Wireless Networks
https://doi.org/10.1007/s11276-018-1712-5

A review on smart home present state and challenges: linked to context-awareness internet of things (IoT)

Zahrah A. Almusaylim[1] · Noor Zaman[1]

Abstract
The smart home is considered as an essential domain in Internet of Things (IoT) applications, it is an interconnected home where all types of things interact with each other via the Internet. This helps to automate the home by making it smart and interconnected. However, at the same time, it raises a great concern of the privacy and security for the users due to its capability to be controlled remotely. Hence, the rapid technologically growth of IoT raises abundant challenges such as how to provide the home users with safe and secure services keeping privacy in the account and how to manage the smart home successfully under the controlled condition to avoid any further secrecy or theft of personal data. A number of the research papers are available to address these critical issues, researchers presented different approaches to overcome these stated issues. This research review will analyze smart home approaches, challenges and will suggest possible solutions for them and illustrate open issues that still need to be addressed.

Keywords Smart home · IoT · Context-awareness · Security · Privacy-aware · Sensors · Energy-aware

1 Introduction

The advanced technologies have enabled things around us to be embedded with sensors and communicated with each other with the help of Wireless Sensor Networks (WSN) and Radio-Frequency Identifications (RFID). Wireless communication that allows the Internet to access into embedded and ubiquitous computing [1]. The communication among these things enters us into a new era of ubiquity where the seamless emergence of several technologies leads to the Internet of Things concept in which it aims at enabling the communication between any types of things, at any place, anytime using network technologies [2]. The things in IoT are uniquely addressed through IP address and they are physical in natures where they can integrate with the network [3]. Figure 1 illustrates an example of the IoT system where the embedded sensors detect the intrusion and notify to the user through the GSM modem, also the user can monitor the intrusion at home from anywhere through the mobile IP based webcam and in case, if the intrusions are real then the user have options such as, play alarm, alert neighbors or report to the police [4].

Sensors in IoT can sense and communicate with their physical environment and collect data remotely over the Internet, and based on the collected data using intelligent decision-making approach they can respond to the environment [5]. According to the study done by the Cisco [6] that in 2003 the number of Internet-connected devices that owned by persons was less than one million (0.8) yet the concept of IoT did not exist, because the Internet-connected things were still relatively small. In 2010 the number of Internet-connected devices increased to 1.84 million which shows that the increase in IoT connected devices increased more than the number of people born in this period. In 2015 the number of Internet-connected devices that each person owned increased to 3.47 million. And by looking to the future, the study predicts that there might be more than 50 Billion number of Internet-

✉ Zahrah A. Almusaylim
zahra.almusaylim@hotmail.com

Noor Zaman
nzaman@kfu.edu.sa

[1] Department of Computer Science, College of Computer Sciences and Information Technology, King Faisal University, Hofuf, Saudi Arabia

Published online: 20 March 2018

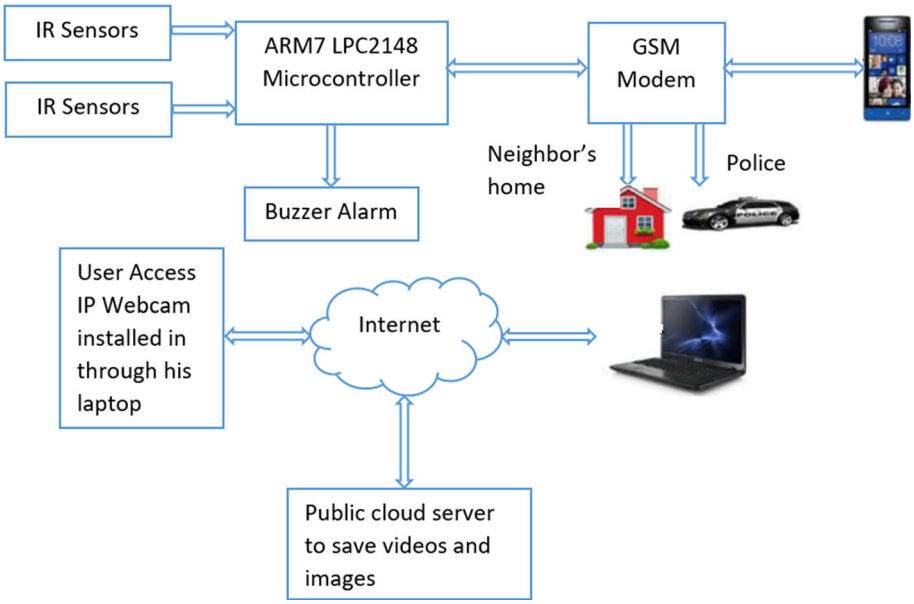

Fig. 1 Proof of concept of IoT [4]

connected devices that each person owns will increase ever to be 6.58 million by 2020 as illustrated in Fig. 2.

Context-awareness is an important characteristic of ubiquitous computing [6]. Due to the huge number of sensors that already exist to collect raw data from their environments, this raw data need to be analyzed and interpreted to have meaningful information from it such as location or time (this informations called contextual information) to be feasible in IoT. Context-Aware Computing helps in this regard as it allows to store the contextual information linked to the raw data collected from sensors and decides which data needs to be processed, so as to make achieving the interpretation more easily. For example, the sensor readings produced by GPS sensors can be considered as raw sensor data. Once we use the Global Positioning System (GPS) sensor readings in such a way that it represents a geographical location, we call it context information. Further, details for the reader about context and context-aware computing is elaborated in [7–10]. Establishing context-aware computing environment at smart home creates more challenges as people can determine what activities they can do and how they can organize their time and space. Hence more attention has to be done to make the smart home more eligible to the homeowners and to fulfill their requirements for social acceptance, usability, low cost, privacy protection and zero administration. Smart home also can provide healthcare support and services to home users. They can monitor and observe home user's health and make a warning if a vital sign of an abnormal condition is detected [11]. Therefore, with the help of context-aware computing, a smart home can be developed and applied to assist users in achieving their tasks at hand in their everyday life and make their quality of life more easier [12]. More information regarding the relationship between context-aware computing linked to the smart home in [13–15]. This paper will present the current challenges in the smart home linked to the context-aware IoT and the most recent work to address these challenges. The remaining of the paper is organized as follow: Literature Review related to smart home challenges, Results and Discussion, and Conclusion.

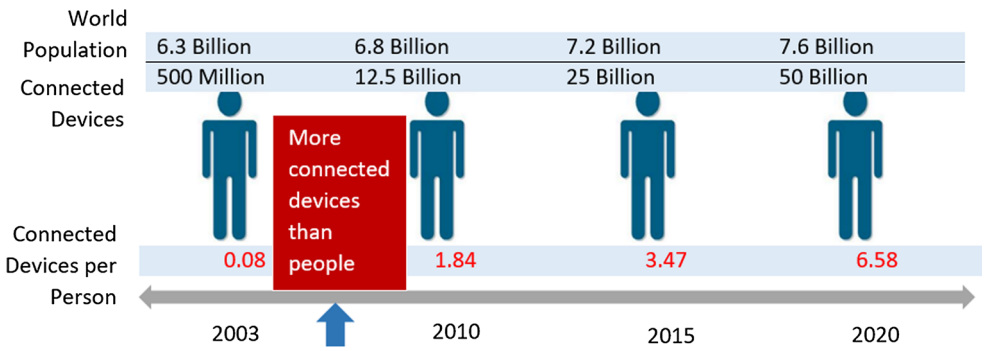

Fig. 2 Growth of IoT [6]

2 Literature review: smart home challenges

Many types of research have been conducted in the area of the smart home linked to context-aware IoT in the past few years. In this section, we review and discuss some important challenges related to smart home based on recently conducted researches. Further, this section will describe the challenges based on different aspects such as Interoperability, Context-Aware Middleware, Energy-Aware Consumption, Security, and Privacy-Aware.

2.1 Interoperability

As the smart home is connected with different things, sensors, devices and different communication networks, connectivity is considered as the cornerstone of IoT because it is built by standards and communication protocols that are used in the environment of smart home [16]. These are connected with each other in the smart home using several communication protocols to react to contextual changes in order to provide safety and comfort to home users [17]. Hence, this creates a huge heterogeneity in the smart home and it is expected to grow significantly so they need to interoperate efficiently without the need for external intervention [18]. The emergence of heterogeneity of them in the smart home environment causes an interoperability challenge in managing them [19] because the smart home environment is a distributed architecture that requires being interoperable to manage heterogeneous systems [20, 21]. Therefore, there is a need for solutions that allow the heterogeneous devices and systems interoperate and talk to each other in an efficient manner regardless of their heterogeneity [20].

There have been several studies and solutions done to achieve interoperability in smart homes. Researchers in [22] proposed a new smart framework for systems in the smart home, as they can perform and coordinate their tasks in an efficient way. The framework is based on web services and Simple Object Access Protocol (SOAP) to exchange messages and manage interoperation among heterogeneous smart home devices. It provides services to break data comes from different heterogeneous sources and services for heterogeneous systems management communication. Authors in [23] proposed an extensible smart home gateway architecture based on Open Services Gateway initiative (OSGi) framework that allows heterogeneous devices and protocols to be seamlessly integrated into the smart home during the runtime. It enables end users to flexibly add, install, manage, access and communicate with diverse devices and protocols during runtime. Also, they proposed an access control and policy model that give the end users and devices different permissions and roles to access the smart home. Researchers in [24] proposed a framework that allows heterogeneous devices in the smart home to communicate with each other in a collaborative manner in which the smart connected devices send a request to the centralized database server that verifies the authenticity of the device and then accepts the requests and supports interoperability among them. The server coordinates and monitors the heterogeneous smart devices by providing remote access control to the smart devices with encryption rules applied to authorization access to the smart home.

The literature reviews discussed above clarified that how the interoperability challenge need to be handled due to a large number of heterogeneous things that belong to different platforms and thus it is an important criterion in building any IoT smart home services to meet the users' needs [25]. Therefore, the provided solutions for interoperability allow devices, communication protocols and services to be dynamically integrated. Table 1 shows critical review of the solutions to achieve interoperability.

2.2 Context-aware middleware

The rapid development of IoT and ubiquitous computing into our lives have led to the growth and generation of contexts which represent what changes happen in the environment and where they exist [26]. The increasing of contexts in the environment will attract the user to them to provide them with current changes happen which will increase user performance [27]. As a consequence, applications of context-aware can adjust their behaviors due to the changes happened in the environment without or with less of human intervention [26].

Applications of Context-Aware usually have elements with single contexts which might be needed by several applications and hence programmers might need context elements through context provider software for getting the desired context types. Thus, developing context-aware stand-alone applications is inefficient due to the reusability standards and the difficulty for software developers to find the available context-aware services. Implementing context-aware applications that are able of obtaining and discovering contextual information from their environment is a major challenge [28]. For these reasons, there is a need for context-aware middleware that is considered to be the main requirement for developing the context-aware applications to collect and analyze the contextual changes efficiently [29]. Context-Aware Middleware is defined as it is a software system that provides an abstracted layer among the context-aware applications and the operating systems [30]. Context-aware middleware at smart home enables a home gateway to collect data and learn user behavior

Table 1 Critical review for interoperability challenge

Feature/ scheme	Flexibility	Adding devices	User experience	Systems discovery	Web services support	Security support	Systems configuration	Remote access control
Ref. [22]	✔	✔	X	✔	✔	X	✔	X
Ref. [23]	✔	✔	✔	✔	✔	✔	✔	✔
Ref. [24]	X	X	✔	X	X	✔	✔	✔

which are context changes from smart devices, then based them it can perform actions and make decisions [31].

There have been several studies and solutions suggested achieving context-aware middleware in smart homes. Guo et al. in [32], proposed a framework for context management that deals with the mobile entity problem in cross-domain context sharing and a transparent query mechanism that enables applications to obtain context information about mobile entities from remote domains. The framework provides the interaction between different domain context managers. The contexts generated from different smart home environments should be managed by home context manager. In [33] researchers presented a context-aware middleware system that simplifies context information sharing through different devices and things in the smart home. The system facilitates the cooperation among software developers by providing mechanisms for context registering and retrieving as services allow them to publish their contexts and also retrieve contexts published by others. The researchers in [34] provided a context middleware architecture system in a smart home in which contexts are modeled based ontology to get semantic information using Web Ontology Language (WOL) and a profile applied reasoning algorithm to infer high-level contexts from available low-level contexts. The architecture consists of three layers that aim at supporting sensors abstraction by hiding sensing details, supporting context information reasoning and processing and facilitating the development of context-aware services.

The literature reviews about context-aware middleware showed that developing and implementing a context-aware middleware is a challenge due to the particular characteristics of devices and contexts such as the limited resources of smart devices and the dynamic nature of contexts. Therefore, the solutions help in building context-aware middleware that has great benefits in reducing the development time of context-aware applications and simplifying the complex behavior of them. Context-aware middleware can help developers to focus on developing applications without concerning about managing the context related to applications [26]. Also, it helps them to find a new way for environments that make them to automatically respond to various contexts without concern of gathering contextual information from several sources [35]. Table 2 shows critical review of the solutions to achieve context-aware middleware.

2.3 Energy aware\efficient consumption

The increased consumption of electrical energy affects the environment and the human budgets [36]. A report in [37] showed that about 13% of the world energy consumption in 2040 will be energy used in homes. In which it is increasing 48% from 2012 to 2040 as a result of the growing demand for energy in the non-OECD (Organization for Economic Cooperation and Development) countries. Figure 3 shows the average annual change in energy consumption of residential sector in OECD countries. The increased costs of electrical energy have led to an increased demand for energy efficient systems. Due to the growing demand for energy, the homeowners are converted into smart home energy management to minimize energy costs as well as make life more comfortable. Therefore, energy efficiency becomes a key requirement for developing modern homes [38, 39]. To overcome this challenge at home, energy-aware smart home is developed capable of measuring the amount of energy consumed by smart devices and control their operations [40]. A more measurable characteristic of the smart home is that it is with diversified ways of energy efficiency at home [41].

Several researchers suggested achieving energy-aware consumption in smart homes, in [43] proposed an energy-prone context (EPC) system to model a context provided by the involved appliances of the context energy consumption. Based on collected historical data of each appliance, there will be a related power consumption status for the appliance with respect to the context. The researchers in [44] proposed a system that is based on context awareness and cloud computing to control and monitor energy saving services that can be accessed online via mobile devices. The system based on context awareness which allows users to make a decision with context information changes. Yang et al. in [45] proposed a home energy management system for smart home based on context-aware services in which it allows home users to collect and analyze historical power information of home

Table 2 Critical review context-aware middleware challenge

Feature/ scheme	Architectural style	Service management	Context discovery	Context aggregation	Security	Reusability	Context dissemination	Scalability
Ref. [32]	Distributed	✔	✔	✔	✔	X	✔	✔
Ref. [33]	Centralized	✔	✔	✔	X	✔	X	X
Ref. [34]	Layered	✔	✔	✔	X	✔	✔	X

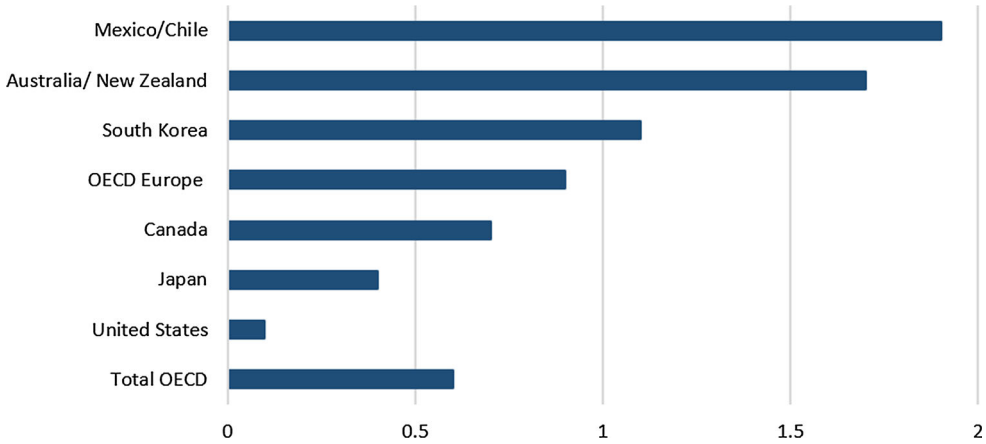

Fig. 3 Average annual change in energy consumption of residential sector [42]

appliances and to customize energy settings and usage to offer energy usage modes like general mode, power-saving mode, and economic mode to provide energy saving efficiently. Khan et al. in [46] proposed an energy-aware smart home system based on Coordinator ZigBee Networking mechanism in which it has: (1) Smart interference control system (SICS) to reduce the interference of coexistence of heterogeneous technologies in the wireless local area networks and wireless sensor networks; (2) Smart energy control system (SECS) to merge natural light with the source light and improves the energy consumption of the home appliances; and (3) Smart management control system (SMCS) to reduce the energy consumption by controlling the active time of the home appliances efficiently.

The literature reviews about energy-aware consumption showed that developing frameworks for an efficient and optimized energy consumption at smart home is a challenge due to the increased amount of energy costs and demands. So it brings the vision of smart home energy efficiency environment [47]. Table 3 shows critical review of the solutions to achieve context-aware middleware.

2.4 Security

As the smart home utilizes devices connected to the Internet and shared via a home network to provide convenience services [48], the home gateway of smart home can control the flow of information among devices and services which requires authenticity, integrity, reliability, and confidentiality [49]. Researchers in [50–53] presented some of the security threats that are addressed in the smart home; some of them are summarized in Table 4. However, the increased number of things and devices connected to the Internet expose the homes' residents to security risks as the information becomes controlled and accessible remotely in new ways. For example, an attacker may eavesdrop on the communication of sensors and other devices and detect the user activities. Also, a malicious user can control the devices at home remotely and use them to hack the smart home system [54].

To stop these kinds of threats it is necessary to secure the data and to check the authenticity of each user and integrity of all the data that are sent and received [55]. Security plays a critical role in smart home management which needs to be solved due to the increased number of users and the number of their requests that should be handled and managed [56]. To overcome the security threats challenges [48], there is a need for solutions that should be applied at smart home as they can provide security features to the homes' residents as well as the smart devices.

There have been several studies and solutions done to achieve security in smart homes. Kumar et al. in [57] proposed an Anonymous Secure Framework (ASF) using lightweight operations for different connected smart devices that are communicated to the home gateway. It

Table 3 Critical review for energy-aware consumption challenge

Feature/ scheme	User interface	Collaboration in energy saving	Remote control of switching devices	Devices operate on schedules	Availability of renewable resources	Management settings	Security
Ref. [43]	✔	✔	X	X	X	✔	X
Ref. [44]	✔	✔	✔	X	X	X	X
Ref. [45]	✔	✔	X	✔	✔	✔	X
Ref. [46]	X	✔	X	✔	✔	X	X

Table 4 Smart home security threats summary

Threats	Possible impacts
Eavesdropping	An attacker eavesdrops the home user traffic illegally such as emails between the internal network of the smart home and the third parties without changing the legitimate communication parties with a goal of violating the communication's confidentiality
Traffic analysis	An attacker observes the traffic pattern between the third party and the owner of the smart home
Denial of service (DoS)	An attacker blocks an authorized user from accessing services or limiting it by making the internal network of the smart home flooded with messages to overload its resources with traffic
Node compromise	An attacker captures and reprograms a legitimate node in the network in order to disrupt the network communication
Sinkhole and wormhole attacks	A malicious node attracts network packets towards it by spreading false routing information to its neighbors in order to make selective forwarding of packets which, in turn, reshape the network's routing behavior
Physical attack	An attacker gains the physical access to sensors which can perform many other attacks such as removing sensors from the network or stealing nodes
Masquerade attack	An attacker pretends a false identity to gain some unauthorized privileges
Replay attack	An attacker gets messages that are sent previously between two parties re-sends them again pretending that it is from an authorized entity
Message modification attack	An attacker alters the content of the message being sent by reordering it or delaying it to produce an illegal effect
Interception attack	An attacker intercepts the data packets sent to the remote user
Season-stealing attack	An attacker waits patiently for authenticated user or node to authenticate itself and then attacker fraudulently takes over the session by impersonating the identity of the genuine user or node
Malicious code	Malicious Codes are software threats that cause negative effects on the Smart Home internal network by exploiting its vulnerabilities

provides efficient authentication, device anonymity, and integrity among communicated devices by utilizing hashing and symmetric cryptosystems. In [58] researchers proposed an intrusion detection and mitigation framework (IoT-IDM) for IoT devices in the smart home. The framework monitors the devices' activities in the network to check whether there is any malicious activity and once an intrusion is detected, the intruder is blocked from accessing the victim device. Researchers in [59] proposed a security framework for smart home devices in which it provides security services for smart home by ensuring authentication of devices, availability, and integrity of data. It prevents the security threats such as information leakage, malicious code or data modification by using access control and self-signing techniques to provide defense against the threats.

The literature reviews about improving the security in smart homes showed that developing frameworks for effective security mechanisms at smart home is a challenge due to the increased number of the new technologies so this increases the number of crimes and the accidents that occur. Therefore, to prevent such these incidents the solutions help in developing security smart home systems that try to prohibit them and provide safe and secure tools and mechanisms to the residents at home. Table 5 shows critical review of the solutions to achieve context-aware middleware.

2.5 Privacy-aware

Nowadays different types of data are collected and can be accessible and available without taking control on those

Table 5 Critical review for security challenge

Feature/ scheme	Detect threat	Authentication	Integrity	Encryption techniques	Unauthorized access support	Prevent attack	Monitoring
Ref. [57]	X	✔	\✔	✔	✔	✔	X
Ref. [58]	✔	X	X	X	X	✔	✔
Ref. [59]	✔	✔	✔	X	✔	✔	✔

who will receive and process the data [60]. Generally, in IoTs, the smart home environment is sensed by sensors and connected devices in which they can transmit the gathered information to the server that communicates with the applications using fixed or mobile communication channels [61]. For example, recent technologies such as wearable devices like Apple iWatch, Apple Health Kit, Google Glass, Apple Home Kit and Google Fit are able to gather user's sensitive information ranging from financial status and health conditions by observing daily activities of them [62]. Moreover, people are generating the huge increased amount of data without being fully aware of their actions or effects and hence when all these data are gathered; either it is processed by third parties or another service provider.

However, the collected data by sensors devices may consist of sensitive personal information depending on the data source and the application type [62]. Therefore, the privacy of the users and protection of their sensitive data have been considered to be the most important sensitive challenge as it may have an impact on users legally and ethically [63]. The private information of the users should be protected in the sensors and devices, during the communication and at processing which can be a facility to disclose the sensitive information [61]; then an adversary can spy and suppose some information about the users at home and use this information for intrusion [64]. Hence to ensure the privacy of sensitive information of users, there is a need for solutions that should be applied at smart home as they can provide efficient privacy mechanisms to the homes' residents to avoid privacy violations of the users [62].

There have been several studies and solutions suggested achieving privacy-aware in smart homes. Chakravorty et al. in [65] proposed a framework to ensure privacy in the smart home for different stages of data lifecycle which are data collection, data transformation, data storage, data processing and data sharing. The data collector module uses SSH transfer protocol to ensure high and secure transfer of data and the data receiver module receives the transferred collected data from data collector and performs some algorithmic functions to transform into two separated datasets to achieve and ensure isolation between the sensitive and non-sensitive data which are stored separately and result provider module controls and authorizes the access of end users to the data processing results and determines the privacy level of any shared data result at smart home. Deva et al. in [66] proposed a privacy-aware context-sensitive framework for mobile devices that enables users to define privacy preferences individually for different contexts. It aims to allow the user to have complete control over their sensitive information of their location to determine if the user's location is shareable with others or not anywhere anytime. The researchers in [67] proposed a framework that allows a robot that is equipped with cameras for monitoring smart home in which it can detect sensitive private moments such as nakedness during a bath and avoid mentoring the person by turning away and informs the person about its intention of not monitoring. Alpár et al. in [68] proposed an Attribute based authentication technique in which when the smart devices or sensors communicate, they can authenticate each other so the amount of data collected become limited.

The literature reviews about improving the privacy awareness of users in smart homes showed that developing frameworks for effective privacy mechanisms at smart home is a challenge due to the huge amount of personal data that is collected by smart devices at home which will be susceptible to privacy threats, leakage, and disclosure. Hence, it will be possible in IoT to develop some applications to improve the privacy in the smart home; for example, an application that may send an Short Messaging Service (SMS) message to the users immediately whenever their personal things are being changed without the user's permission [69]. Therefore, these solutions may help in developing privacy mechanisms that ensure the type and level of data collected from smart devices must be clearly defined. When the data collected will be shared within IoT, there should be privacy policies of the shared information and hence make the users feel comfortable when participating their information in IoT [70]. Table 6 shows critical review of the solutions to achieve context-aware middleware.

Table 6 Critical review for privacy-aware challenge

Feature/scheme	User interaction	User authorization	Personal information management	Access management
Ref. [65]	X	✔	✔	✔
Ref. [66]	✔	X	✔	✔
Ref. [67]	✔	X	✔	X
Ref. [68]	✔	✔	✔	✔

3 Discussion

This section mainly based on the finding of intensive literature review and data analysis done with different tables. The literature review that has presented insight into the researches and studies that have been conducted and made it possible to identify the IoT smart home challenges. There are a lot of solutions for the challenges that are grown in the IoT smart home. From the critical reviews for each challenge in the previous section, we can have a comparison study for each challenge discussed. The solutions for challenges have several common features such as (1) Interoperability solution can be flexible, adding devices/installation, user interface support, Device discovery, web services support, security mechanism, devices/systems configuration and remote access control; (2) Context-Aware Middleware solution can support architectural style, service management, context acquisition/discovery, context reasoning, context abstraction, context aggregation, security and privacy, reusability, context dissemination, quality of context assessment, scalability and fault tolerance; (3) Energy-Aware Consumption solutions can support monitoring through user interface, user collaboration in energy saving, remote control of switching devices, operating devices on schedules, availability of renewable resources, performance optimization, smart appliances' settings management, security and privacy and control different types of energy wastes; (4) Security solutions can support threat detection, authentication, integrity, encryption techniques, unauthorized access support, machine learning, prevent attack and monitoring; and (5) Privacy-Aware solutions can support user interface, user interaction, user authorization, personal information management and access management.

Table 1 shows that the adding and installation of devices can be done through service stub using dynamic manipulation of rules and data in the database in [22] and can be done dynamically by the end users on demands through scanning the barcode of devices in [23]. Devices can be discovered through service stub that contains software dependencies using dynamic manipulation of rules and data in the database in [22] and in [23] devices can be discovered either manually, automatically or semi-automatic. Devices and systems configuration is done automatically through the default web service communication driver tool in [22], dynamically by the end users through downloading the drivers from the cloud in [23] and dynamically by end users through smartphones based on specifications that send a request to the server in [24].

Table 2 shows that [32] supports distributed architectural style, [33] supports centralized architectural style and [34] supports layered architectural style. The only framework that supports security and privacy in [32] in which each a local access control is involved in each context manager that analyzes the contexts against the privacy settings of the user. The only framework in [32] provides context dissemination and scalability through utilizing publish-subscription paradigm for intra-domain context dissemination and query approach for global context dissemination and through context entry engine that will do further queries from the registered domains of the user in which the context are stored in several domains respectively.

Table 3 shows that remote control of switching devices feature is supported only in [44] in which user can access to turn off unnecessary home appliances or turned off automatically by the system. Both frameworks in [45] and [46] support operating devices on schedules feature through appliances scheduling module and by smart management control system that controls the operating time of the electronic appliances, respectively. Moreover, both frameworks in [45, 46] provide availability of renewable resources feature through the use of Photovoltaic (PV) that can recharge the battery management system and through the smart energy control system that integrates sunlight with a light source to tune the illumination level in a room, respectively. Smart appliances' settings management is supported only in [43] in which the appliance's power consumption in EPC is classified into Explicit power consumption and implicit power consumption and in [45] through context-aware services that allow the user to do customized settings and offer energy usage modes on appliances. None of the frameworks support security and privacy feature.

Table 5 shows integrity feature is supported in [57] in which Message integrity is realized by one-way hash functions and in [59] in which the framework checks overall codes of a module through self-signing. Before the insertion into a device, verification is performed in reference to a hash list. Encryption Techniques is provided only in [57] in which the proposed framework is based on the hash function, encryption and decryption and XOR operation. The only framework that uses machine learning in [58] in which it builds predictive models for detecting malicious traffic by deploying signature-based, anomaly-based or stateful protocol analysis methodologies either separately or integrated to provide efficient and accurate detection.

Table 6 shows that the frameworks support user interaction in which in [66] users can individually define different privacy preferences for different contexts. It is intended to give the user full control over her/his sensitive location information to allow the user to determine whenever and wherever the user's location is allowed to be shared, in [67] robot detect user's movement and nakedness and in [68] where some services using smart devices may require users to get a subscription before consuming the service. Therefore, a form of authentication is necessary for the service to check if the devices belong to a valid user while it is not supported in [65].

Conclusively, by comparing all the selected solutions, there are several techniques that are used for improving the abundant challenges that are raised in the IoT smart home. Such as implementing SOAP web services to enable interoperability among heterogeneous devices, providing context-aware middleware to share contextual information between device and sensors, supporting smartphone mobile application to allow the users to explore their energy consumption and suggest them with mechanisms to preserve the energy, allows the users to control and manage their smart home and devices through their smartphone or other devices that are developed with security practices that deploy authentication and authorization with access control techniques and let them achieve the privacy over their sensitive information in which give them control over the type of data they are sharing. Moreover, there are a lot of open issues in which still need to be studied and addressed such as reliability and efficiency of the sensor systems and the processing algorithms, lack of standardization of smart home, cost-effectiveness, legal issues, reimbursement and user experience or acceptance of the services and functionality provided by the smart home [71].

4 Conclusion

The smart home is one of the main research areas in IoT. It widens its benefits and services to the community as well as an environment that is why it is grabbing the great attention of the users and researchers. The context-aware approach is the key to develop an effective IoT-based smart home. It allows storing and using context information linked to the sensory data, which helps by providing relevant and smarter services\data depending on the users' requested tasks. This review paper presents (1) a set of frameworks and research projects proposed for the abundant challenges that are raised in the smart home environment, (2) provides the readers with great understanding of current research challenges linked with privacy, context-aware and security of IoT, (3) suggested appropriate solutions for them, (4) focused on possible set of open issues need to be addressed. This research review will help researchers to understand and develop effective smart homes solutions by providing most related information at one place.

References

1. Kamilaris, A., & Pitsillides, A. (2016). Mobile phone computing and the internet of things: A survey. *IEEE Internet of Things Journal, 03*(06), 885–898.
2. Tan, L., & Wang, N. (2010). Future internet: The internet of things. In *IEEE the 3rd international conference on advanced computer theory and engineering (ICACTE) 2010* (pp. 5–376).
3. Deng, N. (2012). RFID technology and network construction in the internet of things. In *IEEE the international conference on computer science and service system, 2012* (pp. 979–982).
4. Sunehra, D., & Bano, A. (2014). An intelligent surveillance with cloud storage for home security. In *IEEE annual IEEE India conference (INDICON), 2014* (pp. 1–6).
5. Porkodi, R., & Bhuvaneswari, V. (2014). The internet of things (IoT) applications and communication enabling technology standards: An overview. In *IEEE international conference on intelligent computing applications (ICICA), 2014* (pp. 324–329).
6. Evans, D. (2011). The internet of things how the next evolution of the internet is changing everything. Cisco White Paper, 2011, (pp. 1–11).
7. Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2013). Context-aware computing for the internet of things: A survey. *IEEE Journal of Communications Surveys and Tutorials, 16*(01), 414–454.
8. Oxford Dictionary. *Context definition*. Retrieved October 02, 2016, from https://en.oxforddictionaries.com/definition/context.
9. Chen, G., & Kotz, D. (2000). A survey of context-aware mobile computing research (Vol. 1, No. 2.1, pp. 2–1). Technical report TR2000-381, Department of Computer Science, Dartmouth College.
10. Luo, J., & Feng, H. (2016). A web-based framework for light-weight context-aware mobile applications. *SERSC International Journal of Database Theory and Application, 9*(04), 119–134.

11. Alam, M. R., Reaz, M. B. I., & Ali, M. A. M. (2012). A review of smart homes—Past, present and futures. In *IEEE transactions on systems, man, and cybernetics, part C (applications and reviews), 2012* (pp. 1190–1203).
12. Robles, R. J., & Kim, T. H. (2010). Review: Context-aware tools for smart home development. *SERSC International Journal of Smart Home, 04*(01), 1–12.
13. Park, J., Moon, M., Hwang, S., & Yeom, K. (2007). CASS: A context-aware simulation system for smart home. In *IEEE the 5th ACIS international conference on software engineering research, management and applications, 2007* (pp. 461–467).
14. Chong, G., Zhihao, L., & Yifeng, Y. (2011). The research and implement of smart home system based on internet of things. In *IEEE international conference on electronics, communications, and control (ICECC), 2011* (pp. 2944–2947).
15. Van Nguyen, T., Nguyen, H., & Choi, D. (2010). Development of a context-aware virtual smart home simulator. In *CoRR the 3rd international conference on ubiquitous information technologies and applications (ICUT'08) 2010* (pp. 1007–1274).
16. Samuel, S. S. I. (2016). A review of connectivity challenges in IoT-smart home. In *IEEE the 3rd MEC international conference on big data and smart city (ICBDSC), 2016* (pp. 364–367).
17. Warriach, E. U., Kaldeli, E., Bresser, J., Lazovik, A., & Aiello, M. (2011). Heterogeneous device discovery framework for the smart homes. In *IEEE GCC conference and exhibition (GCC), 2011* (pp. 637–640).
18. Souza, A. M., & Amazonas, J. R. (2013). A novel smart home application using an internet of things middleware. In *IEEE proceedings of 2013 European conference on smart objects, systems and technologies (SmartSysTech), 2013* (pp. 1–7).
19. Leong, C. Y., Ramli, A. R., & Perumal, T. (2009). A rule-based framework for heterogeneous subsystems management in smart home environment. *IEEE Transactions on Consumer Electronics, 55*(03), 1208–1213.
20. Perumal, T., Ramli, A. R., Leong, C. Y., Mansor, S., & Samsudin, K. (2008). Interoperability among heterogeneous systems in smart home environment. In *IEEE international conference on signal image technology and internet based systems (SITIS '08), 2008* (pp. 177–186).
21. Chang, C. Y., Kuo, C. H., Chen, J. C., & Wang, T. C. (2015). Design and implementation of an IoT access point for smart home. *MDPI Applied Sciences Journals, 05*(04), 1882–1903.
22. Perumal, T., Ramli, A. R., & Leong, C. Y. (2011). Interoperability framework for smart home systems. *IEEE Transactions on Consumer Electronics, 57*(04), 1607–1611.
23. Kim, J. E., Boulos, G., Yackovich, J., Barth, T., Beckel, C., & Mosse, D. (2012). Seamless integration of heterogeneous devices and access control in smart homes. In *IEEE the 8th international conference on intelligent environments (IE), 2012* (pp. 206–213).
24. Krishna, M. B., & Verma, A. (2016). A framework of smart homes connected devices using internet of things. In *IEEE 2nd international conference on contemporary computing and informatics (IC3I), 2016* (pp. 810–815).
25. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Journal of Communications Surveys and Tutorials, 17*(04), 2347–2376.
26. Li, X., Eckert, M., Martinez, J. F., & Rubio, G. (2015). Context-aware middleware architectures: Survey and challenges. *MDPI Sensors Journals, 15*(08), 20570–20607.
27. Evchina, Y., Dvoryanchikova, A., & Lastra, J. L. M. (2012). Ontological framework of context-aware and reasoning middleware for smart homes with health and social services. In *IEEE the 8th international conference systems, man, and cybernetics (SMC), 2012* (pp. 985–990).
28. Vahdat-Nejad, H. (2014). Context-aware middleware: A review. In P. Brézillon & A. J. Gonzalez (Eds.), *Context in computing* (pp. 83–96). New York: Springer. https://doi.org/10.1007/978-1-4939-1887-4_6.
29. Romero, D., Hermosillo, G., Taherkordi, A., Nzekwa, R., Rouvoy, R., & Eliassen, F. (2010). RESTful integration of heterogeneous devices in pervasive environments. In F. Eliassen & R. Kapitza (Eds.), *Distributed applications and interoperable systems* (pp. 1–14). Berlin: Springer. https://doi.org/10.1007/978-3-642-13645-0_1.
30. Souza, A. M., & Amazonas, J. R. (2013). A novel smart home application using an internet of things middleware. In *IEEE proceedings of European conference on smart objects, systems and technologies, 2013* (pp. 1–7).
31. Son, H., Tegelund, B., Kim, T., Lee, D., Hyun, S. J., Lim, J., & Lee, H. (2015). A distributed middleware for a smart home with autonomous appliances. In *IEEE the 39th annual conference computer software and applications conference (COMPSAC), 2015* (pp. 23–32).
32. Guo, B., Sun, L., & Zhang, D. (2010). The Architecture design of a cross-domain context management system. In *8th IEEE international conference on pervasive computing and communications workshops (PERCOM workshops), 2010* (pp. 499–504).
33. Vahdat-Nejad, H., Zamanifar, K., & Nematbakhsh, N. (2013). Context-aware middleware architecture for smart home environment. *SERSC International Journal of Smart Home, 07*(01), 77–86.
34. Hyun-Wook, K., Hoque, R. M., Hyungyu, S., & Yang, S. H. (2016). Development of middleware architecture to realize context-aware service in smart home environment. *DoiSerbia Journal of Computer Science and Information Systems, 13*(02), 427–452.
35. Kalaiselvi, M. A., Indumathi, M. V., Madhusudanan, M. J., & Venkatesan, V. P. (2012). Implementation of generic context middleware for context-aware applications. *ESRSA International Journal of Engineering Research and Technology (IJERT), 01*(03), 1–7.
36. Nassereddine, M., Rizk, J., Hellany, A., Nagrial, M., Elrafhi, A., Obeid, Z., & Hajar, K. (2016). Electrical energy management for advance smart home systems: Introduction. In *IEEE the 3rd international conference on renewable energies for developing countries (REDEC), 2016* (pp. 1–6).
37. Energy International Admission. (2016). *International energy outlook 2016*. Retrieved November 21, 2016, from https://www.eia.gov/forecasts/ieo/world.cfm.
38. Razzak, F., & Corno, F. (2012). Intelligent energy optimization for user intelligible goals in smart home environments. *IEEE Transactions on Smart Grid, 03*(04), 2128–2135.
39. Lima, W. S., Souto, E., Rocha, T., Pazzi, R. W., & Pramudianto, F. (2015). User activity recognition for energy saving in smart home environment. In *IEEE symposium on computers and communication (ISCC)* (pp. 751–757).
40. Kamilari, A., Tofi, Y., Bekara, C., Pitsillides, A., & Kyriakides, E. (2012). Integrating web-enabled energy-aware smart homes to the smart grid. *IARIA International Journal on Advances in Intelligent Systems, 05*(01), 15–31.
41. Moser, K., Harder, J., & Koo, S. G. M. (2014). Internet of things in home automation and energy efficient smart home technologies. In *IEEE international conference on systems, man, and cybernetics (SMC), 2014* (pp. 1260–1265).
42. Energy International Admission. (2016). *International energy outlook 2016*. Retrieved November 24, 2016, from https://www.eia.gov/forecasts/ieo/buildings.cfm.
43. Weng, M. Y., Wu, C. L., Lu, C. H., Yeh, H. W., & Fu, L. C. (2012). Context-aware home energy saving based on energy-

prone context. In *IEEE international conference on intelligent robots and systems (IROS), 2012* (pp. 5233–5238).
44. Iksan, N., Supangkat, S. H., & Nugraha, I. G. B. B. (2013). Home energy management system: A framework through context awareness. In *IEEE international conference on ICT for smart society, 2013* (pp. 1–4).
45. Yang, T. Y., Yang, C. S., & Sung, T. W. (2015). An intelligent energy management scheme with monitoring and scheduling approach for IoT application in smart home. In *IEEE third international conference on robot, vision and signal processing (RVSP), 2015* (pp. 216–219).
46. Khan, M., Silva, B. N., & Han, K. (2016). Internet of things based energy aware smart home control system. *IEEE Access, 4,* 7556–7566.
47. Jahn, M., Jentsch, M., Prause, C. R., Pramudianto, F., Al-Akkad, A., & Reiners, R. (2010). The energy aware smart home. In *IEEE 5th international conference on future information technology (Future Tech), 2010* (pp. 1–8).
48. Han, J. H., Jeon, Y. S., & Kim, J. N. (2015). Security considerations for secure and trustworthy smart home system in the IoT environment. In *IEEE international conference on information and communication technology convergence (ICTC), 2015* (pp. 1116–1118).
49. Yoon, S., Park, H., & Yoo, H. S. (2015). Security issues on smarthome in IoT environment. In J. Park, I. Stojmenovic, H. Jeong, & G. Yi (Eds.), *Computer science and its applications Lecture notes in electrical engineering* (Vol. 330). Berlin: Springer.
50. Desai, D., & Upadhyay, H. (2014). Security and privacy consideration for internet of things in smart home environments. *International Journal of Engineering Research and Development, 10*(11), 73–83.
51. Olawumi, O., Väänänen, A., Haataja, K., & Toivanen, P. (2017). Security issues in smart home and mobile health system: Threat analysis, possible countermeasures and lessons learner. *International Journal on Information Technologies and Security, 9*(1), 31–52.
52. Ul Rehman, S., & Manickam, S. (2016). A Study of smart home environment and its security threats. *International Journal of Reliability, Quality and Safety Engineering, 23*(03), 1–9.
53. Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications, 111*(07), 1–6.
54. Bugeja, J., Jacobsson, A., & Davidsson, P. (2016). On privacy and security challenges in smart connected homes. In *IEEE 2016 European intelligence and security informatics conference (EISIC), 2016* (pp. 172–175).
55. Hager, M., Schellenberg, S., Seitz, J., Mann S., & Schorcht, G. (2012). Secure and QoS-aware communications for smart home services. In *IEEE 35th international conference on telecommunications and signal processing (TSP), 2012* (pp. 11–17).
56. Elkhodr, M., Shahrestani, S., & Cheung, H. (2015). A smart home application based on the internet of things management platform. In *IEEE international conference on data science and data intensive (DSDIS), 2015* (pp. 491–496).
57. Kumar, P., Braeken, A., Gurtov, A., Iinatti, J., & Ha, P. (2017). Anonymous secure framework in connected smart home environments. *IEEE Transactions on Information Forensics and Security, 12*(04), 968–979.
58. Nobakht, M., Sivaraman, V., & Boreli, R. (2016). A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow. In *IEEE 11th international conference on availability, reliability and security (ARES), 2016* (pp. 147–156).
59. Kang, W. M., Moon, S. Y., & Park, J. H. (2017). An enhanced security framework for home appliances in smart home. *Human-Centric Computing and Information Sciences, 7*(1), 6–7.
60. Maamar, Z., Mahmoud, Q., Sahli, N., & Boukadi, K. (2009). Privacy-aware web services in smart homes. In *ICOST '09 proceedings of the 7th international conference on smart homes and health telematics, 2009 ACM* (pp. 174–181).
61. Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. *IJCA International Journal of Computer Applications, 90*(11), 20–26.
62. Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big data privacy in the internet of things era. *IEEE IT Professional, 17*(03), 32–39.
63. Arabo, A., Brown, I., & El-Moussa, F. (2012). Privacy in the age of mobility and smart devices in smart homes. In *IEEE international conference on privacy, security, risk and trust and 2012 international conference on social computing (SocialCom), 2012* (pp. 819–826).
64. Alami, A., Benhlima, L., & Bah, S. (2015). An overview of privacy-preserving techniques in smart home wireless sensor networks. In *IEEE the 10th international conference on intelligent systems: theories and applications (SITA), 2015* (pp. 1–4).
65. Chakravorty, A., Wlodarczyk, T., & Rong, C. (2013). Privacy preserving data analytics for smart homes. In *IEEE security and privacy workshops, 2013* (pp. 23–27).
66. Deva, B., Garzon, S. R., & Schünemann, S. (2015). A context-sensitive privacy-aware framework for proactive location-based services. In *IEEE the 9th international conference on next generation mobile applications, services and technologies, 2015* (pp. 138–143).
67. Fernandes, F. E., Yang, C., Do, H. M., & Sheng, W. (2016). Detection of privacy-sensitive situations for social robots in smart homes. In *IEEE international conference on automation science and engineering (CASE), 2016* (pp. 727–732).
68. Alpár, G., Batina, L., Batten, L., Moonsamy, V., Krasnova, A., Guellier, A., & Natgunanathan, I. (2016). New directions in IoT privacy using attribute-based authentication. In *ACM CF '16 proceedings of the ACM international conference on computing frontiers, 2016* (pp. 461–466).
69. Alqassem, I., & Svetinovic, D. (2014). A taxonomy of security and privacy requirements for the internet of things (IoT). In *IEEE international conference on industrial engineering and engineering management, 2014* (pp. 1244–1248).
70. Whitmore, A., Agarwal, A., & Xu, L. D. (2015). The internet of things—A survey of topics and trends. *Information Systems Frontiers, 17*(02), 261–274.
71. Wich, M., & Kramer, T. (2016). Enrichment of smart home services by integrating social network services and big data analytics. In 49th *IEEE Hawaii international conference on system sciences (HICSS), 2016* (pp. 425–434).

Zahrah A. Almusaylim received her B.Sc. (Hons) in Computer Science in 2014 from College of King Faisal University; Saudi Arabia. She is currently pursuing her master in Computer Science at King Faisal University since 2015 up to date. Her area of interest includes Internet of Things, Cloud Computing, Context-Aware Computing, machine learning, Sensor networks and Web and Mobile Applications Programming.

Noor Zaman has 16 years of teaching and administrative experience internationally, authored several research papers in indexed and impact factor research journals and conferences, edited 06 international reputed Computer Science area books, focused on research students. He has successfully completed more than 18 international research grants. He is Associate Editor, Regional Editor, and Editorial board member, PC member, reviewer for several reputed international journals and conferences around the globe. His areas of interest include Wireless Sensor Network (WSN), Internet of Things IoT, Mobile Application Programming, Ad hoc Networks, Cloud Computing, Big Data, Mobile Computing, and Software Engineering.