Proceedings of CONF-MLA 2025 Symposium: Intelligent Systems and Automation: AI Models, IoT, and Robotic Algorithms
DOI: 10.54254/2755-2721/2025.LD30021

The Evolution of Smart Home Systems Using Internet of Things Technologies and the Challenges They Encounter Today

Wenbo Hua

Shanghai Pinghe School, Shanghai, China
harrisonhuawenbo@163.com

Abstract. The rapid expansion of the Internet of Things (IoT) brings an abrupt breakthrough in intelligent homes, and allows people to live in a smarter and easier way. In this paper, some basic technologies of intelligent home based on IoT are explored, such as device communication protocols, data processing flow and smart control algorithms. Although these technologies have great potential applications in an intelligent home, there are some significant problems that need to be solved in real life. The different compatibility between devices is the biggest problem that exists now. Meanwhile, data security and protection for users' privacy remain an important problem as well. The system energy consumption and reliability are another barrier that should be improved to satisfy the diversified interests at home. The conclusion can be made that in the future, the research topics should include standardizing techniques and specifications, improving the system security and developing machine learn ability of intelligent devices which can be matched to the intelligent home requirements. It is believed these improvements are necessary for the efficient development and wider application of smart home systems.

Keywords: Internet of Things, Smart Home, Core Technology, Challenges, System Architecture

1. Introduction

A smart home system provides various conveniences, energy conservation, and reliability in terms of daily-life home activities by connecting various types of equipment with intelligent control technology. The market of smart home systems is greatly expanding around the globe under the emerging customer desires of automated and personalized homes [1]. The reason is that various techniques from different fields, such as wireless communication [2], sensor networks [3,4], cloud computing [5], and Artificial intelligence form the root structure of smart homes nowadays.

The evolution of smart home technologies has taken three distinct steps. During the first step, smart home systems are basically composed of individual appliances with minimal integration capabilities. With the breakthrough of new technologies, smart systems had to merge to take advantage of the advantages of implementing new wireless communication technologies, which now allow appliances to better cooperate with each other. Nowadays, the latest systems operate based on

© 2025 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: 10.54254/2755-2721/2025.LD30021

IoT-based systems to manage extensive sets of interconnected appliances. Such an evolution is not an isolated element of technology, because household devices have not just become integration of standalone tools, but key components of smart, interconnected systems, thanks to the proliferation of standardized communication interfaces combined with further data processing improvements to facilitate automation activities to provide necessary assistance to users, who can request functionalities during their daily life depending on the situational context of their environments.

There are a few key issues that make the necessity of investigating these IoT-enabled smart home systems essential and imperative. The first issue relates to the rapid evolution in the number of connected devices in a system, which needs technologies that are technically rigorous and can support performance in a variety of forms. The second issue refers to the rapid development of cyber threats to a system, which should be well-examined to ensure the security of all users and functionality in the long run. The third aspect is related to the energy efficiency of the system, which is being regarded as a crucial topic worldwide. To cover them altogether, we believe that we need a well-established standard smart home system with utmost security and a decent level of flexibility for the upcoming technologies and needs.

In this article, firstly, the basic technology units which constitute smart home systems realized through modern IoT are explored with overall descriptions about their architecture and functionalities. Secondly, it is surveyed about the practical hurdles now dealt with from general directions, such as incompatibility, security threat, power constraint, etc. Thirdly, several solutions and future research trends in this field, which can pave its evolution to a better implementation, are introduced. The discussed contents are based on actual demands in this business scene and fill in the existing research gaps.

2. Core technologies in IoT-based smart home systems

2.1. IoT architecture and communication protocols

IoT-based SHS architecture normally uses a layer-based structure to ensure various devices' integration and data handling. The three-level hierarchical approach generally consists of the Perception layer, the Network layer, and the Application layer. The perception layer is regarded as a physical bottom component, where all sorts of sensors or actuators are used to acquire the surrounding data and execute control commands. The sensors are monitoring the parameters such as temperature, humidity, luminosity, motion, etc., and the actuators are those that will convert the digital data into physical behaviors such as heating control, lighting control, etc. The Network layer is responsible for the data passing within the devices and the central controllers over wired/wireless links. The network layer has its importance in guaranteeing the quality of the system's performance and stability. The Application layer is to handle the acquired data and provide intelligent functionalities over the user interface, automatic rules, and cloud analysis.

Furthermore, having multiple protocols in the same system introduces an opportunity to combine the best capabilities of several technologies and an obstacle of the need for highly intelligent middleware that must translate protocols and standardize data exchange formats, for example, from a ZigBee sensor to a Wi-Fi-based controller via a gateway. More integration needs to be made in the industry involved in standards development (e.g., Matter (a.k.a. Project CHIP)) that has the goal of improving interoperability between devices [1]. One may say that this recognition and more standards development in the smart homes ecosystem are examples of a reaction to the challenges of building larger and more impactful deployments with a variety of integration levels that interconnect various combinations of the most common devices and technologies [1]. The challenges mentioned

DOI: 10.54254/2755-2721/2025.LD30021

are well captured in the security context: As Ali Hassan wrote, “This paper presents and provides a comprehensive review on the IoT security with a concentration on the technology’s architecture, its security features and on the most common threats.” [1]. It is evident how the architecture, in the context of the system and its security, becomes very important [1].

Security measures are integrated throughout all architectural layers and communication protocols. Data exchanged between devices and gateways must be protected using encryption, and authentication mechanisms are essential for preventing unauthorized access to the network. The decentralized nature of IoT systems creates multiple potential attack vectors, from insecure sensors to compromised cloud connections. Recent advancements have introduced end-to-end encryption and regular security updates to mitigate these risks, but challenges persist in maintaining uniform protection across varied device environments. The integration of multiple IoT technologies, each with distinct functions, data processing methods, and security requirements, remains a major challenge in IoT implementation [2], underscoring the ongoing need for comprehensive security approaches.

New design trends of IoT architecture highlight the importance of edge computing, to get away from reliance on the cloud and maximize the system’s responsiveness. By locally processing data near its source, edge device can perform time-critical operations without having to wait for a response from the cloud, saving bandwidth. The notion of Distributed Intelligence is coherent with the increasing intricacy of smart-home systems as they can make decisions local to the system for standard activities while letting advanced analysis run in the cloud for temporal behavioral patterns. In contrast to highly centralized systems, these systems are more scalable and more robust. Future needs of enhancements include modern IoT technologies like WiFi and various means of communication for the research to predict human activities and needs for usable life to help create green and comfortable living environments [3]. This can be perceived of how more adaptable to user oriented and user-friendly system design we will witness in the future.

2.2. Artificial intelligence and machine learning applications

Machine learning and artificial intelligence have been embraced by most of the IoT-based smart home systems, as they allow enhanced automation and customized user experience. These tools help overcome the main disadvantage of rule-based systems and provide the system with self-learning mechanisms to enhance the quality of operations. The three main functionalities of AI/ML implementation in the smart home are predictive analytics to predict users’ requirements, pattern recognition for optimally functioning of devices, and anomaly detection for safety reasons.

Example of usage: learning algorithms that understand users' interaction with smart devices to create tailored automation rules can be used instead of inflexible programmed automation; this will continuously optimize temperature, lighting and device schedules based on what users usually do with the device or depending on the weather conditions. In particular, learning models will use data recorded by the motion sensors correlated with the user's historical thermostat settings in order to establish what is the optimal thermostat temperature depending on the time of day. This will drastically reduce user interactivity in enhancing the end device’s energy management. AI will play a key role in promoting IoT safety and security insofar as it addresses security risks across multiple architectural layers [1], according to Ali Hassan.

Machine learning-based optimization can give ML-based EM systems many advantages: prediction models that forecast consumption patterns given a period’s prior consumption information as well as upcoming weather forecasts and utility rates, and use that information to advise on or automatically apply energy-saving behaviors including finding underutilized devices,

DOI: 10.54254/2755-2721/2025.LD30021

offering optimal timing to run or not run devices, load balancing energy resources available to the dwelling such as rooftop solar and backup battery storage, etc. As Nabeela Awan notes, “power control and secure dispatch information are still open research issues” [4].

3. Current challenges and limitations

3.1. Security and privacy concerns

Security and Privacy are among the most challenging problems facing the IoT-based smart home systems of today’s era. With the smart home ecosystem becoming more and more integrated, devices built by different vendors involve numerous vulnerabilities when processing critical personal data. One of these vulnerabilities is caused by the heterogeneous nature of smart home ecosystems in which devices are built following different security standards. This gives attackers an entry point to utilize different targets [1].

The first security issue is unauthorized access to the smart home network. IoT devices still heavily rely on simple-to-guess default usernames and passwords, or lack any sort of authentication, for access control to the network. This makes them easy targets of brute-force attacks, after which these devices can act as entry points to intrude on the whole home network and reveal personal information or facilitate physical security attacks, like using hacked smart locks or surveillance cameras, causing an immediate danger to safety. The attackability is further exacerbated by the fact that older devices in a home are combined with new smart devices, introducing heterogeneous security levels to control that are cumbersome to manage.

Privacy of data has become increasingly important with the development of cloud computing-based systems. Smart home devices continuously collect users’ personal data, such as lifestyles or personal preferences as well as auditory content or health records. If such data are sent to a cloud computing platform for processing, the users’ privacy is challenged by side-channel attacks, eavesdropping during the transmission or improper or lossless cloud storage schemes. Data privacy leakage during wireless attacks or eavesdropping or transmission could allow hackers to obtain the contents of smart homes. As reported by Ali Hassan, “IoT security threats and risks persist despite the plethora of benefits that IoT system provides to enhance our way of life” [1].

With the growing popularity of always-listening voice assistants and ever-recording security cameras, smart devices now collect audio and/or video signals, which may capture background events, raising privacy concerns in private homes. Though vendors of smart devices like voice assistants and security cameras have used methods such as local data processing and anonymization, users remain uneasy about their data being used by the service providers or authorized third-party apps. Without common data management policies among diverse smart home products, smart devices and related app ecosystems continue to damage user trust.

The involvement of third-party services and applications brings further layers of security that are commonly overlooked by many homeowners. In most smart home applications, external apps can also control devices through application programming interfaces (APIs), and in some cases, apps are granted excessive levels of access permissions. APIs that are not properly protected can become entry points for data leaks or unauthorized access, particularly when users are not aware enough to review the permissions they grant to. This concern increases with the rising level of interconnectedness of smart homes with external platforms such as the smart grids of utility companies or citywide IoT deployments [4].

DOI: 10.54254/2755-2721/2025.LD30021

3.2. Interoperability and standardization issues

Interoperability between various IoT-driven Smart Home systems is faced with major obstacles because of the absence of generic technical specifications of manufacturers/devices. Consumers often face issues connecting devices from various brands as the residential IoT system grows larger. We see three main categories in this fragmentation: communication protocols, data types and control platforms.

At the protocol layer, the smart home devices employ various wireless techniques, including Wi-Fi, ZigBee, Z-Wave, and Bluetooth Low Energy (BLE). Different technical characteristics and application functionalities make them suitable for different purposes. Wi-Fi is often applied for applications requiring a higher data rate, including video transmission, and low-power protocols such as ZigBee is more suitable for sensor and battery-operated devices. The protocol diversity, however, leads to a multiple hubs/gateways setup which makes device integration even more difficult. For example, a Philips Hue lighting setup that is wired via ZigBee cannot easily communicate with a Wi-Fi-based Nest thermostat without additional hardware, although they are all components of the same smart home. A protocol translation lacking a generic, effective method remained one of the main barriers for device compatibility [5].

The closed systems of the controls limit how easy it is to create cooperation between devices. Best in class smart home platforms such as Apple Home Kit, Google Home or Amazon Alexa, depend on closed models with strict certification requirements for plug-and-play devices, granting general access to a limited set of features through application programming interfaces (APIs). Advanced functionalities are almost always locked to the proprietary software ecosystem of the platform itself, meaning that a smart lock certified for HomeKit will only present 30% of its functionality when plugged into Alexa and that users will either need to stay within the same platform or trade away any in-depth functionality altogether. This compartmentalization of proprietary systems goes against the core ideal of the Internet of Things of having a unified and connected systems, and ending up with functional black boxes.

Ad-hoc attempts such as Matter (originally Project CHIP) try to solve these problems through open-source connectivity standards. Driven by industry associations, Matter tries to define a simple way of communicating to any IP-enabled device through a standard protocol, which would allow a certified product to access several platforms. A first implementation seems to improve the simplicity of configuration and interoperability concerning basic functionalities between devices from various vendors. The transition is, however, still very tedious: older products need to be bridged via additional hardware, and the possibilities of new versions rely on a more or less proprietary design. New devices using the Matter protocol and the old ones with their specific protocols will therefore co-exist, and compatibility will not disappear during the evolution of standard [4].

Future efforts towards interoperability need to be adopted across multiple dimensions: rapid adoption of openness such as Matter, the emergence of common language standards for device description and certifications that ensure consistency across the platforms. The efforts should come as a collective effort from industry players to break down competitive walls that can hinder seamless integration. According to Lawal, mainstreaming IoT in our existing buildings also means breaking the technical silo issues. Good standardization is expected to make us, users, more satisfied with our product and also spur innovations by being able to have developers develop applications on integrated platforms as opposed to individual device platforms.

DOI: 10.54254/2755-2721/2025.LD30021

4. Conclusion

This paper primarily explores the core technologies, architectural models, and prevailing challenges of IoT-based smart home systems. It provides a comprehensive overview of the ecosystem, from communication protocols and AI applications to security and interoperability issues.

The study concludes that IoT technologies are pivotal for enabling intelligent home functionalities, yet their widespread adoption faces significant hurdles. Key challenges include a lack of device interoperability due to heterogeneous standards, persistent security vulnerabilities and privacy risks from increased data collection, and the need for improved system energy efficiency and reliability. These findings underscore the critical need for standardized frameworks and robust security measures in future smart home development. My paper does not deeply explore the implementation and comparative effectiveness of specific machine learning algorithms for predictive analytics. Furthermore, it did not employ empirical or quantitative methods to validate the performance and energy efficiency of the proposed architectural solutions. Future research should focus on establishing universal technical standards to ensure device compatibility and ecosystem integration. Another promising direction is the development of advanced, AI-powered security frameworks and the optimization of edge computing architectures to enhance data privacy and system responsiveness.

References

[1] Ali Hassan. "Exploring IoT Security: Architecture, Key Security Features, Attack Methods, Current Challenges, and AI-Driven Future Solutions." Computers, Materials & Continua, 2024, (12): 3499-3559.

[2] Kehinde Lawal. The Trend, Advantages, Risks and Challenges of Internet of Things Application in Residential and Commercial Buildings [J]. Energy and Building Environment, 2022, (3): 251-266.

[3] Yue Yuan. A Review of the Current Status of User-Oriented Control Research for Enhancing Comfort and Energy Efficiency [J]. Building Simulation, 2024, (10): 1675-1692.

[4] Nabeela Awan. Research on Machine Learning-Driven Power Dispatching in Smart Cities Based on the Internet of Things [J]. Computers, Materials & Continua, 2021, (5): 2449-2462.

[5] Xing Yang. A Review of Smart Agriculture: Development Models, Technologies, and Security and Privacy Challenges [J]. IEEE/CAA Journal of Automatica Sinica, 2021, (2): 273-302.