge computing for smart homes: A survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1234–1256, 2021.
59. M. El-Hajjar and K. Saeed, "6G prospects and requirements for massive IoT and smart home ecosystems," *IEEE Network*, vol. 38, no. 4, pp. 64–71, 2024.
60. Y. Zhang, J. Wang, and T. Yang, "Hybrid communication and computing models for smart homes," *IEEE Access*, vol. 10, pp. 13528–13541, 2022.
61. P. G. Silva, J. M. Torres, and H. F. Lima, "Standardizing interoperability: A review of IoT frameworks and semantic models for smart-home devices," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 112–139, 2024.