A Review of Smart Home Applications based on Internet of Things

Mussab Alaa, A.A. Zaidan, B.B. Zaidan, Mohammed Talal, M.L.M. Kiah

PII: S1084-8045(17)30280-1
DOI: http://dx.doi.org/10.1016/j.jnca.2017.08.017
Reference: YJNCA1963

To appear in: Journal of Network and Computer Applications

Received date: 19 February 2017
Revised date: 23 July 2017
Accepted date: 25 August 2017


This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting galley proof before it is published in its final citable form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.
A Review of Smart Home Applications based on Internet of Things

Mussab Alaa\textsuperscript{1}, A.A.Zaidan\textsuperscript{1,2}, B.B.Zaidan\textsuperscript{1,2}, Mohammed Talal\textsuperscript{1}, M.L.M. Kiah\textsuperscript{1}

\textsuperscript{1}Department of Computing, Faculty of Arts, Computing and Creative Industry, Universiti Pendidikan Sultan Idris, Malaysia
\textsuperscript{2}Security Lab, Wisma R&D, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia

Abstract
The new and disruptive technology of smart home applications (hereafter referred to as apps) based on Internet of Things (IoT) is largely limited and scattered. To provide valuable insights into technological environments and support researchers, we must understand the available options and gaps in this line of research. Thus, in this study, a review is conducted to map the research landscape into a coherent taxonomy. We conduct a focused search for every article related to (1) smart homes, (2) apps, and (3) IoT in three major databases, namely, Web of Science, ScienceDirect, and IEEE Explore. These databases contain literature focusing on smart home apps using IoT. The final dataset resulting from the classification scheme includes 229 articles divided into four classes. The first class comprises review and survey articles related to smart home IoT applications. The second class includes papers on IoT applications and their use in smart home technology. The third class contains proposals of frameworks to develop and operate applications. The final class includes studies with actual attempts to develop smart home IoT applications. We then identify the basic characteristics of this emerging field in the following aspects: motivation of using IoT in smart home applications, open challenges hindering utilization, and recommendations to improve the acceptance and use of smart home applications in literature.

Keywords: Smart home application, Remote home, Intelligent home, Home automation system, Automated home, Internet of Things (IoT)

1 Introduction
As an important component of the Internet of Things (IoT), smart homes serve users effectively by communicating with various digital devices based on IoT. In the ideal version of a wired future, all devices in smart homes communicate with one another seamlessly. Smart home technology based on IoT has changed human life by providing connectivity to everyone regardless of time and place [1], [2]. Home automation systems have become increasingly sophisticated in recent years. These systems provide infrastructure and methods to exchange all types of appliance information and services [3]. A smart home is a domain of IoT, which is the network of physical devices that provide electronic, sensor, software, and network connectivity inside a home.

Smart homes are automated buildings with installed detection and control devices, such as air conditioning and heating, ventilation, lighting, hardware, and security systems. These modern systems, which include switches and sensors that communicate with a central axis, are sometimes called “gateways.” These “gateways” are control systems with a user interface that interacts with a tablet, mobile phone, or computer; the network connectivity of these systems is managed by IoT [4].

Since 2010, researchers have analyzed IoT-based smart home applications using several approaches. Regardless of their category, existing research articles focus on the challenges that hinder the full utilization of smart home IoT applications and provide recommendations to mitigate these problems. Research on smart home applications is dynamic and diverse. This survey aims to provide valuable insights into technological environments and support researchers by understanding the available options and gaps in this line of research. It aims to shed light on the efforts of researchers in response to new and disruptive technology, map the research landscape into a coherent taxonomy, and determine the features that characterize this emerging line of research in smart home technology. This paper is organized as follows. In Section 1, IoT and its applications in smart homes are introduced. In Section 2, the research methods, scope, literature sources, and steps in filtering research articles are described. The research landscape based on literature is also mapped into a coherent taxonomy. In Section 3, the results and statistical information of the final set of articles in this study are reviewed. In Section 4, the benefits and challenges extracted
from articles on IoT-based smart homes from 2010 to 2016 are discussed and classified. In Section 5, the conclusion of this review is presented.

2 Method

The most important keyword in this work is “Internet of Things (IoT) and its applications in smart homes.” This keyword excludes any non-IoT-based smart home applications, such as those found on smart grids and any non-application-based use of smart cities. We also limited our scope to English literature but considered all IoT applications in smart home automation. Three digital databases were explored to search for target articles. (1) IEEE Xplore is a scholarly research database that provides the most reliable and wide-ranging articles in the fields of computer science, electronic technologies, and electrical engineering. (2) Web of Science (WoS) offers indexing of cross-disciplinary research in sciences, electronic technologies, social sciences, arts, and humanities. (3) ScienceDirect is a large database of scientific techniques and medical research. These three databases sufficiently cover IoT and its applications in smart home technology and provide a broad view of existing research in a wide but relevant range of disciplines.

Study selection involved a search for literature sources and then three iterations of screening and filtering. In the first iteration of screening and filtering, all unrelated articles were removed. In the second iteration, duplicates and irrelevant articles were removed by scanning the titles and abstracts. In the last iteration, the full-text articles screened from the second iteration were carefully reviewed. All iteration steps applied the same eligibility criteria followed by authors. The search was conducted in April 2016 using the search boxes of ScienceDirect, IEEE Xplore, and WoS. To identify the studies related to IoT, such as AND (“Internet of Things”), we used a mix of keywords containing "smart home," "smart-home," "smart-house," "remote house," "remote-home," "intelligent home," "intelligent house," "home automation system," "house automation system," "automated home," and "automated house" in different variations and combined with the “OR” and “AND” operators followed by “Internet of Things” or “IoT.” The exact query text is shown in Fig. 1. The advanced search options in the search engines were used to exclude book chapters, short communication, correspondence, and letter and gain access to up-to-date scientific works relevant to our survey on this emergent trend of IoT applications in smart homes.

Every article that met the criteria listed in Fig. 1 was included. We set an initial target for mapping the space of research on IoT applications in smart homes into a general and coarse-grained taxonomy of four categories. These categories were derived from a pre-survey of the literature with no constraint (Google Scholar was used to gain insights into the landscape and directions in the literature). After the initial removal of duplicates, articles were excluded in two iterations of screening and filtering if they did not fulfill the eligibility criteria. The exclusion criteria included the following. (1) The article is non-English. (2) The article is focused on a specific aspect of smart grids and smart cities. (3) The subject is limited to smart homes and excludes IoT. To simplify the steps, we read and analyzed the final set of articles in Word and Excel formats. Moreover, the articles were classified in detail using taxonomy and a large collection of highlights and comments. The taxonomy suggested different classes and subclasses, including four main categories: review, application, design, and development. Texts were categorized depending on authors’ preferred style, and the collected data and relevant information were saved in Word and Excel files. All the articles from various sources were analyzed in depth to give readers a comprehensive overview of the subject.
3 Results and Statistical Information of Articles

The initial query resulted in 1,798 papers: 105 from the WoS database, 268 from ScienceDirect, and 1,425 from IEEE Explore. The filtered articles published from 2010 to 2016 were adopted in this research and grouped into three categories. In the three databases, 45 out of 1,753 papers were duplicates. After scanning the titles and abstracts, 1,387 papers were excluded further, for a total of 366 papers. The final full-text review excluded 137 papers, for a total of 229 papers in the final set, all of which were related to smart home IoT technology through different topics. The taxonomy presented in Figure 2 was used to review the main streams of research focusing on IoT and their general use in smart homes. This taxonomy shows the comprehensive development of various studies and applications. The classification suggests different classes and subclasses. The first class includes review and survey articles related to smart home IoT applications (3/229 papers). The second class includes papers on IoT applications and their use in intelligent smart home technology (79/229 papers). The third class comprises framework proposals to develop and operate applications (125/229 papers). The final class includes studies with actual attempts to develop smart home IoT applications (22/229 papers). The observed categories are listed in the following sections for statistical analysis.
3.1 Review and survey articles
The review and survey articles summarize the current state of understanding on IoT and its applications in smart homes. Two studies involve smart home systems based on IoT [1], [5]. The last study provides a review of the challenges in IoT smart homes [2], IoT, and its use in smart homes.

3.2 Studies conducted on IoT applications and their use in smart homes
This section reviews the applications of IoT and its use at home. These articles were divided into various topics and applications. Selected works were classified into broad categories depending on the IoT applications in smart homes.

3.2.1 Evaluation studies
One category comprises evaluation studies. Works under this category evaluate risk models to assist in managing devices from security systems [6], energy consumption based on photovoltaic systems in smart homes [7], [8], [9], [10], data management in smart home devices [11], [12], and the performance and applications of Wi-Fi and ZigBee devices (ZigBee is wireless technology designed for personal area networks) in smart homes [13]. Evaluation is a trust management protocol for smart home systems [14]. User experience, such as the proper use of smart home devices [15], [16]; Bluetooth devices, which reduce energy consumption in smart homes [17]; and body sensor networks in smart homes to monitor the activities of the elderly [18] are evaluated. Other works assess remote control systems for smart home devices [19] and the use of fingerprints in indoor localization systems in smart homes [20]. Other related works focus on the evaluation of Bluetooth applications in smart home systems based on IoT [21]. Electronic appliances in homes are also evaluated to determine the efficiency and accuracy of their energy consumption [22]. Another study presents a scenario to evaluate several sensors communicating with a smart
gateway over Bluetooth Low Energy to ensure the accurate transmission of information [4]. The performance of the novel architecture of IoT implemented using radio frequency identification in smart homes is also evaluated [23]. In another work, selection criteria are used to evaluate the challenges and integration of IoT and cloud computing paradigms in smart homes [24].

3.2.2 Activities involving IoT applications

This section presents the types of smart home applications based on IoT. Automated transportation, smart closed-circuit television (CCTV), energy management system applications, network architecture, mobile apps, security applications, and environmental monitoring are all examples of IoT applications for smart homes.

3.2.2.1 Security and privacy applications

Other works are classified into small categories according to the security activities and efficiencies in smart home systems based on IoT. These works focus on security systems and applications for smart homes using IoT [25], [26], [27], [28], [29], [30], [31], secure data management in various devices [32], security enhancement in smart home systems and applications [33], [34], [35], and network system security and privacy control for home intelligence and IoT devices [36]. Other works discuss secure healthcare architecture [37] and communication of nodes in a Constrained Application Protocol (CoAP; an application layer protocol that is prepared for use in Internet devices in IoT smart homes, such as wireless sensor network nodes) network [38], as well as security challenges between heterogeneous devices and different applications in smart homes [39], [40], [41]. Some studies focus on password security and applications for IoT smart home systems [42], [43], secure software updates in smart home devices [44], and security system devices (e.g., surveillance cameras) and their use in smart homes [45]. Home automation and security threats are also defined [46]. A new solution is presented to address risk reduction in cases of privacy breaches in smart energy management systems [47]. Another work discusses the research and implementation of machine-to-machine technology in smart homes and security systems [48].

3.2.2.2 Network architecture applications

Another category covers articles on network architecture and applications between different devices in IoT-based smart homes. Works under this category discuss network connections between various devices and applications in home automation systems [49], [50], [51], [52] and home automation gateways and applications [53], [54]. Network architecture and implementation in smart homes based on IoT relationships between IoT in home automation and applications are established using smart home cloud computing based on software defined networking (SDN). SDN is a cover terminology used in several types of network domains to make the network architecture in home automation agile and flexible [55]. A study presents the application of ubiquitous networks in the smart home domain [56]. Smart home applications and solutions over content-centric networks are also presented [57]. Other studies conduct experimentation using a combination of smart home sensors in a network architecture [58].

3.2.2.3 Monitoring applications and their use in health services

A small category includes studies on mobile management and its use in health services. These studies focus on cloud mobile apps in smart homes [59], [60], [61] and Android mobile apps in smart homes for managing various aspects of the lives of the elderly and people with disabilities [62]. Other works are classified under a small category of mobile management studies related to health systems in IoT-based smart homes [63], [64], [65]. Control smart home systems and apps for the elderly and people with disabilities are also presented [66]. Medical reminder and monitoring system apps are explored for use by elderly people in smart homes [67].

3.2.2.4 Overview applications

A small category includes studies related to energy management and applications of control of electrical loads in smart homes [68]. The Web of Objects platform, which involves web-based IoT application services using heterogeneous devices in smart home systems such as pet care services, and its applications in smart homes are also presented [69]. An IoT-based device control system for intelligent homes is proposed [70]. Actual data are tested to assess the performance of multi-control center household appliances [71]. IoT with motion sensing is utilized in smart homes [72]. Training procedures are established for control smart home systems and applications based on IoT technology [73]. IoT software and applications of smart home systems are built [74]. Complex
processing for IoT and its use in smart homes are described [75]. Communication and collaboration are established between persons and devices, e.g., users send SMS to IoT-based smart homes [76]. Large data are managed with network architecture in IoT in smart homes [77]. General applications and their implementation in smart homes are described [78]. Different user activities and applications in IoT-based smart home systems are presented [79]. Smart home applications based on an IoT management platform are also described [80]. Smart home applications and architectures based on resource name services are established to control smart home devices [81]. Challenges in the design of overall smart home systems are described [82].

3.2.3 Comparative studies
A few works compare compassionate use applications between two network protocols, namely, CoAP and Network Time Protocol (NTP). CoAP is an Internet Application Protocol for constrained devices, and NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. Both protocols are widely adopted for IoT-based smart home systems and applications [83].

3.3 Proposals for system design and framework to develop and operate applications
The system design process defines the architecture framework, modules and interfaces, and data for a system to satisfy specified requirements. System design can be regarded as the application and implementation of system theories for product development. In these sections, we briefly review all the design studies included in this work.

3.3.1 System designs and its implementations
These studies focus on security system designs for smart homes [106], [107], [108], [109], [110] and secured multimedia authentication systems for wireless sensor network data related to IoT in smart homes [111]. Distributed malware attacks against IoT in smart homes are evaluated [112]. Secure Kerberos authentication is designed for home automation systems based on IoT [113]. A security mechanism of a terminal gateway group system [114] and a control system with multiple functions in smart homes are designed [115], [116], [117], [118], [119]. Smart home control systems based on General Packet Radio Service and ZigBee are established [120]. Home automation wireless power control based on IoT [121] and an energy management system to reduce energy consumption in smart houses are designed [122], [123], [124], [125], [126]. A system is designed to provide recommendations for users when they detect energy wastage [127]. A ZigBee wireless device is designed and implemented to avoid energy wastage in smart homes [128]. Sockets are designed based on intelligent control and energy management [129]. A ZigBee-based system is designed and implemented to manage power consumption [130]. A modern healthcare system facility and an elderly caring system for smart homes are designed [131]. A healthcare system with mobile sensing and network analytics support is developed [132]. A wireless sensor network is designed and installed in smart homes [133], [134], [135], [136]. A minimalistic system for smart homes is developed using three modules: a home gateway, a cloud server, and a user interface [137]. Devices with machine-to-machine integration for smart home systems are designed and implemented [138], [139]. IoT-based media content sharing services in home automation [140] and smart house gateways for social Web of Things are designed and implemented [141], [142]. A system and the application of low-cost smart homes under IoT systems and cloud computing are designed [143]. In another work, a wireless intelligent light control system based on ZigBee light link is developed [144]. Home automation based on ZigBee wireless sensor networks is designed and implemented [145] along with an IoT access point for home automation [146]. A design solution involving embedded uninterruptible power supply (UPS) is used for long-distance monitoring and control of UPS based on an IoT network [147]. A smart home system based on a Wi-Fi network is designed and implemented [148]. A system is developed to derive and manage data transmission for home devices [149], [150]. A smart home control system is designed to manage data transmission between devices [151]. A data synchronization system for smart homes based on Multipurpose Infrastructure for Network Applications (MINA) is developed and adopted. MINA can be utilized in IoT-based smart homes to make scalable, high-performance network applications [152]. A smart home system and applications based on IoT are designed and developed [153], [154], [155], [156], [157] along with a smart home system for complex applications [158], [159], [160], [161], [162]. An IoT-based home automation system is designed [163]. A smart home architecture [164], system for home automation management [165], and Design Home Localization System for Misplaced objects (HLSM) are built. In particular, HLSM involves multiple devices connected to a central server either by Ethernet or Wi-Fi depending on the reader type. The mobile readers then communicate with the server via Wi-Fi. This system helps people find certain things in IoT-based smart homes, such as glasses, wallets, and
A system based on IoT home and ZigBee/Global Positioning System technology is designed and adopted [167]. ZigBee devices are developed and implemented in smart homes [168]. An architecture and implementation system is designed to support smart home services and applications based on IoT [169]. A Domain Name System name autoconfiguration for IoT in smart homes [170] and a gas detector position computer system based on ARM (a powered intelligent home security system and monitoring system) are developed [171]. A system based on IoT services is developed and implemented in support of users [172]. Raspberry Pi, as a sensor web node for smart home systems [173], and a smart house power management system are designed and implemented based on a human–computer interaction model [174]. A ZigBee device-based smart home monitoring system is developed and installed [175]. A software ecosystem that allows users with different skills to develop location-aware services to autonomously manage smart homes is designed and implemented [176]. A Bluetooth system is developed and applied in IoT-based smart homes [177]. Hardware and software solutions for communication techniques are used for the initial configuration of embedded devices [178]. The distance between IoT devices and mobile devices is measured using Bluetooth with improved accuracy [179]. A smart home energy management system is designed and its applications are assessed [180], [181]. A design prediction device is developed to identify solutions to problems in IOT-based smart homes [182]. An IoT-based smart home system is designed for the provision of services [183]. Techniques that enable smart human device interfaces and an appliance usage prediction engine to aid home automation systems are designed [184]. A mobile robot for an old-age-compliant smart home environment is designed to fulfill the needs of elderly people [185].

3.3.2 Module designs and methods
Privacy and security are modeled for smart homes [186]. An IoT management model and methods based on Web of Objects for home data mining are described [3]. A model life cycle tracking system for LED bulbs of home automation devices is proposed [187]. The Web technology Raspberry Pi is utilized to control different LED devices to include modules and provide an alternative in the implementation of smart homes [188]. A method enabling the “brand-free plug-n-play” deployment of smart devices is integrated, tested, and validated in home automation systems using BLE [189]. A modular smart home is designed and implemented using a wireless network [190]. An IoT-centralized management model for smart homes is developed [191]. A mobile smart home model is designed and applied [192]. A model based on a basic mathematical approach is developed and applied to describe the success of human interactions in smart home applications [193]. An IoT network model for smart homes is proposed [194]. A module in IoT smart homes is designed and implemented [195]. A smart home based on IoT technology is designed and simulated [196]. Electrical models are developed to deal with the humanized interaction between humans and computers in smart homes [197].

3.3.3 Framework designs
A web-based application framework for smart homes is designed [198]. A framework architecture for smart homes is developed [199]. BlinkToSCoAP, an IoT security management framework for IoT devices in smart homes, is developed as a security framework architecture [200]. A framework is designed to manage energy consumption and IoT devices in smart homes [201]. A home automation framework is developed [202]. A framework for managing the energy efficiency of smart homes is designed [203]. A cognitive management framework is developed for IoT in smart homes [204]. A framework for cloud-based smart homes is proposed [205]. A framework is designed to develop a home automation system [206]. A middleware framework for sensor nodes is developed to achieve network virtualization in smart homes [207]. A visual programming framework is designed for wireless sensor networks in house intelligence applications [208]. A gateway software framework for heterogeneous networks in smart home applications is designed [209]. A general framework is developed to solve the security requirements of a cloud–IoT paradigm and applied to remote mobile medical monitoring [210]. An IoT service framework is designed for smart homes [211]. A controller application communication framework for smart homes is described [212]. A framework for sharing data with multiple systems in smart homes is developed [213]. A designed framework is aimed at creating a complete software tool chain to tackle integration issues for IoT in smart homes in general [214]. A conceptual framework for a smart home system is designed [215]. An overall system architecture is illustrated based on the layer framework of IoT [216]. An information-centric networking framework is tailored to the smart home domain [217]. A smart home service framework is designed and applied [218]. A framework called eDomus, which is based on social networks such as Facebook, is designed to allow users to interact remotely with home networks [219]. A framework for smart home automation is designed [220]. An OSGi framework is described as a preferable platform for IoT services in combination with a Raspberry Pi-embedded hardware board, which is also
known to ensure gateway features in smart homes [221]. An IoT device management framework for smart home scenarios is designed [222]. A smart home system framework is developed and implemented [223]. A modeling framework for smart environments is designed [224]. A theoretical framework is presented in a previous study [225]. A developed framework can be used for IoT-based smart home systems [226]. A management framework is designed and implemented in smart home systems [227]. A communication framework that leverages the information-centric networking paradigm for local machine-to-machine communications is designed [228]. A new middleware framework for Ambient Assisted Living (i.e., SHAAL) is designed based on the virtualization of sensor networks to enable multiple independent applications to run on different heterogeneous sensor networks in IoT-based smart homes [229].

3.4 Reports on actual attempts to develop applications
The final category includes studies that attempt to develop smart home IoT applications. These works develop Cloud of Things architecture for smart homes [84], IoT technology-based smart home services [85], and low-cost systems for smart home appliances. A developed system takes information from devices and posts it to Twitter [86]. Other home systems are also developed on the basis of IoT technologies [87]. Other studies develop IoT applications on the basis of smart home technology [88], [89], [90], [91], a network monitoring system for mobile devices in smart homes [92], and system applications in voice-controlled multifunctional smart home systems [93]. An intelligent energy management system with approaches for IoT applications in smart homes is also developed [94]. Sensor network architectures in smart homes based on IoT technology are established [95]. A smart energy monitoring system in IoT-based smart homes is developed [96]. A novel smart home application is developed on the basis of an architecture and middleware of IoT technologies [97]. Some works develop a smart gateway architecture to improve smart home network applications based on IoT [98], IoT technology for wireless sensor networks and systems for monitoring temperature [99], and IoT technologies for enhancing health smart home systems [100]. Security and privacy features are developed for IoT devices [101], and security issues and corresponding solutions for sensor networks in smart homes are explored [102]. Some studies discuss the development of innovative products and entirely new services in smart home technology based on IoT [103] and emergency alert systems based on Internet Protocol television platforms in smart homes [104]. Energy monitoring systems based on ZigBee devices are developed for smart homes to reduce energy consumption [105].

4 Distribution results
Figure 3 shows that the three digital databases store numerous research works. The results of the review are divided into four main categories, namely, development, design, applications, and review papers.

![Figure 3 Number of included articles in different categories according to publication journals](image-url)
The total number of selected published articles from ScienceDirect is 33, consisting of 4 articles for development, 15 for design, 14 for applications, and 0 for review papers. The total number of selected published articles from the WoS database is 42, consisting of 6 articles for development, 24 for design, 11 for applications, and 1 for review papers. The total number of selected published works from IEEE Explore is 154, comprising 12 articles for development, 86 for design, 54 for applications, and 2 for review papers.

4.1 Distribution by year of publication
Figure 4 indicates the number of included articles in the four categories according to the year of publication. The distribution of scholarly papers from 2010 to 2016 is shown.

![Figure 4 Number of included articles in different categories by year of publication](image)

Exactly 97 papers included in this review were published in 2015. None were published in 2010, while 12 were published in 2011. Exactly 15 and 28 papers were published in 2012 and 2013, respectively. Among the selected articles, 49 were published in 2014, and 28 were published in 2016.

4.2 Distribution by Authors’ Nationality
Figure 5 shows that the articles on IoT-based smart homes that were included in this review hailed from 39 countries and nationalities. These articles generally involve study cases conducted in the 39 countries.
The value $n = 229$. In particular, the geographical distribution of the selected articles on IoT-based smart homes in terms of numbers and percentages shows that the most productive authors are from China, with 67 study cases. This was followed by Korea and India with 23 study cases each; Italy with 16 study cases; Taiwan with 14; Germany and the US with 9 each; the UK with 8; Sweden, Brazil, and Finland with 5 each; Singapore with 4; Serbia, Greece, Australia, and Japan with 3 each; New Zealand, Bosnia and Herzegovina, Switzerland, Malaysia, Spain, and Czech with 2 each; and Vietnam, Turkey, Slovenia, Cyprus, France, Norway, Ireland, Bulgaria, Indonesia, Chile, Austria, Slovakia, France, UAE, Oman, Canada, and Poland with 1 study case each.

5 Discussion

This review presents the most relevant studies on state-of-the-art smart home applications based on IoT technologies. The objective of this work is to highlight the research trends in this area. This survey differs from previous reviews because it is current and it focuses on the literature on applications rather than on the applications...
themselves. A taxonomy of the related literature is proposed. Developing a taxonomy of the literature in a research area, particularly an emerging one, can provide several benefits. On the one hand, a taxonomy of published works organizes various publications. A new researcher who studies smart home applications may be overwhelmed by the large number of papers on the subject and the absence of any kind of structure and may thus fail to obtain an overview in this area. Various articles address the topic from an introductory perspective, whereas other works examine existing applications in smart homes. Some studies develop actual applications for use in smart homes. A taxonomy of the related literature helps sort out these different works and activities into a meaningful, manageable, and coherent layout. On the other hand, the structure introduced by the taxonomy provides researchers with important insights into the subject in several ways. First, it outlines the potential research directions in the field. For example, the taxonomy of smart home applications in the current work shows that researchers are inclined to propose frameworks to develop and operate applications, thus providing a possible path in this area. Other areas include IoT applications and their use at home, including the assessment of current smart home applications. Second, a taxonomy can reveal gaps in research. Mapping the literature on smart home applications into distinct categories highlights weak and strong features in terms of research coverage. For example, the taxonomy in this work shows how groups of individual applications receive significant attention in review and evaluation (as reflected in the proliferation of their categories) at the expense of integrated solutions and frameworks, as well as development efforts. Combined with a survey on an adequate and a representative sample of the literature, the taxonomy also highlights the lack of studies on the development of smart home IoT applications. Traditional smart home technologies receive considerable attention in the literature. Studies in this area attempt to develop smart home IoT applications or share their experiences in the process.

Statistical data on the individual categories of the taxonomy identify the sectors involved in smart homes to cope with new trends and strengthen inactive areas. Similar to taxonomies in other fields, the proposed taxonomy in this review employs a common language for researchers to communicate and discuss emerging works, such as development papers, comparative studies, and reviews on smart home applications based on IoT.
5.1 Motivations
The benefits of using smart home applications based on IoT are evident and compelling. This section lists a few of the advantages reported in the literature, which are grouped into categories depending on similar benefits. The corresponding references are cited for further discussion (see Fig. 6).

- Bluetooth Low Energy apps
- Control system/monitoring system
- Data management
- Devices apps over IoT
- DNS (Name Autoconfiguration for IoT Devices)
- Emergency alarm system
- Energy management, apps and efficiency
- Fingerprint based indoor localization system
- Gas detector position system
- Healthcare/robot system
- IoT access point applications in smart home
- IoT apps in smart home system
- Light control system
- Light time synchronization applications
- Management smart home system
- Mobile smart home applications
- Network architecture
- Password authentication
- Remote access
- RFID apps in smart home
- Router technology applications
- Security and privacy applications
- Smart home algorithm and implementation
- Smart home sensor and applications
- Smart home services and implementation
- Smart home solutions
- Smart home system apps based on ZigBee/GPRS
- Software update and applications
- Training
- Trust management protocol
- User experience
- Wifi and ZigBee apps
- ZigBee based on smart home monitoring system

Figure 5. Number of Articles on Smart Home Applications Based on IoT

The survey conducted revealed three aspects of the literature content: the motivations behind developing smart home applications based on IoT, the challenges to the successful utilization of these technologies, and the recommendations to alleviate these difficulties.
5.1.1 Benefits related to smart home IoT energy conservation

Energy conservation is considered important in home automation. IoT devices in smart homes are used to provide advanced technology to control smart systems and reduce energy wastage. These devices improve efficiency and power factor while conserving energy [116], [68], [127], [203], [57]. For example, smart home lighting systems provide automated lighting control through LED lights. These systems automate the action of turning lights on and off [40]. Smart homes manage energy efficiently. Lighting systems maximize self-produced electricity and save energy in almost all areas in a smart home. During daytime, self-produced electricity can be utilized to run appliances. At night, standby devices can be automatically switched off to reduce power consumption [201], [128]. Lights of IoT devices in smart homes automatically shut off when residents vacate rooms or leave their homes to minimize energy consumption [56], [5], [122], [107]. In smart homes, various appliances, such as lighting systems with automatic adjustment or remote control via a centralized controller, are used to increase the convenience and efficiency of daily activities. Appliances are controlled to maintain energy [205]. Conserving energy in smart homes while improving the lifestyle of residents is an important issue [123]. Residents in smart homes use mobile applications to maintain consumer energy usage for monetary savings [59], [180], [156] and reduce expenses [105]. Energy saving is an important issue. Indoor and outdoor temperatures are constantly changing, and the amount of energy consumed can increase at specific times. For example, air conditioning systems can regulate indoor climate and provide a comfortable environment with the lowest energy consumption according to the activities inside using energy control based on IoT technology [75]. An energy system is developed to conserve energy without the intervention of residents [211]. System security is crucial in energy conservation because the lack of security causes significant energy loss [109]. Wireless technology is a potential energy-conserving technology [17], [206], [4].

5.1.2 Benefits related to healthcare

Smart homes non-evasively enhance home care for the elderly and people with disabilities. These homes maintain the health of these individuals and prevent loneliness [152], [18]. In northwestern Italy, the government decided to establish a village with smart homes to provide the elderly with opportunities to experience healthy, successful, and suitable living arrangements [163]. Robotic devices in smart homes assist the elderly and people with disabilities for them to achieve long and healthy lives [36], [185], [40], [207], [212], [150], [132]. Remote health monitoring for
elderly people in smart homes provides immediate clinical health care and improves access to medical services within smart homes, services that are usually unavailable in ordinary homes [63], [14], [8]. Smart homes for the elderly anticipate their needs without direct human intervention [64], [86]. They help the elderly check whether they are following their specific treatments, including taking their prescribed medicine on time [65], [216]. The population of elderly and people with disabilities in Singapore has significantly increased, thus intensifying the demand for caregivers and domestic helpers [66]. The elderly need supervised monitoring for them to take their medicines on time; thus, smart homes can prove useful [67]. In general, elderly parents live with their children in China, Japan, the United States, and Europe, but adult children cannot always take care of their elderly parents. Mobile smart homes help elderly parents and provide them a good life [192], [100]. In a smart home, medical staffers monitor environmental conditions inside the home using CCTV for the elderly [227], [131]. Mobile robots in smart homes specialize in fulfilling the needs of the elderly and people with disabilities [185].

5.1.3 Reducing the cost of basic needs in smart homes
Several devices are utilized by residents of smart homes to save money on basic needs [5]. Remote health monitoring increases the access of the elderly and people with disabilities to care and decreases healthcare delivery costs. Such a system, which is often unavailable in hospitals and clinics, can improve access to medical services and reduce costs [63]. Wireless network technology in smart homes is adopted instead of wired systems to increase flexibility and liquidity and reduce cost and energy [167], [86], [48]. Energy conservation in smart homes reduces costs [156], [59], [83], [10], [7], [201]. A security system conserves energy because it avoids the failure of any machine that can cause confusion in energy use and lead to significant energy consumption [58]. IoT in connected healthcare networks reduces the frequency of doctor visits, thereby reducing medical costs for the elderly and people with disabilities [32], [65], [207]. Adopting IoT in smart home applications significantly reduces cost [45]. The proper behavior of residents is also known to conserve money and energy [180].

5.1.4 Entertainment and comfort
Smart automation systems in smart homes provide comfort to residents, ensure their safety and security, and allow devices to operate at all times [5], [25], [72], [73], [70], [78], [79], [40], [16], [63], [58], [155], [205]. All these devices are equipped with sensors with different functions and wireless communication tools based on IoT technology [138], [182]. For example, when residents leave their smart homes, the devices inside their homes automatically turn off [205]. Residents can also conveniently pay their bills [7]. Mobile devices are suitable for residents in smart homes [66], and residents can use these devices instead of a physical key. Smart homes can be controlled using mobile devices [46] or through remote control [19], [62], [6], [187].

5.2 Challenges
Although smart home applications based on IoT offer numerous benefits, these technologies are not believed to be the perfect solution in communication network delivery. The surveyed works indicate that researchers are concerned about the challenges associated with smart home applications and their use based on IoT. The main challenges in adopting smart home applications are listed below, along with citations for further discussion. The challenges are classified according to their nature (see Fig. 7).
5.2.1 Concerns on data management

Several researchers are concerned about the flow of data between heterogeneous devices and the risk of electrical hardware failures in IoT-based smart homes which could lead to considerable amounts of data loss [106], [129], [6], [212]. The flow of large amounts of data and complex control impose a significant burden on home automation systems [205], [75], [109], [36], [35], [41], [32], [211], [185], [3], [30]. Many devices in smart homes that can share data and are controlled through the Internet may become vulnerable to several types of attacks; hackers may attempt to remotely control devices, acquire confidential data, or change the contents of messages during transmission [39]. When large amounts of private data flow in smart home devices, data may be lost during the connection process unless the data are controlled properly and according to the preferences of residents [199], [51]. The following data-related problems occur in smart home devices. Stored information in databases is sometimes unstructured [77]. A home gateway system has several obstructions because the gateway system deals with heterogeneous sensors scattered in a home environment, e.g., when a failed transmission of the test data of a network system is applied in ZigBee wireless data transmission, the rate of data loss of the network system is 0.4%; when a user in a smart home starts remote video monitoring, the system loss rate reaches approximately 7.6% [98], [163], [13], [151], [95], [136]. The absence of security systems puts data at risk via the connection of smart home devices [209], [97], [138], [186], [27], [80]. Unreliable data resources (e.g., inaccurate sensor reading or unreliable external environment data acquisition networks (e.g., packet losses at routers) or the inability to determine whether a phenomenon has actually occurred given available information can be attributed to uncertainty. These problems cause data loss in smart home devices [38], [196], [11], [111], [158]. Various challenges in IoT-based smart home devices obstruct efficient data transfer. Data theft is defined as the process of obtaining transmitted information and data between a terminal host and a home gateway by intercepting data packets and tapping lines. During a virus attack, a hacker adds a virus to a data packet and releases it to the system. The virus takes up system resources through constant self-replication. Hence, the system cannot complete relevant work and becomes ineffective. The
latest DoS attacks involve organizing vast amounts of data to access home gateways at the same time. The server cannot verify user legitimacy, complete normal data access, and perform its function. In the illegal processing of user data, an attacker modifies stolen data and sends an error message to a home gateway or to end hosts [102].

5.2.2 Concerns on marketing

Vendors face various challenges in selling smart home software and devices. These problems pertain to complexity, competition among suppliers, and non-compliance to standards, all of which cause difficulties in achieving security and privacy in a scattered market situation [106]. Various device managers for smart homes are not appropriate and efficient [6], [46], [182]. Users can easily and inadvertently download malicious software to their smart devices and appliances. In 2011, more than 50 applications were withdrawn from the market because they contained malware [39]. Although the concept of smart homes is well known in the market, these technologies are expensive [162]. Various problems occur in smart home routers. Wireless control based on 315 and 433 m frequency ranges and others lack a network protocol and can only send simple control commands, e.g., a control network based on a ZigBee device registers a small range and exhibits poor through-wall performance, complex protocol, and inordinate price; the network is also exclusive and incompatible with devices in the market. Wi-Fi has a small control range and is limited to only a few connected devices [182]. Various types of smart home devices have emerged in the market. The behavior of several devices has been studied, and the vulnerabilities of some of these devices have been identified [35]. Some devices do not function in smart home appliances because of differences in brand manufacturing. For example, brand A light bulbs cannot be controlled with brand B gateways [189]. Pressing concerns exist about the privacy of data associated with e-health. Devices must be compatible with the compliance requirements of Health Insurance Portability and Accountability (US legislation that provides data privacy and security provisions for safeguarding medical information) and PCI (security standard), both of which handle healthcare and e-commerce applications. Thus, loopholes occur for sellers because non-compliant and incompatible devices cause security violations to end users in smart homes [14].

5.2.3 Concerns on device connectivity

Communication problems occur among various devices from manufacturers or companies that adopt different techniques and standards [2]. Communication problems among devices in smart homes also exist because these devices use different sensors and networking gadgets from various manufacturers [5]. Some devices in smart homes cannot be used and are unprotected by security systems; thus, these devices sometimes damage smart home systems [48], [25], [41], [35], [27], [39], [29], [40], [14]. Properly regulating the growing use of smart devices and the interaction of smart home systems may pose a threat to the privacy and security of citizens [36]. Some devices in smart homes depend on batteries; poor battery performance causes communication problems among these devices [30]. Some devices in smart homes perform comparably with other devices in terms of operational efficiency, whereas other devices fail. For example, an air conditioning unit that runs continuously for hours could malfunction [75]. One of the most significant challenges in using complex heterogeneous devices is the dynamic environment in smart home technology [180], [4], [62], [11]. Communication is another issue to consider in dealing with a large number of devices in IoT-based smart homes. Devices must be able to produce substantial data in a network under any circumstance. Faulty network architecture for devices may occur in smart home systems. Thus, service providers cannot easily solve this problem because different devices connected to the IoT in a smart home communicate with each other, generating a large amount of traffic [55], [51], [181], [153]. The heterogeneity problem of devices and identifiers leads to poor compatibility in smart home systems [81]. Some of the challenges associated with managing smart homes involve hardware, the improper control of devices, and the need to handle applications that encounter difficulties [6]. Although most IoT devices in smart homes that are connected to gateway architectures are small in scale and battery powered, the key challenge is to extend the lifetime of these devices without recharging or replacing their batteries.

5.2.4 Concerns on security and privacy

IoT raises security concerns, including authorization, authentication, and access control, all of which need to be classified. Security applications must be adopted in smart homes. Research is conducted on the techniques regarding security operations [80]. Loose security systems in IoT environments are identified as one of the top barriers of smart home automation. When motion and environmental detectors identify abnormal conditions (e.g., fuel, smoke, water leakage, window breakage, and person trapped in a bathroom), alerts are raised to residents via phone or the Internet, or surveillance cameras in all vulnerable areas are turned on [106], [6], [178], [209], [205],...
The security of an entire smart home depends heavily on security systems; failures in a security system can cause a house to malfunction [173], [112]. Problems in smart homes that disrupt electricity cause lights to turn off, while smart devices interconnected in the scheme of operations become vulnerable to attacks [39]. The dangers from these systems are alarming. Various intelligent network devices in modern buildings possess limited security features or lack such features altogether. Thus, these devices are easily targeted by potential attacks, which can disrupt the proper functioning of entire buildings and threaten the safety of building occupants [24]. In smart homes, IoT is a buildup of heterogeneous devices, which are sometimes at risk for attacks of or access from strangers and malicious or unauthorized persons; thus, physical damage or alteration of the specific functionalities of these devices must be prevented [41], [32], [26]. The development of IoT and its related technologies has improved homes and lifestyles. The ever-increasing assimilation of these technologies constantly fuels innovations from technical giants. Although these technologies are pervasive, they are often unsecure and use dedicated servers for communication between clients and end devices. Moreover, the problem of securely providing access to houses and industries remains unaddressed and largely depends on the physical presence of users in smart houses. Few systems provide similar secure solutions [45]. Privacy and security issues are likely to be more important in IoT than in the Internet. IoT actuators can influence the safety of individuals if a malicious attacker takes over or sends wrong information to impair their decision process. A tool or technology that enforces policies for IoT actuators is necessary to avoid the execution of actions that affect safety [199], [109], [1]. Some attackers manipulate data in smart homes; thus, security systems are crucial to protect data and patient information [37], [37]. Using IoT in smart homes provides opportunities for malicious parties to carry out attacks that can directly affect the residents of smart homes. Security challenges include sniffing operation techniques, CCTV systems, and DoS attacks [110], [46]. Accidents in security and response time can cause catastrophic failure within the Internet, resulting in a breakdown in communication in a network or a reduction in speed [75]. Smart homes use a one-time password, which is valid for only one login session or transaction, in smart home devices. This lock works to prevent attacks on smart homes [42]. In pin code unlocking, a door lock sends a hybrid app to a smartphone to show a keypad GUI that can be used to enter a pin code in combination with some certificates on the phone to grant access, thus enhancing security because some devices can be hacked through malicious network activities [61]. Data leakage causes various problems in smart homes. Thus, security vulnerability must be considered in an IoT environment [31]. Some appliances in smart homes are not secure and lack proper data encryption or correct authentication; thus, they are susceptible to DoS attacks, man-in-the-middle attacks, or other malicious exploits that compromise the connectivity and physical security of residents. In London, approximately 27% of Wi-Fi networks are poorly secured or are not secured at all [27]. Intelligent mobile home systems control household devices through mobile devices using wireless communication. Security risks may occur in smart homes, including unauthorized mobile access by hackers. Security issues may also be related to privacy because hackers can eavesdrop [192]. The packet transmission route of sensor networks is a connectionless routing in smart homes. Wrong channels, unsecured wireless communication channels, collisions, and delays may lead to packet loss transmission because of the absence of a security system [102].

### 5.2.5 Concerns on safety

Secure IoT technologies are still being developed. Although surveillance and image processing are widely exploited to address issues related to safety and surveillance in smart homes, services may not be provided to the elderly because of the absence of a safety system [100]. Some applications and processes may affect the safety of residents in smart homes. An example is sending wrong information to users. Such cases affect decision-making processes. Proper procedures must be applied to avoid executing measures that affect safety [199]. An intelligent power outlet system for smart homes uses software control, which is regarded as relatively slow and subject to software errors. The latter problem can be addressed by performing intensive tests under harsh conditions. This system quickly responds and avoids overconsumption and electrocutions, making second-generation homes relatively safe and smart [128]. Security problems increase with the emergence of IoT. The lack of security reduces safety [114], [87], [80]. In cases of events such as illegal invasion and gas leaks, warning messages are sent to a system server and the mobile phones of residents [216]. Smart homes are never safe from attackers. Smoke detectors, intrusion detection devices, security cameras, and smart door locks are examples of security devices [40]. Safety systems are crucial to protect patient data from strangers [207]. Unreliable and unauthorized devices must be avoided because they are unsafe, and user access should not be allowed [31]. As residents do not always occupy their homes, they cannot constantly monitor their smart homes [187]. Maintaining total electricity load restriction ensures the safety of users from electrical problems. However, the amount of electricity load is restricted or cut off when it is larger than the set limit, causing inconvenience to users [68]. The on-field implementation of compromised IoT devices results in...
safety complications. Attackers can utilize these devices to physically harm users. Compromised industrial IoT devices, such as the CL200 Centron Smart Meter, can be used to damage cyber-physical systems, such as electricity grids. Excessive power consumption can lead to the uncontrolled overloading of grids, causing loss and equipment failure in extreme cases [101]. Smart homes can create safe environments for individuals. For example, smart mobile homes can provide warnings to individuals of potentially hazardous activities, such as when children are near a boiling cauldron and when invaders enter a home [192]. Wireless sensor networks should be a safety concern in sensor networks. Sensor nodes can be easily manipulated. Thus, other technologies can be developed further to improve the safety performance of sensor networks. Utilizing key management mechanisms is effective within a sensor network. During communication, establishing a temporary session key can enhance confidentiality, and authentication can be solved via non-symmetrical cryptography or symmetric cryptography programs [102]. Dangers such as fires may also exist in smart homes, seriously affecting safety operations inside home automation systems and causing significant damage in smart homes [173]. Home automation systems are equipped with intelligent emergency alert schemes, but these schemes cannot be applied to other systems because of the different architectures and data or protocol formats. Disasters where networks and devices can be badly affected are not considered. Recent disasters (such as the earthquakes or tsunamis in Japan and New Zealand) highlight the need for the mass deployment of intelligent emergency alert systems [104]. A smart home system monitors and ensures the safety of a house. When an unsafe condition is detected, warning messages are sent to residents. Some unforeseen events, such as the automatic turning on of TV and gas leaks, can be detected by sensor nodes anywhere in a home [216].

5.2.6 Concerns on energy consumption
An important concern is that users may cause problems in energy consumption [5]. Security is identified in IoT environments as one of the most significant obstacles to achieving energy-efficient smart homes. The risks associated with the use and potential misuse of information about houses must be understood. The absence of a security system increases the risks associated with the use, potential abuse, and utilization of information about homes, thus elevating energy consumption [106], [41], [200], [186], [80], [28], [47]. Various factors cause problems in energy consumption in smart home systems, including systematic misuse of services, inefficient maintenance, lack of or ineffective security systems, and mismanagment of applications, which is linked to the requirements set by users. The management of resources, such as electricity and water, is related to the external costs of resources and energy consumption [6], [74], [146], [125], [46], [124], [84], [59]. One problem that increases energy consumption in smart homes is electrical fires. The most common sources of electrical fires are power overloads and short circuits. Released energy must be lower than the maximum load capacity of a transmission medium to avoid irreparable damage. Power overloads occur in some devices in smart homes [128]. In home automation, the gateway architecture of networking equipment requires constant work, which equates to significant energy consumption [105]. Problems such as device irregularities and inefficiencies cause large energy consumption. Some users overuse devices, resulting in significant energy wastage, e.g., when a TV is turned on but the user is sleeping in another room and a washing machine is operating in a separate room. Washing machines must not be used during peaks of electricity usage. A smart home system provides suggestions to users. A user leaves room A with the television on and cooks in room B while air conditioning equipment continues to operate at the highest speeds for two hours [123], [75], [40], [53]. In some instances, users may forget to turn off some of the electrical devices in their smart homes, resulting increased energy consumption [198]. Total delay data, potential battery drain (power outage), average level of remaining battery power, complex devices, limited capacity, and leakage of energy storage devices delay comprehensive data and increase power consumption [4].

5.2.7 Concerns on healthcare
The problems related to services for the elderly pose significant pressure and challenges to global healthcare systems. Approximately 25% of the elderly do not follow their prescribed medication, which may lead to poor health outcomes and increased mortality [65]. The elderly population in Europe is expected to increase from 25% to 53% by 2060, causing a surge in healthcare costs mainly needed to employ caregivers and clinicians to care for the elderly. At present, the elderly in the US comprises 13% of the US population, but they consume more than 40% of the US healthcare budget. According to the 2000 census of the Department of Statistics of Malaysia, the percentage of elderly people increased from 5.9% in 1991 to 6.2% (approximately 1.5 million individuals) in 2000. This figure indicates that the aging population in Malaysia is taking shape. The 2000 census also projected that the proportion of the elderly will increase to 9.5% by 2020, which is equal to 3.2 million people. Aging causes cognitive decline and
age-related diseases and restricts physical activities, such as vision and hearing [229]. However, installing devices such as cameras in smart homes raises issues about privacy because these devices constantly monitor the elderly and their movements, thereby causing inconvenience to some.

5.3 Recommendations

This section provides a summary of the most important recommendations in the literature to mitigate the challenges and facilitate the safe and effective use of smart home applications comprising sensors and devices based on IoT (see Fig. 8).

![Figure 8. Categories of Recommendations for IoT Applications in Smart Homes](image)

5.3.1 User recommendations

This section presents important recommendations for users of smart homes and considers the prediction of user behavior, the correct use of devices, and the commitment to the operating times of some devices. To reduce power consumption and the cost of household appliances efficiently, we recommend that users commit to the set runtime [105]. Home energy services are mainly responsible for responding to queries regarding the power consumption information of household appliances, conducting energy efficiency analyses of household appliances, and providing recommendations about household power consumption [130],[47]. A system presents recommendations for users to reduce energy consumption [127]. A system provides recommendations for mobile users when an intruder is detected [192]. Users are recommended to reduce their energy consumption [122]. Although the relationships among devices are useful for fault diagnoses and providing semantic recommendations, generating these relationships is complex for users in smart home systems. Thus, an automatic generation scheme is proposed to reduce the burden to users and service providers. When an IoT device connects to a home switch, an SDN-based home cloud recognizes the device information, such as the model name, manufacturer, and network protocol. The SDN controller easily captures packets that pass through SDN switches. Hence, the controller provides a status graph containing the information for each IoT device. After recognizing the IoT device, it automatically creates four social relationships on the basis of the information. The status is stored in an RDF/XML format to provide a semantic query. Examples of usage of stored information include home diagnosis systems and semantic query systems dealing with home IoT faults [55].
5.3.2 Health recommendations
Health institutions and organizations mainly provide support and guidance and ensure the quality of medical applications in smart homes and in healthcare in general. Health institutions support the elderly at home by providing correct instructions, such as appropriate exercises through TV tutorials [212]. Recommendations are given to patients in smart homes, including medical guidelines, patient diagnoses, and assistance for the elderly and people with disabilities [50].

5.3.3 Safety recommendations
Instructions on how fire systems and electrical devices are utilized and managed in smart homes are provided [227]. A recommendation system to manage IoT–network relationships between IoT devices, networks, and operation techniques helps implement appropriate schemes, diagnose errors in smart homes, and provide recommendations in using household appliances [55]. A hardware security module must be utilized in smart homes to enhance the security of appliances and maintain the efficient transfer of data between devices [31]. A protection system in complex networks inside smart homes is recommended for safe data transfer processes and prevent data loss during data transfer within a network [37], [27]. A recommendation system is designed specifically for smart homes to provide instructions and predictions in different situations. An example is when a user simultaneously uses two similar devices, such as a DVD player and a music player. The system provides recommendations regarding the behavior of the user [184].

6 Limitations
First, the most relevant limitation of this review is the number and identity of the source databases, although the selected sources are reliable and are broad representative collections. Second, the rapid progress in this field limits the timeliness of the survey. Third, an overview of research activities on these smart home applications based on IoT does not necessarily reflect the actual use or effects of the applications. The findings of this work reflect the response of the research community to current trends, which is the objective of this review.

7 Conclusions
A recent disruptive trend has emerged in the use of IoT and applications in smart home technology. Research on this trend is ongoing, although related descriptions and limitations remain vague. Obtaining insights into this emerging trend is important. This article aims to contribute such insights by surveying and taxonomizing related works. Specific patterns can be drawn from the various works on smart home apps. These works are roughly classified into four categories, namely, reviews or surveys, research studies on apps, development attempts, and broad design proposals. An in-depth analysis of the articles helps identify and describe the challenges, benefits, and recommendations relevant to IoT and applications in smart homes. The results indicate the types of available applications in the market and the existing gaps in the use of such applications in IoT smart homes. Researchers have identified issues and provided recommendations, including in the proper use of devices. We also recommend that users commit to the set runtime. Numerous applications of smart home systems provide recommendations for users, including reducing their energy consumption, warnings of defective devices, selecting reliable devices and software, diagnoses, providing correct instructions such as appropriate exercises for the elderly through TV tutorials, medical guidelines, patient diagnoses and assistance, instructions for use and management of fire systems and electrical devices, and provision of security systems and device connectivity. These recommendations can solve the challenges facing IoT applications in smart homes and open up opportunities for research in this area. These problems are related to energy consumption, safety, device connectivity, marketing, and security systems. The insights are identified in the current review, and a summary of previously published studies about IoT and applications in smart homes is presented. The review of these works may serve as a reference for researchers. People will continue to adopt new technologies, and thus, researchers must learn about emerging trends and technologies. The next feature in smart homes may be wearable gadgets connected to IoT. These gadgets are managed by applications and powered by new-generation built-in sensors. At present, research has yet to explore smart home applications based on IoT that control wearable devices or embedded sensors in actual situations. Another consideration for research is adopting interdisciplinary approaches with other technological and scientific fields.
References


34. You-guo, L. and J. Ming-fu. The reinforcement of communication security of the internet of things in the field of intelligent home through the use of middleware. in Knowledge Acquisition and Modeling (KAM), 2011 Fourth International Symposium on. 2011. IEEE.


50. Wang, Z. and X. Xu. Smart home m2m networks architecture. in Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE Ninth International Conference on. 2013. IEEE.


64. Miori, V. and D. Russo. Anticipating health hazards through an ontology-based, IoT domotic environment. in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on. 2012. IEEE.


72. Tseng, S.-P., et al. An application of Internet of things with motion sensing on smart house. in Orange Technologies (ICOT), 2014 IEEE International Conference on. 2014. IEEE.


87. Jie, Y., et al. Smart home system based on IOT technologies. in Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on. 2013. IEEE.


125. Li, Y. *Design of a key establishment protocol for smart home energy management system*. In *Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on*. 2013. IEEE.


157. Lazarevic, I., et al. Modular home automation software with uniform cross component interaction based on services. in Consumer Electronics-Berlin (ICCE-Berlin), 2015 IEEE 5th International Conference on. 2015. IEEE.


175. Yiqi, W., et al. *A ZigBee-based smart home monitoring system*. in *Intelligent Systems Design and Engineering Applications (ISDEA)*, 2014 Fifth International Conference on. 2014. IEEE.


218. Li, Q., et al. Smart home services based on event matching. in Fuzzy Systems and Knowledge Discovery (FSKD), 2013 10th International Conference on. 2013. IEEE.


220. Thiyagarajan, M. and C. Raveendra. Integration in the physical world in IoT using android mobile application. in Green Computing and Internet of Things (ICGCloT), 2015 International Conference on. 2015. IEEE.

221. Stusek, M., et al. Performance analysis of the OSGi-based IoT frameworks on restricted devices as enablers for connected-home. in Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2015 7th International Congress on. 2015. IEEE.


**B.B.Zaidan** received his B.Sc. in Applied Mathematics in 2004 from Saddam University (currently Al-Nahrain University), Baghdad, Iraq. in 2009. He received his M.Sc. in Data communications and Information Security from University of Malaya, Malaysia. Recently, he is in progress to complete his PhD. at Multimedia University, Malaysia. He has published more than 120 papers at various international conferences and journals. His research interests include Smart home apps, Remote house, Intelligent home, Home automation system, Automated home, Internet of Things (IoTs)

**A.A.Zaidan** received his first class B.Eng. degree in Computer Engineering in 2004 from University of Technology, Baghdad, Iraq. Then, he received his M.Sc. degree on Data Communications and computer network in 2009 from University of Malaya, Malaysia. Then, following his Ph.D degree on artificial intelligence in 2013 from Multimedia University, Malaysia. Currently, he is in working as senior lecturer at Department of computing, University Pendidikan Sultan Idris. He led or member for many funded research projects and He has published more than 120 papers at various international conferences and journals. His research areas are: Smart home apps, Remote house, Intelligent home, Home automation system, Automated home, Internet of Things (IoTs)

**M.L. Mat Kiah** received her B.Sc. (Hons) in Computer Science from University of Malaya (UM), Malaysia in 1997, M.Sc. in 1998 and Ph.D. in 2007 from Royal Holloway, University of London, UK. She joined the Faculty of Computer Science & Information Technology, UM as a tutor in 1997. Her current research interests include key management, secure group communication and wireless mobile security. She is also interested in routing protocols and mobile Ad-Hoc networks. A total of 42 (journal: 16, conference: 11, book chapter: 01) publications.

---

**Highlights**

- Mapping the research landscape of smart home based on internet of Things into a coherent taxonomy.
• Figure out the motivation of using the internet of things in smart home.
• Highlight the open challenges that hinder the utility internet of things in smart home.
• Recommendations lists to improve the acceptance of used the internet of Things in smart home in the literature.