# IoT Technologies for Smart Home Systems: Protocols and Architectures

Jiaxuan Niu *

Admiral Farragut Academy TianJin, Tianjin, 300000, China

* Corresponding Author Email: Mtp9wj@163.com

**Abstract.** Intelligent home development is very fast and it is greatly promoted by the growth of the Internet of Things. This study aims to analyze the important Internet of Things (IoT) technologies in intelligent home systems, such as communication protocols (WiFi, Zigbee, Z-Wave, Bluetooth), sensor technology, cloud and edge computing, security framework, and so on. And then it makes a comparative study of their characters, applications, and limitations. The result shows that there is no best technology widely, the existing network is a widely heterogeneous network. so, the feasibility and safety of the solution are determined by the integration technique, paying attention to user experience will become one of the development trends in the future. In conclusion, the future development of the intelligent home depends on security, interoperability, and energy efficiency to make the goal of achieving smart home system a reality.

**Keywords:** Internet of Things (IoT), Smart Home, Communication Protocols, Sensors.

## 1. Introduction

The idea of a smart home emerged in science fiction movies and books, and now it is a step closer to reality with the rapid growth of the Internet of Things. An IoT-enabled smart home is a system that connects almost everything from light to thermostat to sensor to microwave to any physical object into a new whole that can be automatically controlled, remotely monitored, and intelligently controlled [1, 2]. It brings residents unprecedented convenience, security, and energy efficiency [3]. Enabling technologies such as low-power wireless communication protocols, low-cost sensors and powerful cloud and edge computing platforms have proliferation and have been the key driver of this revolution [4].

Despite the obvious benefits and enabling technologies, the development and widespread adoption of smart homes still have many challenges. IoT has many prevalent communication standards, such as WiFi, Zigbee, Z-Wave, Bluetooth; each has its own advantages and disadvantages, so it will causes interoperability problems. Besides, a large number of sensors will produce a huge amount of data, computing architecture is needed to complete the computing. Low-latency response is required for some critical events, while deep analytical ability is needed for intelligence. At the same time, security and privacy issues are also a big challenge. Therefore, the key IoT technology comparative study, characteristics, application and limit, and integrated use are needed.

In this paper, this study examines some important IoT technologies in smart home systems, such as communication protocols (WiFi, Zigbee, Z-Wave, Bluetooth), sensor technology, cloud and edge computing, security framework, and then this paper will make a comparative study about their characteristics, applications and limit. The rest of this paper is organized as follows. In Section 2, this article will compare some commonly used communication protocols, and then it will studies the characteristics of these protocols. In Section 3, the role of sensing, actuation, and cloud-edge computing in data processing and automation are investigated. Finally, in Section 4, the application of heterogeneous technology in real smart home automation are discussed. The rest of this paper is organized as follows. Section 2 presents the key IoT technologies for smart homes, including communication protocols, sensing/actuation, and computing architecture. Section 3 provides discussion and comparative analysis. Finally, in Section 4, the conclusion is presented with possible future research directions.

## 2. Key IoT Technologies for Smart Homes

Communication protocols are the nervous system of a smart home, enabling communication between devices and between devices and users. These protocols can be broadly classified into short-range and long-range protocols, which make different trade-offs in power consumption, data rate, range, and application scenario. Short-range protocols, such as Zigbee, Z-Wave, and Bluetooth Low Energy (BLE), are usually used in the home environment. These protocols are designed to consume low power and to work reliably in large numbers of devices, which makes them suitable for devices with battery power consumption, such as sensors, smart switches, and lighting systems. In contrast, long-range protocols, such as Long Range Area Network (LoRaWAN) and Narrow-Band internet of things (NB-IoT), are used to connect geographically dispersed devices, such as smart meters or garden sensors, directly to the network [5,6]. These protocols have an extensive range and excellent penetration, but the data rate is relatively low, and the module price is higher. Since there is no best protocol in all aspects, contemporary smart homes must use a heterogeneous architecture. That is, they will use different technologies in different scenarios and selectively leverage the advantages of complementary technologies (such as using short-range protocols in dense home environments and long-range protocols in specific external scenarios) to build a highly connected ecosystem.

### 2.1. Communication and Network Protocols

Communication protocols are the nervous system of a smart home, enabling communication between devices and between devices and users. These protocols can be broadly classified into short-range and long-range protocols, which make different trade-offs in power consumption, data rate, range and application scenario. Short-range protocols are usually used in the home environment. These protocols are designed to consume low power and to work reliably in large numbers of devices. Therefore, these protocols are suitable for devices with battery power consumption, such as sensors, smart switches and lighting systems. In contrast, long-range protocols are used to connect geographically dispersed devices directly to the network, such as smart meters or garden sensors. These protocols have an extensive range and excellent penetration, but the data rate is relatively low and the module price is higher. Since there is no best protocol in all aspects, contemporary smart homes must use a heterogeneous architecture. That is, they will use different technologies in different external and internal scenarios and selectively leverage the advantages of complementary technologies (such as using short-range protocols in dense home environments and long-range protocols in specific external scenarios) to build a highly connected ecosystem.

#### 2.1.1 Short-Range Wireless Protocols

Zigbee is a low-power, low-data-rate mesh network. In mesh topology, devices can help each other forward messages [4]. Its advantages are low power consumption and a reliable network. Zigbee is applied in many devices, such as smart lighting systems (Philips Hue), security sensors and smart locks. Its characteristics are as follows: (1) Low power consumption. Devices can work for years with battery power; (2) Typical range is 10-100 meters per node; (3) Data rate could be up to 250 kbps [6].

Z-Wave, on the other hand, is a low-power mesh networking protocol. It operates in sub-1 GHz frequency bands, which results in less interference and slightly better wall penetration. Data rate is relatively low (~100 kbps) when compared with Zigbee. It is often found in home automation products such as sensors and dimmers. Its strength lies in strong interoperability due to the strict certification program. Its disadvantage is a relatively slow data rate and possibly high cost.

Bluetooth Low Energy (BLE) is designed for very low power consumption and simple point-to-point applications. It has low power consumption, a communication range <10 meters, and moderate data rates. Bluetooth Low Energy (BLE) is a technology mostly used for personal area networking in smart homes for direct communication with other smart devices, such as smart locks, wearables, etc in smart homes. Its strength is its ease of integration with mobiles. Limitations of Bluetooth Low Energy (BLE) are its short range and lack of native support for mesh networks. This makes this protocol ill-suited for whole-home automation.

### 2.1.2 Long-Range/ Local Area Network Protocols

These are protocols used for devices that need high bandwidth or connectivity to the cloud, etc, at the expense of higher power consumption. Wi-Fi is a ubiquitous Local Area Network (LAN) protocol that provides high data rates and direct connectivity to the internet [7]. It has high power consumption, depending on the range of the router, and very high data speeds. Wi-Fi is used for bandwidth-intensive devices such as smart cameras, smart TVs, streaming devices, speakers, voice assistants, etc. Its advantages are high speed and ease of use. Its major disadvantages are high power consumption at a level that is not acceptable for many sensor devices and congestion when a large number of devices try to connect to the network. LoRaWAN is a Low-Power Wide-Area Network (LPWAN) in contrast to Wi-Fi. It has extremely low power consumption, a very long range (several kilometers in open areas), very low data rate. This protocol is not commonly found in core smart home applications, but it can be used to connect utility meters or smart agriculture sensors in a smart home application. Its advantage is its long range and long battery life. Its crippling disadvantage is its inability to transmit any video or audio.

## 2.2. Sensing and Actuation Technologies

This category includes the most basic hardware through which the smart home system interacts with the environment. These are the system's "eyes", "hands," and "feet", which are critical for overcoming the digital-physical split. The following sections on sensing technologies (temperature, humidity, motion, contact sensors, etc.) and actuation technologies (smart switches, motorized valves, audible alarms, etc.) fall into this category [2]. Only when these loops of sensing-intelligence-actuation can be established can we expect home automation applications, from thermostat controls to appliance controls, environment regulation, and security [8].

### 2.2.1 Sensor Technology

Sensors are the perceptual system of a smart home that measures data from the environment. They can be categorized according to their function. Environmental sensors, such as temperature and air quality sensors, monitor the environment for comfort control. As shown in the IoT environmental monitoring applications, sensors give the data inputs for the rest of the intelligent system [9]. Door/window contact sensors detect the change of binary status (open/closed). Motion sensors (e.g., PIR sensors) detect motion in an environment for security and automation applications.

### 2.2.2 Actuator Technology

Actuator Technology Actuators are the "limbs" of the smart home system that perform actions after the intelligent decision has been made (based on data collected from sensors) or user commands. They complete the control loop. Examples include smart switches (control electrical flow to lights, outlets, and appliances), smart locks (convert a signal to mechanical movement to lock doors), and smart valves (when a valve receives a leak detection signal from a sensor, it can automatically shut off the water flow and minimize damage).

### 2.2.3 Data Processing and Computing Architectures

The raw data collected by sensors needs intelligent processing to enable various forms of intelligent automation. Cloud and edge computing are two complementary paradigms that facilitate such processing. Cloud computing pools the enormous computing resources and storage of remote data centers and thus is well-suited for data-intensive, non-real-time tasks, such as long-term trends analysis and training in machine learning. In contrast, edge computing processes data on the edge devices or gateways nearby, thus reducing the latency of responses and ensuring privacy (because the systems need to be less dependent on always-on Internet connectivity). The cloud has virtually unlimited resources, but its transmission latency is too high for many time-critical applications. In contrast, although the edge has limited raw computational capacity, it provides the necessary immediacy. Given the complementary advantages and disadvantages of these two computing paradigms, the cloud-edge collaborative architecture is increasingly becoming the norm in smart

home systems. In this architecture, the edge layer is responsible for the time-critical and safety-critical responses to ensure that the system provides instantaneous operational responses, and the heavy-duty computational tasks and global optimization are performed by the cloud backend. This architecture forms a more efficient, reliable, and scalable system that handles the need for low-latency responses and the need for powerful global intelligence [5].

## 3. Comparative Analysis and Applications

### 3.1. Technological Interplay and Architectural Trade-offs

The smart home system does not move toward a single technological solution. In fact, its architecture is characterized by a plurality of protocols and computing paradigms that address different parts of the requirements. This technological heterogeneity is not an interim phase, but a direct result of the different performance requirements of various home automation tasks. The framework proposed by Papadopoulos et al. aims to handle the underlying complexity by abstracting it away [10].

By analyzing the computing architecture, we find that the system evolves to a more centralized model. The early cloud-only approach is powerful for handling analytics, but the latency bottleneck introduced by the cloud is unacceptable for the time-critical, safety-critical responses. In contrast, a purely edge-based topology is responsive but lacks the computational power to perform deep learning and long-term trends analysis. The approach based on a hybrid cloud-edge topology is effectively validated by Ma et al. [5]. In this symbiotic architecture, the edge node (similar to the home controller defined in Ref. [10]) is responsible for the time-critical actuation and local data filtering, and the computationally intensive tasks, such as model training, are performed by the cloud backend that handles the global macro trends analysis. This division of labor is effective for different applications. For example, in environmental monitoring, as defined in Ref. [9], Ma et al. use this architecture to implement appliance control based on predicted user behavior. Djajadi and Wijanarko [9].

This computational balancing act also occurs at the communication layer, which is segmented into proprietary protocols. Gateways are thus required to enable interactions across these protocols to solve this problem [10,11]. Mesh protocols such as Zigbee and Z-Wave serve as the backbone for most ambient sensing and control, providing robust, low-data-rate mesh networks with hundreds of low-power devices. These standards tend to operate in relatively closed worlds.

High-throughput data streams from devices such as security cameras are instead handled by Wi-Fi, which provides a power-efficient backbone for occasional reports from these sensors. These examples illustrate how platforms providing integration across these worlds can expose a single interface to applications that are able to present this value proposition. This is the focus of the connected home platform of Papadopoulos et al. [10] and the semantic interoperability framework of Kim et al. [1].

### 3.2. Scenario-Specific Technology Integration

The technological trade-offs just described become evident when there are deliberate choices about the application scenario in which the device is operating and the choice of protocol and computing location reflects this. A new generation of security systems is a cyber-physical system with tight integration between the sensing, networking, and computing layers. The perceptual layer, consisting of sensors for status and motion, must run on reliable, long-lasting mesh protocols such as Zigbee or Z-Wave to ensure that the system is always aware of the environment. The requirement for the system to respond instantaneously to an intrusion implies that the computing must be done at the edge. It must be able to trigger alarms and locks without waiting for commands from the cloud. The importance of this has been emphasized by the latency requirements identified in cloud-edge architectures [5].

Meanwhile, bandwidth-intensive cameras running on Wi-Fi provide high-definition video feeds to the cloud for storage and sharing to users who access them remotely. This is a data-rich operating

environment that also places heavy demands on access control. The attribute-based policies described in [1] enable the system to dynamically control which users need fine-grained access to prevent or view sensitive footage based on context-aware rules.

Management systems for the environment use sensor information to shape the built environment around the user. In addition to the modules used for ambient sensing by Djajadi and Wijanarko [9], management systems monitor environmental conditions such as temperature and air quality. The control loop may span the cloud-edge. The edge component might make immediate adjustments to actuators such as thermostats to meet a setpoint. It ensures responsiveness. Meanwhile, data collected by the cloud over time moves beyond simple reactive regulation to learn occupants' habits in order to control HVAC schedules for comfort and energy savings, collaborative intelligence [5].

In healthcare applications, particularly ambient assisted living, requirements for reliability, privacy, and unobtrusiveness drive strict demands on the technology choices. In general, wearable devices communicate with a personal gateway, typically a smartphone, using Bluetooth Low Energy BLE, which is an energy and performance-efficient option. Another class of applications, such as ambient occupancy detection with PIR motion sensors, requires the stable mesh networks provided by either Zigbee or Z-Wave. As for the processing paradigm, edge processing is essential to generate alerts like falling events immediately while keeping privacy by reducing raw data egress. Nested analysis is performed on anonymized trend data on the cloud, which may provide useful information for healthcare providers. These designs are built upon a secure access control mechanism as proposed by Kim et al. [1].

### 3.3. Persistent Challenges and Inherent Limitations

Despite the aforementioned advanced technological solutions, there are still several deep-rooted problems hindering the maturity and popularization of smart homes. These problems, which have been widely recognized by the literature, will be summarized below. Firstly, interoperability and fragmentation are the most typical problems. To make matters worse, various, typically incompatible communication protocols, Zigbee, Z-Wave, Wi-Fi, Bluetooth Low Energy, exist at the same time. This is a fundamental problem. The technical solutions like multiple gateway solutions [10, 11] and semantic abstraction layers [1] are proposed to bridge the gap, but the lack of a universal standard leads to a series of proprietary ecosystems. Consumers are forced to make locked-in choices and the integration of various systems becomes a challenge. Secondly, more security and privacy issues are raised by the attack surfaces of connected homes. While advanced access control models [1] can manage authorized interactions at the first line of defense, there are still security issues at device firmware level, communication links, and the cloud service interfaces. The intrinsic challenge of the cloud-edge model [5] on data privacy is aggravated. At the very beginning, a deliberate data governance policy needs to be made to clarify what information is sensitive and will be processed locally and what will be uploaded to the cloud to reduce the latters impact on data exposure. Finally, the complexity of system configuration and management is another challenge. This problem has been recognized in platform development studies [10]. The initial configuration and subsequent maintenance of a multi-vendor, multi-protocol smart home is too complicated for ordinary users to achieve. As envisioned in [1], the integration of smart home becomes easy as plug-and-play connections. This problem is amplified by reliability issues. Because of the heavy reliance on the cloud for advanced functionalities, one of the most critical components in the system becomes a single point of failure. For the hybrid cloud-edge architecture, although more reliable, it introduces new challenges in managing the failover states and the performance of the system under varying network conditions.

## 4. Conclusion

This paper has surveyed several important IoT technologies forming a smart home system. The results of the analysis show that the ecosystem is highly heterogeneous, and the solution is a synergy

of specialized technologies. The former two protocols, e.g., Zigbee, are suitable for sensor networks, while Wi-Fi is used for the high bandwidth applications. The smart home gateway is the key to the synergy of heterogeneous devices. Additionally, the collaborative cloud-edge computing architecture has been proven to be the optimal solution for the IoT ecosystem. The edge provides real-time responsiveness, and the cloud does the powerful backend analytics. The results show that the main challenge is no longer what each technology can do, but how these technologies can be integrated effectively and securely. In this paper, the importance of designing for interoperability and user-centricity from the ground up has been emphasized. For the researchers and developers, the above discussion means that they need to focus on the standardization of communication interfaces, the robust middleware platform, and the strong security framework protecting the user's privacy without sacrificing application functionality in the future. The future works can be several promising directions. First, the energy efficiency should be improved by energy harvesting techniques for these sensors and low-power communication protocols. Second, the advance of artificial intelligence to achieve more predictive and context-aware automation that can really adapt to the residents' behaviors is another opportunity. Finally, the most important issue to solve in the future is the critical issues of security, privacy, and standardized interoperability across vendors' ecosystems to achieve the smart home vision.

## References


[1] Kim Ji Eun, Boulos George, Yackovich, et al. Seamless Integration of Heterogeneous Devices and Access Control in Smart Homes. 2012 Eighth International Conference on Intelligent Environments, Guanajuato, Mexico, 2012, pp. 206-213.

[2] Fangfang. Research on power load forecasting based on Improved BP neural network. Harbin Institute of Technology, 2011.

[3] Dan Ding, et al. Sensor technology for smart homes. Maturitas, 2011, 69(2):131-136.

[4] Sikora A, Groza V F. Coexistence of IEEE802.15.4 with other Systems in the 2.4 GHz-ISM-Band. IEEE Instrumentation & Measurement Technology Conferenc. 2005 IEEE Instrumentationand Measurement Technology Conference Proceedings, Ottawa, ON, Canada, 2005, pp. 1786-1791.

[5] Ma Qiangfei, Huang hua, Zhang Wentao, et al. Design of Smart Home System Based on Collaborative Edge Computing and Cloud Computing. 2020, 355-366.

[6] Sethuraman M, and S Jayanth. Low cost and high efficiency Smart HEMS by using Zigbee with MPPT techniques. International Journal of Advanced Research In Computer Science and Software Engineering 4.11(2014):4.

[7] Afifi Wessam, et al. Throughput-fairness tradeoff evaluation for next-generation WLANs with adaptive clear channel assessment. IEEE 2016.

[8] Rashidi Parisa, Cook D. J. IEEE TRANSACTIONS ON SYSTEMS MAN & CYBERNETICS, PART A 1 Keeping the Resident in the Loop: Adapting the Smart Home to the User. (2013).

[9] Djajadi A, and Wijanarko M. Ambient environmental quality monitoring using IoT sensor network. (2016).

[10] Papadopoulos, et al. A Connected Home Platform and Development Framework for Smart Home Control Applications. IEEE International Conference on Industrial Informatics, IEEE, 2009.

[11] Zhu Qian, et al. IOT Gateway: BridgingWireless Sensor Networks into Internet of Things. IEEE/IFIP International Conference on Embedded & Ubiquitous Computing IEEE, 2011.