Proceedings of CONF-SEML 2026 Symposium: Learning and Decision Making in Multi Agent Software Systems
DOI: 10.54254/2755-2721/2026.BA32249

IoT-Enabled Smart Homes: Technology Integration, Challenges and Future Trends

Jiaqi Shen

School of Software and Communication, Tianjin Sino-German University of Applied Sciences, Tianjin, China
18500959240@163.com

Abstract. Against the backdrop of rapid advancement of Internet of Things (IoT) technology, smart homes have seen continuous improvements in connectivity, accessibility, and application performance and they provide residents with more comfortable domestic experiences. This has significantly enhanced convenience in daily life and heightened the sense of well-being within the home. However, at the same time, issues such as security vulnerabilities and system fragmentation have become increasingly prominent, forming the bottlenecks restricting the development of the industry. Based on literature analysis and review methodologies, this paper investigates integration technologies concerning the IoT in smart homes. What's more, it analyses existing challenges and future development trends, aiming to establish an efficient, secure, and sustainable smart home system. The conclusions indicate that the development of smart homes must incorporate security protection protocols, while technological integration requires low-power design in embedded systems, which holds considerable promise for the future. With technological progress and the increasing maturity of IoT technology, related applications will become more beneficial to the public and widely adopted. This study seeks to offer theoretical support and practical guidance for technological innovation and risk prevention in smart homes within the context of the IoT.

Keywords: Internet of Things, Smart Home, Sensor, Raspberry PI

1. Introduction

With social progress, people's expectations for household appliances extend beyond basic control functions. Instead, they now desire intelligent, convenient and personalised devices that cater to diverse aspects of their daily lives [1]. Recent breakthroughs in the continuous advancement of Internet of Things technology are steadily transforming smart homes from mere concepts into tangible realities. The Internet of Things realizes universal connectivity, serving as a bridge between physical devices and the digital world. With a ubiquitous interconnection architecture, IoT technology enables real-time data exchange and coordinated control among household appliances [2].

In this smart home ecosystem, the embedded system depends on high integration and low power consumption and Strong real-time function to serve as the "nerve centre" of the smart home. Multi-protocol coordination at edge gateways (such as Raspberry Pi) ensures efficient operation across the

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2026.BA32249

entire end-to-end chain, from environmental awareness to command implementation [3]. Meanwhile, sensors serve as the system's sensory nerves, gathering multi-dimensional data such as temperature, humidity, light levels and motion. This information acts as foundational input for different settings involving intelligent security and energy-efficient temperature control, empowering home environments to shift from passive response to active adaptation [4]. This study seeks to offer theoretical support and practical guidance for technological innovation and risk prevention in smart homes within the context of the IoT.

2. Technology integration

At present, the development of the Internet of Things within the smart home sector has established a relatively comprehensive system, comprising various sensors, actuators, control units, and communication networks. This infrastructure enables functions such as remote control and automatic sensing. Hardware, as a vital part of the overall smart home system, lays the foundation for realising the process of 'sensing — transmission — control — execution — interaction'. Generally speaking, a thorough smart home system contains various hardware devices. For example, gateway, all kinds of sensors and the necessary network communication protocol. This study will principally discuss technical integration in relation to hardware composition.

2.1. Gateway

Raspberry pie is usually used as the hardware carrier for edge gateways and it is currently the most popular and has a wide range of applications. It features low cost, high performance and easy scalability, and its size is much smaller than what people generally think of as a computer. It can also be regarded as an open-source tiny computer motherboard.

It comes with physical components such as the central processing unit (CPU), memory, network port, and General Purpose Input/Output (GPIO) interface. Additionally, it integrates a complete Linux operating system along with several universal interfaces that could connect to devices such as keyboards and mice. These external components allow the Raspberry Pi to offer a considerable range of functionality despite its compact size.

2.1.1. Edge computing of Raspberry PI

When conducting edge computing, though it can rely directly on the cloud, once the network connection is lost, the system becomes inoperative. If large amounts of unprocessed data are uploaded directly to the cloud, it will significantly consume the bandwidth, resulting in high transmission costs. Research tends to prefer using Raspberry Pi as an edge computing device, as it can address issues such as high latency, heterogeneous nodes with different kinds of sensors, and the difficulty of integrating (device) data [3].

Given that the Raspberry Pi is equipped with external USB interfaces, it is capable of connecting to a camera. When carrying out real-time data analysis, it is common to deployOpen Source Computer Vision Library(OpenCV). OpenCV has an extensive broad range of applications.

In the field of smart home systems, OpenCV is a computer vision library incorporating classic object detection algorithms such as the Haar feature classifier and Local Binary Pattern (LBP), enabling highly efficient real-time object detection within images or videos [5]. It also facilitates local analysis and processing of video or sensor data, including motion tracking, face detection, and feature extraction. Alternatively, single-frame image information may be applied [6], thereby

DOI: 10.54254/2755-2721/2026.BA32249

reducing computing time and enhancing the efficiency of data processing. This approach enhances the system's fluidity, allowing users to experience greater speed and comfort in its operation.

2.1.2. The differences between a Single Chip Micyoco (SCM) and a Raspberry PI

During the process of searching for literature, much research into smart homes employs microcontrollers. As Edge nodes/terminal devices, microcontrollers possess limited computational power. Data collected locally is uploaded to the cloud via edge gateways. There are many differences between Raspberry PI and SCM. A microcontroller is a single-chip device centred about an 8-bit or 32-bit microprocessor with integrated memory and input/output interfaces.

As microcontrollers lack an independent operating system, their computational capabilities are sufficient merely for basic data acquisition and command execution. They are incapable of tackling complex data processing tasks and are categorized as specialized embedded control chips. Moreover, microcontrollers suffer from limited interface ports and weak expansion capabilities, typically only able to connect one or two types of simple sensors or actuators. Due to the inability to expand high-speed peripherals and wireless communication modules, it is suitable for localised, lightweight control of individual rooms and single devices, such as lighting adjustment in a single room or switch control for an individual socket.

2.2. Technical integration of sensors

Sensors, the core component of the perception layer within the five-layer architecture of smart homes, are the pivotal foundation enabling environmental interaction and data acquisition throughout the entire smart home system, and play an indispensable fundamental role [4]. Sensors are the most crucial component of this research; without effective sensing, the system would be unable to obtain environmental information and thus become non-functional.

Found in multiple smart home environments such as bathrooms and living rooms, it serves as a key component of the system. It is commonly used for sensing temperature, smoke concentration in the air, as well as for door and window detection, and light sensing. Sensors are characterized by their capability to transform abstract phenomena into computer-interpretable signals, which fulfill the function of data acquisition. For instance, physical signals accessible to the human body are transformed into electrical signals, which are then converted into digital signals.

The intelligent upgrading and coordinated operation of smart home systems are fundamentally dependent on the integration of sensor technology, which constitutes the most critical core link throughout the entire system. Its essence lies in the deep and organic integration of sensors with diverse types and functional dimensions, embedded systems, IoT technology, artificial intelligence (AI) algorithms, and communication modules. Through this integrated framework, efficient collection and transmission of perceptual data can be fully realized, which in turn greatly elevates the overall operational efficiency of smart home systems and optimizes the quality of user experience.

In practical integrated applications, various functional sensors are accurately connected to embedded processors (such as Raspberry Pi and advanced RISC chips) through standard interfaces like GPIO pins. The embedded system uses preconfigured high-precision data processing algorithms to filter, calibrate, and perform preliminary analysis on the raw environmental data collected by the sensors. This process effectively eliminates invalid interference data and corrects system deviations arising during measurement, after which the standardized processed data is accurately transmitted to

DOI: 10.54254/2755-2721/2026.BA32249

the upper-level system of the smart home, providing reliable support for subsequent data applications [5].

2.3. Data exchange

Among the five-layer architecture of the Internet of Things, data exchange belongs to the transport layer. Its responsibilities are designed to ensure the efficient, secure and reliable flow of information. Within the multi-protocol integrated system covered by this research, the Zigbee protocol is one of the core protocols. It effectively addresses the communication difficulties of low-energy consumption sensor nodes in smart homes, while laying a foundation for integrating heterogeneous networks of various sensors.

The data exchange is mainly accomplished through network communication protocols, where the commonly adopted low-power wide-area protocol is Zigbee protocol paired with Wi-Fi. Integrating Zigbee, Wi-Fi and Bluetooth modules into the Raspberry Pi will make the data exchange process far simpler and quicker. For instance, sensors transmit raw data to the Raspberry Pi via the Zigbee/MQTT protocol, after which the edge gateway performs data preprocessing to reduce unnecessary data and minimise transmission latency.

3. Key challenges

Despite the rapid growth of smart homes under the Internet of Things, numerous issues remain. Security-related issues arising from sensors and communication protocols, as well as battery life concerns, remained the key focus points during this research.

3.1. Security capability

As illustrated in Figure 1, research findings reveal that among the hundreds of current studies on smart home systems within the Internet of Things, it is evident that alongside thematic index terms such as 'Internet of Things', 'sensors' and 'intelligent', security and privacy constitute a significant and noteworthy proportion of the discourse. This not only undermines the quality of data integration but also increases the risk of system security vulnerabilities.

Based on the author's research and reflections, it is widely acknowledged that security safeguards are a critical foundation for residents to gain a sense of well-being and enjoy comfortable, convenient living in smart home environments. Furthermore, they represent a necessary condition for the long-term sustainable development of the smart home industry.

DOI: 10.54254/2755-2721/2026.BA32249



Figure 1. Word frequency in the literature

It is worth noting that one of the core contributing factors to the current lack of security in smart home systems is the absence of a unified standard system for smart homes across the industry. As a result, different types of sensors adopt diverse data formats and communication protocols, with no effective interconnection mechanisms. This frequently gives rise to problems including data conflicts and coordination failures. This not only compromises the quality of data integration but also exacerbates system security risks.

3.2. The endurance aspect

Initially, one of the design purposes of smart home technology was to reduce household electricity bills.

Hardware such as sensors consumes power and faces the risk of malfunctioning after running out of power without emergency replacement measures, which can cause inconvenience to people.

At the present time, home design that emphasizes human experience and humanitarian care must incorporate space for manual operation [7], so as to improve the quality of daily living experience and comfort. Although a series of studies and improvement proposals have already been developed regarding the aforementioned issues, as illustrated in current research, for example, the "micro-nano sensors + nano power generation devices" combination currently employed in research enables the entire system to achieve electrical self-sufficiency [8]. However, this category of products may face issues such as higher prices and complex installation, leading consumers to avoid them as their first choice when making purchases.

DOI: 10.54254/2755-2721/2026.BA32249

4. Conclusion

Up to the present, smart home systems based on IoT possess a fairly comprehensive functional framework. The primary research centres on designing innovations in areas such as sensor data collection and subsequent processing at edge gateways, which has seen breakthrough progress. The IoT-based smart home system is gradually evolving from single-device intelligent control and passive user operation towards a mature direction characterized by whole-home integrated proactivity, seamless autonomous operation, and multi-device ecosystem interconnectivity.

This paper has not been able to explore the software aspects of smart homes in depth. For the future development of smart homes within the Internet of Things, emphasis should be placed on the practical deployment and implementation of such systems. To promote the popularization and application of IoT smart home systems, the first priority is to ensure rigorous quality control over products, reduce production costs, and enhance cost-effectiveness, thereby increasing the number of households adopting smart home technology. Consequently, this fosters the further development and improvement of such devices. Moreover, continuous development remains necessary to ensure that privacy information collected by sensors is not disclosed, and to address emergency procedures following battery discharge and power depletion, thereby safeguarding the safety of users and households.

References

[1] Li Chunhong, Yan Fuqiang& Guo Xiong. The Design and Implementation of Smart Home System Based on ESP8266. Internet of Things Technologies, 21(01), 111-113+126. https: //doi.org/10.14004/j.cnki.ckt.2025.0071.
[2] Xu Chengxin, Xu Xihan, Han Guangchang & Li Anqi.(2025). The Application and Innovation of Embedded Systems in Smart Home Control, 26(06), 83-85+144. doi: 10.16009/j.cnki.cn13-1295/tq.2025.06.050.
[3] Eltresy, N. A., Dardeer, O. M., Al-Habal, A., Elhariri, E., Abotaleb, A. M., Elsheakh, D. N., ... & Abdallah, E. A. (2020). Smart home IoT system by using RF energy harvesting. Journal of Sensors, 2020(1), 8828479.
[4] Zhang Yuying & Xu Zheying.(2025). Research on Smart Home Security System Based on Internet of Things.Computer Knowledge and Technology, 21(08), 83-85+89. https: //doi.org/10.14004/j.cnki.ckt.2025.0404.
[5] Sabit, H. (2025). Artifical Intelligence-Based Smart Security System Using Internet of Things for Smart Home Applications. Electronics, 14(3), 608: 2
[6] Jiang Zhiguo.(2024). A smart home security system integrating the Internet of Things and multiple sensors.Journal of Taiyuan University(Natural Science Edition), 42(03), 20-26. https: //doi.org/10.14152/j.cnki.2096-191X.2024.03.004.
[7] Sepasgozar, S., Karimi, R., Farahzadi, L., Moezzi, F., Shirowzhan, S., M. Ebrahimzadeh, S., ... & Aye, L. (2020). A systematic content review of artificial intelligence and the internet of things applications in smart home. Applied Sciences, 10(9), 3074: 37-38
[8] Haroun, A., Le, X., Gao, S., Dong, B., He, T., Zhang, Z., ... & Lee, C. (2021). Progress in micro/nano sensors and nanoenergy for future AIoT-based smart home applications. Nano Express, 2(2), 022005: 2