Journal of Network and Computer Applications 97 (2017) 48–65

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

A review of smart home applications based on Internet of Things

Mussab Alaa[b], A.A. Zaidan[a,b,*], B.B. Zaidan[a,b], Mohammed Talal[b], M.L.M. Kiah[b]

[a] Department of Computing, Faculty of Arts, Computing and Creative Industry, Universiti Pendidikan Sultan Idris, Malaysia
[b] Security Lab, Wisma R & D, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia

ARTICLE INFO

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

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.

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 (Gaikwad et al., 2015; Samuel, 2016). 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 (Kim et al., 2015). 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 (Galinina et al., 2015).

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.

* Corresponding author at: Department of Computing, Faculty of Arts, Computing and Creative Industry, Universiti Pendidikan Sultan Idris, Malaysia
E-mail address: aws.alaa@gmail.com (A.A. Zaidan).

http://dx.doi.org/10.1016/j.jnca.2017.08.017
Received 19 February 2017; Received in revised form 23 July 2017; Accepted 25 August 2017
Available online 03 September 2017
1084-8045/

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 1798 papers: 105 from the WoS database, 268 from ScienceDirect, and 1425 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 1753 papers were duplicates. After scanning the titles and abstracts, 1387 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 Fig. 2 was used to review the main streams of research focusing on IoT and their general

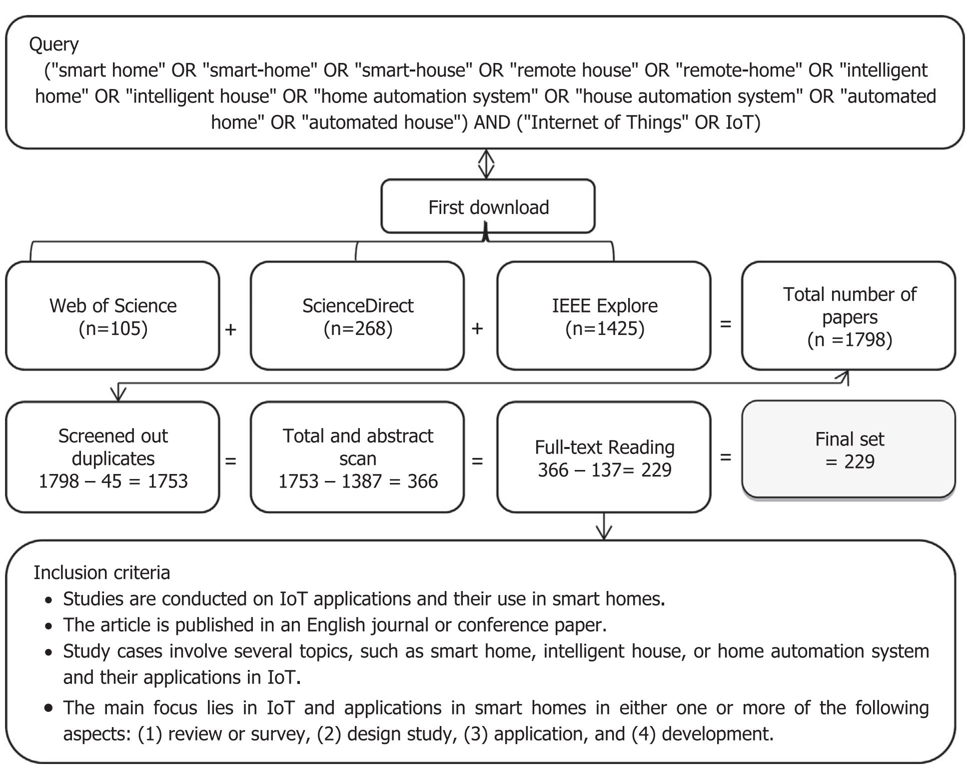

Fig. 1. Flowchart of study selection, including search query and inclusion criteria.

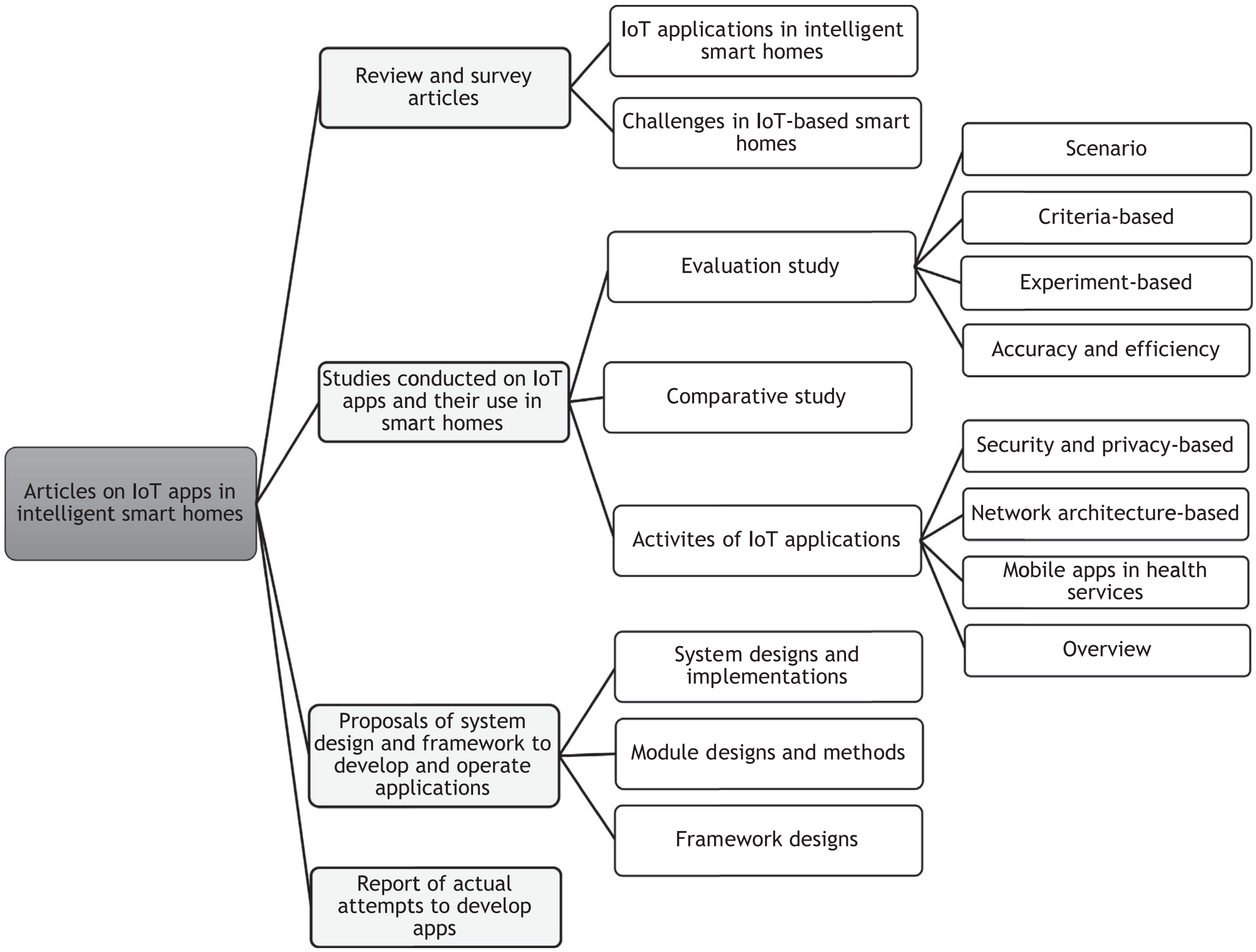

Fig. 2. Taxonomy of literature on IoT-based smart home applications.

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 (Gaikwad et al., 2015; Moser et al., 2014). The last study provides a review of the challenges in IoT smart homes (Samuel, 2016), 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 (Kirkham et al., 2014), energy consumption based on photovoltaic systems in smart homes (Yao et al., 2015; Khan et al., 2016; Kim et al., 2015; Cabras et al., 2015), data management in smart home devices (Ganz et al., 2015; Ma et al., 2015), and the performance and applications of Wi-Fi and ZigBee devices (ZigBee is wireless technology designed for personal area networks) in smart homes (Han et al., 2012). Evaluation is a trust management protocol for smart home systems (Addo et al., 2014). User experience, such as the proper use of smart home devices (Seo et al., 2016; Mehrabani, 2015); Bluetooth devices, which reduce energy consumption in smart homes (Collotta and Pau, 2015); and body sensor networks in smart homes to monitor the activities of the elderly (Chen et al., 2015) are evaluated. Other works assess remote control systems for smart home devices (Lee et al.,) and the use of fingerprints in indoor localization systems in smart homes (Kanaris et al., 2016). Other related works focus on the evaluation of Bluetooth applications in smart home systems based on IoT (Gentili et al., 2016). Electronic appliances in homes are also evaluated to determine the efficiency and accuracy of their energy consumption (Chen et al., 2013). 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 (Galinina et al., 2015). The performance of the novel architecture of IOT implemented using radio frequency identification in smart homes is also evaluated (Atishay and Ashish, 2011). In another work, selection criteria are used to evaluate the challenges and integration of

IoT and cloud computing paradigms in smart homes (Magruk, 2015).

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 (Alohali et al., 2014; Huth et al., 2015; Yoshigoe et al., 2015; Jacobsson et al., 2014; Greensmith, 2015; Rahman and Shah, 2016; Han et al., 2015), secure data management in various devices (Fisher and Hancke, 2014), security enhancement in smart home systems and applications (Sundaram et al., 2015; You-guo and Ming-fu, 2011; Sivaraman et al., 2015), and network system security and privacy control for home intelligence and IoT devices (Sanchez et al., 2014). Other works discuss secure healthcare architecture (Moosavi et al., 2015) 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 (Bergmann et al., 2012), as well as security challenges between heterogeneous devices and different applications in smart homes (Arabo, 2015; Lee et al., 2014; Matharu et al., 2014). Some studies focus on password security and applications for IoT smart home systems (Shivraj et al., 2015; Witkovski et al., 2015), secure software updates in smart home devices (Huth and Duplys, 2016), and security system devices (e.g., surveillance cameras) and their use in smart homes (Rajiv et al., 2016). Home automation and security threats are also defined (Schiefer, 2015). A new solution is presented to address risk reduction in cases of privacy breaches in smart energy management systems (Ukil et al., 2015). Another work discusses the research and implementation of machine-to-machine technology in smart homes and security systems (Jiang et al., 2015).

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 (Li et al., 2016; Wang and Xu, 2013; Waltari and Kangasharju, 2016; Kasnesis et al., 2015) and home automation gateways and applications (Hosek et al., 2014; Lin, 2015). 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 (Kim and Lee, 2015). A study presents the application of ubiquitous networks in the smart home domain (Möller and Vakilzadian, 2014). Smart home applications and solutions over content-centric networks are also presented (Srivastava et al., 2014). Other studies conduct experimentation using a combination of smart home sensors in a network architecture (Trinchero et al., 2011).

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 (Wright et al., 2015; Le Vinh et al., 2015; Yunge et al., 2015) and Android mobile apps in smart homes for managing various aspects of the lives of the elderly and people with disabilities (Mainetti et al., 2014). Other works are classified under a small category of mobile management studies related to health systems in IoT-based smart homes (Puustjärvi and Puustjärvi, 2015; Miori and Russo, 2012; Yang et al., 2014). Control smart home systems and apps for the elderly and people with disabilities are also presented (Tang et al., 2015). Medical reminder and monitoring system apps are explored for use by elderly people in smart homes (Zanjal and Talmale, 2016).

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 (Yin et al., 2015). 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 (Lee et al., 2014). An IoT-based device control system for intelligent homes is proposed (Wang et al., 2013). Actual data are tested to assess the performance of multi-control center household appliances (Liu et al., 2015). IoT with motion sensing is utilized in smart homes (Tseng et al., 2014). Training procedures are established for control smart home systems and applications based on IoT technology (Dovydaitis et al., 2015). IoT software and applications of smart home systems are built (Sivieri et al., 2016). Complex processing for IoT and its use in smart homes are described (Chen et al., 2014). Communication and collaboration are established between persons and devices, e.g., users send SMS to IOT-based smart homes (Su et al., 2012). Large data are managed with network architecture in IoT in smart homes (Sun et al., 2014). General applications and their implementation in smart homes are described (Madakam and Ramaswamy, 2014). Different user activities and applications in IoT-based smart home systems are presented (Bourobou and Yoo, 2015). Smart home applications based on an IoT management platform are also described (Elkhodr et al., 2015). Smart home applications and architectures based on resource name services are established to control smart home devices (Yang et al., 2014). Challenges in the design of overall smart home systems are described (Biswas et al., 2011).

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 (Son et al., 2016).

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 (Jacobsson et al., 2016; Tian et al., 2015; Peng et al., 2015; Cebrat, 2014; Oriwoh and Sant, 2013) and secured multimedia authentication systems for wireless sensor network data related to IoT in smart homes (Suryadevara et al., 2013). Distributed malware attacks against IoT in smart homes are evaluated (Min and Varadharajan, 2015). Secure Kerberos authentication is designed for home automation systems based on IoT (Gaikwad et al., 2015). A security mechanism of a terminal gateway group system (Yuan and Peng, 2012) and a control system with multiple functions in smart homes are designed (Lin et al., 2015; Jiang et al., 2016; Han and Zhao, 2014; Ye et al., 2012; Pavithra and Balakrishnan, 2015). Smart home control systems based on General Packet Radio Service and ZigBee are established (Zhang et al., 2015). Home automation wireless power control based on IoT (Qi and Bai, 2014) and an energy management system to reduce energy consumption in smart houses are designed (Schweizer et al., 2015; Wang et al., 2012; Bhilare and Mali, 2015; Li, 2013; Yang et al., 2013). A system is designed to provide recommendations for users when they detect energy wastage (Lima et al., 2015). A ZigBee wireless device is designed and implemented to avoid energy wastage in smart homes (Fernández-Caramés, 2015). Sockets are designed based on intelligent control and energy management (Feng et al.,). A ZigBee-based system is designed and implemented to manage power consumption (Yongqing and Dan, 2013). A modern healthcare system facility and an elderly caring system for smart homes are designed (Zhang et al., 2012a, 2012b). A healthcare system with mobile sensing and network analytics support is developed (Kan et al., 2015). A wireless sensor network is designed and installed in smart homes (Fu et al., 2013; Lin et al., 2013; Salihbegovic et al., 2015; Ghayvat et al., 2015). A minimalistic system for smart homes is developed using three modules: a home gateway, a cloud server, and a user interface (Pang et al., 2014). Devices with machine-to-machine integration for smart home systems are designed and implemented (Jalali, 2013; Lu, 2015). IoT-based media content sharing services in home automation (Hu et al., 2013) and smart house gateways for social Web of Things are designed and implemented (Chung et al., 2014; Guoqiang et al., 2013). A system and the application of low-cost smart homes under IoT systems and cloud computing are designed (Wei and Qin, 2013). In another work, a wireless intelligent light control system based on ZigBee light link is developed (Wang et al., 2013). Home automation based on ZigBee wireless sensor networks is designed and implemented (Chunlong et al., 2012) along with an IoT access point for home automation (Chang et al., 2015). A design solution involving embedded uninterruptible power supply (UPS) is used for long-distance monitoring and control of UPS based on an IoT network (Zhang et al., 2012a, 2012b). A smart home system based on a Wi-Fi network is designed and implemented (Santoso and Vun, 2015). A system is developed to derive and manage data transmission for home devices (Park et al., 2014; Wu et al., 2013). A smart home control system is designed to manage data transmission between devices (Shi et al., 2014). 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 (Liu and Guo, 2015). A smart home system and applications based on IoT are designed and developed (Li and Yu, 2011; Gao and Wei, 2014; Du and Wang, 2012; Kim et al., 2014; Lazarevic et al., 2015) along with a smart home system for complex applications (Xiao et al., 2015; Wang, 2014; Hu et al., 2016; Soliman et al., 2013; Chong et al., 2011). An IoT-based home automation system is designed (Bing et al., 2011). A smart home architecture (Prakash et al., 2015), system for home automation management (Perešíni and Krajčovič, 2015), 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 keys (Huynh et al., 2014). A system based on IoT home and ZigBee/Global Positioning System technology is designed and adopted (Wang, 2013). ZigBee devices are developed and implemented in smart homes (Moravcevic et al., 2015). An architecture and implementation system is designed to support smart home services and applications based on IoT (Wang et al., 2013). A Domain Name System name autoconfiguration for IoT in smart homes (Lee et al., 2016) and a gas detector position computer system based on ARM (a powered intelligent home security system and monitoring system) are developed (Shi et al., 2013). A system based on IoT services is developed and implemented in support of users (Kim et al., 2014). Raspberry Pi, as a sensor web node for smart home systems (Vujović and Maksimović, 2015), and a smart house power management system are designed and implemented based on a human–computer interaction model (Zhao et al., 2013). A ZigBee device-based smart home monitoring system is developed and installed (Yiqi et al., 2014). A software ecosystem that allows users with different skills to develop location-aware services to autonomously manage smart homes is designed and implemented (Mainetti et al., 2015). A Bluetooth system is developed and applied in IoT-based smart homes (Zhao, 2013). Hardware and software solutions for communication techniques are used for the initial configuration of embedded devices (Brzoza-Woch and Szydlo, 2015). The distance between IoT devices and mobile devices is measured using Bluetooth with improved accuracy (Cho et al., 2015). A smart home energy management system is designed and its applications are assessed (Shamszaman et al., 2014; Lee et al., 2016). A design prediction device is developed to identify solutions to problems in IOT-based smart homes (Bhide and Wagh, 2015). An IoT-based smart home system is designed for the provision of services (Lee et al., 2015). Techniques that enable smart human device interfaces and an appliance usage prediction engine to aid home automation systems are designed (Bhole et al., 2015). A mobile robot for an old-age-compliant smart home environment is designed to fulfill the needs of elderly people (Schwiegelshohn et al., 2015).

3.3.2. Module designs and methods

Privacy and security are modeled for smart homes (Jacobsson and Davidsson, 2015). An IoT management model and methods based on Web of Objects for home data mining are described (Kim et al., 2015). A model life cycle tracking system for LED bulbs of home automation devices is proposed (Pandey et al., 2015). 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 (Cheuque et al., 2015). A method enabling the “brand-free plug-n-play” deployment of smart devices is integrated, tested, and validated in home automation systems using BLE (Papp et al., 2015). A modular smart home is designed and implemented using a wireless network (Hasibuan et al., 2015). An IoT-centralized management model for smart homes is developed (Yin et al., 2015). A mobile smart home model is designed and applied (Bao et al., 2014). A model based on a basic mathematical approach is developed and applied to describe the success of human interactions in smart home applications (Gechev et al., 2014). An IoT network model for smart homes is proposed (Jung et al., 2015). A module in IoT smart homes is designed and implemented (Liu et al., 2015). A smart home based on IoT technology is designed and simulated (Song et al., 2012). Electrical models are developed to deal with the humanized interaction between humans and computers in smart homes (Du et al., 2013).

3.3.3. Framework designs

A web-based application framework for smart homes is designed (Kamilaris and Pitsillides, 2013). A framework architecture for smart homes is developed (Neisse et al., 2015). BlinkToSCoAP, an IoT security management framework for IoT devices in smart homes, is developed as a security framework architecture (Peretti et al., 2015). A framework is designed to manage energy consumption and IoT devices in smart homes (Huang et al., 2014). A home automation framework is developed (Miclaus et al., 2014). A framework for managing the energy efficiency of smart homes is designed (Kibria and Chong, 2014). A cognitive management framework is developed for IoT in smart homes (Sasidharan et al., 2014). A framework for cloud-based smart homes is proposed (Ye and Huang, 2011). A framework is designed to develop a home automation system (Pham-Huu et al., 2015). A middleware

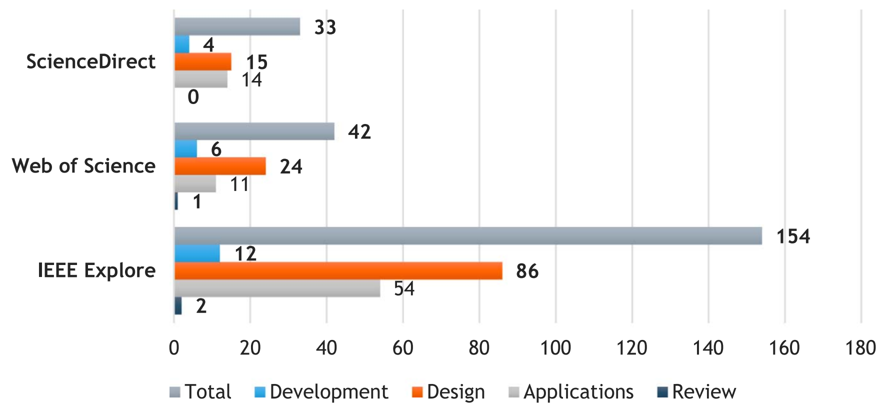

Fig. 3. Number of included articles in different categories according to publication journals.

framework for sensor nodes is developed to achieve network virtualization in smart homes (Khalid et al., 2014). A visual programming framework is designed for wireless sensor networks in house intelligence applications (Serna et al., 2015). A gateway software framework for heterogeneous networks in smart home applications is designed (Xie et al., 2011). A general framework is developed to solve the security requirements of a cloud–IoT paradigm and applied to remote mobile medical monitoring (Ren et al., 2015). An IoT service framework is designed for smart homes (Li et al., 2015). A controller application communication framework for smart homes is described (Konstantinidis et al., 2015). A framework for sharing data with multiple systems in smart homes is developed (Jagatheesan et al., 2015). A designed framework is aimed at creating a complete software tool chain to tackle integration issues for IoT in smart homes in general (Su et al., 2011). A conceptual framework for a smart home system is designed (Hu et al., 2011). An overall system architecture is illustrated based on the layer framework of IoT (Hu et al., 2013). An information-centric networking framework is tailored to the smart home domain (Amadeo et al., 2015). A smart home service framework is designed and applied (Li et al., 2013). A framework called eDomus, which is based on social networks such as Facebook, is designed to allow users to interact remotely with home networks (Briante et al., 2014). A framework for smart home automation is designed (Thiyagarajan and Raveendra, 2015). 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 (Stusek et al., 2015). An IoT device management framework for smart home scenarios is designed (Perumal et al., 2015). A smart home system framework is developed and implemented (Yan et al., 2014). A modeling framework for smart environments is designed (Zhao et al., 2014). A theoretical framework is presented in a previous study (Mital et al., 2016). A developed framework can be used for IoT-based smart home systems (Datta, 2016). A management framework is designed and implemented in smart home systems (Kelaidonis et al., 2012). A communication framework that leverages the information-centric networking paradigm for local machine-to-machine communications is designed (Amadeo et al., 2016). 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 (Khalid et al., 2014).

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 (Zhou et al., 2013), IoT technology-based smart home services (Kang et al., 2015), and low-cost systems for smart home appliances. A developed system takes information from devices and posts it to Twitter (Lloret et al., 2012). Other home systems are also developed on the basis of IoT technologies (Jie et al., 2013). Other studies develop IoT applications on the basis of smart home technology (Hernández and Reiff-Marganiec, 2015; Wang and Zheng, 2014; Mao et al., 2013; Patel and Cassou, 2015), a network monitoring system for mobile devices in smart homes (Kovac et al., 2015), and system applications in voice-controlled multifunctional smart home systems (Mittal et al., 2015). An intelligent energy management system with approaches for IoT applications in smart homes is also developed (Yang et al., 2015). Sensor network architectures in smart homes based on IoT technology are established (Sezer et al., 2015). A smart energy monitoring system in IoT-based smart homes is developed (Cho et al., 2016). A novel smart home application is developed on the basis of an architecture and middleware of IoT technologies (Souza and Amazonas, 2013). Some works develop a smart gateway architecture to improve smart home network applications based on IoT (Ding et al., 2016), IoT technology for wireless sensor networks and systems for monitoring temperature (Shah and Mishra, 2016), and IoT technologies for enhancing health smart home systems (Mano et al., 2016). Security and privacy features are developed for IoT devices (Wurm et al., 2016), and security issues and corresponding solutions for sensor networks in smart homes are explored (Li et al., 2012). Some studies discuss the development of innovative products and entirely new services in smart home technology based on IoT (Yun et al., 2015) and emergency alert systems based on Internet Protocol television platforms in smart homes (Truong Cong et al., 2011). Energy monitoring systems based on ZigBee devices are developed for smart homes to reduce energy consumption (Bian et al., 2011).

4. Distribution results

Fig. 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.

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

Fig. 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.

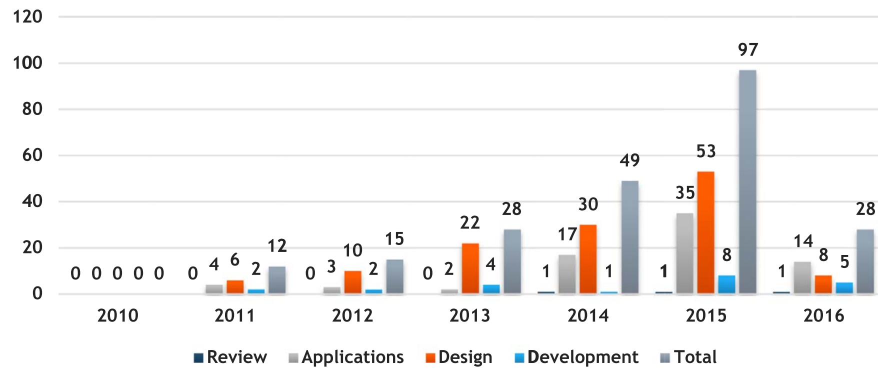

Fig. 4. Number of included articles in different categories by year of publication.

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

Fig. 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.

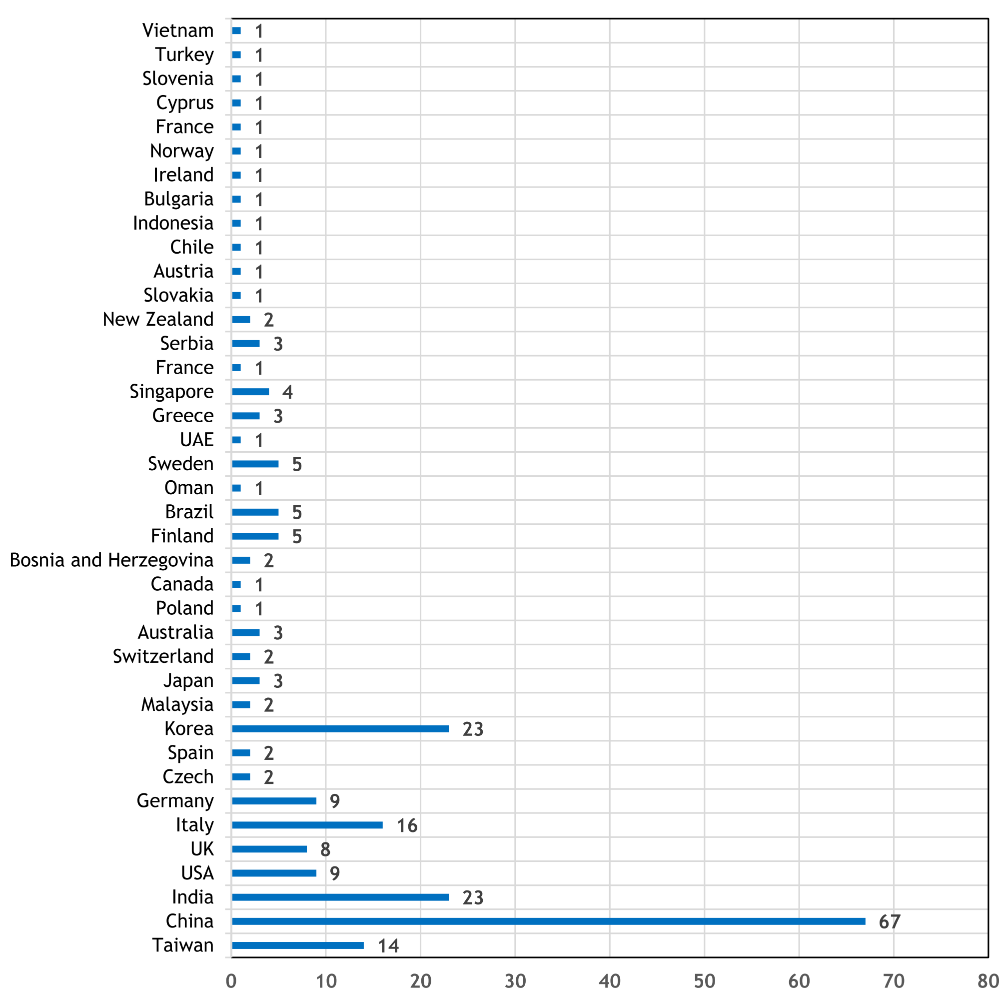

Fig. 5. Distribution by authors' nationality.

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 (Fig. 6).

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. 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. 7).

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 (Srivastava et al., 2014; Yin et al., 2015; Jiang et al., 2016; Lima et al., 2015; Kibria and Chong, 2014). For example, smart home lighting systems provide automated lighting control through LED lights. These systems automate the action of turning lights on and off (Lee et al., 2014). 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 (Huang et al., 2014; Fernández-Caramés, 2015). Lights of IoT devices in smart homes automatically shut off when residents vacate rooms or leave their homes to minimize energy consumption (Moser et al., 2014; Möller and Vakilzadian, 2014; Tian et al., 2015; Schweizer et al., 2015). 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 (Ye and Huang, 2011). Conserving energy in smart homes while improving the lifestyle of residents is an important issue (Wang et al., 2012). Residents in smart homes use mobile applications to maintain consumer energy usage for monetary savings (Wright et al., 2015; Kim et al., 2014; Shamszaman et al., 2014) and reduce expenses (Bian et al., 2011). 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 (Chen et al., 2014). An energy system is developed to conserve energy without the intervention of residents (Li et al., 2015). System security is crucial in energy conservation because the lack of security causes significant energy loss (Cebrat, 2014). Wireless technology is a potential energy-conserving technology (Galinina et al., 2015; Collotta and Pau, 2015; Pham-Huu et al., 2015).

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 (Chen et al., 2015; Liu and Guo, 2015). 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 (Bing et al., 2011). Robotic devices in smart homes assist the elderly and people with disabilities for them to achieve long and healthy lives (Sanchez et al., 2014; Lee et al., 2014; Kan et al., 2015; Wu et al., 2013; Schwiegelshohn et al., 2015; Khalid et al., 2014; Konstantinidis et al., 2015). 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 (Khan et al., 2016; Addo et al., 2014; Puustjärvi and Puustjärvi, 2015). Smart homes for the elderly anticipate their needs without direct human intervention (Miori and Russo, 2012; Lloret et al., 2012). They help the elderly check whether they are following their specific treatments, including taking their prescribed medicine on time (Yang et al., 2014; Hu et al., 2013). The population of elderly and people with disabilities in Singapore has significantly increased, thus intensifying the demand for caregivers and domestic helpers (Tang et al., 2015). The elderly need supervised monitoring for them to take their medicines on time; thus, smart homes can prove useful (Zanjal and Talmale, 2016). 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 (Mano et al., 2016; Bao et al., 2014). In a smart home, medical staffers monitor environmental conditions inside the home using CCTV for the elderly (Zhang et al., 2012a, 2012b; Kelaidonis et al., 2012). Mobile robots in smart homes specialize in fulfilling the needs of the elderly and people with disabilities (Schwiegelshohn et al., 2015).

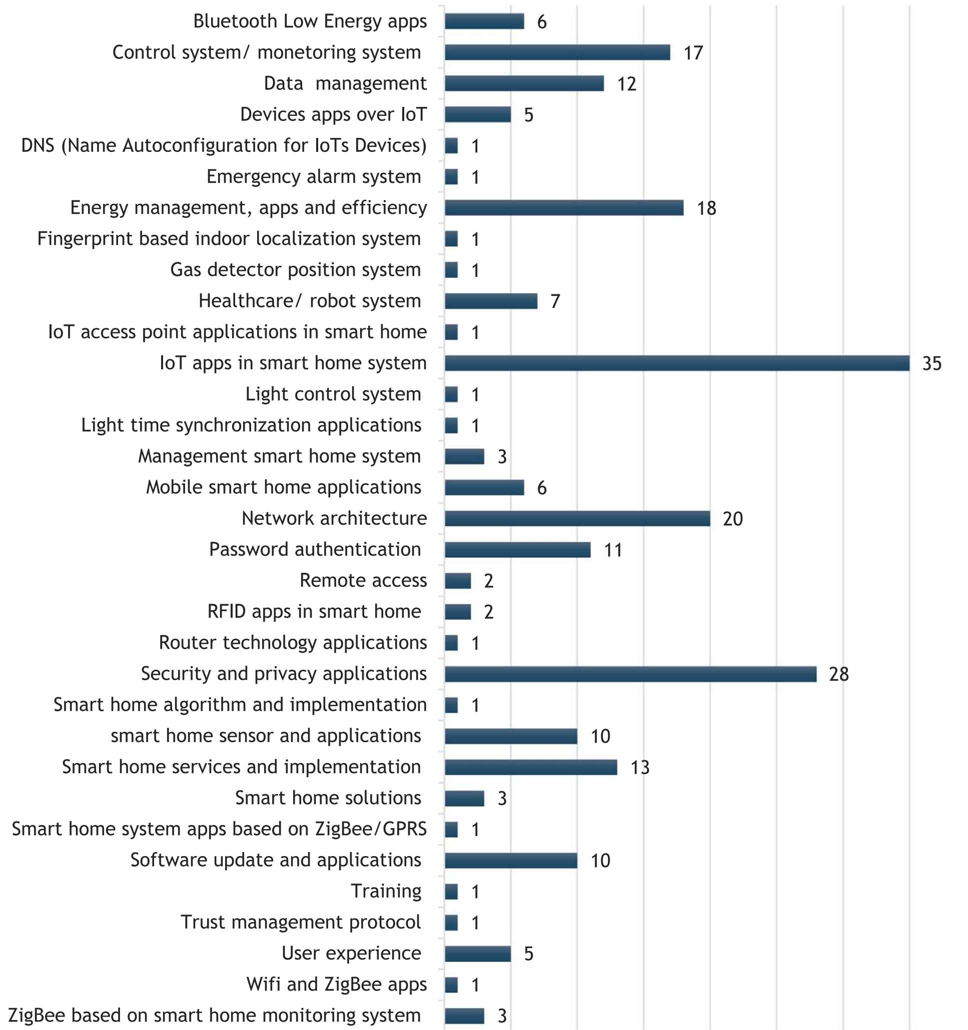

Fig. 6. Number of articles on smart home applications based on IoT.

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 (Moser et al., 2014). 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 (Puustjärvi and Puustjärvi, 2015). Wireless network technology in smart homes is adopted instead of wired systems to increase flexibility and liquidity and reduce cost and energy (Jiang et al., 2015; Lloret et al., 2012; Wang, 2013). Energy conservation in smart homes reduces costs (Yao et al., 2015; Cabras et al., 2015; Wright et al., 2015; Son et al., 2016; Kim et al., 2014; Huang et al., 2014). 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 (Trinchero et al., 2011). IoT in connected healthcare networks reduces the frequency of doctor visits, thereby reducing medical costs for the elderly and people with disabilities (Fisher and Hancke, 2014; Yang et al., 2014; Khalid et al., 2014). Adopting IoT in smart home applications significantly reduces cost (Rajiv et al., 2016). The proper behavior of residents is also known to conserve money and energy (Shamszaman et al., 2014).

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 (Moser et al., 2014; Mehrabani, 2015; Alohali et al., 2014; Lee et al., 2014; Trinchero et al., 2011; Puustjärvi and Puustjärvi, 2015; Wang et al., 2013; Tseng et al., 2014; Dovydaitis et al., 2015; Madakam and Ramaswamy, 2014; Bourobou and Yoo, 2015; Du and Wang, 2012; Ye and Huang, 2011). All these devices are equipped with sensors with different functions and wireless communication tools based on IoT technology (Jalali, 2013; Bhide and Wagh, 2015). For example, when residents leave their smart homes, the devices inside their homes automatically turn off (Ye and Huang, 2011). Residents can also conveniently pay their bills (Yao et al., 2015). Mobile devices are suitable for residents in smart homes (Tang et al., 2015), and residents can use these devices instead of a physical key. Smart homes can be controlled using mobile devices (Schiefer, 2015) or through remote control (Kirkham et al., 2014; Lee et al., ; Mainetti et al., 2014; Pandey et al., 2015).

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. 8).

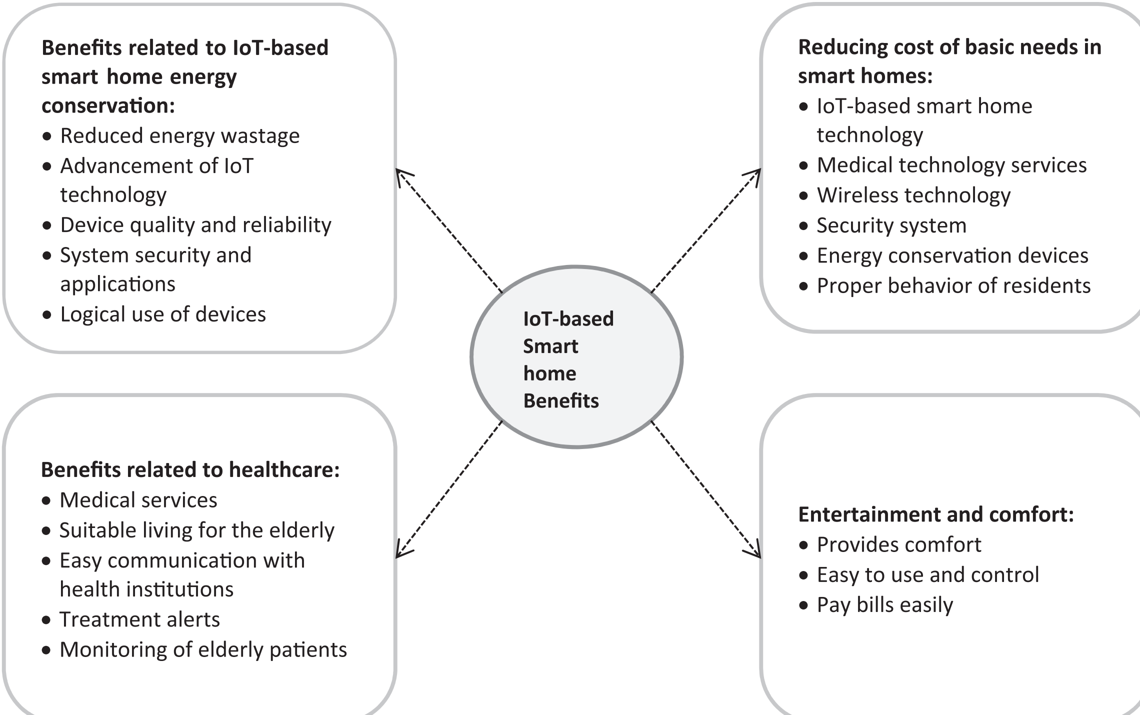

Fig. 7. Categories of benefits of smart home applications based on IoT.

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 (Kirkham et al., 2014; Jacobsson et al., 2016; Feng et al., ; Konstantinidis et al., 2015). The flow of large amounts of data and complex control impose a significant burden on home automation systems (Kim et al., 2015; Rahman and Shah, 2016; Fisher and

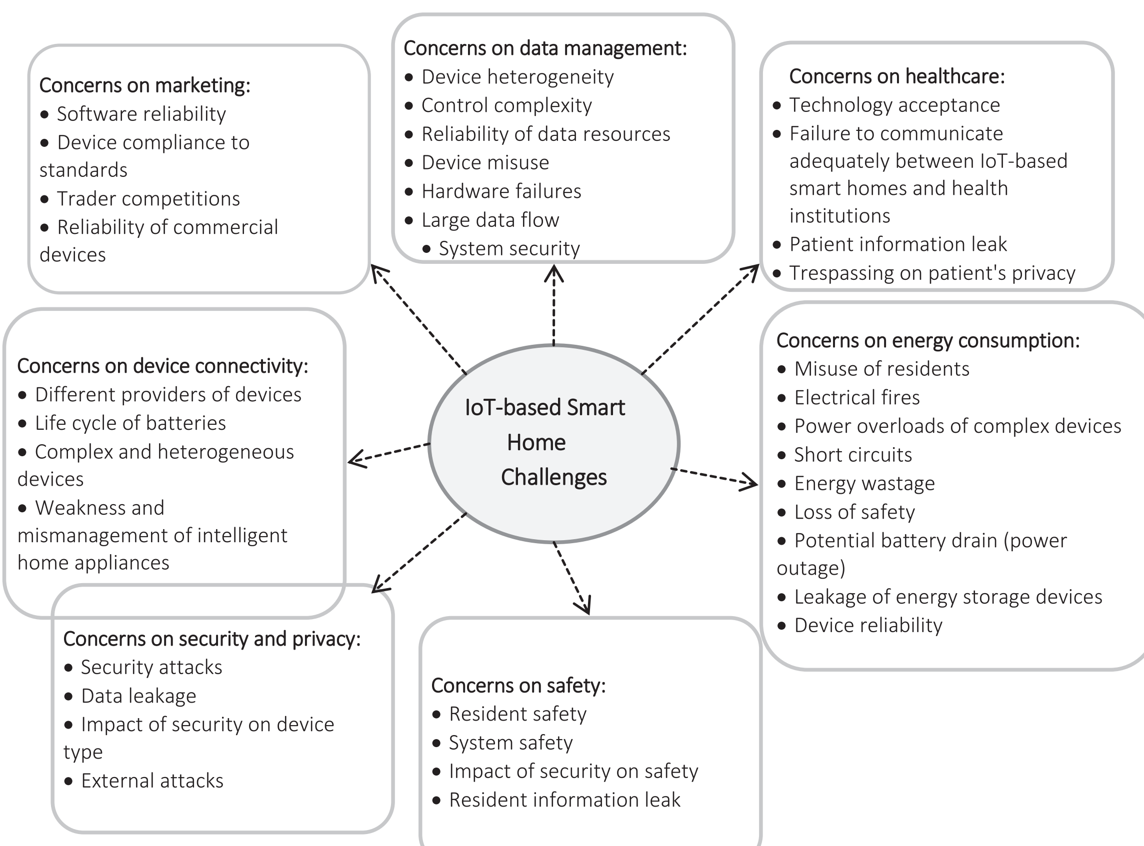

Fig. 8. Categories of challenges for smart home applications based on IoT.

Hancke, 2014; Sivaraman et al., 2015; Sanchez et al., 2014; Matharu et al., 2014; Chen et al., 2014; Cebrat, 2014; Schwiegelshohn et al., 2015; Ye and Huang, 2011; Li et al., 2015). 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 (Arabo, 2015). 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 (Waltari and Kangasharju, 2016; Neisse et al., 2015). The following data-related problems occur in smart home devices. Stored information in databases is sometimes unstructured (Sun et al., 2014). 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% (Han et al., 2012; Sezer et al., 2015; Ding et al., 2016; Ghayvat et al., 2015; Shi et al., 2014; Bing et al., 2011). The absence of security systems puts data at risk via the connection of smart home devices (Souza and Amazonas, 2013; Jalali, 2013; Jacobsson and Davidsson, 2015; Xie et al., 2011; Yoshigoe et al., 2015; Elkhodr et al., 2015). 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 (Ganz et al., 2015; Bergmann et al., 2012; Suryadevara et al., 2013; Xiao et al., 2015; Song et al., 2012). 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 (Li et al., 2012).

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 (Jacobsson et al., 2016). Various device managers for smart homes are not appropriate and efficient (Kirkham et al., 2014; Schiefer, 2015; Bhide and Wagh, 2015). 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 (Arabo, 2015). Although the concept of smart homes is well known in the market, these technologies are expensive (Chong et al., 2011). 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 (Bhide and Wagh, 2015). 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 (Sivaraman et al., 2015). 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 (Papp et al., 2015). 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 (Addo et al., 2014).

5.2.3. Concerns on device connectivity

Communication problems occur among various devices from manufacturers or companies that adopt different techniques and standards (Samuel, 2016). Communication problems among devices in smart homes also exist because these devices use different sensors and networking gadgets from various manufacturers (Moser et al., 2014). Some devices in smart homes cannot be used and are unprotected by security systems; thus, these devices sometimes damage smart home systems (Addo et al., 2014; Alohali et al., 2014; Yoshigoe et al., 2015; Greensmith, 2015; Sivaraman et al., 2015; Arabo, 2015; Lee et al., 2014; Matharu et al., 2014; Jiang et al., 2015). 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 (Sanchez et al., 2014). Some devices in smart homes depend on batteries; poor battery performance causes communication problems among these devices (Rahman and Shah, 2016). 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 (Chen et al., 2014). One of the most significant challenges in using complex heterogeneous devices is the dynamic environment in smart home technology (Galinina et al., 2015; Ganz et al., 2015; Mainetti et al., 2014; Shamszaman et al., 2014). 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 one another, generating a large amount of traffic (Waltari and Kangasharju, 2016; Kim and Lee, 2015; Li and Yu, 2011; Lee et al., 2016). The heterogeneity problem of devices and identifiers leads to poor compatibility in smart home systems (Yang et al., 2014). 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 (Kirkham et al., 2014). 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 (Elkhodr et al., 2015). 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 (Kirkham et al., 2014; Jacobsson et al., 2014, 2016; Lee et al., 2014; Suryadevara et al., 2013;

Yuan and Peng, 2012; Brzoza-Woch and Szydlo, 2015; Ye and Huang, 2011; Xie et al., 2011). The security of an entire smart home depends heavily on security systems; failures in a security system can cause a house to malfunction (Min and Varadharajan, 2015; Vujović and Maksimović, 2015). 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 (Arabo, 2015). 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 (Magruk, 2015). 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 (Huth et al., 2015; Fisher and Hancke, 2014; Matharu et al., 2014). 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 (Rajiv et al., 2016). 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 (Gaikwad et al., 2015; Cebrat, 2014; Neisse et al., 2015). Some attackers manipulate data in smart homes; thus, security systems are crucial to protect data and patient information (Moosavi et al., 2015). 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 (Schiefer, 2015; Oriwoh and Sant, 2013). 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 (Chen et al., 2014). 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 (Shivraj et al., 2015). 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 (Yunge et al., 2015). Data leakage causes various problems in smart homes. Thus, security vulnerability must be considered in an IoT environment (Han et al., 2015). 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 (Yoshigoe et al., 2015). 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 (Bao et al., 2014). 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 (Li et al., 2012).

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 (Mano et al., 2016). 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 (Neisse et al., 2015). 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 (Fernández-Caramés, 2015). Security problems increase with the emergence of IoT. The lack of security reduces safety (Elkhodr et al., 2015; Jie et al., 2013; Yuan and Peng, 2012). 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 (Hu et al., 2013). Smart homes are never safe from attackers. Smoke detectors, intrusion detection devices, security cameras, and smart door locks are examples of security devices (Lee et al., 2014). Safety systems are crucial to protect patient data from strangers (Khalid et al., 2014). Unreliable and unauthorized devices must be avoided because they are unsafe, and user access should not be allowed (Han et al., 2015). As residents do not always occupy their homes, they cannot constantly monitor their smart homes (Pandey et al., 2015). 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 (Yin et al., 2015). 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 (Wurm et al., 2016). 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 (Bao et al., 2014). 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 (Li et al., 2012). 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 (Vujović and Maksimović, 2015). 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 (Truong Cong et al., 2011). 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 (Hu et al., 2013).

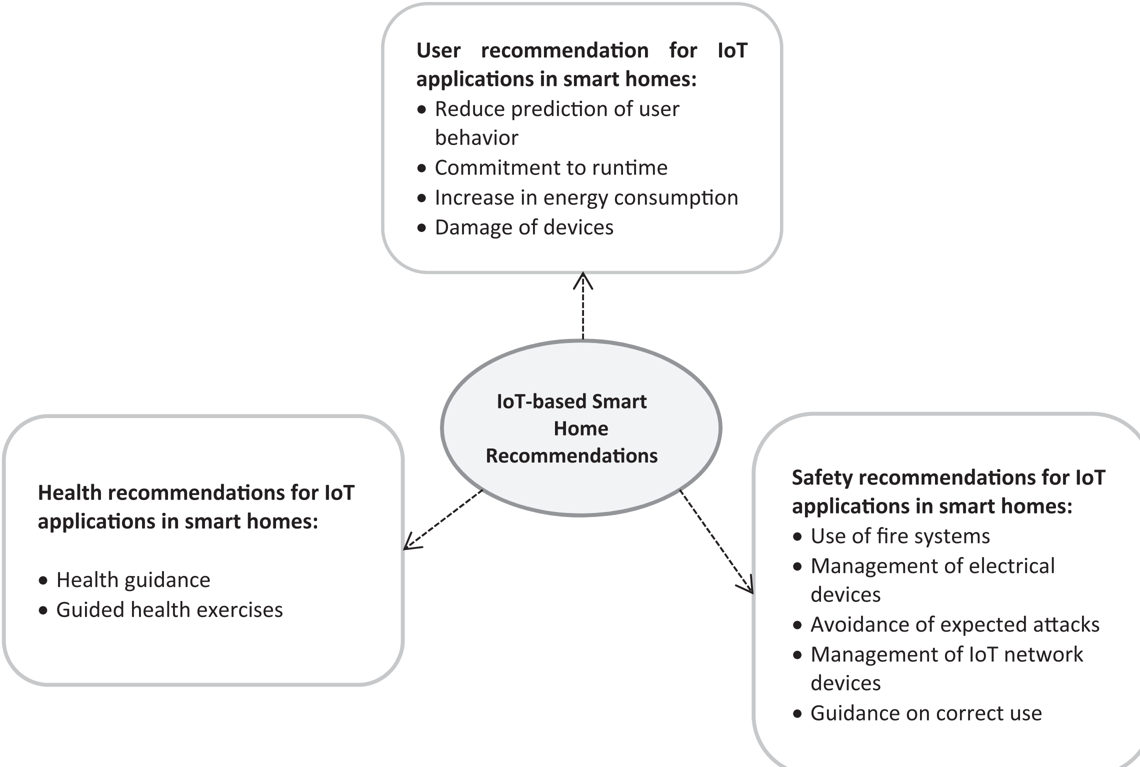

Fig. 9. Categories of recommendations for IoT applications in smart homes.

5.2.6. Concerns on energy consumption

An important concern is that users may cause problems in energy consumption (Moser et al., 2014). 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 (Jacobsson et al., 2014, 2016; Matharu et al., 2014; Ukil et al., 2015; Elkhodr et al., 2015; Jacobsson and Davidsson, 2015; Peretti et al., 2015). 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 mismanagement 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 (Kirkham et al., 2014; Schiefer, 2015; Wright et al., 2015; Sivieri et al., 2016; Zhou et al., 2013; Bhilare and Mali, 2015; Li, 2013; Chang et al., 2015). 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 (Fernández-Caramés, 2015). In home automation, the gateway architecture of networking equipment requires constant work, which equates to significant energy consumption (Bian et al., 2011). 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 (Lee et al., 2014; Hosek et al., 2014; Chen et al., 2014; Wang et al., 2012). In some instances, users may forget to turn off some of the electrical devices in their smart homes, resulting increased energy consumption (Kamilaris and Pitsillides, 2013). 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 (Galinina et al., 2015).

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 (Yang et al., 2014). 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 (Khalid et al., 2014). 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. 9).

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 (Bian et al., 2011). 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 (Ukil et al., 2015; Yongqing and Dan, 2013). A system presents recommendations for users to reduce energy consumption (Lima et al., 2015). A system provides recommendations for mobile users when an intruder is detected (Bao et al., 2014). Users are recommended to reduce their energy consumption (Schweizer et al., 2015). 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 (Kim and Lee, 2015).

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 (Konstantinidis et al., 2015). Recommendations are given to patients in smart homes, including medical guidelines, patient diagnoses, and assistance for the elderly and people with disabilities (Wang and Xu, 2013).

5.3.3. Safety recommendations

Instructions on how fire systems and electrical devices are utilized and managed in smart homes are provided (Kelaidonis et al., 2012). 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 (Kim and Lee, 2015). 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 (Han et al., 2015). 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 (Yoshigoe et al., 2015; Moosavi et al., 2015). 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 (Bhole et al., 2015).

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

Addo, I.D., Yang, J.-J., Ahamed, S.I., 2014. SPTP: a trust management protocol for online and ubiquitous systems. In: Proceedings of 38th Annual Computer Software and Applications Conference (COMPSAC), IEEE.

Alohali, B., Merabti, M., Kifayat, K., 2014. A secure scheme for a smart house based on Cloud of Things (CoT). In: Proceedings of Computer Science and Electronic Engineering Conference (CEEC), 6th. IEEE.

Amadeo, M., et al., 2016. Information-centric networking for M2M communications: design and deployment. Comput. Commun..

Amadeo, M., et al., 2015. Information Centric Networking in IoT scenarios: The case of a smart home. In: Proceedings of IEEE International Conference on Communications (ICC), IEEE.

Arabo, A., 2015. Cyber security challenges within the connected home ecosystem futures. Procedia Comput. Sci. 61, 227–232.

Atishay, J. Ashish, T., 2011. Architecture for High Density RFID Inventory System in Internet of Things. In: Proceedings of International Conference on Computer Science and Information Technology, Springer.

Bao, H., et al., 2014. Are Chinese consumers ready to adopt mobile smart home? An empirical analysis. Int. J. Mob. Commun. 12 (5), 496–511.

Bergmann, O., et al., 2012. Secure bootstrapping of nodes in a CoAP network. In: Proceedings of Wireless Communications and Networking Conference Workshops (WCNCW), IEEE.

Bhide, V.H., Wagh, S., 2015. i-learning IoT: An intelligent self learning system for home automation using IoT. In: Proceedings of International Conference on

Communications and Signal Processing (ICCSP), IEEE.
Bhilare, R., Mali, S., 2015. IoT based smart home with real time E-metering using E-controller. In: Proceedings of Annual IEEE India Conference (INDICON), IEEE.
Bhole, M., et al., 2015. Delivering analytics services for smart homes. In: Proceedings of IEEE Conference on Wireless Sensors (ICWiSe), IEEE.
Bian, J., Fan, D., Zhang, J., 2011. The new intelligent home control system based on the dynamic and intelligent gateway. In: Proceedings of the 4th IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT).
Bing, K., et al., 2011. Design of an Internet of things-based smart home system. In: Proceedings of the 2nd International Conference on Intelligent Control and Information Processing (ICICIP), IEEE.
Biswas, J., et al., 2011. From context to micro-context–issues and challenges in sensorizing smart spaces for assistive living. Procedia Comput. Sci. 5, 288–295.
Bourobou, S.T.M., Yoo, Y., 2015. User activity recognition in smart homes using pattern clustering applied to temporal ann algorithm. Sensors 15 (5), 11953–11971.
Briante, O., et al., 2014. eDomus: User-home interactions through Facebook and Named Data Networking. In: Proceedings of the Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), IEEE.
Brzoza-Woch, R., Szydlo, T., 2015. Blinker: method for transferring initial configuration for resource-constrained embedded devices. IFAC-Pap. 48 (4), 77–82.
Cabras, M., Pilloni, V., Atzori, L., 2015. A novel smart home energy management system: Cooperative neighbourhood and adaptive renewable energy usage. In: Proceedings of IEEE International Conference on Communications (ICC), IEEE.
Cebrat, G. Secure web based home automation: Application layer based security using embedded programmable logic controller. In: Proceedings of the 2nd International Conference on Information and Communication Technology (ICoICT), IEEE.
Chang, C.-Y., et al., 2015. Design and implementation of an IoT access point for smart home. Appl. Sci. 5 (4), 1882–1903.
Chen, C.Y., et al., 2014. Complex event processing for the internet of things and its applications. In: Proceedings of IEEE International Conference on Automation Science and Engineering (CASE), IEEE.
Chen, S.-Y., et al., 2013. Intelligent home-appliance recognition over IoT cloud network. In: Proceedings of the 9th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE.
Chen, Y.-H., et al., 2015. Monitoring Elder's Living Activity Using Ambient and Body Sensor Network in Smart Home. In: Proceedings of IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE.
Cheuque, C., et al., 2015. Towards to responsive web services for smart home LED control with Raspberry Pi. A first approach. In: Proceedings of the 34th International Conference of the Chilean Computer Science Society (SCCC), IEEE.
Cho, H., et al., 2015. Measuring a distance between things with improved accuracy. Procedia Comput. Sci. 52, 1083–1088.
Cho, K., et al., 2016. Performance analysis of device discovery of Bluetooth Low Energy (BLE) networks. Comput. Commun. 81, 72–85.
Chong, G., Zhihao, L., Yifeng, Y., 2011. The research and implement of smart home system based on internet of things. In: Proceedings of International Conference on Electronics, Communications and Control (ICECC), IEEE.
Chung, T.-Y., et al. Design and implementation of light-weight smart home gateway for Social Web of Things. In: Proceedings of the Sixth International Conference on Ubiquitous and FutureNetworks (ICUFN), IEEE.
Chunlong, Z., et al., 2012. Smart home design based on ZigBee wireless sensor network. In: Proceedings of the 7th International ICST Conference on Communications and Networking in China (CHINACOM).
Collotta, M., Pau, G., 2015. Bluetooth for internet of things: a fuzzy approach to improve power management in smart homes. Comput. Electr. Eng. 44, 137–152.
Datta, S.K., 2016. Towards securing discovery services in Internet of Things. In: Proceedings of IEEE International Conference on Consumer Electronics (ICCE), IEEE.
Ding, F., et al., 2016. A smart gateway architecture for improving efficiency of home network applications. J. Sens. 2016, 10.
Dovydaitis, J., et al., 2015. Training, retraining, and self-training procedures for the fuzzy logic-based intellectualization of IoT & S environments. Int. J. Fuzzy Syst. 17 (2), 133–143.
Du, K.-K., Wang, Z.-L., Mi, H., 2013. Human machine interactive system on smart home of IoT. J. China Univ. Posts Telecommun. 20, 96–99.
Du, K., Wang, Z., 2012. The management system with emotional virtual human based on smart home. In: Proceedings of the 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), IEEE.
Elkhodr, M., Shahrestani, S., Cheung, H., 2015. A Smart Home Application based on the Internet of Things Management Platform. In: Proceedings of IEEE International Conference on Data Science and Data Intensive Systems, IEEE.
Feng, J., et al., 2015. Design of socket based on intelligent control and energy management. Int. J. Adv. Comput. Sci. Appl. 1 (6), 105–110.
Fernández-Caramés, T.M., 2015. An intelligent power outlet system for the smart home of the Internet of Things. Int. J. Distrib. Sens. Netw. 2015, 1.
Fisher, R., Hancke., G., 2014. DTLS for Lightweight Secure Data Streaming in the Internet of Things. In: Proceedings of the Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), IEEE.
Fu, Y., et al., 2013. Design of a Wireless Sensor Network Platform for Real-Time Multimedia Communication. In: Proceedings of the 2012 International Conference on Communication, Electronics and Automation Engineering, Springer.
Gaikwad, P.P., Gabhane, J.P., Golait S.S., 2015. A survey based on Smart Homes system using Internet-of-Things. In: Proceedings of International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), 2015.
Gaikwad, P.P., Gabhane, J.P., Golait, S.S., 2015. 3-level secure Kerberos authentication for Smart Home Systems using IoT. In: Proceedings of the 1st International Conference on Next Generation Computing Technologies (NGCT), IEEE.
Galinina, O., et al., 2015. Smart home gateway system over Bluetooth low energy with wireless energy transfer capability. EURASIP J. Wirel. Commun. Netw. 2015 (1), 1–18.
Ganz, F., et al., 2015. A practical evaluation of information processing and abstraction techniques for the internet of things. IEEE Internet Things J. 2 (4), 340–354.
Gao, Y.Z., Wei, L.Y., 2014. Implementation of Smart Home System Based on Internet of Things. Appl. Mech. Mater..
Gechev, M., et al., 2014. Node discovery and interpretation in unstructured resource-constrained environments. In: Proceedings of the 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), IEEE.
Gentili, M., Sannino, R., Petracca, M., 2016. BlueVoice: voice communications over bluetooth low energy in the Internet of Things scenario. Comput. Commun..
Ghayvat, H., et al., 2015. WSN-and IOT-based smart homes and their extension to smart buildings. Sensors 15 (5), 10350–10379.
Greensmith, J., 2015. Securing the Internet of Things with Responsive Artificial Immune Systems. In: Proceedings of the Annual Conference on Genetic and Evolutionary Computation, ACM.
Guoqiang, S., et al., 2013. Design and Implementation of a Smart IoT Gateway. in Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), In: Proceedings of IEEE International Conference on and IEEE Cyber, Physical and Social Computing.
Han, J.-H., Jeon, Y., Kim., J., 2015. Security considerations for secure and trustworthy smart home system in the IoT environment. In: Proceedings of International Conference on Information and Communication Technology Convergence (ICTC), IEEE.
Han, T., et al., 2012. Coexistence study for wifi and zigbee under smart home scenarios. In: Proceedings of the 3rd IEEE International Conference on Network Infrastructure and Digital Content, IEEE.
Han, X. Zhao, C., 2014. Distributing Monitor System Based on WIFI and GSM Supporting SCPI. In: Proceedings of the 13th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES), IEEE.
Hasibuan, A., et al., 2015. Design and implementation of modular home automation based on wireless network, REST API, and WebSocket. In: Proceedings of International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), IEEE.
Hernández, M.E.P.Reiff-Marganiec, S., Autonomous and self controlling smart objects for the future internet. In: Proceedings of the 3rd International Conference on Future Internet of Things and Cloud (FiCloud), IEEE.
Hosek, J., et al., 2014. M2M gateway: the centerpiece of future home. In: Proceedings of the 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), IEEE.
Hu, H., et al., 2011. Semantic web-based policy interaction detection method with rules in smart home for detecting interactions among user policies. Commun., IET 5 (17), 2451–2460.
Hu, S., et al., 2016. A distributed and efficient system architecture for smart home. Int. J. Sens. Netw. 20 (2), 119–130.
Hu, C.-L., et al., 2013. Design and Implementation of Media Content Sharing Services in Home-Based IoT Networks. In: International Conference on Parallel and Distributed Systems (ICPADS), IEEE.
Hu, S., et al., 2013. Connected intelligent home based on the internet of things. In: Proceedings of IET International Conference on Information and Communications Technologies (IETICT 2013), IET.
Huang, Z., et al., 2014. Co-locating services in IoT systems to minimize the communication energy cost. J. Innov. Digit. Ecosyst. 1 (1), 47–57.
Huth, C., Duplys, P., 2016. Secure software update and IP protection for untrusted devices in the Internet of Things via physically unclonable functions. In: Proceedings of IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), IEEE.
Huth, C., et al., 2015. Securing systems on the Internet of Things via physical properties of devices and communications. In: Proceedings of 9th Annual IEEE International Systems Conference (SysCon), IEEE.
Huynh, S.M., et al., 2014. Novel RFID and ontology based home localization system for misplaced objects. IEEE Trans. Consum. Electron. 60 (3), 402–410.
Jacobsson, A., Boldt, M., Carlsson, B., 2016. A risk analysis of a smart home automation system. Future Gener. Comput. Syst. 56, 719–733.
Jacobsson, A., Davidsson, P., 2015. Towards a model of privacy and security for smart homes. In: Proceedings of IEEE 2nd World Forum on Internet of Things (WF-IoT), . IEEE.
Jacobsson, A., Boldt, M., Carlsson, B., 2014. On the risk exposure of smart home automation systems. In: Proceedings of International Conference on International Conference on Future Internet of Things and Cloud (FiCloud), IEEE.
Jagatheesan, A., et al., 2015. Drops: A multi-producer and multi-consumer data sharing framework with human experience. In: Proceedings of the 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), IEEE.
Jalali, S., 2013. M2M solutions—Design challenges and considerations. In: Proceedings of IEEE Recent Advances in Intelligent Computational Systems (RAICS), IEEE.
Jiang, T., Yang, M., Zhang, Y., 2015. Research and implementation of M2M smart home and security system. Secur. Commun. Networks 8 (16), 2704–2711.
Jiang, Y., Liu, X., Lian, S., 2016. Design and implementation of smart-home monitoring system with the Internet of Things technology. In: Wireless Communications, Networking and Applications. Lecture Notes in Electrical Engineering 348. Springer, New Delhi, India, 473–484.
Jie, Y., et al., 2013. Smart home system based on IOT technologies. In: Proceedings of the

Fifth International Conference on Computational and Information Sciences (ICCIS), IEEE.
Jung, J., Chun, S., Lee, K.-H., 2015. Hypergraph-based overlay network model for the Internet of Things. In: Proceedings of IEEE 2nd World Forum on Internet of Things (WF-IoT), IEEE.
Kamilaris, A., Pitsillides, A., 2013. Towards interoperable and sustainable smart homes. In: Proceedings of IST-Africa Conference and Exhibition (IST-Africa), IEEE.
Kan, C., et al., 2015. Mobile sensing and network analytics for realizing smart automated systems towards health Internet of Things. In: Proceedings of IEEE International Conference on Automation Science and Engineering (CASE), IEEE.
Kanaris, L., et al., 2016. Sample Size Determination Algorithm for fingerprint-based indoor localization systems. Comput. Netw. 101, 169–177.
Kang, B., et al., 2015. IoT-based monitoring system using tri-level context making model for smart home services. In: Proceedings of IEEE International Conference on Consumer Electronics (ICCE), IEEE.
Kasnesis, P., Patrikakis, C.Z., Venieris, I.S., 2015. Collective domotic intelligence through dynamic injection of semantic rules. In: Proceedings of IEEE International Conference on Communications (ICC), IEEE.
Kelaidonis, D., et al., 2012. Virtualization and cognitive management of real world objects in the internet of things. In: Proceedings of IEEE International Conference on Green Computing and Communications (GreenCom), IEEE.
Khalid, Z., et al., 2014. Middleware framework for network virtualization in SHAAL. In: Proceedings of IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), IEEE.
Khalid, Z., et al., 2014. System Design in Sensor Network Virtualization for SHAAL. In: Proceedings of the 5th International Conference on Intelligent Systems, Modelling and Simulation, IEEE.
Khan, M., et al., 2016. Context-aware low power intelligent SmartHome based on the Internet of things. Comput. Electr. Eng..
Kibria, M.G., Chong, I., 2014. A WoO based knowledge driven approach for smart home energy efficiency. In: Proceedings of International Conference on Information and Communication Technology Convergence (ICTC), IEEE.
Kim, Y., Lee, S., Chong, I., 2014. Orchestration in distributed web-of-objects for creation of user-centered iot service capability. Wirel. Personal. Commun. 78 (4), 1965–1980.
Kim, J.Y., et al., 2015. Smart home web of objects-based IoT management model and methods for home data mining. In: Proceedings of 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE.
Kim, S., et al., 2014. Restful Design and Implementation of Smart Appliances for Smart Home. in Ubiquitous Intelligence and Computing, In: Proceedings of the 11th International Conference on and IEEE 11th International Conference on and Autonomic and Trusted Computing, and IEEE 14th International Conference on Scalable Computing and Communications and Its Associated Workshops (UTC-ATC-ScalCom), IEEE.
Kim, Y., Lee, Y., 2015. Automatic Generation of Social Relationships between Internet of Things in Smart Home Using SDN-Based Home Cloud. In: Proceedings of the 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA), IEEE.
Kim, Y.-P., Yoo, S., Yoo, C., 2015. DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things. In: Proceedings of IEEE International Conference on Consumer Electronics (ICCE), IEEE.
Kirkham, T., et al., 2014. Risk driven Smart Home resource management using cloud services. Future Gener. Comput. Syst. 38, 13–22.
Konstantinidis, E.I., et al., 2015. A lightweight framework for transparent cross platform communication of controller data in ambient assisted living environments. Inform. Sci. 300, 124–139.
Kovac, D., et al., 2015. Keeping eyes on your home: Open-source network monitoring center for mobile devices. In: Proceedings of the 38th International Conference on Telecommunications and Signal Processing (TSP), IEEE.
Lazarevic, I., et al., 2015. Modular home automation software with uniform cross component interaction based on services. In: Proceedings of the 5th International Conference on Consumer Electronics-Berlin (ICCE-Berlin), IEEE.
Le Vinh, T., et al., 2015. Middleware to integrate mobile devices, sensors and cloud computing. Procedia Comput. Sci. 52, 234–243.
Lee, Y.-T., et al., 2016. An integrated cloud-based smart home management system with community hierarchy. IEEE Trans. Consum. Electron. 62 (1), 1–9.
Lee, C., et al., 2014. Securing smart home: Technologies, security challenges, and security requirements. In: Proceedings of IEEE Conference on Communications and Network Security (CNS), IEEE.
Lee, K.-M., Teng, W.-G., Hou, T.-W., 2016. Point-n-Press: An Intelligent Universal Remote Control System for Home Appliances.
Lee, N., et al., 2015. Implementation of smart home service over web of object architecture. In: Proceedings of International Conference on Information and Communication Technology Convergence (ICTC), IEEE.
Lee, N., Lee, H., Ryu, W., 2014. WoO based pet-care service in smart home. In: Proceedings of International Conference on Information and Communication Technology Convergence (ICTC), IEEE.
Lee, S., Jeong, J.P., Park, J.-S., 2016. DNSNA: DNS name autoconfiguration for Internet of Things devices. In: Proceedings of the 18th International Conference on Advanced Communication and Technology (ICACT), IEEE.
Li, B., Yu, J., 2011. Research and application on the smart home based on component technologies and Internet of Things. Procedia Eng. 15, 2087–2092.
Li, F., et al., 2012. Research on sensor-gateway-terminal security mechanism of smart home based on IOT. (Ed.), Internet of Things, Communications in Computer and Information Science, Springer, Berlin, Heidelberg, vol. 312, pp. 415–422.
Li, H., et al., 2016. Enabling Semantics in an M2M/IoT Service Delivery Platform. In: IEEE Proceedings of the Tenth International Conference on Semantic Computing (ICSC), IEEE.
Li, Q., et al., 2013. Smart home services based on event matching. In: Proceedings of the 10th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), IEEE.
Li, X., et al., 2015. An IoT Service Framework for Smart Home: Case Study on HEM. In: Proceedings of IEEE International Conference on Mobile Services, IEEE.
Li, Y. Design of a key establishment protocol for smart home energy management system. In: Proceedings of the Fifth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), IEEE.
Lima, W.S., et al. 2015. User activity recognition for energy saving in smart home environment. In: Proceedings of IEEE Symposium on Computers and Communication (ISCC).
Lin, W., et al., 2013. OPCPP: an online plug-configure-play experiment platform for WSN. Int. J. Distrib. Sens. Netw. 2013.
Lin, H., et al., 2015. Promote the industry standard of smart home in China by intelligent router technology. In: Proceedings of Science and Information Conference(SAI), IEEE.
Lin, P.-C., 2015. Optimal smart gateway deployment for the Internet of Things in smart home environments. In: IEEE Proceedings of the 4th Global Conference on Consumer Electronics (GCCE), IEEE.
Liu, F., Guo, W., 2015. The Design and Implementation of MINA-Based Smart Home Data Synchronization System. In: Proceedings of the Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), IEEE.
Liu, F., Xiao, M., Feng, W., 2015. Design of Cordova Based Message Push Module for Cross-Platform Smart Home Application. In: Proceedings of the Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), IEEE.
Liu, J., Lu, Y., Li, Y., 2015. A multi-control center household appliances coordinated control method based on Events and Actions. In: Proceedings of the Third International Conference on Cyberspace Technology *(CCT 2015)*, IET.
Lloret, J., et al., 2012. Ubiquitous monitoring of electrical household appliances. Sensors 12 (11), 15159–15191.
Lu, C.-H., 2015. IoT-enabled smart sockets for reconfigurable service provision. In: Proceedings of IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), IEEE.
Ma, M., Wang, P., Chu, C.-H., 2015. LTCEP: Efficient Long-Term Event Processing for Internet of Things Data Streams. In: Proceedings of IEEE International Conference on Data Science and Data Intensive Systems, IEEE.
Madakam, S., Ramaswamy, R., 2014. Smart Homes (Conceptual Views). In: Proceedings of the 2nd International Symposium on Computational and Business Intelligence (ISCBI), IEEE.
Magruk, A., 2015. The most important aspects of uncertainty in the Internet of Things field–context of smart buildings. Procedia Eng. 122, 220–227.
Mainetti, L., Mighali, V., Patrono, L., 2014. An android multi-protocol application for heterogeneous building automation systems. In: Proceedings of the 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM), IEEE.
Mainetti, L., Mighali, V., Patrono, L., 2015. An IoT-based user-centric ecosystem for heterogeneous Smart Home environments. In: Proceedings of IEEE International Conference on Communications (ICC), IEEE.
Mano, L.Y., et al., 2016. Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. Comput. Commun..
Mao, M.Y., Jiang, Y.H., Yu, C.M., 2013. The Research of Embedded Internet Applied in Smart Home. Applied Mechanics and Materials, Trans Tech Publ..
Matharu, G.S., Upadhyay, P., Chaudhary, L., 2014. The Internet of Things: Challenges & security issues. in Emerging Technologies (ICET), International Conference on, IEEE.
Mehrabani, M., Bangalore, S., Stern, B., 2015. Personalized speech recognition for Internet of Things. In: Proceedings of IEEE 2nd World Forum on Internet of Things (WF-IoT), IEEE.
Miclaus, A., Riedel, T., Beigl, M., 2014. End-user installation of heterogeneous home automation systems using pen and paper interfaces and dynamically generated documentation. In: Proceedings of International Conference on the Internet of Things (IOT), IEEE.
Min, B., Varadharajan, V., 2015. Design and Evaluation of Feature Distributed Malware Attacks against the Internet of Things (IoT). In: Proceedings of the 20th International Conference on Engineering of Complex Computer Systems (ICECCS), IEEE.
Miori, V., Russo, D., 2012. Anticipating health hazards through an ontology-based, IoT domotic environment. In: Proceedings of the Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), IEEE.
Mital, M., et al., 2016. Adoption of cloud based Internet of Things in India: a multiple theory perspective. Int. J. Inf. Manag..
Mittal, Y., et al., 2015. A voice-controlled multi-functional Smart Home Automation System. In: Proceedings of Annual IEEE India Conference (INDICON), IEEE.
Möller, D.P., Vakilzadian, H., 2014. Ubiquitous networks: power line communication and Internet of things in smart home environments. in IEEE International Conference on Electro/Information Technology, IEEE.
Moosavi, S.R., et al., 2015. SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Comput. Sci. 52, 452–459.
Moravcevic, V., et al., 2015. An approach for uniform representation and control of ZigBee devices in home automation software. In: IEEE Proceedings of the 5th

International Conference on Consumer Electronics-Berlin (ICCE-Berlin), IEEE.
Moser, K., Harder, J., Koo, S.G., 2014. Internet of things in home automation and energy efficient smart home technologies. In: Proceedings of IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE.
Neisse, R., et al., 2015. SecKit: a model-based security toolkit for the internet of things. Comput. Secur. 54, 60–76.
Oriwoh, E., Sant, P., 2013. The Forensics Edge Management System: A Concept and Design. in Ubiquitous Intelligence and Computing, In: Proceedings of the 10th IEEE International Conference on Autonomic and Trusted Computing (UIC/ATC).
Pandey, S., Paul, A., Chanu, L.J., 2015. Life-Cycle Tracking System of home automation devices (LED Bulbs). In: Proceedings of International Conference on Green Computing and Internet of Things (ICGCIoT), IEEE.
Pang, Z., et al., 2014. Preliminary study on wireless home automation systems with both cloud-based mode and stand-alone mode. In: Proceedings of the 17th International Conference on Computational Science and Engineering (CSE), IEEE.
Papp, I., et al., 2015. Uniform representation and control of Bluetooth Low Energy devices in home automation software. In: Proceedings of the 5th International Conference on Consumer Electronics-Berlin (ICCE-Berlin), IEEE.
Park, S., et al., 2014. Inaudible Dual Tone Data transmission for home appliances. In: Proceedings of the Fourth International Conference on Consumer Electronics Berlin (ICCE-Berlin), IEEE.
Patel, P., Cassou, D., 2015. Enabling high-level application development for the Internet of Things. J. Syst. Softw. 103, 62–84.
Pavithra, D., Balakrishnan, R., 2015. *IoT based monitoring and control system for home automation*. in Communication Technologies (GCCT), 2015 Global Conference on, IEEE.
Peng, Z., et al., 2015. Intelligent home security system using agent-based IoT Devices. In: Proceedings of the 4th Global Conference on Consumer Electronics (GCCE), IEEE.
Perešíni, O., Krajčovič, T., 2015. Internet controlled embedded system for intelligent sensors and actuators operation. In: Proceedings of International Conference on Applied Electronics (AE), IEEE.
Peretti, G., Lakkundi, V., Zorzi, M., 2015. BlinkToSCoAP: An end-to-end security framework for the Internet of Things. In: Proceedings of the 7th International Conference on Communication Systems and Networks (COMSNETS), IEEE.
Perumal, T., Datta, S.K., Bonnet, C., 2015. IoT device management framework for smart home scenarios. In: Proceedings of the 4th Global Conference on Consumer Electronics (GCCE), IEEE.
Pham-Huu, D.-N., et al., 2015. Towards an Open Framework for Home Automation Development. In: Proceedings of International Conference on Advanced Computing and Applications (ACOMP), IEEE.
Prakash, L., et al., 2015. Self-sufficient smart prosumers of tomorrow. Procedia Technol. 21, 338–344.
Puustjärvi, J., Puustjärvi, L., 2015. The role of smart data in smart home: health monitoring case. Procedia Comput. Sci. 69, 143–151.
Qi, X., Bai, M., 2014. Smart Home Wireless Power Control Design Based on Internet of Things.
Rahman, R.A., Shah, B., 2016. Security analysis of IoT protocols: A focus in CoAP. In: Proceedings of the 3rd MEC International Conference on Big Data and Smart City (ICBDSC). IEEE.
Rajiv, P., Raj, R., Chandra, M., 2016. Email based remote access and surveillance system for smart home infrastructure. Perspect. Sci..
Ren, W., et al., 2015. A Robust and Flexible Access Control Scheme for Cloud-IoT Paradigm with Application to Remote Mobile Medical Monitoring. In: Proceedings of the Third International Conference on Robot, Vision and Signal Processing (RVSP), IEEE.
Salihbegovic, A., et al. 2015. Design of a domain specific language and IDE for Internet of things applications. In: Proceedings of 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE.
Samuel, S.S.I. 2016. A review of connectivity challenges in IoT-smart home. In: Proceedings of the 3rd MEC International Conference on Big Data and Smart City (ICBDSC). IEEE.
Sanchez, I., et al., 2014. Privacy leakages in smart home wireless technologies. In: Proceedings of International Carnahan Conference on SecurityTechnology (ICCST), IEEE.
Santoso, F.K., Vun, N.C., 2015. *Securing IoT for smart home system*. in *2015 International Symposium on Consumer Electronics (ISCE)*, IEEE.
Sasidharan, S., et al., 2014. *Cognitive management framework for Internet of Things:—A prototype implementation*. In: Proceedings of *IEEE World Forum on Internet of Things (WF-IoT),* IEEE.
Schiefer, M., 2015. Smart Home Definition and Security Threats. In: Proceedings of the Ninth International Conference on IT Security Incident Management & IT Forensics (IMF), IEEE.
Schweizer, D., et al., 2015. Using Consumer Behavior Data to Reduce Energy Consumption in Smart Homes: Applying Machine Learning to Save Energy without Lowering Comfort of Inhabitants. In: Proceedings of the 14th International Conference on Machine Learning and Applications (ICMLA), IEEE.
Schwiegelshohn, F., et al., 2015. A Holistic Approach for Advancing Robots in Ambient Assisted Living Environments. in Embedded and Ubiquitous Computing (EUC), In: Proceedings of the 13th IEEE International Conference on, IEEE.
Seo, D.W., et al., 2016. Hybrid reality-based user experience and evaluation of a context-aware smart home. Comput. Ind. 76, 11–23.
Serna, M.Á., Sreenan, C.J., Fedor, S., 2015. A visual programming framework for wireless sensor networks in smart home applications. In: Proceedings of the Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), IEEE , IEEE.
Sezer, O.B., Can, S.Z., Dogdu, E., 2015. Development of a smart home ontology and the implementation of a semantic sensor network simulator: An internet of things approach. In Proceedings of International Conference on Collaboration Technologies and Systems (CTS), IEEE.
Shah, J., Mishra, B., 2016. Customized IoT enabled wireless sensing and monitoring platform for smart buildings. Procedia Technol. 23, 256–263.
Shamszaman, Z.U., Lee, S., Chong, I., 2014. WoO based user centric Energy Management System in the internet of things. In: Proceedings of the International Conference on Information Networking 2014 (ICOIN2014). IEEE.
Shi, L., Zhao, H., Cai, H., 2013. Design and Implementation of Gas Detector Position Computer System Based on ARM. Appl. Mech. Mater..
Shi, K., Tang, M., Wang, Z., 2014. Research of Heterogeneous Network Protocol Data Fusion in Smart HomeControl System Based on Spatial Outlier. in Instrumentation and Measurement, Computer, Communication and Control (IMCCC), In: Proceedings of the Fourth International Conference on, IEEE.
Shivraj, V., et al., 2015. One time password authentication scheme based on elliptic curves for internet of things (IoT). In: Proceedings of the 5th National Symposium on *Information Technology: Towards New Smart World (NSITNSW),* IEEE.
Sivaraman, V., et al., 2015. Network-level security and privacy control for smart-home IoT devices. In: IEEE Proceedings of the 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE.
Sivieri, A., Mottola, L., Cugola, G., 2016. Building Internet of Things software with ELIoT. Comput. Commun..
Soliman, M., et al., 2013. Smart home: Integrating internet of things with web services and cloud computing. In: IEEE Proceedings of the 5th International Conference on Cloud Computing Technology and Science (CloudCom), IEEE.
Son, S.-C., et al., 2016. A time synchronization technique for coap-based home automation systems. IEEE Trans. Consum. Electron. 62 (1), 10–16.
Song, Y., et al., 2012. Modeling and simulation of smart home scenarios based on Internet of Things. In: Proceedings of the 3rd IEEE International Conference on Network Infrastructure and Digital Content, IEEE.
Souza, A.M., Amazonas, J.R., 2013. A novel smart home application using an internet of things middleware. In: Proceedings of 2013 European Conference on Smart Objects, Systems and Technologies (SmartSysTech), VDE.
Srivastava, V., Kim, D., Ko, Y.-B., 2014. A smart home solution over CCN. In: Proceedings of International Conference on Information and Communication Technology Convergence (ICTC), IEEE.
Stusek, M., et al., 2015. 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), 7th International Congress on, IEEE.
Su, K., et al., 2012. Instant Messaging Application for the Internet of Things. in Computer Science & Service System (CSSS), International Conference o*n*, IEEE.
Su, X., et al., 2011. Towards an integrated solution to internet of things-a technical and economical proposal. In: Proceedings of the 15th International Conference on Intelligence in Next Generation Networks (ICIN), IEEE.
Sun, Y., et al., 2014. Organizing and querying the big sensing data with event-linked network in the internet of things. Int. J. Distrib. Sens. Netw. 2014.
Sundaram, B.V., et al., 2015. Encryption and hash based security in Internet of Things. In: Proceedings of the 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), IEEE.
Suryadevara, J., Sunil, B., Kumar, N., 2013. Secured multimedia authentication system for wireless sensor network data related to internet of things. In: Proceedings of the Seventh International Conference on Sensing Technology (ICST), IEEE.
Tang, L.Z.W., et al., 2015. Augmented reality control home (ARCH) for disabled and elderlies. In: IEEE Proceedings of the Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), IEEE.
Thiyagarajan, M., Raveendra, C., 2015. Integration in the physical world in IoT using android mobile application. In: Proceedings of International Conference on Green Computing and Internet of Things (ICGCIoT), IEEE.
Tian, C., et al., 2015. Analysis and design of security in Internet of things. In: Proceedings of the 8th International Conference on Biomedical Engineering and Informatics (BMEI). IEEE.
Trinchero, D., et al., 2011. Integration of smart house sensors into a fully networked (web) environment. In: Sensors, IEEE.
Truong Cong, T., et al., 2011. Towards a full-duplex emergency alert system based on IPTV platform. In: Proceedings of the 3rd International Conference on Awareness Science and Technology (iCAST).
Tseng, S.-P., et al., 2014. An application of Internet of things with motion sensing on smart house. In: Proceedings of IEEE International Conference on Orange Technologies (ICOT), IEEE.
Ukil, A., Bandyopadhyay, S., Pal, A., 2015. Privacy for IoT: Involuntary privacy enablement for smart energy systems. In: Proceedings of IEEE International Conference on Communications (ICC). IEEE.
Vujović, V., Maksimović, M., 2015. Raspberry Pi as a sensor web node for home automation. Comput. Electr. Eng. 44, 153–171.
Waltari, O., Kangasharju, J., 2016. Content-centric networking in the internet of things. In: Proceedings of the 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE.
Wang, H., Zheng, B.G., 2014. Research and implementation of the smart home system based on Internet of Things environment. Appl. Mech. Mater..
Wang, J., Zhu, Q., Ma, Y., 2013. An agent-based hybrid service delivery for coordinating internet of things and 3rd party service providers. J. Netw. Comput. Appl. 36 (6), 1684–1695.
Wang, Y.M., 2013. The Internet of Things smart home system design based on ZigBee/GPRS technology. Appl. Mech. Mater..

Wang, Z., 2014. Smart home system design based on Internet of things. Appl. Mech. Mater..

Wang, J., et al., 2012. *A location-aware lifestyle improvement system to save energy in smart home*. In: *Proceedings of the 4th International Conference on Awareness Science and Technology*. IEEE.

Wang, M., et al., 2013 *An IoT-based appliance control system for smart homes*. in *Intelligent Control and Information Processing (ICICIP), Proceedings of the Fourth International Conference on*. IEEE.

Wang, T., Zheng, B., Liang, Z.-L., 2013. The design and implementation of wireless intelligent light control system base on Zigbee light link. In: Proceedings of the 10th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), IEEE.

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

Wei, X., Qin, Q., 2013.The design and application of low-cost smart home under the internet of things and cloud computing platform. In: Proceedings of LISS 2012, Springer, pp.959–965.

Witkovski, A., et al., 2015. An IdM and Key-based Authentication Method for providing Single Sign-On in IoT. In: Proceedings of IEEE Global Communications Conference (GLOBECOM). IEEE.

Wright, D., et al., 2015. A cloud to mobile application for consumer behavior modification. Procedia Comput. Sci. 62, 343–351.

Wu, Q., et al., 2013. Internet of things based data driven storytelling for supporting social connections. in Green Computing and Communications (GreenCom), IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, IEEE.

Wurm, J., et al., 2016. Security analysis on consumer and industrial iot devices. In: Proceedings of the 21st Asia and South Pacific Design Automation Conference (ASP-DAC), IEEE.

Xiao, B., et al., 2015. Design and implementation of rule-based uncertainty reasoning in Smart House. In: IEEE Proceedings of the 16th International Conference on CommunicationTechnology (ICCT), IEEE.

Xie, X., Deng, D., X. Deng, X., 2011. Design of embedded gateway software framework for heterogeneous networks interconnection. in Electronics and Optoelectronics (ICEOE), International Conference on, IEEE.

Yan, Y., Xu, Z.F., Zhu, X., 2014. A middleware of IoT-based smart home based on service. Appl. Mech Mater..

Yang, G., et al., 2014. A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. IEEE Trans. Ind. Inform. 10 (4), 2180–2191.

Yang, M., et al., 2013. Application of power IoT in intelligent community. Adv. Mater. Res..

Yang, C., et al., 2014. A Smart Home Architecture Based on Resource Name Service. In: Proceedings of the 17th International Conference on Computational Science and Engineering (CSE), IEEE.

Yang, T.-Y., Yang, C.-S., Sung, T.-W., 2015. An Intelligent Energy Management Scheme with Monitoring and Scheduling Approach for IoT Applications in Smart Home. In: Proceedings of the Third International Conference on Robot, Vision and Signal Processing (RVSP), IEEE.

Yao, L., Lai, C.-C., Lim, W.H., 2015. Home Energy Management System Based on Photovoltaic System. In: Proceedings of IEEE International Conference on Data Science and Data Intensive Systems, IEEE.

Ye, J., et al., 2012. The research of an adaptive smart home system. in Computer Science & Education (ICCSE), In: Proceedings of the 7th International Conference on, IEEE.

Ye, X., Huang, J., 2011. A framework for cloud-based smart home. In: Computer Science and Network Technology (ICCSNT), International Conference on, IEEE.

Yin, S., Lu, Y. and Li, Y., 2015. Design and implementation of IoT centralized management model with linkage policy. In: Proceedings of the Third International Conference on Cyberspace Technology (CCT 2015), IET.

Yin, Z., Che, Y. and He, W. 2015. A hierarchical group control method of electrical loads in smart home. In: Proceedings of the 6th International Conference on Power Electronics Systems and Applications (PESA), IEEE.

Yiqi, W., et al., 2014. A ZigBee-based smart home monitoring system. In: Proceedings of the Fifth International Conference on Intelligent Systems Design and Engineering Applications (ISDEA), IEEE.

Yongqing, G., Dan, S., 2013. The research of home Intelligent power system based on ZigBee. In: Proceedings of the 3rd International Conference on Consumer Electronics, Communications and Networks (CECNet).

Yoshigoe, K., et al., 2015. Overcoming invasion of privacy in smart home environment with synthetic packet injection. In: Proceedings of TRON Symposium (TRONSHOW), IEEE.

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

Yuan, X. Peng, S., 2012. *A research on secure smart home based on the internet of things*. In: Proceedings of IEEE International Conference on Information Science and Technology, IEEE.

Yun, J., et al., 2015. A device software platform for consumer electronics based on the Internet of Things. IEEE Trans. Consum. Electron. 61 (4), 564–571.

Yunge, D., et al., 2015. Hybrid Apps: Apps for the Internet of Things. In: Proceedings of EEE 17th International Conference onHigh Performance Computing and Communications (HPCC), 2015 IEEE Proceedings of the 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), IEEE.

Zanjal, S.V., Talmale, G.R., 2016. Medicine reminder and monitoring system for secure health using IOT. Procedia Comput. Sci. 78, 471–476.

Zhang, D.-g., Dong, D.-c., Peng, H.-t., 2012. Research on development of embedded uninterruptable power supply system for IOT-based mobile service. Comput. Electr. Eng. 38 (6), 1377–1387.

Zhang, Q., Chen, Z., Zhang, P., 2012. Internet of Things applied in the home-based caring system for the aged. In: Advances in Electronic Commerce, Web Application and Communication. Springer, 467–471.

Zhang, W., Li, G. and Gao, W., 2015. The Embedded Smart Home Control System Based on GPRS and Zigbee. In: Proceedings of MATEC Web of Conferences. EDPSciences.

Zhao, X.F., 2013. The Application of Bluetooth in the Control System of the Smart Home with Internet of ThingsAdvanced Materials Research. Trans Tech Publ..

Zhao, M., et al., 2014. Discrete Control for Smart Environments Through a Generic Finite-State-Models-Based Infrastructure. in European Conference on Ambient Intelligence. Springer.

Zhao, X., Zhou, C. and Huang, W., 2013. Smart home power management system design based on human-computer interaction model. In: Proceedings of the 3rd International Conference on Computer Science and Network Technology (ICCSNT), IEEE.

Zhou, J., et al., 2013. Cloudthings: A common architecture for integrating the internet of things with cloud computing. In: Proceedings of the 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 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.