Internet of Things 1–2 (2018) 81–98

Contents lists available at ScienceDirect

Internet of Things

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

IoT-based smart homes: A review of system architecture, software, communications, privacy and security

Dragos Mocrii[a], Yuxiang Chen[b], Petr Musilek[a,c,*]

[a] Electrical and Computer Engineering, University of Alberta, Edmonton, Canada
[b] Civil and Environmental Engineering, University of Alberta, Edmonton, Canada
[c] Cybernetics, Faculty of Science, University of Hradec Králové, Czechia

ARTICLE INFO

Article history:
Received 10 August 2018
Accepted 18 August 2018
Available online 4 September 2018

Keywords:
Smart home
Architecture
Internet of Things
Software
Communication technologies
Privacy
Security

ABSTRACT

This article presents a review of major technologies of IoT-based smart homes. It starts with definition of the smart home that sets the perspective adopted in the review. In addition to describing the complementary user and system functions of the smart home, it introduces its general, IoT-based architecture and sets smart homes within the larger context of the smart grid. The following sections concentrate on software solutions and components of smart home management systems, related communication technologies, and issues of privacy and security associated with the connected nature of modern smart homes. A separate section presents current challenges of smart home technologies and their dispersion, and points to some interesting solutions and future trends.

1. Introduction

Smart home has been described as a contemporary application of ubiquitous computing that incorporates intelligence into dwellings management and operation for "comfort, healthcare, safety, security, and energy conservation" [1]. This view, also adopted in this survey paper, exemplifies the convergence of two complementary perspectives of smart home functionality: user- and system-centric, that respectively concentrate on the comfort of the occupants and efficiency of the building system [2]. The user- or home-centric approach to smart homes started in the first half of the 20th century and evolved for decades. The system- or building-centric view only came about with the advancement of information and communication technology (ICT) and the advent of smart energy infrastructure.

Over the past decade, there has been a surge in the development of new "smart" devices that can connect to the Internet and be controlled using applications remotely. This network of devices and other items embedded with sensors, electronics, software and connectivity is called the Internet of Things (IoT). Together with another new technology of cloud computing, it has led to cloud-centric IoT-based solution for smart home development [3].

The IoT makes the shift from functionality to connectivity and data-driven decision making, meaning that a device can become more useful if it is interconnected with other devices. However, the IoT is not simply a bunch of devices and sensors connected to each other in a wired or wireless network – it is a dense integration of the virtual and the real world, where

* Corresponding author at: Electrical and Computer Engineering, University of Alberta, Edmonton, Canada.
E-mail address: petr.musilek@ualberta.ca (P. Musilek).
URL: http://www.ualberta.ca (P. Musilek)

https://doi.org/10.1016/j.iot.2018.08.009
2542-6605/

Nomenclature

ACD	adaptive critic designs
API	application programming interface
BAN	body area network
BLE	Bluetooth low energy
DoS	denial of service
FHSS	frequency hopping spread spectrum
FMCW	frequency modulated carrier waves
HAN	home area network
HMM	hidden Markov models
ICT	information and communication technology
IoT	Internet of Things
LAN	local area network
MCU	micro-controller unit
NIST	National Institute of Standards and Technology
OS	operating system
OSI	open system interconnection
OTA	over the air
PAN	personal area network
PLC	power line communication
PSO	particle swarm optimization
PV	photovoltaic
QoE	quality of experience
QoS	quality of service
RF	radio frequency
RFID	radio frequency identification
RTOS	real time operating system
SG	smart grid
SH	smart home
SVM	support vector machine
WLAN	wireless local area network
WPAN	wireless personal area network
WSN	wireless sensor network

the communication between people and devices takes place. It can be considered an interwoven medium of networks of different sizes [4], that makes up a large global network.

The focus of This review paper focuses on the new aspects of smart homes brought by the introduction of the new computing paradigms. Section 2 defines smart home and introduces its cloud-based architecture. It also briefly touches upon the connection of smart homes and smart grids. Section 3 reviews three classes of software important for the IoT-based smart homes - operating systems, systems for occupant tracking, and software for data acquisition and processing. Section 4 examines commonly used communication technologies and protocols, both wired and wireless. The issues of data privacy and security of smart home systems are covered in Section 5. Challenges and and future direction in smart home development are identified in Section 6. Section 7 provides a brief summary and concludes the review.

2. Smart homes

This section provides the background of the reviewed smart home technologies. It starts with definitions of smart home and intelligence in the smart home context, followed by a description of a cloud-based smart home architecture. It also identifies important properties of smart homes that make them valuable, active participants in the modern smart grids.

2.1. Defining smart home

The concept of smart home first appeared in 1930s' vision of the "homes of tomorrow" [5] as marvel domestic efficiency. Most promises of "unprecedented levels of luxury, relaxation and indulgence," and "benefits of modern living with less effort from householders" were not realized until the final decades of the century. In parallel, the emphasis on domestic efficiency expanded towards energy efficiency. Darby [2] identifies two main smart home definitions:

Home- and user-focused that defines smart home as a highly automated residential building with integrated appliances, emphasizing modern technology, convenience and (domestic) efficiency.

Building- and system-focused that concentrates on building energy performance, ancillary services and distributed energy generation; and how they can be addressed using information and communication technology.

The author then points out that both definitions share the significance of communications to link devices with each other and to enable remote access and control, and to provide of services [2].

When talking about smart homes, one should also consider how "smart" or "intelligent" can be defined. What makes a smart home different from a conventional home most of us still live in? According to Edwards and Grinter [6], the intelligence has the following four characteristics, in the context of smart environments and ubiquitous computing:

1. The environment can use the sensor data to assess the current state of the world (e.g. if a motion sensor detector has been triggered, it means there must be someone walking nearby).
2. The environment can assume its current state, by taking into consideration multiple factors at once (e.g. if there are multiple people at the table, the system might infer that it's dinner time).
3. The environment may predict a user's intent, by assessing the situation from its own point of view (e.g. if subsequent motion detectors are triggered, it means the user is walking along a corridor, and so the user might want to have their way lighted up).
4. The environment may act preemptively based on the intent assumption (e.g. the system might decide to turn on the lights ahead of time, so that the user can walk on their path safely).

We can think of a smart environment as an intelligent agent that can assess the state of the residence, its occupants and their physical surrounding using sensors, and act on the environment using effectors in such a way that specified performance measures are optimized [7]. The performance measures to be maximized in a smart home can be comfort and productivity of its inhabitants, whereas those to be minimized are the operation costs (i.e. cost of energy and other utilities) [8].

For a system to be intelligent, it has to be customizable, context-aware, adaptive, and anticipatory [9,10]. An intelligent living space is characterized by the environment's ability to respond to the needs of its residents [11]. Therefore, we must draw a line between smart home intelligence and automation. Automation is just a subset of an intelligent environment, and people have been using automation techniques for a long time (thermostats, the washing machine, etc). Automation does not see the bigger picture though, since it is only concerned with managing a limited number of things. Intelligence on the other hand, is defined by having a larger image of the whole environment through all the interconnected devices and sensors, and therefore can better adapt and make predictions based on the current state of the system and previous knowledge about the inhabitants.

2.2. Smart home architecture

A smart home contains at least few devices, such as sensors, appliances, or actuators, that are not necessarily smart on their own. A sensor generates data, but it does not add any value to the home environment on its own. Similarly, a thermostat is not considered smart, if the homeowner has to regulate the temperature based on the external temperature, humidity, and other factors. It can maintain a constant temperature, but that is automation, not "smartness". It is only when all data about the environment is collectively stored and analyzed, patterns extracted, and decisions made without the user's intervention, that an environment can be called smart. The architecture of a smart home is determined by the way devices communicate with one another, how and where the information from sensors and appliance usage habits is stored, how this information is processed and trends are extracted, and how the user can interact with the devices and vice versa. Several types of architectures have been investigated in previous studies.

Soliman et al. [12] created a system architecture for a smart home. Sensor and actuator are connected to a micro-controller and used to collect data about the environment and perform certain actions. The data is communicated from the micro-controller enabled sensors to a central server using the wireless ZigBee technology. The server then uploads the data to a cloud storage via an application programming interface (API). The Cloud solution is comprised of a back-end application, storage, and a front-end application. The data is processed and analyzed in the back-end (Google App Engine). The user can visualize the environment and control devices using a Web application.

Cook et al. [13] proposed an architecture with the physical layer made of controllers (computer servers), sensors (motion/light/door/temperature sensors), and actuators (relays). The communication layer is based on wireless communication technology such as ZigBee wireless mesh. The middleware layer is based on a publish/subscribe pattern.

Jie et al. [14] proposed an architecture model that tackles the issue of scalability. By using the proposed model with uniform interfacing, devices can be added to or removed from the smart home infrastructure with minimal effort. The architecture is divided into five layers: (1) the resource layer (end devices, sensors, appliances); (2) the interface layer (abstraction layer between higher level layers and the devices); (3) the agent layer (agents are responsible for managing individual resources, by using RFID tags); (4) the kernel layer (agent management and main controller); (5) user application layer (user's interface to manage services and devices).

Zhou et al. [15] proposed a cloud based architecture, called CloudThings, aimed at speeding up IoT application, development, and management. End devices (Things) use the CoAP protocol with 6LowPAN, and therefore they have a direct access to the Internet. CloudThings is an online platform that leverages the complete application infrastructure for developing,

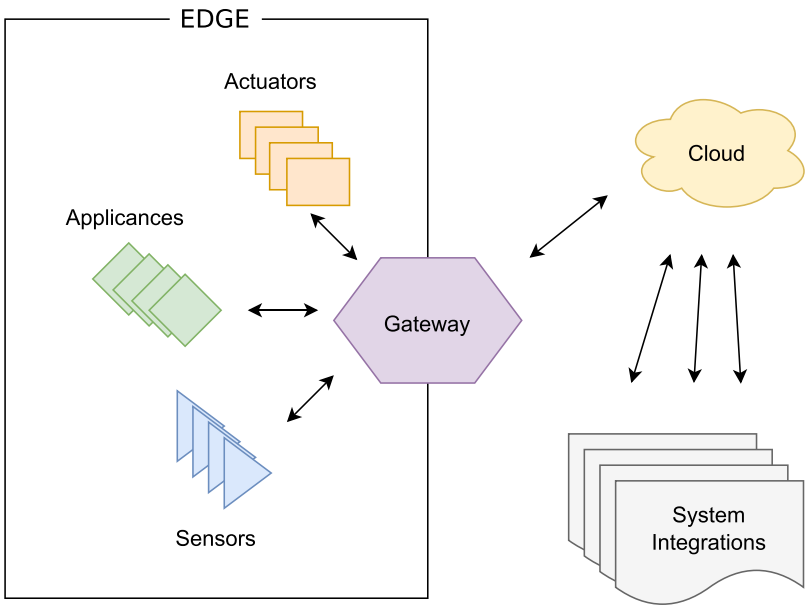

Fig. 1. Cloud-based architecture of a smart home.

deploying, managing and composing Things applications and services. This architecture is based on three components: (1) Infrastructure as a service (IaaS) that provides all the infrastructure needs in the cloud, without the need to worry about computation power, storage, scalability, or managing servers; (2) Platform as a service (PaaS) that serves as a framework for developers to develop and deploy capabilities around the Things; (3) Software as a service (SaaS), which provides the means to handle and support specialized services like Things discovery, Things composition, data mining, etc.

Fig. 1 presents a general, cloud-based architecture of a smart home. The inner network (BAN, PAN) is composed of end devices, sensors, appliances and actuators. These devices are communicating with a gateway located at the edge of the network, that facilitates the connection between the inside networks and the external Internet.

A gateway device bridges the communication gap between the end devices, sensors, systems, and the cloud. In [16] Hosek et al. describe the hardware and technology requirements for a smart home gateway device. Guoqiang et al. [17] propose a smart home gateway design that is configurable in terms of communication protocols supported, and which can translate heterogeneous sensor data into a uniform format.

The gateway is generally a device that supports multiple communication protocols for interoperability with the end devices. It is powerful enough to do some processing at the edge of the network, before sending the data to the cloud. The gateway also adds a layer of security to the smart home network, since it bridges the communication between end devices and the outer world, and therefore all communication can be filtered before commands make it to the end devices (which are resource constrained, low powered, have lower security layers, and are therefore more vulnerable to attacks). The could essentially provides means to increase availability, reliability and security, while at the same time taking advantage of higher computation power and scalable architecture. The cloud can integrate with many third party services, such as data visualization, smart home device management, or user access and role management.

2.2.1. Cloud computing

The National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [18].

In the context of smart home architecture, cloud is used to aggregate all data from different sources (sensor, actuators, appliances and other devices) and process it. The cloud is the most advanced level of the architecture [19] that provides massive data storage and processing infrastructure [3] with high reliability, scalability and autonomy [20]. Due to the central role the cloud plays in this framework, it is often called cloud-based or cloud-centric architecture [3].

2.2.2. Fog computing

Fog computing is a recent computing paradigm first coined by Cisco in 2014 [21] for the extended cloud computing model and adopted in a number of related applications [22–24]. As with many emerging technologies, fog computing suffers from some inherent security and privacy issues [25,26].

The cloud computing paradigm has worked very well since its adoption about a decade ago. However, due to an ever increasing number of IoT devices that produce more data and need to connect and push the data to the cloud, some issues with this model have started to appear. One of the biggest issues in modern computing is that CPU processing power has increased dramatically over the years, however bandwidth for memory and data transmission in general has not been able to keep up with the growth trend [27]. As a result, network bandwidth has become a bottleneck, hindering the performance of cloud-based systems. Fog computing addresses this issue by bringing computing closer to where the data is generated. This way, data can be processed in between the data source and the cloud, before the trimmed down data is sent to the cloud. In the context of a smart home, fog computing refers to data computations occurring on the gateway device. Since the gateway is closer to the source, data can be transferred from the end devices to the gateway very quickly. The data is then merged from all sources, preprocessed, compressed, and then sent to the cloud for further, more intensive computations. The information sent to the cloud is therefore not "raw" data anymore, but a trimmed version of the original data that takes less bandwidth to transmit. The main objectives of fog computing are [28]

- Reducing the amount of data sent to the cloud;
- Decreasing network latency;
- Improving system response time in mission-critical situations.

Fog computing also has the benefit of avoiding single point of failure situations. For example, if the Internet connection were to drop, the smart home gateway would still collect the data from the end devices, process it, and send it to the cloud when the Internet connection is resumed. Moreover, the benefits in regards to the cloud are bidirectional: not only a gateway device helps to decrease the amount of data sent to the cloud, but also the cloud only needs to send messages to the gateway which then broadcasts the messages to the appropriate end devices.

2.2.3. Edge computing

Edge computing is another computing paradigm. It shares the same objectives as fog computing, but differs in how the objectives are met. Lopez et al. [29] discussed the concept with an emphasis on human-driven applications, where edge computing enables humans to stay anonymous and maintain their privacy. Multiple case studies have been analyzed by Shi et al. [30] along challenges and opportunities of the paradigm. Shi and Dustdar [31] also identified some open issues regarding privacy and security in edge computing.

Compared to fog computing, edge computing takes localized computation even further, by making each end device in the smart home capable of deciding if the data should be stored locally, processed locally, or sent to the cloud. Since each individual end device is capable of performing some inference and communicating with the cloud, the resulting system is more decentralized further decreasing the risk of single-point-of-failure. In other words, in edge computing, data processing and decision making is brought to the gateways at the edge of the Internet network.

2.3. Smart home and smart grid

In the past decade, there has been an observed global consciousness towards energy consumption, especially regarding energy efficiency measures and the use of renewable energy sources. This has been made possible by the introduction of the concept of smart grid (SG) as a vehicle to modernize the electricity grid. Its first official definition provided ten characteristics of SG infrastructure [32]. Half of these characteristics are directly related to smart homes (original item numbering is used in the list reproduced below):

(4) Development and incorporation of demand response, demand-side resources, and energy-efficiency resources.
(5) Deployment of 'smart' technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.
(6) Integration of 'smart' appliances and consumer devices.
(7) Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal storage air conditioning.
(8) Provision to consumers of timely information and control options.

Smart grid features thus expand energy efficiency beyond the delivery infrastructure and into the home. By allowing electricity and information to flow in both directions between the home and the grid, the electricity system becomes more flexible, interactive, and can provide real-time feedback.

An important feature of a smart grid is demand response (DR) [33]. By coordinating operation of low priority home appliances (such as washing machines or water heaters), DR can take advantage of the most desirable energy sources, and at most favorable prices. There are two type of energy scheduling:

1. Energy resource scheduling (which deals with the timing of when specific energy sources are used, i.e. when to use the grid and when the home installed PV panel system); and
2. Energy consumption scheduling (where the objective is to optimize the timing when various home appliances should be active, due to constraints such as residual amount of locally stored energy, or current cost of electricity under a time-of-use pricing scheme).

Fuselli et al. [34] proposed a new method of energy resource scheduling using action dependent heuristic dynamic programming. Based on a class of adaptive critic designs (ACD), it is composed of two neural networks: action network, which defines the control state; and critic network, that criticizes the action network and improves the optimal state of the former over time. The objective is to minimize a utility function, given a set of constraints. The parameters of both networks are pre-trained using particle swarm optimization (PSO) algorithm. This combined approach results in a considerable improvement of scheduling accuracy and scheduling horizon over previous methods involving ADC without PSO [35–37].

Because information can flow alongside with electricity from the consumer to the grid, and vice versa, this opens up some possibilities of control over a smart home's appliances. Smart meters can measure the amount of energy used sometimes down to the level of individual appliances. This information can be gathered, stored, and processed in a smart home energy management system (HEMS) [38]. HEMS is a device operating within the home's premises that can schedule the operation of appliances (e.g. based on the time-of-use pricing), as to minimize electricity costs and maximize efficiency. However, it is not possible to manage all home appliances, because some are not schedulable. In general, home appliances can be classified into two groups [38]:

- Non-schedulable appliances that cannot be scheduled, due to the nature of the task they are designed to accomplish (i.e. the fridge, a lamp, an electric kettle); and
- Schedulable appliances that can be scheduled (i.e. a washing machine, a dryer, a domestic hot water boiler); they can be further divided into:
  - Interruptible appliances: these are appliances which can be interrupted from operation at any time (i.e. a domestic hot water boiler, an electric vehicle charger)
  - Non-interruptible appliances: these appliances cannot be interrupted once they start operating (i.e. a washing machine, a dishwasher).

These few examples show that smart grids rely on smart homes. The use of smart appliances, the data gathered through various sensors and smart meters, allows a smart home to optimize its quantitative and temporal electricity demand from the grid, and to minimize the cost of electricity (or even make profits, if electricity is generated on site and exported to the grid). However, a detailed treatment of this aspect of smart homes is outside the scope of this survey. An interested reader may refer to numerous other resources in the literature, e.g. [39–41].

3. Software

This section reviews the most important software components of modern smart homes. After outlining important features of operating systems for smart homes and devices, it proceeds with describing two major software subsystems: occupant behavior tracking and data processing.

3.1. Operating system

IoT is composed of devices embedded with micro-controller unit (MCU) based systems and interconnected through different communication means. Indeed, software plays an important role in IoT operation. In general, there are two types of IoT components that are embedded with operating systems: end devices and gateways.

The end devices could be sensors, actuators, switches, that can normally perform only a limited set of operations. These devices are typically small and have a resource (e.g. RAM, ROM, and energy) constrained MCU that is highly energy efficient, and supports short range, low power communication protocols. Traditionally, MCUs have an embedded system on them that is flashed in the ROM at the factory, and cannot be changed or updated after the product has exited the production line. However, MCUs are getting cheaper to produce and at the same time more complex and powerful (e.g. moving from 8/16 to 32 bit architectures). As a result, it is now feasible to install software that can do more on the device itself, and that can receive hot security patches over the air (OTA). This software can be an entire operating system (OS) that can add more functionality and more security on the device. Since these end devices are still limited in resources, the data has to be collected and communicated in real-time with no buffering, these operating systems are called real time operating systems (RTOS). The use of RTOS also enable a programmer or system integrator to be more productive, since most of the low-level operations are available to them through the OS [42]. In order to collect the data from these end devices (sensors), or to send a command for execution based on some event (actuators), a more powerful device is needed – the gateway.

Gateway devices act as a bridge between the many IoT devices in a smart home, since they support more communication protocols and have more resources to gather and process the data. Moreover, if cloud services are part of a smart home architecture, then these gateway devices are also referred to as edge gateway, since they sit at the intersection of the external Internet and the internal local Intranet. Hence, these devices are more powerful and need to run an operating system that supports different communication technologies. They must also be secure and resilient to penetration attacks from the external Internet. Unlike the end devices, gateway devices usually have a user interface for managing various parts of the network, or for data visualization.

The main features to consider when selecting an operating system for IoT devices include [43,44]:

- Footprint: since most end devices are constrained in available resources, the OS must have a small footprint for running on the device. This might not apply to gateway devices that usually have generous resources available.

Table 1
IoT operating systems.

OS name	Min RAM	Min ROM	Program. model	Realtime	Language	License
Contiki	10KB	30KB	Proto-threads	Partial	C	Open-src
TinyOS	1KB	4KB	Event-driven	No	NesC	Open-src
RIOT	1.5KB	5KB	Threads	Yes	C, C++	Open-src
Mantis	14KB	50KB	Threads	Partial	C	Open-src
FreeRTOS	1KB	10KB	Threads	Yes	C	Open-src
Nano-RK	2KB	18KB	Threads	Yes	C	Open-src
LiteOS	4KB	128KB	Threads/ Events	Yes	LiteC++	Open-src
Apache Mynewt	16KB	128KB	Threads	Yes	Assembly, C, Go	Open-src
Zephyr OS	8KB	128KB	Threads	Yes	Multiple	Open-src
Ubuntu Core Snappy	128MB	350MB	Threads	No	Multiple	Open-src
Android Things	512MB	4GB	Threads	No	C, Java, Kotlin	Open-src
Windows 10 IoT	256MB	200MB	Threads	Partial	Multiple	Propriet.
WindRiver VxWorks	1MB	128KB	Processes	Yes	C, C++	Propriet.
Micrium μC/OS	1KB	6KB	Threads, Tasks	Yes	C	Propriet.
MicroEJ OS	32KB	128KB	Threads	Yes	C, C++, Java	Propriet.
Express Logic ThreadX	1KB	2KB	Threads	Yes	C	Royalty-Free
Nucleus RTOS	2KB	12KB	Threads	Yes	C, C++	Propriet.

- Scalability: the OS needs to scale depending on the available resources, or architecture of the CPU.
- Modularity: the OS needs to be modular, and the system integrator should be able to choose which modules to include. Normally, the OS will provide just the barebone functionality needed to load programs on the MCU, but if additional modules (like supporting alternative communication protocols, or other add-ons) are needed, the OS needs their inclusion out of the box.
- Portability: the OS needs to be portable on different types of hardware, possibly with different architecture. This is usually accomplished through abstraction of hardware requirements.
- Connectivity: ability to communicate with other devices is essential for an IoT device. The OS must support communication technologies like Ethernet, Wi-Fi, Bluetooth LE, etc.
- Security: the OS needs to provide the means to add security measures as needed. Lighter systems have smaller number of default security features, but the developer needs to be able to add more if needed.
- Reliability: the OS needs to be reliable since most end devices are not meant to be serviced regularly, and need to be running error-free for long periods of time. This means that they should also pass certain certifications, especially when used in mission-critical situations.

Another important aspect of an operating system is the ability to run programs concurrently. This is especially important for Real Time operating systems, because processes have tight deadlines, and cannot take too much time blocking other processes waiting for the allocation of their resources. There are several programming models which characterize the way in which code is executed and how resources are allocated to processes. There are different paradigms based on the purpose for which the operating system is designed for [43,45]:

- Process: is an instance of a computer program that is loaded into memory in binary format, has allocated resources, and is being executed. Processes are independent of each other.
- Thread: is a lightweight sub-unit of execution within a process. They have their own stack, can access the shared data in their parent process' heap, and can communicate between each other easily.
- Proto-thread: is an extremely lightweight stackless thread that is designed for severely constrained memory systems. Since it is a sequential implementation of a state machine, it works great on an event-driven system.
- Event: is triggered as a result of an action in an event-driven system. The event is dispatched and an event handler picks it up, but only one event handler can run at a time.
- Task: is a unit of work, that is assigned to a worker from a pool of workers. Workers can be threads, processes, or machines.

Table 1 shows a list of the several popular IoT operating systems. The list compares the systems based on their minimum footprint, programming model, whether the system is an RTOS or not, what languages are supported programming, and license under which it is issued. Some of these systems have a smaller footprint (for example TinyOS, RIOT, FreeRTOS), making them suitable for end-devices. Other systems are more demanding in terms of resources (for example Windows 10 IoT, Android Things, Ubuntu Core Snappy), and are therefore more suitable for running on gateway devices. The lower the footprint, the smaller the set of features that are supported by the OS, and the less security is provided out of the box. Therefore, for gateway devices, the use of a full-featured OS (such as Android Things) makes it easier to bridge multiple end-devices without much configuration, and also provides higher level of security against vulnerabilities from the external Internet.

3.2. Human activity tracking

Smart home is designed to improve the standard of living of its occupants and/or to optimize its performance. In both cases, it is important that the system is able to analyze and recognize activities of its occupants [13]. A few examples of activity recognition mediums are: video cameras, heat cameras, radars, floor pressure sensors, etc. It is important that the activity recognition be performed in real-time, so that the smart home can "react" and "adapt" instantly if need be. Fog and edge computing are enablers of this, which will be discussed later. Activity recognition and prediction is a two step process. The first is the activity discovery, that is done with unsupervised learning methods. The second is the activity recognition and prediction, which use supervised learning techniques, and is facilitated with the clustered data obtained in the previous step.

Unobtrusive tracking and sensing methods. For smart homes to offer a higher level of comfort and convenience, it is important that sensing and tracking is done in a non-intrusive way. In other words, the occupants should not be aware at all times that they are being tracked or required to wear specific wearable body sensors. There have been several major steps in this direction achieved using wireless signals. This technology was originally developed for military applications including detection of people behind walls, or trapped under collapsed structures [46,47]. However, the military grade technology used high power wireless signals and reserved wireless spectrum, rendering it infeasible for use in consumer applications. Researchers at MIT have developed a new way to measure breathing and heart rate, by using a radar technique called frequency modulated carrier waves (FMCW). This technology can detect chest movements due to breathing, and skin vibrations due to heartbeats [48]. With properly positioned sensors, it can monitor a person from up to 8 meters away, even behind a wall; this is plenty of coverage for an average sized house. Even more impressive is the accuracy: 99.3% for breathing, and 98.5% for heartbeats. Similar work has been done with Doppler radars [49]. A comprehensive survey on advances in radar sensors has been conduced by Li et al. [50]. Alternative methods include accelerometric sensors mounted on mattress [51].

Although techniques for unobtrusive vital signs detection are currently developed mainly for medical purposes, the full potential of these technologies can be realized in other application domains as well. Since the purpose of the smart home is to use "intelligence" to provide a comfortable and adaptive environment, having access to the refined information about the inhabitants (such as breathing and heart rates) can further improve responsiveness of the smart home systems and the level of comfort they provide. For example, currently the optimal temperature in a house is determined by measuring the inside and outside temperatures, relative humidity, pressure and other environmental metrics, without consideration of the inhabitants themselves. If their breathing and heart rates were considered, better decisions for setting the optimal temperature in the house could be reached, as these vital signs are directly correlated with body temperature and well-being [52].

Activity discovery. An important part of human activity tracking is activity discovery. Since the various sensors (motion detectors, cameras) will continuously generate streams of data, efficient algorithms need to be implemented that can identify new types of activities, that can later be used for recognition. To our best knowledge, unsupervised learning methods are best suitable for discovering patterns in large amounts of data, which is what activity discovery is about.

Cook et al. [13] use an unsupervised learning algorithm, that partitions the data stream into smaller classes, which then simplifies the activity recognition step. The activity detection, is stored as a compressed sequence of data from multiple sensors.

Bourobou et al. [53] have used the K-pattern clustering algorithm to identify activity patterns in large amounts of data collected from sensors. They also compared K-patterns algorithm to other popular algorithms like K-means, expectation maximization, and Farthest First, but K-pattern provides the best performance in terms of running time and numbers of clusters identified.

Activity recognition and prediction. Activity recognition and prediction is what enables a smart environment to react to what the user is doing. For example, if an inhabitant entered a room after 10 p.m., laid in bed, and stayed still for a period of time, the smart home might assume that the person has fallen asleep, and therefore decide to turn off the lights, and set the house temperature to a value that is comfortable for sleeping. The key part of making this possible is that the smart home needs to understand the human activities and recognize them in real-time, and so researchers are actively working on implementing various methods and frameworks to bring activity recognition and prediction capability to smart homes.

Cook et al. [13] have tested various machine learning methods, such as support vector machines (SVM), naive Bayes classifiers, hidden Markov models, and conditional random fields. The best performer they found was SVM. In addition to a superior performance, it also had the advantage of returning the degree of match for a particular activity type.

However, no single technique can serve as a universal solution, and therefore multiple methods have to be used together to obtain better results and form more complex hybrid intelligent systems [54]. For example, genetic algorithms (GA) or methods of swarm intelligence are a good fit for improving the machine learning and prediction capabilities of a system. Exploitation of their complementary paradigms of competition and cooperation can be used to link the performance of multiple agents into a single, better performing model [55].

Jalal et al. [56] propose to use a depth camera (Microsoft Kinect) to perform Human Activity Recognition. Since activity recognition is based on a sequence of actions, the authors have chosen hidden Markov models (HMM) for training, using the

previously obtained code representations of the motions. The authors have found that HMM with 4 hidden states generate the best results, with a 92.33% accuracy.

Fatima et al. [57] propose a unified framework for activity recognition and prediction in a smart home using SVM kernel classifier and conditional random fields. The authors reported accuracy scores of 92.70–94.11% for activity recognition, and 79.71–84.78% for activity prediction.

Bourobou and Yoo [53] have proposed to use Artificial Neural Networks (ANN) and J48 decision trees to solve the activity recognition problem for smart home applications. The authors argue that ANN are better at activity prediction than Hidden Markov Models, Naive Bayes, or C4.5 decision trees, because ANN does not face the challenges of long training times, and interleaving events. The accuracy of the model trained with ANN and J48 is 83% for a two week activity period. However, the authors do not specify which dataset was used to perform the experiments.

3.3. Data acquisition and use

The ever-growing number of IoT devices generates a tremendous amount of data that requires new infrastructure and technologies to store and manage it. This phenomenon, called big data, is characterized as a byproduct of three drivers, called the "three Vs": Volume, Velocity, and Variety [58]. This definition, proposed by Gartner in 2001, has been recently updated to align with current standards by adding two more "Vs" [59]:

- Volume refers to the amount of data that is generated each second from various sources, and has to be stored and analyzed.
- Velocity characterizes the speed at which data is generated, stored, and processed.
- Variety defines the heterogeneity of the data (structured and unstructured).
- Veracity is is a qualitative measure of data trustworthiness that determines how usefulness and meaningful the data is.
- Value refers to the importance or worthiness of the data. It is directly proportional to veracity, because as the value of the data increases, so does the need of assuring the data integrity and accuracy.

In this paper, we are interested in the application of big data in the context of IoT and smart homes. For a comprehensive, general survey on Big Data related topics, the reader may refer to [60–64].

Data acquisition. Data acquisition is the initial stage in the life-cycle of Big Data. In the context of a smart home, data can come from three sources: from active interaction with the user, from passive interaction with the user, or from non-user generated sources:

- The active user interaction source is data that is directly generated by the user: voice commands, gesture recognition, triggering actions from pushing a button, interacting with a touch screen.
- The passive user interaction source is the data generated as a result of a human action: motion detector sensors, video from cameras, silhouettes from depth cameras, RFID identification tags, smart floor sensors, wearable body sensors.
- The non-user generated data, is the data obtained from other IoT devices or smart devices: thermostat readings, humidity sensors, air flow sensors. In the context of the smart grid, the non-user generated data would be the electricity usage for each smart device, the time and duration when those devices are used, market pricing data, etc.

The classification of generated data can be used for (1) evaluation of source-dependent data trustworthiness; (2) attribution of data ownership and other legal implications, (3) inference about the structure of the data (user generated data is usually unstructured, with more noise, whereas sensor readings from electricity usage have a known type and measurement units).

Data fusion. Data collected by different sensors in a smart home needs to be merged and processed to extract meaningful information about the state of the environment and the inhabitants. This can be accomplished using data fusion techniques that "combine data from multiple sensors, and related information from associated databases, to achieve improved accuracies and more specific inferences than could be achieved by the use of a single sensor alone" [65].

Merging data from multiple sensors is known in the literature as multisensor fusion. It is an inherently difficult task, because of the heterogeneous nature of the data, and constantly increasing volume of sensed information.

Zheng et al. [66] identified three categories of data fusion algorithms:

Statistical approaches include the simplest approach of weighted average, along with multivariate statistical analysis and most state-of-the-art data mining algorithms [67]. The statistical approach might not be a good fit for incommutable data or when used with estimators/classifiers that have different performances [68].

Probabilistic approaches include maximum likelihood methods and Kalman filtering [69,70], probability theory [71] and evidence theory. Kalman filter is often used because of its low complexity, ease of implementation and mean-squared error optimality. However, it cannot be used with data whose error characteristics are not easily described in terms of parameters.

Artificial intelligence methods such as genetic algorithms, neural networks and decision trees. In many applications, neural networks are used both to develop classifiers and as a data fusion tool [67,68]

Data fusion can be performed in a centralized or decentralized fashion. In centralized fusion, the data is merged at a central location (e.g. at a smart home gateway). In this case, the data is fused from their sources based on predefined set of rules. In decentralized fusion, data is merged at the source (i.e. the sensor) that needs to have adequate computational power [72].

Data processing. Before the data is ready for use, it generally goes through a series of transformations. This process can be viewed as a number of interconnected funnels connected to each other, and data percolating through each funnel before it reaches the final state. This metaphor forms the basis of the 6-level Joint Directors of Laboratories (JDL) model for information exploitation [73]:

Level 0 – Data alignment: the raw data obtained from the sensors is corrected from bias, standardized, and key information is extracted.
Level 1 – Entity assessment: data from level 0 is combined with data previously obtained from other sensors, to estimate identity and characteristics of individual entities.
Level 2 – Situation assessment: relationships between entities are interpreted based on their relation to the current context or environment.
Level 3 – Impact assessment: consequences of current situation are estimated by predicting the system evolution.
Level 4 – Process refinement: subsequent data is monitored to optimize the utilization of sensor information.
Level 5 – User refinement: the fusion system is optimized to improve the efficiency of supporting a human operation.

A comprehensive analysis of the state-of-the-art methods on data transmission, data processing, storage systems and cloud infrastructures in the context of a smart home can be found in the work by Díaz et al. [74].

4. Connectivity and communication protocols

In a smart home environment, devices need to be interconnected to exchange information. Intelligence, as we previously defined it, is when the environment is able to understand the state of the current system. For this to happen, a single sensor is not enough to extract much useful information, and therefore multiple sensors are needed which can communicate with each other and extend the usefulness of the acquired information. The ways in which these devices and sensors can communicate are determined through communication protocols. These protocols, which define how information is transmitted, are developed by organizations and alliances that define their specifications, hardware requirements, and licensing.

Communication protocols are generally classified into three main groups, according to the medium of propagation: (1) wired, (2) wireless, and (3) hybrid. The choice of the right technology to use depends on the use case. Some communications protocols offer longer ranges, some higher security, and others lower power consumption. Furthermore, the choice also depends on the size of the network. In the context of a smart home body area networks (BAN), personal area networks (PAN), and local area networks (LAN) are commonly used.

A detailed comparison of multiple communication technologies for home area networks (HAN) is provided in [75]. The authors also assembled a comprehensive list of characteristics and requirements for a HAN. According to Zheng et al. [66] the most important aspect of using WPAN (wireless personal area network)/WLAN (wireless local area network) is to assure the quality of service (QoS), which is defined by latency, transmission power, reliability and bandwidth. This is critical for health care applications, where all four requirements have to be met simultaneously.

Smart home wireless sensor networks (WSN), typically composed of BAN and PAN, are susceptible to interference with higher power wireless technologies, such as Wi-Fi. As a result, WSN devices may sometimes fail to receive commands, or send sensed data, negatively affecting QoS in the smart home. Li and Lin [76] propose a method to bypass this limitation by combining WSN and power line communication (PLC) technologies. Placement of PLC transceivers close to WSN guarantees minimization of interference from other radio frequency (RF) technologies, and maximization of the likelihood that the sensor data is picked up and sent to the destination (i.e. the hub or gateway) or that commands sent from the central management unit are received by the sensors/actuators.

Due to the heterogeneity of IoT devices present in a smart home, the problem of interoperability between devices using different communication protocols arises. Interoperability between devices is important, because low-power devices use communication technologies that have short range coverage areas, but can be extended using multi-hop transmission in a mesh-grid topology. Bello and Zeadally [77] discuss the challenges on implementing network-level interoperability between different technologies, using the 6LowPAN protocol as the middle ground solution.

The remaining part of this section provides an overview of the most common and emerging technologies for wired and wireless communication, and provides guidance for choosing the appropriate technology.

4.1. Wired communication protocols

Wired communication refers to the transmission of information over a wire medium. It is one of the oldest way to transmit information, dating back to the days when messages were sent by electrical telegraph. Advantages of wired over wireless data transmission are:

Table 2
Wired communication protocols.

	Ethernet	X10	UPB	INSTEON	MoCA	KNX
Frequency	100–500 MHz	120 kHz; 310–433.92 MHz	4–40 kHz	131.65; 868–924 MHz	0.5–1.5 GHz	110/132 kHz; 868.3 MHz
Data rate	1 Mbps-100 Gbps	20–60 bps; 9.6 kbps	480 bps	13.165 kbps; 38.4 kbps	175 Mbps-2.5 Gbps	1.2/2.4 Mbps
Range	100 m	500–1000 m	80–500 m	500 m; 40 m	90 m	1000 m; 100 m
Network topology	Bus, star	None; star	P2P	P2P, mesh, dual mesh	P2P, mesh	Tree, line star
Encryption	None	None	None	AES-256	DES-56, AES-128	None; AES-128

Security: since network connection requires to physically connect the device with a cable, it is almost impossible to eavesdrop or tamper with the data in the network from the outside.
Ease of use: connecting to a network is as easy as plugging in the cable to the device; there is no need to choose the right network from a list of networks, or enter a password, as in the case of wireless networks.
Distance: data transmission over wire will go further than what common wireless protocols (Wi-Fi 802.11ac) can achieve; since wire cables are enclosed media, the transmission is not affected by issues like interference or obstacles.
Data rate: theoretical data rates over Ethernet can achieve 100 Gbps, while the maximum theoretical speed of Wi-Fi 802.11ac is 1.3 Gbps.
Reliability: data transmission over wire is constant and not affected by interference, or obstacles; in wireless networks, it is common for the transmission rate to fluctuate.

However, wired communication technologies also have some common disadvantages:

Cost and complexity: installing a wired network requires professional work and planning; implementing a wired network in a smart home needs to be done when the home is built, otherwise running cables through walls at a later time can become a tedious work, and not look aesthetically pleasing.
Mobility: once the cables are set in place, it's not possible to change the location of the device, without rewiring or extending the cable.
Power: normally, wired connections require power for the network to operate; in a critical situation, if the power is cut, the network may not be able to run on a battery, as wireless network can.
Expansion: extending the coverage of a wired network is not as easy as adding a new wireless router, and may require additional wiring and hardware (hubs).

The following paragraphs provide information on the most commonly used wired protocols used in smart homes. Their main characteristics are also summarized in Table 2.

Ethernet. Ethernet, based on the IEEE 802.3 standard, is one of the most widely adopted solutions for building wired networks, both for LAN and WAN [78]. It has a range of up to 100 m, and is not affected much by electromagnetic interference.

X10. X10 can be considered the first general purpose communication protocol used for signaling and control in home devices. It uses the power line for transmitting information, but it is actually a hybrid technology, since it also has a RF extension meant to increase the reliability of the network. Since the technology has been developed in 1975, it has some flaws (e.g. low data rates, wiring complexity, no encryption support, small number of maximum connected devices, interferences, and message loss) that are apparent when used in contemporary smart homes [75,79].

UPB. Universal Powerline Bus is a proprietary technology that uses the power line for communication, just like X10. It offers some improvements over X10, such as increased data rates (but still low compared to other technologies), less noise from AC lines, and more devices supported due to peer-to-peer connectivity (up to 64,000). The disadvantage is lack of encryption, and overall minor market adoption [80].

INSTEON. INSTEON is a rather new hybrid technology that uses both the power line and RF communication to remotely control devices in a smart home. Since it uses a mesh topology, it does not require a central hub, and all INSTEON devices are able to communicate with each other and repeat the messages to extend the coverage area. On the pros list, there are reliability, ease of use, compatibility, fast message propagation, and a large number of devices to choose from. On the cons, there are slow data rates, which makes the technology a good fit for controlling devices, but not good for use in sensors that generate large amount of data [75,80].

MoCA. Multimedia over Coax is a technology that uses coaxial cables in a home to guarantee content delivery. It is a secure and reliable communication protocol, with only 10^{-6} packet error rate [75]. It is also used with Wi-Fi repeaters to increase Wi-Fi coverage with no data rate loss. Maximum theoretical data rate for MoCA 2.5 is 2.5 Gbps.

Table 3
Wireless communication protocols.

	Wi-Fi 802.11n	Bluetooth	Bluetooth LE	ZigBee	Z-Wave	6LowPAN
Frequency	2.4–5.8 GHz	2.402–2.48 GHz	2.402–2.48 GHz	868/915 MHz, 2.4 GHz	868/915 MHz	868/921 MHz, 2.4–5 Ghz
Data rate	450 Mbps	0.7–2.1 Mbps	2 Mbps	20/40 kbps, 250 kbps	10–100 kbps	10–40 kbps, 250 kbps
Range	10–100 m	15–20 m	10–15 m	10–100 m	30–50 m	10–100 m
Network size	Thousands (mesh)	8	N/A	65,536	232	250
Network Topology	Star, tree, P2P, mesh	Star	Star	Star, mesh, cluster tree	Mesh	Star, mesh, P2P
Encryption	WPA2	AES-128	AES-128	AES-128	AES-128	AES-128

KNX. KNX is a standardized (EN 50090, ISO/IEC 14543) OSI-based network communication protocol that was designed specifically for smart buildings. KNX requires its own wiring, which increases the complexity and costs. It has a low data rate and so is best suited for signaling and control of devices. It supports three topologies: line, tree, and star. KNX has support for multiple transmission media: KNX-TP for twisted pair wiring, KNX-PL for power line networks, KNX-RF for RF communication, and KNX-IP for Ethernet [80].

4.2. Wireless communication protocols

Wireless communication implies no use of wires to transmit and receive information using RF signals. Wireless communication protocols are becoming popular in smart home networks, due to the ease of use and lower costs of setting up the network and installing new devices. There are several advantages of wireless over wire communication:

Mobility: since connecting a device to a network does not require any physical linkage, the device can be moved around without loosing connectivity; moving the device to a different wireless network is also easy.
Expandability: adding new devices to a network is easy, as long as the maximum number of supported devices is not exceeded; wireless networks are easy to scale up or down as needed, with no or minimal costs.
Costs: setting up a wireless network is quite simple, often without any professional help.
Flexibility: creating a wireless network in a new place, is as easy as connecting the device to power; this makes it easy to experiment with new devices, or sensor placement.

The disadvantages of wireless communication include:

Security: although current encryption mechanisms are strong, packets travel through the air and can be intercepted, and possibly decrypted (although it's highly unlikely); most security issues arise when the wireless network is not protected at all, due to lack of proper configuration.
Data rates: wireless networks have theoretical speeds lower than wired networks (such as Ethernet or MoCA); in practice, however, the data rates are often sufficient for most smart home applications.
Interference: wireless networks are susceptible to interference; this can disrupt or affect the quality of service provided by the network.
Coverage: theoretically, wireless networks have more coverage in a specific area than wired networks; however, obstacles or poor placement of the devices, can decrease the coverage area, and lead to loss of commands/messages.

The following paragraphs provide information on the most commonly used wireless protocols used in smart homes. Their main characteristics are also summarized in Table 3.

Wi-Fi. Wi-Fi, or Wireless Fidelity, is a wireless communication protocol based on the IEEE 801.11 standard. Wi-Fi does not require a license, and thus has become one of the most popular wireless technologies in use today. It has a theoretic coverage area of 45 m indoors, but the range can be extended with Wi-Fi repeaters and redundant access points, which makes it suitable for WLANs. The technology supports WPA2 encryption, and runs in the 2.4–5.8 GHz frequency spectrum. Disadvantages of Wi-Fi technology include high power demand and susceptibility to interference. In addition, indoor obstacles may affect the network speed and reliability [80].

Bluetooth. Bluetooth, based on the IEEE 802.15.1 standard, is arguably the most popular wireless technology for PANs. It operates in frequency spectra of 2402–2480 MHz, or 2400–3483.5 MHz 79 channels are supported, with 1 MHz per channel, but certain channel restrictions are enforced in some countries. The technology is smart to avoid busy channels, with frequency hopping spread spectrum (FHSS) to change channels [81]. Bluetooth is very popular in mobile and wearable devices. BLE (Bluetooth Low Energy) is a subset of Bluetooth, which is aimed for low power devices that can run on a cell battery for a long period of time. Bluetooth 5 introduced several improvements for the BLE version, with a focus on emerging IoT device support, such as improved range, improved channel selection, and increased data rate.

ZigBee. ZigBee, based on the IEEE 802.15.4 standard, is a reliable, low cost, low rate communication technology aimed at devices with limited power supply (such as those running on a battery). Because the technology is open-source and free to use by anyone, it is a very popular choice by vendors building low-powered devices. Typical data rates are between 20–250 kbps, and the area of effect is up to 70 m [78,80]. ZigBee supports multi-hop transmission to extend the range of action, but this can sometimes lead to a "popcorn effect", which is reflected by a delay in the action due to the message being propagated from one device to another before it reaches the final destination. Also, the default maximum number of hops is 5, which means that if the message does not reach the destination after 5 hops (this can be changed in the configuration), the message will be discarded, and the intended receiver will never receive it.

Z-Wave. Z-Wave is another technology aimed at low-powered devices, designed with reliability in mind. Unlike ZigBee, Z-Wave is a proprietary technology, for which vendors need to acquire a license and get a certification from the Z-Wave Alliance [81]. Transfer rates are up to 100 kbps, with up to 50 m of range. Z-Wave can form mesh-networks, which means that devices can communicate to each other, without the need of a central gateway or controller. If a device is not in immediate vicinity, then messages can hop up to 4 times between nodes to reach the destination [82].

6LowPAN. 6LowPAN is an open-source and free to use standard for building low powered PANs over Internet Protocol v6 [77]. It is based on the IEEE 802.15.4 standard, which means it is similar to ZigBee. The technology supports data rates of 20–250 kbps depending on the frequency, with a range from 10 to 100 m. Because it is based on IPv6, every device has a unique IPv6 address and is accessible from the Internet (unlike ZigBee and Z-Wave which are only accessible within the PAN). Thread [83] is a joint effort of over 50 companies to standardize the 6LowPAN technology as the de facto communication protocol for smart home devices.

5. Privacy and security

The concept of smart home would have not been possible without pervasive computing and multitude of sensors scattered around a house. Unfortunately, the use of these devices, which are usually connected to the Internet (directly or indirectly) and/or use wireless communication, opens up new opportunities for attacks to the security and privacy of the people living in the smart home.

5.1. Data privacy and security

Security, in the context of a smart home, is mostly related to the security and privacy of the data and ensuring the privacy of the inhabitants. While physical security and safety (e.g. against natural elements or unlawful entry), are also extremely important, they are outside the scope of this review.

According to Zheng et al. [66] security has to deal with the following issues:

1. Avoiding data breaches (making sure that unauthorized entities cannot access the data);
2. Authorization (defining entities that have access to the data);
3. Ensuring the privacy of the user.

The usual method to securing the data is using symmetric and asymmetric key cryptography. Alternative methods of encrypting data shared between wearable sensing devices are based on the use of biometric traits, such as nerve interpulse intervals [84], or vascular blood volume [85]. A limitation of these methods is energy efficiency and computation power, since these measurements can be demanding for small portable devices.

Generally, a smart home is vulnerable to two types of threats: internal and external. The internal attacks are possible when the cybercriminal is located in close proximity to the house, whereas the external ones are possible through an Internet connection. Either way, the attacker intends to compromise the smart home's infrastructure or gain access to information stored using cloud services. There are several common threats that could be used by a cybercriminal on a smart home and its inhabitants [86,87]:

Eavesdropping: if the the attacker obtains access to a victim's router, they can intercept all traffic coming to and out of the house, and therefore compromise the privacy and confidentiality of the inhabitants; if the attacker is in close proximity to the house, they can use special hardware to intercept the messages sent from the various sensors and devices (which are normally sent using wireless technologies), and obtain valuable information about the victim's habits; these are usually passive attacks, however the attacker can use the information to plan a further active or physical attack.

Impersonation: this type of threat is when an attacker will try to act on behalf of the legitimate user, by either using the victim's credentials, or by performing a man in the middle attack; these types of attack are possible based on the eavesdropping technique, when the criminal gains access to the victim's credentials and may also modify or replay requests on the network to perform some malicious activity.

Software exploitation: this type of attack is mostly due to negligence of users not taking basic security measures; for example, many users will set up a device as part of the smart home infrastructure (router, sensor, etc), but will not take the necessary measures to change the default administration password; website `insecam.com` [88] is a clear testimony of the large number of surveillance cameras left operating with default credentials, which exposes thousands of properties around the world for anyone to stalk; another vulnerability in this category is the result of not keeping software up to date and patched for security issues - this allows cybercriminals to take advantage of the vulnerabilities left open on the device, and gain administrative access on the device, which can further open up new opportunities for exploits.

Denial of service: DoS attacks occur when attackers hamper the normal operation of sensors or routers, by sending many requests at once to the device, or send corrupted messages that the device cannot process and therefore ends up crashing; this way, attackers can disrupt the Internet connectivity in a smart home, which will prevent the user to gain access to their home through the Internet.

Ransomware: this is a relatively new type of attack, where the cybercriminals gain access to a victim's device, encrypting the information stored on the drives with a secret key, and then ask for ransom to provide the secret key for decrypting the information.

5.2. Stakeholder responsibilities

To prevent and mitigate threat issues, all stakeholders of smart home devices need to be actively involved. The European Union Agency for Network and Information Security (ENISA) has put together a compendium describing the threats and possible measures to enhance the current status of cybersecurity in smart home environments, in a more general IoT context [89]. According to ENISA, the non-exhaustive list of stakeholders of a smart home ecosystem includes the vendors (e.g. hardware and software manufacturers), the service and solution providers (e.g. cloud service providers), the electronic communication providers (e.g. Internet service providers), and the consumers (end users, the inhabitants of a smart home). All these parties play an important role in ensuring that a smart home environment is secure and resilient to outside attacks.

6. Challenges and future trends

Risteska-Stojkoska and Trivodaliev [3] identify a number of challenges for IoT-based smart homes and propose several solutions. In the area of edge (fog) computing, the authors point out the need to optimize communication among the SH devices and suggest development of lightweight algorithms for local data processing and reducing the number of transmissions among the devices. The big amounts of data generated by the devices then require new, big data approaches for integration, storage and analysis. Possible solutions include distributed data processing system, NoSQL databases and business intelligence platforms. Networking solutions for SH are should be base on flexible mesh topologies using wired of wireless protocols also review in Section 4 of this review. With connectivity also come the issue of interoperability, currently being addressed by development of standards to ensure that different vendors build interoperable devices. The last issue associated with operation of IoT-based smart homes is related to security and privacy (cf. Section 5).

A challenge on its own is the slow diffusion of smart homes and their adoption by customers. Shin et al. [90] developed a technology acceptance model to describe the smart home adoption rates. Their results show that the major factors contributing to decision to purchase are compatibility, perceived ease of use, and perceived usefulness. They also report that older consumers are more inclined to purchase smart homes compared to younger consumers. The study concludes that, to increase market demand, a strategy targeting young consumers is required. Closely related to the issue of customer adoption of smart homes is the way they are used and they keep the promises of comfort enhancement, convenience, security and leisure along with energy management. An in-depth qualitative analysis by Hargreaves et al. [91] explores the adoption of a range of smart home technologies. The authors identify four core themes related to smart home technologies:

1. Technical and social disruptiveness;
2. Need for adaptation and familiarization from householders;
3. Difficulty of and little support for learning to use; and
4. Lack of evidence of substantial energy savings and a risk of energy intensification.

The authors then discus wider practical, research and theoretical implications of this analysis and suggest that SH domestication must go beyond new technologies, considering specific biographies of different users to capture the wider influences on their everyday lives and practices.

Pilloni et al. [92] concentrate on the energy efficiency aspect of SH development and introduce the concept of occupant-perceived quality of experience (QoE). The authors then propose a QoE-aware SH energy management system (EMS) relying on the amount of annoyance caused by changes of appliance operations for the sake of energy savings. Similarly, Zhang and Musilek [93] introduce discomfort measures to encourage long term, active user participation in demand management programs.

Future high penetration of SH will bring vast numbers of devices to the grid and allow their participation in system-level and local coordination tasks. The data and computational resources of these devices can be utilized to maintain a dynamic balance of supply and demand under the transactive energy (TE) framework. In TE systems, this balancing is based on the

flexibility of various generation and load resources. Using real-time, decentralized decision making, TE has the potential to bring benefits for the entire grid system, while respecting the preferences and behaviors of the individual participants [94]. Marzband et al. [95] analyzed a TE framework for grid-connected multiple home systems (e.g. neighborhoods, microgrids), based on individual and coalition operations conducted by the occupants. The authors report decrease of the market clearing price of electricity for about 15% of the time, increase responsive load consumption by about 30%, and promotion of local generation.

To allow real-time operation, TE systems require an efficient communication and computing infrastructure to facilitate information exchange and sophisticated decision-making. Blockchain-based approaches [96] provide decentralized security and privacy, but at high energy and computational costs. Dorri et al. [97] proposed a lightweight blockchain instantiation particularly geared for the use in IoT-based smart homes. The authors showed that security and privacy gains can be obtained without significant overheads in terms of traffic, processing time and energy consumption.

Sensors, appliances and other devices are the enablers of SH technologies. However, SH performance and quality of services it provides are determined by the smart home management platforms. To allow adaptation to different SH usage scenarios and user demands, a flexible development platform is required. Xu et al. introduce the concept of software-defined smart homes [98] that promises to provide this flexibility along with ease of implementation. The proposed platform is based on the design principles of virtualization, openness, and centralization, allowing effective integration of heterogeneous SH devices and paving the road for interoperability and standardization. Interesting features offered by this flexible architecture include location-based home automation, configurable lifestyle management and SH condition monitoring.

7. Conclusions

Smart homes are no longer in the domain of science-fiction. There have been tremendous amounts of research and development, and numerous smart homes have been piloted and deployed around the world. However, purchase of a smart home is still not a mainstream choice, due to costs, complexity, and lack of awareness among the general public. Therefore, in addition to continuing innovation and development efforts, there is a strong need for usability studies [91] and targeted information strategies [90] to increase the market demand.

For smart homes to become widespread, simple and effective designs are important. Lack of interoperability between devices, high complexity of setting up a smart home network and absence of unified interfaces for device management are issues that have to be solved. Major vendors need to reach a consensus on technology stacks, because the heterogeneity of available devices is confusing to the consumers. Regular home owners do not want to be involved in technological details in order to make their home more convenient, enjoyable and energy efficient [99]. Some recent developments, such as software defined smart homes [98], may also alleviate some of the flexibility- and interoperability-related issues.

Security and privacy is also an important factor for successful dispersion of smart homes. Living in space that is filled with sensors and cameras, having every action captured and possibly stored, opens up opportunities for cybercriminals. Privacy and security should be the top priority factor in developing smart home technologies. Just as every house has locks for protection from the outside threats, a smart home must have proper security measures put in place to protect against cyberattacks and privacy compromises. This requirement comes hand in hand with development of safe and secure data storage and computing infrastructure, likely supplemented by a blockchain-like distributed trust platform [96,97].

Last but not the least, the smart home is a joint effort of many. Computer engineers play an important role by experimenting and developing implementation platforms for tasks necessary for smart home operation (sensor technologies; machine learning for activity discovery, recognition, and prediction; ways to deal with large amounts of data coming from various sensors, and ways to fuse the data to extract meaningful information; and devices implementing energy efficiency measures). But other specialists must also be involved in smart home projects to make them well integrated systems that can respond to occupant needs and environmental events, and evolve with changing priorities of their users. Involvement of architects, building scientists, economists, social scientists and other experts is needed to develop future smart homes that will be accepted by the customers and penetrate the currently limited market. They will become the enabler for higher level societal organizations, such as smart grids, smart neighborhoods, smart cities, smart governments and, eventually, smart planet.

Acknowledgments

Support provided by the Natural Sciences and Engineering Research Council of Canada (NSERC RGPIN-2017-05866) is gratefully acknowledged.

References

[1] M.R. Alam, M.B.I. Reaz, M.A.M. Ali, A review of smart homes-past, present, and future, IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.) 42 (6) (2012) 1190–1203, doi:10.1109/TSMCC.2012.2189204.
[2] S.J. Darby, Smart technology in the home: time for more clarity, Build. Res. Inf. 46 (1) (2018) 140–147, doi:10.1080/09613218.2017.1301707.
[3] B.L. Risteska Stojkoska, K.V. Trivodaliev, A review of Internet of Things for smart home: challenges and solutions, J. Clean. Prod. 140 (2017) 1454–1464, doi:10.1016/J.JCLEPRO.2016.10.006.
[4] T. Kramp, R. van Kranenburg, S. Lange, Introduction to the Internet of Things, in: Enabling Things to Talk, Springer, Berlin, Heidelberg, 2013, pp. 1–10, doi:10.1007/978-3-642-40403-0_1.

[5] Y. Strengers, Smart Energy Technologies in Everyday Life: Smart Utopia?, Springer, 2013.
[6] W.K. Edwards, R.E. Grinter, in: At Home with Ubiquitous Computing: Seven Challenges, Springer, Berlin, Heidelberg, 2001, pp. 256–272, doi:10.1007/3-540-45427-6_22.
[7] D.J. Cook, S.K. Das, Smart Environments: Technologies, Protocols, and Applications, John Wiley, 2005.
[8] S. Das, D. Cook, A. Battacharya, E. Heierman, Tze-Yun Lin, The role of prediction algorithms in the MavHome smart home architecture, IEEE Wirel. Commun. 9 (6) (2002) 77–84, doi:10.1109/MWC.2002.1160085.
[9] R. Blasco, Á. Marco, R. Casas, D. Cirujano, R. Picking, A smart kitchen for ambient assisted living, Sensors 14 (12) (2014) 1629–1653, doi:10.3390/s140101629.
[10] F. Buttussi, L. Chittaro, MOPET: a context-aware and user-adaptive wearable system for fitness training, Artif. Intell. Med. 42 (2) (2008) 153–163, doi:10.1016/J.ARTMED.2007.11.004.
[11] A. Jalal, J.T. Kim, T.-S. Kim, Development of a Life Logging System via Depth Imaging- based Human Activity Recognition for Smart Homes(2012). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.456.9125&rep=rep1&type=pdf.
[12] M. Soliman, T. Abiodun, T. Hamouda, J. Zhou, C.-H. Lung, Smart home: integrating internet of things with web services and cloud computing, in: Proceedings of the IEEE Fifth International Conference on Cloud Computing Technology and Science, IEEE, 2013, pp. 317–320, doi:10.1109/CloudCom.2013.155.
[13] D.J. Cook, A.S. Crandall, B.L. Thomas, N.C. Krishnan, CASAS: a smart home in a box., Computer 46 (7) (2013), doi:10.1109/MC.2012.328.
[14] Y. Jie, J.Y. Pei, L. Jun, G. Yun, X. Wei, Smart home system based on IOT technologies, in: Proceedings of the International Conference on Computational and Information Sciences, IEEE, 2013, pp. 1789–1791, doi:10.1109/ICCIS.2013.468.
[15] J. Zhou, T. Leppanen, E. Harjula, M. Ylianttila, T. Ojala, C. Yu, H. Jin, CloudThings: a common architecture for integrating the Internet of Things with Cloud Computing, in: Proceedings of the IEEE Seventeenth International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE, 2013, pp. 651–657, doi:10.1109/CSCWD.2013.6581037.
[16] J. Hosek, P. Masek, D. Kovac, M. Ries, F. Kröpfl, IP home gateway as universal multi-purpose enabler for smart home services 13145 (2014) 123–128, doi:10.1007/s00502-014-0209-x.
[17] S. Guoqiang, C. Yanming, Z. Chao, Z. Yanxu, Design and Implementation of a Smart IoT Gateway, in: Proceedings of the IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, IEEE, 2013, pp. 720–723, doi:10.1109/GreenCom-iThings-CPSCom.2013.130.
[18] P.M. Mell, T. Grance, SP 800–145. The NIST Definition of Cloud Computing, Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, United States, 2011. https://csrc.nist.gov/publications/detail/sp/800-145/final
[19] L.D. Xu, W. He, S. Li, Internet of things in industries: a survey, IEEE Trans. Ind. Inf. 10 (4) (2014) 2233–2243, doi:10.1109/TII.2014.2300753.
[20] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): a vision, architectural elements, and future directions, future generation computer systems 29 (7) (2013) 1645–1660. Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services and Cloud Computing and Scientific Applications Big Data, Scalable Analytics, and Beyond. doi:10.1016/j.future.2013.01.010.
[21] Fog Computing and the Internet of Things: extend the Cloud to where the things are. https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf.
[22] M. Chiang, T. Zhang, Fog and IoT: an overview of research opportunities, IEEE Internet Things J. 3 (6) (2016) 854–864, doi:10.1109/JIOT.2016.2584538.
[23] M. Aazam, E.-N. Huh, Fog Computing and Smart Gateway Based Communication for Cloud of Things, in: Proceedings of the International Conference on Future Internet of Things and Cloud, IEEE, 2014, pp. 464–470, doi:10.1109/FiCloud.2014.83.
[24] S. Yi, Z. Hao, Z. Qin, Q. Li, Fog Computing: platform and applications, in: Proceedings of the Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb), IEEE, 2015, pp. 73–78, doi:10.1109/HotWeb.2015.22.
[25] S. Yi, Z. Qin, Q. Li, in: Security and Privacy Issues of Fog Computing: A Survey, Springer, Cham, 2015, pp. 685–695, doi:10.1007/978-3-319-21837-3_67.
[26] I. Stojmenovic, S. Wen, The Fog Computing Paradigm: Scenarios and Security Issues, in: M. Ganzha, L. Maciaszek, M. Paprzycki (Eds.), Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, 2, ACSIS, 2014, pp. 1–8.
[27] C. Carvalho, The Gap between Processor and Memory Speeds. https://pdfs.semanticscholar.org/6ebe/c8701893a6770eb0e19a0d4a732852c86256.pdf.
[28] Fog vs. Edge Computing: what's the difference?. http://info.opto22.com/fog-vs-edge-computing.
[29] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, E. Riviere, Edge-centric computing, ACM SIGCOMM Comput. Commun. Rev. 45 (5) (2015) 37–42, doi:10.1145/2831347.2831354.
[30] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge Computing: vision and challenges, IEEE Internet Things J. 3 (5) (2016) 637–646, doi:10.1109/JIOT.2016.2579198.
[31] W. Shi, S. Dustdar, The promise of Edge Computing, Computer 49 (5) (2016) 78–81, doi:10.1109/MC.2016.145.
[32] US Congress, Energy Independence and Security Act of 2007, December 18, 2007.
[33] X.H. Li, S.H. Hong, User-expected price-based demand response algorithm for a home-to-grid system, Energy 64 (2014) 437–449, doi:10.1016/J.ENERGY.2013.11.049.
[34] D. Fuselli, F. De Angelis, M. Boaro, S. Squartini, Q. Wei, D. Liu, F. Piazza, Action dependent heuristic dynamic programming for home energy resource scheduling, Int. J. Electr. Power Energy Syst. 48 (2013) 148–160, doi:10.1016/J.IJEPES.2012.11.023.
[35] T. Huang, D. Liu, Residential energy system control and management using adaptive dynamic programming, in: Proceedings of the International Joint Conference on Neural Networks, IEEE, 2011, pp. 119–124, doi:10.1109/IJCNN.2011.6033209.
[36] R.L. Welch, G.K. Venayagamoorthy, Optimal control of a photovoltaic solar energy system with adaptive critics, in: Proceedings of the International Joint Conference on Neural Networks, IEEE, 2007, pp. 985–990, doi:10.1109/IJCNN.2007.4371092.
[37] R. Welch, G. Venayagamoorthy, Comparison of two optimal control strategies for a grid independent photovoltaic system, in: Proceedings of the Conference Record of the 2006 IEEE Industry Applications Conference Forty-First IAS Annual Meeting, 3, IEEE, 2006, pp. 1120–1127, doi:10.1109/IAS.2006.256673.
[38] B. Zhou, W. Li, K.W. Chan, Y. Cao, Y. Kuang, X. Liu, X. Wang, Smart home energy management systems: concept, configurations, and scheduling strategies, Renew. Sustain. Energy Rev. 61 (2016) 30–40, doi:10.1016/J.RSER.2016.03.047.
[39] P. Siano, Demand response and smart grids – a survey, Renew. Sustain. Energy Rev. 30 (2014) 461–478.
[40] M.L. Tuballa, M.L. Abundo, A review of the development of smart grid technologies, Renew. Sustain. Energy Rev. 59 (2016) 710–725.
[41] H.T. Haider, O.H. See, W. Elmenreich, A review of residential demand response of smart grid, Renew. Sustain. Energy Rev. 59 (2016) 166–178.
[42] William Lamie, The Benefits of RTOSes in the Embedded IoT | EE Times. https://www.eetimes.com/author.asp?section_id=36&doc_id=1327623.
[43] A. Milinković, S. Milinković, L. Lazic, Choosing the right RTOS for IoT platform, INFOTEH-JAHORINA 14 (2015) 504–509.
[44] IoT operating systems. https://devopedia.org/iot-operating-systems.
[45] T. Reusing, Comparison of Operating Systems TinyOS and Contiki, in: Proceedings of the Seminar Sensor Nodes Operation, Network and Application (SN), Chair for Network Architectures and Services, Department of Computer Science, Technische Universität München, 2012.
[46] R. Zetik, S. Crabbe, J. Krajnak, P. Peyerl, J. Sachs, R. Thomä, in: Detection and Localization of Persons Behind Obstacles Using M-sequence Through-the-Wall Radar, 6201, International Society for Optics and Photonics, 2006, p. 62010I, doi:10.1117/12.667989.
[47] A.R. Hunt, in: A wideband imaging radar for through-the-wall surveillance, 5403, International Society for Optics and Photonics, 2004, p. 590, doi:10.1117/12.542718.
[48] F. Adib, H. Mao, Z. Kabelac, D. Katabi, R.C. Miller, Smart homes that monitor breathing and heart rate, in: Proceedings of the Thirty-Third Annual ACM Conference on Human Factors in Computing Systems – CHI '15, ACM Press, New York, NY, USA, 2015, pp. 837–846, doi:10.1145/2702123.2702200.
[49] O. Postolache, P.S. Girao, R.N. Madeira, G. Postolache, Microwave FMCW Doppler radar implementation for in-house pervasive health care system, in: Proceedings of the IEEE International Workshop on Medical Measurements and Applications, IEEE, 2010, pp. 47–52, doi:10.1109/MEMEA.2010.5480207.

[50] C. Li, V.M. Lubecke, O. Boric-Lubecke, J. Lin, A review on recent advances in doppler radar sensors for noncontact healthcare monitoring, IEEE Trans. Microwave Theory Tech. 61 (5) (2013) 2046–2060, doi:10.1109/TMTT.2013.2256924.
[51] F. Studnicka, P. Seba, D. Jezbera, J. Kriz, Continuous monitoring of heart rate using accelerometric sensors, in: Proceedings of the Thirty-Fifth International Conference on Telecommunications and Signal Processing, TSP 2012, 2012, pp. 559–561.
[52] P. Davies, I. Maconochie, The relationship between body temperature, heart rate and respiratory rate in children, Emer. Med. J. 26 (9) (2009) 641–643, doi:10.1136/emj.2008.061598.
[53] S. Bourobou, Y. Yoo, User activity recognition in smart homes using pattern clustering applied to temporal ANN algorithm, Sensors 15 (5) (2015) 11953–11971, doi:10.3390/s150511953.
[54] B. Qela, H.T. Mouftah, Observe, Learn, and Adapt (OLA) an algorithm for energy management in smart homes using wireless sensors and artificial intelligence, IEEE Trans. Smart Grid 3 (4) (2012) 2262–2272, doi:10.1109/TSG.2012.2209130.
[55] P. Rocca, M. Benedetti, M. Donelli, D. Franceschini, A. Massa, Evolutionary optimization as applied to inverse scattering problems, Inverse Probl. 25 (12) (2009) 123003, doi:10.1088/0266-5611/25/12/123003.
[56] A. Jalal, S. Kamal, D. Kim, A depth video sensor-based life-logging human activity recognition system for elderly care in smart indoor environments, Sensors 14 (12) (2014) 11735–11759, doi:10.3390/s140711735.
[57] I. Fatima, M. Fahim, Y.-K. Lee, S. Lee, a unified framework for activity recognition-based behavior analysis and action prediction in smart homes, Sensors 13 (2) (2013) 2682–2699, doi:10.3390/s130202682.
[58] D. Laney, Application Delivery Strategies(2001). https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.
[59] The V's of big data: velocity, volume, value, variety, and veracity. https://www.xsnet.com/blog/bid/205405/the-v-s-of-big-data-velocity-volume-value-variety-and-veracity.
[60] M. Chen, S. Mao, Y. Liu, M. Chen, S. Mao, Y. Liu, Big data: a survey, Mob. Netw. Appl. 19 (2014) 171–209, doi:10.1007/s11036-013-0489-0.
[61] Xindong Wu, Xingquan Zhu, Gong-Qing Wu, Wei Ding, Data mining with big data, IEEE Trans. Knowl. Data Eng. 26 (1) (2014) 97–107, doi:10.1109/TKDE.2013.109.
[62] C.L.P. Chen, C.-Y. Zhang, Data-intensive applications, challenges, techniques and technologies: a survey on Big Data, Inf. Sci. 275 (2014) 314–347, doi:10.1016/j.ins.2014.01.015.
[63] I. Abaker, T. Hashem, I. Yaqoob, B. Anuar, S. Mokhtar, A. Gani, S.U. Khan, The rise of big data on Cloud Computing. Review and open research issues (2014). 10.1016/j.is.2014.07.006https://ac.els-cdn.com/S0306437914001288/1-s2.0-S0306437914001288-main.pdf?_tid=e6eed775-53dc-48ea-b7e9-77225a5889f2&acdnat=1520912247_020d1f7d40aa535f618fa69a44da85a8.
[64] A. Gandomi, M. Haider, Beyond the hype: big data concepts, methods, and analytics, Int. J. Inf. Manag. 35 (2) (2015) 137–144, doi:10.1016/J.IJINFOMGT.2014.10.007.
[65] D. Hall, J. Llinas, An introduction to multisensor data fusion, Proc. IEEE 85 (1) (1997) 6–23, doi:10.1109/5.554205.
[66] Y.-L. Zheng, X.-R. Ding, C.C.Y. Poon, B.P.L. Lo, H. Zhang, X.-L. Zhou, G.-Z. Yang, N. Zhao, Y.-T. Zhang, Unobtrusive sensing and wearable devices for health informatics, IEEE Trans. Biomed. Eng. 61 (5) (2014) 1538–1554, doi:10.1109/TBME.2014.2309951.
[67] J. Han, M. Kamber, Data Mining : Concepts and Techniques, Elsevier, 2012.
[68] S. Hashem, Sherif, Optimal linear combinations of neural networks, Neural Netw. 10 (4) (1997) 599–614, doi:10.1016/S0893-6080(96)00098-6.
[69] D. Huang, H. Leung, An expectation maximization-based interacting multiple model approach for cooperative driving systems, IEEE Trans. Intell. Transp. Syst. 6 (2) (2005) 206–228, doi:10.1109/TITS.2005.848366.
[70] A. Mohammad-Djafari, Probabilistic methods for data fusion, in: Maximum Entropy and Bayesian Methods, Springer, Dordrecht, Netherlands, 1998, pp. 57–69, doi:10.1007/978-94-011-5028-6_5.
[71] D. Dubois, H. Prade, Possibility Theory, Springer, Boston, MA, US, 1988, doi:10.1007/978-1-4684-5287-7.
[72] M. Mitici, J. Goseling, M. de Graaf, R.J. Boucherie, Decentralized vs. centralized scheduling in wireless sensor networks for data fusion, in: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2014, pp. 5070–5074, doi:10.1109/ICASSP.2014.6854568.
[73] E. Blasch, A. Steinberg, S. Das, J. Llinas, C. Chong, O. Kessler, E. Waltz, F. White, Revisiting the JDL model for information exploitation, in: Proceedings of the Information Fusion (FUSION), Istanbul, Turkey, 2013.
[74] M. Díaz, C. Martín, B. Rubio, State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing, J. Netw. Comput. Appl. 67 (2016) 99–117, doi:10.1016/J.JNCA.2016.01.010.
[75] T. Mendes, R. Godina, E. Rodrigues, J. Matias, J. Catalão, Smart home communication technologies and applications: wireless protocol assessment for home area network resources, Energies 8 (7) (2015) 7279–7311, doi:10.3390/en8077279.
[76] M. Li, H.-J. Lin, Design and implementation of smart home control systems based on wireless sensor networks and power line communications, IEEE Trans. Ind. Electr. 62 (7) (2015) 4430–4442, doi:10.1109/TIE.2014.2379586.
[77] O. Bello, S. Zeadally, Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT), Ad Hoc Netw. 57 (2017) 52–62, doi:10.1016/J.ADHOC.2016.06.010.
[78] M. Kuzlu, M. Pipattanasomporn, S. Rahman, Review of communication technologies for smart homes/building applications, in: Proceedings of the IEEE Innovative Smart Grid Technologies – Asia (ISGT ASIA), IEEE, 2015, pp. 1–6, doi:10.1109/ISGT-Asia.2015.7437036.
[79] P. Darbee, Insteon WHITEPAPER: Compared. http://cache.insteon.com/documentation/insteon_compared.pdf
[80] M. Poulakis, S. Vassaki, G. Pitsiladis, C. Kourogiorgas, A. Panagopoulos, G. Gardikis, S. Costicoglou, Wireless sensor network management using satellite communication technologies, in: Emerging Communication Technologies Based on Wireless Sensor Networks, CRC Press, 2016, pp. 201–232, doi:10.1201/b20085-12.
[81] O. Horyachyy, Comparison of wireless communication technologies used in a smart home: analysis of wireless sensor node based on Arduino in home automation scenario (2017). http://www.diva-portal.org/smash/get/diva2:1118965/FULLTEXT02.
[82] C. Withanage, R. Ashok, C. Yuen, K. Otto, A comparison of the popular home automation technologies, in: Proceedings of the IEEE Innovative Smart Grid Technologies – Asia (ISGT ASIA), IEEE, 2014, pp. 600–605, doi:10.1109/ISGT-Asia.2014.6873860.
[83] Introducing Thread: A New Wireless Networking Protocol For The Home. https://www.threadgroup.org/news-events/press-releases/ID/20/Introducing-Thread-A-New-Wireless-Networking-Protocol-for-the-Home
[84] C. Poon, Yuan-Ting Zhang, Shu-Di Bao, A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health, IEEE Commun. Mag. 44 (4) (2006) 73–81, doi:10.1109/MCOM.2006.1632652.
[85] K.K. Venkatasubramanian, A. Banerjee, S.K.S. Gupta, Plethysmogram-based secure inter-sensor communication in Body Area Networks, in: Proceedings of IEEE Military Communications Conference, MILCOM 2008, IEEE, 2008, pp. 1–7, doi:10.1109/MILCOM.2008.4753199.
[86] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, G. Baldini, Security and privacy issues for an IoT based smart home, in: Proceedings of the Fortieth International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, 2017, pp. 1292–1297, doi:10.23919/MIPRO.2017.7973622.
[87] C. Lee, L. Zappaterra, Kwanghee Choi, Hyeong-Ah Choi, Securing smart home: Technologies, security challenges, and security requirements, in: Proceedings of the IEEE Conference on Communications and Network Security, IEEE, 2014, pp. 67–72, doi:10.1109/CNS.2014.6997467.
[88] Insecam - World biggest online cameras directory. https://www.insecam.org/.
[89] Security and Resilience of Smart Home Environments(2015). http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/SecurityandResilienceofSmartHomeEnvironments(1).pdf.
[90] J. Shin, Y. Park, D. Lee, Who will be smart home users? an analysis of adoption and diffusion of smart homes, Technol. Forecast. Soc. Change 134 (2018) 246–253.
[91] T. Hargreaves, C. Wilson, R. Hauxwell-Baldwin, Learning to live in a smart home, Build. Res. Inf. 46 (1) (2018) 127–139.

[92] V. Pilloni, A. Floris, A. Meloni, L. Atzori, Smart home energy management including renewable sources: a qoe-driven approach, IEEE Trans. Smart Grid 9 (3) (2018) 2006–2018.
[93] S. Zhang, P. Musilek, User-centric energy management for the smart grid, in: Proceedings of the Sixteenth IEEE International Conference on Environment and Electrical Engineering (EEEIC 2016), 2016, pp. 95–106.
[94] S. Chen, C. Liu, From demand response to transactive energy: state of the art, J. Mod. Power Syst. Clean Energy 5 (1) (2017) 10–19.
[95] M. Marzband, F. Azarinejadian, M. Savaghebi, E. Pouresmaeil, J.M. Guerrero, G. Lightbody, Smart transactive energy framework in grid-connected multiple home microgrids under independent and coalition operations, Renew. Energy 126 (2018) 95–106.
[96] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.
[97] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: the case study of a smart home, in: Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017, 2017, pp. 618–623.
[98] K. Xu, X. Wang, W. Wei, H. Song, B. Mao, Toward software defined smart home, IEEE Commun. Mag. 54 (5) (2016) 116–122.
[99] C. Links, What is SHaaS? And why should you care?, Qorvo White Paper, 2016, http://www.zigbee.org/wp-content/uploads/2016/11/Qorvo-Whitepaper-SHaaS.pdf.