Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338

Volume 15 Issue 01s, 2026

Comprehensive Study on the Role of IoT in Intelligent Home Automation Systems

[1]Dr. Rashmita Pradhan , [2]Dr. Tanuja Mahajan, [3]Ms, Punam Fegade, [4]Ms. Aquila Shaikh, [5]Ayush Ashok Mishra

[1,2,4,5]L.B.H.S.S.T's Institute of Computer Application, Bandra(E) , Mumbai.

Email: [1]rashmitap@gmail.com,[2]tanujamahajan18@gmail.com,[4]aquishaikh@gmail.com

Peer Review Information

Submission: 05 Dec 2025

Revision: 25 Dec 2025

Acceptance: 10 Jan 2026

Keywords

Internet of Things (IoT), Smart Home, Home Automation, Artificial Intelligence (AI), Cloud Computing, Sensors and Actuators, Interoperability, Data Privacy, Cybersecurity, Intelligent Systems, Edge Computing, Energy Efficiency, Context-Aware Automation, IoT Architecture, Residential IoT.

Abstract

The Internet of Things (IoT) most recently stood as an essential pillar of intelligent home automation systems with respects to technology through connectivity, real-time monitoring, and self- governing decisions through a network of connected smart devices. The paper presented here offers a thorough summary of the state of the art and architecture and applications of IoT in smart homes while paying special attention to how sensors, actuators, cloud platforms, and artificial intelligence combine to create an elevated level of increased residential comfort, security, and energy performance. We also elaborate on significant technology frameworks and applications, and highlight important challenges such as interoperability, data privacy, and cyber security. We discuss the emerging trends and best practices, and future considerations based on our findings based on analysis.

Introduction

Advancements in the Internet of Things (IoT) have accelerated the digital transformation of the world around us, and this digitization is altering the world of housing and living. As a result of the IoT, smart homes—in which the structure and inside content is connected, networked and digital—leverage IoT technologies to automate traditional household functions like heating/cooling (climate control), lighting, security and devices connected to the internet. By combining many smart devices and sensors or actuators, IoT smart home devices obtain data from connected devices and are able to share and transfer data in order to perform independent functions or based upon users' command. There has been an increase in the use of smart home devices in the past couple of years as a result of a number of factors, including a large number of low-cost IoT devices, an increase in availability of broadband and continuing demand for energy efficiency and home security. IoT smart homes provide more than just convenience and quality of life; they help make our lives more sustainable by reducing energy use and enabling intelligent resource management [1].

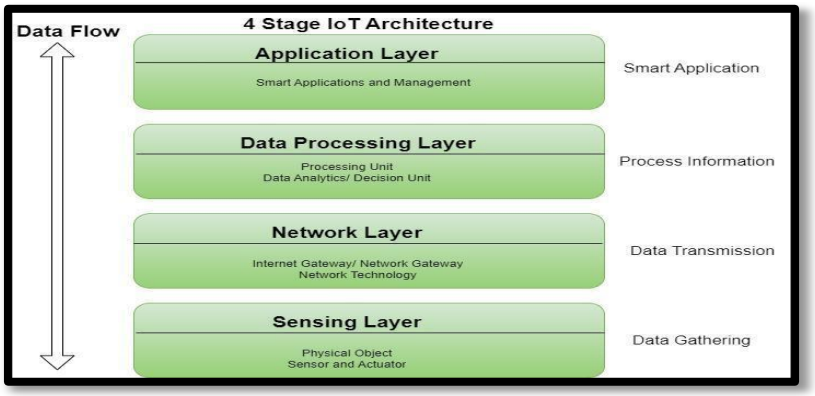

Figure. 1: IoT Architecture Layers for Smart Homes

It is important for policymakers to keep in mind, however, that despite the potential benefits there will be considerable challenges to implementing smart home technology. For example, consumer distrust in data privacy, network security, device interoperability, and scalability of all systems are clearly important factors. As the home becomes even more connected, it is vital to address data privacy concerns, security issues, and interoperability in order to promote IoT-based solutions in a reliable way. The purpose of this paper, therefore, is to give a thorough account of the role of the IoT in smart home automation systems, by providing a description of critical technologies and applications and architectural measures, while also considering some of the hurdles that exist in IoT today. Also, we will consider how future growth may lead to robust user-centric smart homes [2].

Literature Review

The application of the Internet of Things (IoT) to home automation has generated considerable research interest during the past decade. This extensive research has provided answers to many significant aspects associated with the architecture of IoT systems, communication protocols, connectivity of devices, security mechanisms, and user-centric automation models. This section provides an overview of significant contributions that have shaped the development of smart home technologies.

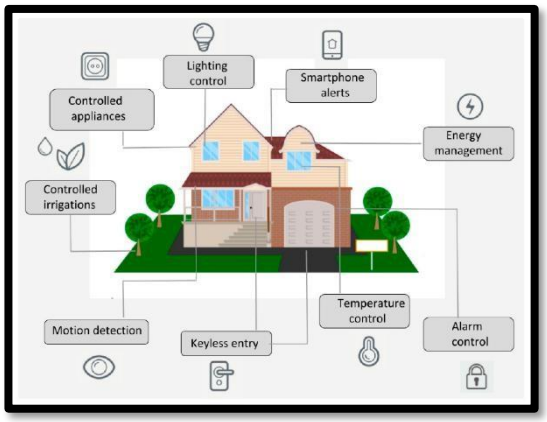

Figure. 2: Smart Home Automation Use Case

During my one-month internship at Techplement, I worked as a Front-End Developer Intern where I had the opportunity to contribute to the development of an Online Resume Maker web application. My responsibilities included: Design Implementation: I translated design mockups into responsive web pages using HTML, CSS, and JavaScript, ensuring a smooth and intuitive user interface. Interactive Form Handling: I helped in building dynamic forms that allowed users to input personal, educational, and professional details for resume creation. Component Development: I developed reusable components for the resume builder using React.js, enhancing modularity and code maintainability. Real-Time Preview: I implemented features that allowed users to preview their resumes in real-time while filling out the form. Cross-Browser Testing & Responsiveness: I tested and optimized the

site for various screen sizes and browsers to ensure a consistent user experience. Gubbi et al. offered one of the earliest studies on IoT architecture, consisting of multiple layers, namely a perception layer, a network layer, and an application layer [1]. Their study provided a foundational understanding of the interactions between sensors and connected devices associated with IoT. Accordingly, their architecture bridges the collection and processing of environmental and user-related data in smart homes to inform automation decisions. Alaa et al. presented a more thorough survey of IoT platforms used in smart home environments, by comparing their degree of flexibility, scalability, and interoperability [2]. Of significant importance was their overall conclusion that unified standards are required to address fragmentation and to improve compatibility amongst systems. Ahmad et al. examined similar dimension, cloud computing, and particularly how cloud computing enhances and integrates with smart home systems [3].

Specifically, they identified a significant role for cloud computing in developing analytics, that enables users to determine how multiple devices can be connected to gain insight from disparate IoT information. Security and privacy have also featured heavily in literature related to the IoT, with Roman et al. combining issues of potential threats to smart home network including unauthorized access, leakage of sensitive data, and denial of service [4]. They offered several security measures including device authentication, encrypted communication, and intrusion detection to cover potential risks. Recently, work has emerged looking at the incorporation of artificial intelligence (AI) to improve the "intelligence" of smart homes. For instance, Saeed et al. noted the use of machine learning algorithms would allow for context aware automation as the smart home learns user habits and preferences [5]. Even though the discussions in the literature usually focus on several elements of IoT enabled smart homes, there is much room for research that amalgamates the findings examined. Currently, literature continues to explore various siloed parts of smart home with limited awareness of the compound challenges faced in developing increasingly scalable interoperable, and secure smart home ecosystems; literature has focused on networking, security, or user interactions, but not as a complete whole.

Problem Definition

Even though IoT technologies have progressed quickly and been widely adopted in the home space, creating and implementing real intelligent smart home automation systems has additional significant challenges to overcome. The challenges discussed below negatively affect system performance or user experience and raise other concerns such as security, scalability, and standardization. One of the main barriers is interoperability between smart devices made by different manufacturers. The lack of universal standards has led to super-fragmented smart home ecosystems with devices dispersed into silos with little means to build cohesive automated smart home experiences. Build, install, integrate, and manage processes for different ecosystems vary widely and are difficult even for tech-savvy users to navigate. Data security and privacy are also serious problems for smart home devices. Smart home devices are constantly profiling individuals and sending sensitive personal data like occupancy patterns, biometric, and voice information. Insufficient encryption schemes, weak access authentication processes, and insecure communication protocols leave significant opportunities for cyber-user threats and sorted data hacking, surveillance, or theft. Moreover, the scalability and adaptability of the system remain important issues. As more devices are connected to a home system, the network infrastructure could become overloaded and result in less desirable performance outcomes and increased latency. Moreover, many systems lack intelligent learning capabilities limiting their knowledge of user behavior over time, or the ability to adjust for dynamically changing environmental factors. Finally, upfront costs and complex installation processes discourage adoption of smart home systems generally, and even more so in developing countries. Many smart home devices and solutions require specific, proprietary hardware that cannot be installed and maintained by the average consumer unless they have previous technical experience with the system in question. This paper will investigate the architectural and operational constraints of currently existing and operating IoT-based smart home systems and suggest processes to improve security, interoperability, and user-ability functionality. These issues must be addressed before the realities of intelligent home automation can be fully realized in generating safe, effective, and sustainable living environments.

Figure. 3: AI Integration in Smart Homes

Objectives of the Research

The main goal of this research is to evaluate the current state of IoT-enabled smart home automation systems and pinpoint the significant technological, operational, and security-related barriers that inhibit their operational efficiency, and widespread adoption or use. More specifically, this research intends to:

- Understand what intelligent home automation systems entail, and their architecture denoted with the term IoT technologies.
- Review examples of applications of IoT in smart homes which include lighting systems, energy aware systems, smart security systems, and voice based systems.
- Identify major barriers, such as interoperability, data privacy, and scale.
- Explore existing solutions and frameworks and further analyse their efficacy.
- Make recommendations towards designing more interoperable, secure, and user-friendly home automation systems.

Scope of the Research

The endeavor of this research is limited to investigating the application of IoT strictly within residential contexts, and as such will particularly focus on:

- The architecture of smart homes comprised of devices, communication protocols, and cloud technologies.
- Automation systems and services involving remote control, scheduling, energy monitoring, and tailored responses.
- Security and privacy issues associated with data collection and transmission in smart homes.
- How emerging technologies such as artificial intelligence and edge computing will influence the existing IoT-based smart home systems.
- Case studies and practical implementations used to illustrate the limitations and potentials of existing technologies.

This study will not include industrial and large-scale IoT applications such as smart cities and smart factories unless relevant conclusions are drawn to aid the reader's situational awareness about smart home systems. Overall, the effort of this analysis is aimed at providing a thorough analysis of IoT facilitating convenience, sustainability, and safety for residential applications.

Methodology

In order to investigate the use of IoT in smart homes, we followed a qualitative research approach based on secondary data analysis and system modeling. The approach had three main phases:

Literature Analysis:

We reviewed extensive peer reviewed articles, white papers, and technical publications, highlighting smart home architecture, communication protocols, device management, and integration with AI [1]–[5].

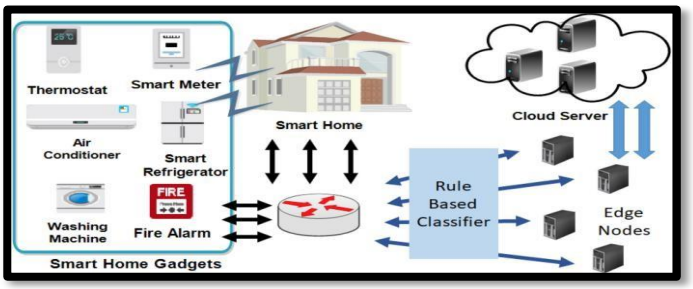

Figure. 4: IoT Data Flow in Smart Home Systems

System Architecture Modeling: Drawing from knowledge obtained, we abstracted a layered architectural model identifying key elements such as sensors, actuators, edge gateways, cloud interfaces, and mobile access (Fig. 1) [1].
Comparative Case Studies: We compared diverse applications of smart home deployments, including lighting control, AI-driven surveillance, and climate monitoring. The AWS IoT-based smart home dashboard architecture (Fig. 4) provided a contemporary case study of holistic cloud services [6].
This approach allows for the identification of real- world bottlenecks like interoperability, and comparative assessment of frameworks on the basis of scalability, user experience, and data privacy.

Result And Discussion

The study uncovered the following major findings:
Architectural Diversity: A majority of smart home architectures are based on a three-layered architecture: perception, network, and application.
Yet, they differ in protocol stacks and device support.
AI Integration: AI-based systems (particularly with edge computing) demonstrated improved personalization and context-aware automation but added to the system complexity and privacy issues.
Security and Privacy: Although device encryption and secure cloud platforms are evolving, most consumer-grade systems remain underwhelmingly protected.
Energy Efficiency: Smart HVAC and lighting installations saved family energy use by 20–30%, demonstrating the potential of automation for energy efficiency.
User Experience: Efficient user interfaces, voice integration (e.g., Alexa, Google Assistant), and easy-to-use mobile applications highly enhanced usability, although cross-platform compatibility remained an issue.

Future Work

The potential for IoT in smart homes grows by the day, especially with developments in artificial intelligence, edge computing, and upcoming connectivity such as 5G. However, to achieve the complete benefit of IoT in smart homes and make current challenges subsist, future research and development need to focus on the following main areas:

1. Standardization and Interoperability Frameworks

There is an urgent need for international standards that will be able to ensure interoperability across IoT devices from multiple makers. Future work will have to go into creating open protocols and standard APIs that allow plug-and-play connectivity between platforms, minimizing configuration burdens for end-users and developers.

2. Improved Edge Intelligence

Placing computation closer to where the data originates (i.e., edge devices) can potentially dramatically reduce latency and dependence on cloud infrastructure. Next-generation home systems will have to incorporate advanced edge AI algorithms for local decision-making, especially for real-time use cases such as security, health monitoring, and energy management.

3. Self-Learning and Context-Aware Systems

Machine learning algorithms embedded in smart home devices need to enhance to support real-time context awareness. Adaptive learning systems that adapt device behavior based on changing user habits, interests, and environmental contexts without being manually programmed can be the area of future research.

4. Privacy-Preserving IoT Architectures

With increasing amounts of data being created, there has also been growing concern for revealing personal data. The future research must include privacy-preserving technologies such as federated learning, differential privacy, and homomorphic encryption to safeguard data but allow smart systems to learn and evolve.

5. Energy-Aware and Sustainable IoT Design

Green IoT is a new concept that reduces the carbon footprint of networked devices. Future technologies need to explore energy-efficient communication techniques, power-aware hardware design, and integrating renewable energy to develop smart homes in a sustainable manner.

6. Robust Security Mechanisms

Security remains a significant adoption hindrance. Work in the future must enhance mechanisms for authentication, anomaly detection models, and intrusion prevention systems specifically for low power and resource-constrained IoT devices typically used in home environments.

7. User-Centric Design and Accessibility

Future research can aim at inclusive smart home systems that assist older people, people with disabilities, and those who know less about technology. Studies can explore voice-operated access, gestural interfaces, and multi-language support to make it more accessible.

8. Integration with Smart Cities and Grid Systems

Smart homes will not exist in a vacuum. Future research can explore how homes interoperate

with larger systems like smart grids, neighborhood surveillance, and emergency response, building a smarter and more responsive citywide system.

Conclusion

The incorporation of Internet of Things (IoT) technologies into smart homes offers revolutionary chances to raise the level of residential comfort, security, and energy efficiency. The paper has examined the underlying architecture of IoT-based smart home systems, emphasized the key functions of sensors, actuators, cloud computing, and artificial intelligence in supporting intelligent automation, and outlined present applications enhancing quality of life.

But the promise of smart homes that are fully functional and user-centric is limited by paramount challenges including interoperability between heterogeneous devices, data privacy, and security vulnerabilities. The solutions to these lies in common standards, strong encryption techniques, and edge-cloud hybrid intelligent solutions to ensure responsiveness while keeping data secure.

Furthermore, AI-powered context-aware automation systems' evolution has the potential to transform intelligent home environments through enabling adaptive, personalized, and predictive capabilities. Future development and research need to be directed at conquering issues of scalability, user-centricity, and provision of equitable access to these technologies in order to achieve maximum societal benefits.

In conclusion, although IoT in smart homes is a rapidly evolving field with considerable shortcomings, continuous improvement and cross disciplinary work are leading the way to safer, more efficient, and smarter living environments that can contribute sustainably to daily life.

References

[1] 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, Sep. 2013.

[2] M. Alaa, A. Abuarqoub, M. Mohamad, and M.A. I. Mehmood, "A Survey on Smart Home Environment Systems: Architectures,Technologies, and Application Areas," *IEEE Access*, vol. 8, pp. 182708–182736, 2020.

[3] A. Ahmad, M. R. Javed, and I. A. Khan, "Smart Home Automation using IoT and Cloud Computing," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 12, pp. 564–570, 2020.

[4] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9,

[5] pp. 51–58, Sep. 2011.

[6] A. Saeed, M. R. Asghar, M. A. Shah, and A. M. Alwakeel, "A Review on Smart Homes Using Internet of Things," *Sensors*, vol. 20, no. 15, pp. 4504, Aug. 2020.

[7] Gajula, S. (2024). Cybersecurity risk prediction using graph neural networks. *Journal of Information Systems Engineering and Management,* 9(4S), 3301–3315.

[8] S. Singh, P. K. Sinha, and A. Kapoor, "A Review on Challenges and Techniques for IoT- based Smart Homes," *Journal of Network and Computer Applications*, vol. 143, pp. 145–158, Oct. 2019.

[9] L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233– 2243, Nov. 2014.

[10] P. P. Ray, "A Survey on Internet of Things Architectures," *Journal of King Saud University – Computer and Information Sciences*, vol. 30, no. 3,pp. 291–319, July 2018.

[11] H. Habibzadeh, T. Soyata, M. Kantarci, B. K. Sodagari, and M. T. Bouguettaya, "Large-Scale Distributed Healthcare Monitoring and Analytics Using IoT," *IEEE Transactions on Big Data*, vol. 4, no. 3, pp. 247–262, Sep. 2018.

Image References

- Fig 1 – GeeksforGeeks: https://www.geeksforgeeks.org/architecture-of- internet-of-things-iot/
- Fig 2 – MDPI: https://www.mdpi.com/1424-8220/21/11/3784
- Fig 3 – DM WebSoft: https://dmwebsoft.com/the-convergence-of-iot- and-ai-smart-home-automation-and-beyond
- Fig 4 – Springer: https://link.springer.com/article/10.1007/s4297 9-021-00979-w