Internet of Things for Modern Energy Systems

State-of-the-Art, Challenges, and Open Issues

Shakerighadi, Bahram; Anvari-Moghaddam, Amjad; Vasquez, Juan C. ; Guerrero, Josep M.

Published in:
Energies

DOI (link to publication from Publisher):
10.3390/en11051252

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

energies

MDPI

Review

Internet of Things for Modern Energy Systems: State-of-the-Art, Challenges, and Open Issues

Bahram Shakerighadi *, Amjad Anvari-Moghaddam, Juan C. Vasquez and Josep M. Guerrero

Department of Energy Technology, Aalborg University, 9220 Aalborg, Denmark; aam@et.aau.dk (A.A.-M.); juq@et.aau.dk (J.C.V.); joz@et.aau.dk (J.M.G.)

* Correspondence: bas@et.aau.dk; Tel.: +45-93562324

Received: 3 April 2018; Accepted: 9 May 2018; Published: 14 May 2018

Abstract: The Internet of Things (IoT) is beginning to shape the future of many industries and emerging markets. One of the target markets for IoT is the energy systems. IoT is a matter of producing, transferring, and processing information, therefore all parts of the system including software and hardware parts should be considered as a whole. In this paper, a state-of-the-art of the IoT-based energy systems is presented to review the recent activities on every component of IoT in energy systems. Challenges in this subject area are discussed, and some solutions are presented thereafter.

Keywords: Internet of Things; energy internet; integrated energy systems; smart grid

1. Introduction

One of the main challenges in reliable operation and control of a given system is managing information produced by its components. This includes data collecting, transmitting, and processing. By introducing more useful information to data processing systems, more appropriate decision can be made based on the knowledge pool. The new concept of the Internet of Things (IoT) is introduced for systems in which the components are connected via the Internet [1]. This system of interrelated physical systems and computing devices introduces many opportunities as every object in the system can communicate with related objects of the system by using two-way communications. Specifically talking about energy systems, IoT could offer advanced connectivity of heterogeneous objects to form a single system [2]. However, there are some challenges in seamless integration of different domains once various services have to be offered beyond machine-to-machine (M2M) communications. The situation gets worse as a number of systems such as power systems, control systems, and communication systems are integrated into a bigger system while each is following its unique set of objectives. Although a great effort can be found in the literature about every issue of energy systems, integration of subsystems is a hot research topic at this time [1–3].

In this regard, a deep perception of every aspect of energy systems and their rightful assortment is of high importance. Figure 1 shows a categorization of energy systems in a general aspect. As can be seen, compared to the traditional energy systems, modern energy systems are designed in a full grid sensor layout with automatic monitoring and recovery capabilities, which enable distributed energy generation.

This architecture becomes bolder as Microgrids (MGs) are introduced into energy systems. MGs are the integration of some distributed generations (DGs) and loads that are capable of running in grid-connected or island mode [4]. MGs are defined in many ways, considering who are dealing with and how they are using it. For instance, a mobile phone can be defined as an MG, while a wind farm can be defined in the same respect. With this in mind, there is no standard mentioning directly

MGs, while there are some standards such as IEC 61850, which define DGs as key players [5]. Based on these standards, many efforts about stability, reliability, control, etc. on MGs can be found in the literature [4,6]. A general review of many features such as reliability, resiliency, and Power Quality (PQ) in some aspects like protection control, communications, and economics of MGs can be found in [7]. A great effort has been done on IEC/ISO 62264 regarding communication structure of MGs represented in a five-level architecture. In this hierarchical structure, in which higher level has a priority to the lower one, a common standard for communication of Distribution Energy Resources (DERs) is considered.

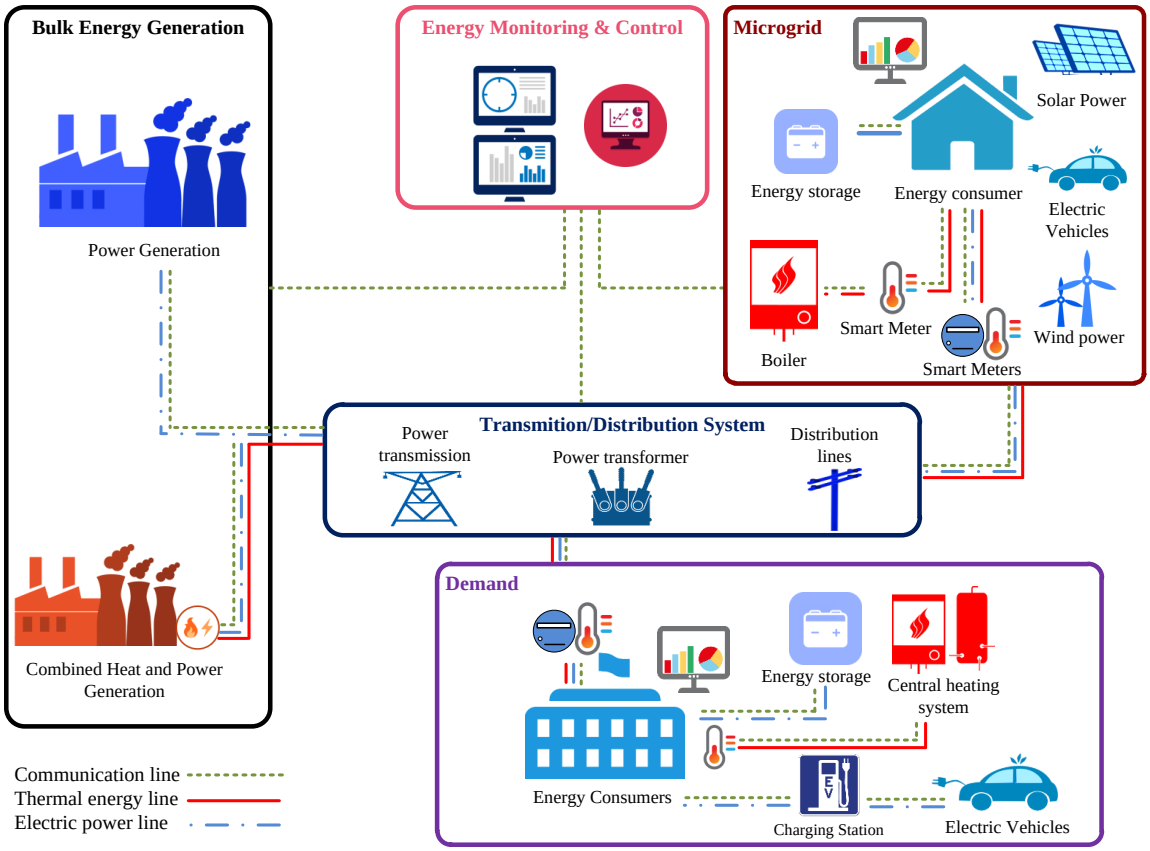

Figure 1. Energy system scheme including electrical, thermal, and communication infrastructures.

On the other hand, in IoT-enabled energy systems, communication infrastructure is a key part that has to be well-established at each level of the system starting from a wide-area network down to a building unit [8,9]. In addition, to design a communication system for a given energy system, there are some factors like system size, installation and maintenance costs, flexibility of the system for future expansions, etc., which need to be considered [8]. More importantly, security of the system should be considered in every step of designing a communication system [10]. Based on what is needed from the system, different communication technologies may also be used in the system. For example, when a wired system like Power Line Carrier (PLC) is accessible, it is logical to use this facility. In contrast, for using synchronous communication in large power systems, wireless networks such as Wide Area Measurement Systems (WAMS) will be a good choice [9,11].

With all this in mind, to study an energy system properly, a good comprehension of the system's components is not a recommendation, but a requirement. This means, that based on the application and the needs, an energy system should be modeled not only in every single aspect, but also in an integrated framework. In [3], it has been mentioned that there is no great effort about the integration of communication systems and power systems, which leads to some unreal simulation.

Talking about IoT, integration of all subsystems is important because IoT is a matter of communication among smart objects, regardless of their category. In this manner, co-simulation is proposed in some attempts [12–15]. For example, in [12], a well-integrated simulation considering both the power system and communication system is presented to find a cost-effective communication system for MGs avoiding a steep learning curve between the mentioned two parts. In [13], a framework is presented for co-simulation of energy systems using a middleware which helps to get the benefits of standard software like MATPOWER 6.0, which is an open-source Matlab-based simulation package, Mosaik, which is a co-simulation framework for smart grids, etc. In this manner, different analyzing models in steady-state and transient mode can be considered in a unified framework. In [14], a co-simulation model taking into account events in both power and communication simulations is designed to minimize synchronization delay error. In [15], a centralized co-simulation architecture is designed to model power and communication system of an energy system. In this manner, PSCAD/EMTDC, which is a power simulation software, is used to simulate the transient part of the power system, Optimized Network Engineering Tool (OPNET) is hired to simulate communication network, and Cyber Physical Java Simulator is used as an interface between the mentioned platforms. This centralized co-simulation is used for testing protection behavior of MGs. Mostly, a framework or architecture should be defined in advance to specify the domain of each application in every subsystem. To make it clear, let us consider a Smart Home (SH) environment where a wireless local area networking based on WiFi communication is used. In such system, devices should not only follow the communication requirements based on the IEEE 802.11 standards, but also meet the required electrical specifications at the low-voltage distribution network (e.g., IEC 60038). In a higher level, a communication infrastructure based on wired LAN, WLAN, WiMaX, or optical fiber can be used to form a Wide-Area Measurement System (WAMS) [16,17].

To date, there has also been a lot of effort on IoT and its application in fields like healthcare, SHs, etc. [2,18,19]. However, there are many challenges in this area. In [18], it has been mentioned that, as new concepts like Cyber Physical Systems (CPSs) and IoT are introduced into energy systems, security of the system is threatened by cyber-attacks. The other challenge mentioned in [19] is how to connect different devices developed by different protocols and standards in a single IoT platform. In [20], authors discussed challenges in Energy Internet from the software viewpoint. In addition, different aspects of implementing the IoT into energy systems such as tool-vendor's and programmer's perception are discussed, physical constraints are not considered and explained. In [21], a great effort has been done in order to assess different challenges such as security, power management, sensing challenges, etc. of the Energy Internet. Although some recommendations are introduced in order to overcome the aforementioned challenges, modern power systems challenges such as different system architectures and integration of the various energy types are not discussed in detail in this review paper. In [22], the main issues in IoT-based energy systems are introduced, yet no specific recommendation is introduced.

To the best of the author's knowledge, the main challenge still exists in development of solutions for information management among subsystems of a typical IoT-enabled energy system.In this regard, what is really missing in the literature is a review of the recent activities in respect of IoT based energy systems, and showing the potential areas that need efforts to improve. Based on that, in this survey, reviewing existing literature about the IoT-based energy systems and exploring challenges in this field of research are tried. The main contributions of this paper with respect to the other surveys are listed as follows:

- Integration of different components of the energy systems regarding the IoT. In this manner, it is tried to have a comprehensive understanding of IoT-based energy systems in different layers. By doing so, new IoT-based energy systems may be designed based on their requirements.
- Reviewing the standards in communication infrastructures related to the energy systems. This gives an appropriate sense of which technology may be used in various energy systems based on its needs.

- Discussing IoT-based energy system architecture. Although there are several architectures introduced in the literature about IoT, only some of them fit energy systems. This issue is discussed in this paper and an appropriate IoT-based energy system architecture is introduced.
- Illustrative examples are introduced regarding the energy systems and their IoT challenges are discussed accordingly.

With all this in mind, the main purpose of this paper is to review the recent works on IoT in energy systems, to discuss existing challenges and issues in this area and to outline a working architecture for IoT-based energy systems. To do so, first, subsystems of the Energy Internet will be introduced. Then, challenges regarding the IoT-based energy systems will be discussed. Eventually, some solutions will be introduced with respect to the discussed challenges.

The rest of the paper is organized as follows: In Section 2, key features of an IoT-enabled energy system, also known as energy Internet, is presented. Section 3 elaborates on some challenges of IoT in energy systems. Then, in Section 4, some illustrative examples are introduced to show the challenges and open issues of IoT in the real-world situation. Finally, conclusions are drawn in Section 5.

2. Key Features in the Energy Internet

Energy Internet is the integration of energy systems and Information and Communications Technology (ICT) systems [23]. What is new in this area of research is how to integrate the needed component considering technical aspects and logical investment aspects while making the platform widely acceptable. To suitably address these questions, one must well understand every aspect of IoT in energy systems. This section, therefore, outlines the key elements in an IoT-driven system and provides a platform for their co-operation and integration in an intelligent way.

2.1. Energy Sources

In modern energy systems, generation of energy is distributed among the system making many aspects of the system such as stability, reliability, and security more complex. Talking about MGs, energy is generated mostly by Power Electronic-based (PE-based) energy sources, which brings more constraints like controllability to the operation management problem. In [24], new indices are introduced to indicate controllability of DGs in a distributed system, as system variables' thresholds are affected by DGs' capacities and their locations in an energy system. Energy sources, as the main building blocks of every energy system, have to be studied from the different points of views such as their stochastic nature, controllability, and emission awareness. These three main viewpoints are discussed as follows:

- Stochastic and deterministic nature of the energy source

Some energy sources such as wind and solar power have stochastic behaviors meaning that they are directly influenced by the weather and their energy generation would be a nonlinear function of atmospheric variables. Thus, it is unlikely that their power production level stays the same from one hour to the next, or during the day and at night [25]. On the other hand, there are some energy sources such as conventional ones (thermal powers from coal, petroleum, and natural gas or hydroelectric power from high velocity of running water) that have a fixed nature meaning that the system output can be defined based on certain deterministic inputs. By increasing the level of uncertainty in energy systems, it becomes necessary to develop mathematical programming techniques in order to find the optimal production schedule. This leads to uncertain unit commitment models for energy systems in which stochastic nature of the thermal, hydro, and renewable generation units are taken into account through optimization under data uncertainty methods [26].

- Controllability of energy sources

Many factors affect controllability of the system. As an example, the control system of a wind turbine has to deal with stochastic nature of the wind. Mostly, a probabilistic energy source is defined

as an uncontrollable one while conventional energy sources can be treated as controllable energy sources. The other factor that affects control system design of energy systems is the system size, i.e., bulk energy sources' control systems differ from the ones for distributed energy sources. This is also true for big and small energy consumers control systems. In this regard, the level of controllability varies based on the system size, the nature of the energy source, and the system configuration [27,28].

- Emission-awareness

As global warming becomes one of the most important issues of this world, supplying energy in an environmentally friendly manner is a matter of importance. Some energy sources such as renewables inherently have an emission-aware nature and can play a great role in clean air/environment policies [29,30]. As it is reported in [30], it seems that Renewable Energy Sources (RESs) are the only solution for the future global emission challenge, and there is going to be more investments in solar and wind power.

2.2. Energy Consumers

Although energy is used in many forms (e.g., thermal, chemical, electrical, etc.), some are well-accepted at the end-use due to easier transmission and conversion [31]. Consumers of energy mostly use an electrical form, as it is easy to use and transfer and related infrastructures are well developed. However, energy consumers act differently based on their needs (i.e., demand level) and their types (e.g., residential, commercial, industrial, etc.). In this regard, some features of the energy consumers that should be considered are as follows:

- Controllability of the loads

Some loads can be curtailed, while others cannot be curtailed or shed. This significantly affects energy management of the system [32,33] and it has pros and cons either from a system operator's or end-user's perspective. If the system could shed a load whenever it wants, then it may be able to reach its optimum point easier. On the other hand, this facility will cost money for the system, as it may be undesirable from the end-user's viewpoint. In the manner of Smart Grids, Internet of things can be used interchangeably with ICT. Therefore, it is involved in Demand Response (DR) of the smart grid, as it is widely discussed in [34]. On the other hand the energy consumption pattern of a system can be detected by studying the consumers' behavior over time: collecting information via sensors, storing, and analyzing the information by defining a data processing system. Finally, a logical decision can be made to shed or curtail loads regarding decision makers' benefit and/or consumers' preferences [35]. Other applications, which can be applied in energy systems in respect of load controlling, is related to time-shiftable loads and thermostatically controllable loads [36–38]. In this regard, system operators control shiftable loads by using incentive-based offers.

- Mobility of the loads

Some loads have the ability to move from one place to another. This brings both challenges and opportunities to energy systems. The main challenge lies in efficient scheduling of these loads over different time scales and locations. On the other hand, the main opportunity relates to the mobility and load shaping capability. As an example, optimal charging/discharging scheduling of Electric Vehicles (EVs) can help smoothing the system load profile [39]. EVs bring a new aspect of EMS in smart grids, as real-time machine to machine communications are needed in order to exchange information among EVs and local or central controllers [40].

- Load type and nature

According to loads nature and function, loads can be categorized and modeled in different types, and, subsequently, their behavior can be simulated differently [41,42]. Based on that, systems behavior can be studied in different ways. As an example, when nonlinear loads are connected to the grid, they draw harmonic currents, which cause voltage harmonics and losses over the system [43].

- Effect of loads on global emission

Without any doubt, global warming affects industries. This feature really changes the future of loads. Loads that produce greenhouse gases will be less used in near future; instead, there will be a tremendous increase in the number of loads that are green. This means that people wish to use electric vehicles instead of traditional cars, which results in both a change and opportunities in energy consumption [44].

2.3. Communication Infrastructure

Communication infrastructure is deemed as the backbone of the communications system upon which different broadcasting and telecommunication services are operated [45]. Many architectures are designed in respect of Information and Communication Technology (ICT), based on the need of the system and valid facilities. Generally, communication infrastructures are divided into two categories: (a) wired communication systems like Asymmetric Digital Subscriber Line (ADSL), PLC, and Ethernet; and (b) wireless communication systems like WiFi, Cellular, and Satellite [46]. The main goal of every communication system is to obtain, collect, process, and save the information from each component of the system. In this manner, information sensing and processing are defined as a part of communication infrastructure in energy systems [31]. After sensing information and processing it, the next step is to send commands from decision-makers to low-level parts of the system; this means that bi-directional or two-way communication systems are needed to handle data exchange among components. The whole process of receiving, processing, and sending back the data is affected by the stochastic nature of the loads. This means that uncertainty in the energy demand affects the designed structure of the communication system. Therefore, stochastic nature of loads should be considered in planning of the communication system [47]. To overcome this drawback, in [47], two robust applications based on multi-layer and mixed-line-rate network design are introduced for the communication network in order to deal with uncertain input parameters.

Talking about collecting information in an energy system, which can be considered as a key part of communication infrastructure, gateways are needed to overcome this part, for which they are responsible to reach information from sensors and send it to data collectors [48]. In addition, in some cases, information could be shared with some parts of the system. However, what is understood from every communication system is that a well-designed architecture is needed for the communication system, so each component of the system can be named in a level [49].

In the IoT perspective, communication infrastructure is mostly included in network layers that provide networking supports and data transfer using wireless and wired network for industries [50]. In the IoT-based systems, communication networks face challenges like scalability of the system, quality of the service requirements, and optimizing communication related power consumption. In addition, as in this system, things are supposed to communicate with each other with minimal human intervention; then, each subsystem, in this case the communication system, should be able to be organized and healed by themselves. In this manner, standards and protocols need to be agreed by the society in order to have a mutual perception. To do so, in [51], communication protocols are categorized in three main classes that are contention-based, contention-free, and hybrid protocols. More details about communication infrastructures could be found in [51,52].

Machine-Type Communication (MTC) is defined as the data exchange and processing among machines with the minimum intervention of human, which is generally used in IoT-based systems. To establish data connection among things in MTC, several steps must be followed: first of all, things that are supposed to be connected should establish a session between them (Figure 2). In this step, the flow and direction of data flow need to be controlled. Depending on the nature of the application, full duplex, half duplex, or simplex communication mode will be established. In this manner, applications must know when and how long they should send information. For this step, International Organization for Standardization (ISO) introduces a detailed protocol in order to establish the connection between objects in communication systems [53]. In the second step, they may exchange

their main information. Based on the importance of the establishment of the access or the importance of the main data (payloads), several MTC technologies are used. For example, in the Long-Term Evolution (LTE) standard, to establish the connection of User Equipment (UE) with a higher level Evolved Node B (eNodeB), it is possible that a collision happens during the process [54]. The collision may happen if two or more UEs try to send preambles simultaneously. Then, as eNodeB is not able to recognize a collision happens, it will send a Random Access Response (RAR) to the recognized UEs. To increase the chance of successful connection, several attempts will be done by UEs accordingly. This access reservation procedure has a probabilistic characteristic, and the packet may be lost during the data transmission both in the uplink and downlink processes, or even failure and limitations in the system bottlenecks [54,55]. Different perspectives of MTC challenges are defined and tried to overcome in the third Generation Partnership Project (3GPP) by different solutions and technologies like LTE and Low Power Wide Area Network (LPWAN) introduced as NarrowBand IoT (NB-IoT) [56,57].

Aside from probability characteristic of communication systems, especially wireless communication systems, coverage range, throughput, latency, capacity, power efficiency, and complexity are the issues raised in this field [58].

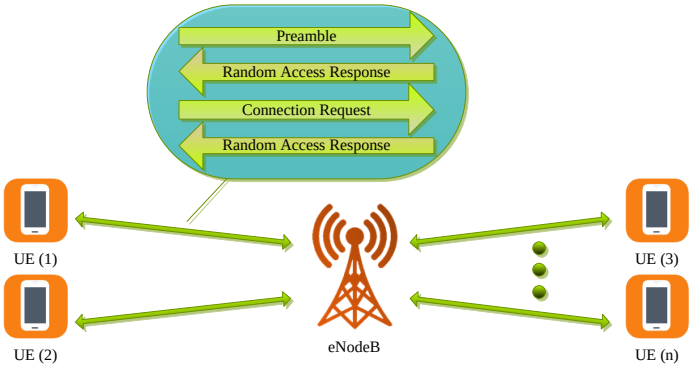

Figure 2. Establishing a communication link between end users and Evolved Node B (eNodeB).

2.4. Security and Privacy

One of the main questions every system faces is that who is in charge of the system, and to what extent an authority can control the system, especially in modern energy systems with many independent players [59,60]. Security is an inseparable part of IoT architecture because of its importance and effect on the whole system performance [59]. As energy systems become more complex, security concerns are raised. In other words, integration of IoT with energy systems makes the security issue more vulnerable; therefore, more attention must be paid to system security [60]. As an example, integration of wireless and wired communication network in energy systems increases accessibility to information and subsequently makes system security more vulnerable [61]. On the other hand, a key feature to implement the IoT in the energy system is trust. If system components, in this case, people, want to use a facility, it would be more appropriate if system asks for their permission in advance. In this manner, there would be less violation of users' privacy [62]. Moreover, in [63], users are involved in management of their security and privacy. This leads to a trusted privacy management system where both sides (consumers and service providers) have a degree of controllability over their privacy.

As Big Data (BD) is available on an IoT platform, many service providers, like public and private health care companies, can access different types of information. In this manner, users' information can be shared with some third parties, which in turn raises issues about the privacy of the end-users. Generally, it is suggested that every accessibility to information is possible with the permission of end-users, unless the information will not be shared with service providers [64]. The privacy issue drives the problem into a more complex one, as adaptive service scenario should be designed.

Generally, there are two types of information related to security of an IoT system. The first type of information is that people do not want to share it for the sake of their privacy, such as the position of their electric vehicle during a day. The second type of information is that end-users are worried about the security of their information, as they may suffer financial loss if specific third parties are informed about it, like their bank account or the monthly energy consumption. A solution for privacy issue of IoT systems for both cases, mentioned in [65], is to ask end-users to use their information for a specific purpose or to inform them that the information shall not be shared with any other third parties. What is obviously accepted here is that consumers feel more confident when they are asked for the accessibility of their information.

Aside from this, a key feature to meet the end-users' and service providers' trust is to ensure that the system is secure. A great effort has been done in reviewing most parts of security of Cyber Physical Systems (CPS) such as threats, attacks, and controls in [66]. In [67], an encryption scheme is introduced to secure energy information from unauthorized manipulations. In this manner, energy systems are divided into four categories: appliance group, monitor group, central controller, and interface with users. Each level needs its own security scheme. To do so, data integrity, computational complexity, and needed memory size must be taken into account to have the best energy efficiency.

More security is demanded when data is transferred among IoT components, including communication between IoT devices and the gateways, gateways and data store, data store and data access layer, and users and data access layer [68]. This trade-off is an ongoing challenge for energy internet systems, as in one hand, the more information that is transferred among IoT components, the more benefit they could gain; and, on the other hand, the more information end-users share with third parties, the more they could be threatened, and in this manner system may become more vulnerable. This uncomfortable feeling can be balanced by incentive offers from service providers.

In IoT-based systems, a tremendous amount of heterogeneous objects is connected together. As the number of things rises, traditional methods used for cyber security and control systems become insufficient. For example, for a large IoT system in which a large geographical area and many components are included, it is more practical to implement distributed or decentralized control system than centralized control systems, for the sake of more reliable decision-making [69]. On the other hand, in distributed and decentralized system architectures with different levels of controllability, different levels of security may be applied. In this manner, advanced machine learning and data mining methods are developed with respect to of cyber security [70]. This happens in IoT framework because data is collected from different sources, which may be located in different security but the same physical level [71,72]. In this regard, many aspects of security in energy internet arise such as privacy and trust of the end-users, authentication, access control, etc. [73]. As an example, in [74], a method is developed to give access to the end-users' position in emergency conditions.

In summary, security in energy systems includes three main parts: (a) data confidentiality; (b) privacy; (c) and trust area [71]. Related parts should be defined in detail and in an understandable way for both end-users and service providers. For instance, it is not beneficial to explain encryption of data for end-users, but they should be convinced that their information is safe with the system.

2.5. Energy Management Systems in IoT framework

One of the main motivations for developing integrated energy systems and what is called energy internet is to manage energy in an optimal way. To make it clear, assume an IoT-based energy system including Electric Vehicles (EVs) [75]. In this attempt, each EV tries to maximize its objective (paying less money), while an energy retailer tries to maximize its own objective (earning more money). Both sides act smart and try to maximize their own profit, which in this case their objective is in conflict. A solution to find an optimum point, in which both sides satisfy with their profit, is to hire IoT infrastructure (e.g., WiFi or WiMAX systems and sensors to collect information from EVs).

To do so, many efforts have been done to improve EMS considering different objectives such as reducing energy losses, minimizing the costs or even some technical objectives like minimizing

voltage deviation [33,76,77]. In the new paradigm of energy systems, customers of energy may produce and inject energy (also known as prosumers) to an upper level, which may be a distribution system. The role of prosumers energy management systems is highlighted in the literature as their role in peak demand management [78]. In this regard, not only electrical systems should be reconfigured, but also communication systems have to change fundamentally. Moreover, prosumers can not only exchange energy, but also data with the system using bi-directional connections [76]. In this regard, control objectives and settings of the EMSs have to be reconfigured as well. In [77], a dynamic control strategy is introduced and limitations of the communication system are considered as a drawback that makes challenges in a fast response of the designed control system. On the other hand, with the growing trend in the use of internet in smart buildings and cities, it is a must to design an energy-efficient, cost-effective, secure, and reliable IoT-based platform for energy management purposes [79]. IoT solutions for EMS are developed in regards of either reduce or shift energy consumption by applying incentive offers or optimize utilization of energy sources.

Generally, there are two types of energy/power management strategies, used in smart energy applications, named as passive schemes based on self-autonomy, and interactive schemes, based on information sharing mechanisms. In a given interactive power/energy management system (IP/EMS), local and global system information (such as line currents, nodal voltages, frequency and powers) is communicated in the system and exchanged between corresponding nodes in order to determine operation point of each controllable DG or consumption unit. These strategies also benefit from a sort of intelligence in the integration of the computing and communications technologies, which help them to define and develop the communication structure based on the computation burden of each node and other related system's objectives and constraints. In this regard, three different communication schemes can be realized for an IP/EMS: centralized, decentralized, and hybrid. In centralized EMS, a centralized decision-maker is used to find the optimum point for the objective of the system based on the information of every component [80,81]. In this manner, mostly energy sources and end-users have no authority to manage the energy unless the decision maker (centralized controller) decide for an action. In [80], a centralized EMS using model predictive control is designed for isolated MGs. In this regard, lack or loss of information can significantly affect the mentioned method. In centralized control scheme, not only a centralized controller controls system features like frequency and voltage, but also it is responsible for some challenges like harmonic mitigation [81]. In a decentralized EMS, every player in the system decides individually to optimally manage its energy production/consumption level [82,83]. A decentralized system is more reliable, as every sub-system decide independently. In contrast, these systems have a more complex communication system architecture, as sub-systems need to transact information with each other. Distributed EMS is implemented to decentralized system category in order to have more reliability of the system in some cases [84]. In distributed EMS, each node shares specific information with the neighboring nodes using a bidirectional communication system, yet they act independently and decide to optimize their performance based on the shared information. In this manner, more complex communications are needed (compared to other schemes), but more controllability can be achieved over a system wide operation.

In each of the mentioned schemes, different communication technologies such as microwave (uW), power line carrier (PLC), fiber-optics, infrared, and/or wireless radio networks (such as global system for mobile (GSM) communications and code division multiple access (CDMA)) can be effectively used and integrated into the existing infrastructure.

On the other hand, self-autonomy of operation for a local controller without having information from neighboring nodes is the main idea of a passive power/energy management scheme (PP/EMS). In this structure, it is assumed that making an information sharing mechanism is too costly or not viable, thus independent operation of energy sources is required. In this realization, it is important to clearly define the control objective of each node to assure reliable operation of the system. It should also be mentioned that this category includes limited accessibility and communication links. Mostly, it includes simple energy management in which local optimization is needed. This category of energy

management may also be used for very low harvested power levels [85]. As the level of energy is very low, for instance in sensors, it is logical to observe energy from sensors' environment and then use it for any kind of applications. Therefore, there may be the maximum level of energy to be managed [86].

3. IoT Challenges in Energy Systems

There are many challenges in applying IoT in energy systems. Some of them are mentioned as follows.

3.1. Identification of Things on the Internet

As the number of things connected via the internet increases, item identification becomes a major challenge [87]. It has been mentioned in [80] that every real thing in IoT framework should be identified as a virtual object. The first challenge in identifying a real-world object with a virtual one is in its concept: Does a virtual object present all information of its real-world match? For instance, based on the services provided by a service provider, specific identifications will be allocated to an object. Hence, a real object could have several virtual identifications representing several virtual objects/services. Then, the challenge appears when objectives of services are in contrast with each other, and then there will be a conflict in the thing's behavior, which means that an object tries to follow different objectives simultaneously. Using identification methods like IPv4 could solve the mentioned issues; however, it becomes limited only to some local usage such as some point-to-point links. Other standards like IPv6 can also provide an identification and location system for objects on networks, but it suffers in certain conditions such as the mobility of objects in energy systems (EVs for instance) [88,89]. This is because, as the position of an object changes in the system, the object may be connected to a new node of the communication system. Then, the object should be addressed again. This is even more challenging in the energy internet where there are heterogeneous objects and there is going to be a mismatch of identification when different protocols used for addressing objects [90].

3.2. Supplying Energy for Sensors

In IoT-driven environments, every object sends and receives information to other objects or a cloud of information. This means that a sensor should be used to sense the information for each individual object and an energy source should also be defined to supply each sensor. Considering thousands of these sensing nodes, a tremendous amount of energy would be needed to run the things. This is a serious challenge that IoT will face in the near future [91]. A new hierarchical architecture including three layers of hardware, middleware, and application layer is designed in [84] in order to save energy consumed by sensors in an IoT-based system. In this attempt, sensors are switched into sleep mode in certain conditions to save energy: (1) whenever it is not necessary to use them; (2) whenever using sensors will affect its battery life; or (3) when battery energy is lower than a threshold. In [92], a new framework is introduced for IoT systems in order to decrease human interaction in system management and decrease energy consumption. In this regard, the self-organized system is designed, which is able to optimize energy efficiency, which leads to more saving in energy used by sensors. This self-organized IoT framework is called Self-organized Things (SoT).

Aside from software solutions for saving energy or optimizing energy efficiency used by sensors, there are methods to provide sufficient energy sources in hardware point of view. In [93], wireless energy harvesting is introduced as one of the best ways to supply energy for many sensors. In this regard, energy harvested from environmental sources like solar power is used to supply sensors.

3.3. Big Data (BD) Processing

As the amount of information becomes large in an IoT-based system, data handling with traditional methods becomes impractical. BD analysis is one of the main challenges in IoT systems, as systems should be able to store data, analyze it, and plan for future, based on the present and the past data. In designing algorithms to deal with this condition, uncertainty and lack of data should also

be considered. On the other hand, data is collected from different sources, and BD analysis in real time is a key to apply IoT systems in real world situations [94]. Therefore, modern methods with specific architecture are needed for BD processing. In this regard, some toolboxes such as toolboxes in Matlab are developed to deal with BD [95,96]. One solution to deal with BD is using localize processing of data. In this regard, devices are aware of the state of the main server and their neighbors, which makes it possible to save more network bandwidth. In addition, by using localized algorithm, it is possible to deal with BD, as data mostly process locally [94].

In respect of BD analysis, as the system enjoys more detailed information, data processor systems are able to analyze information in more detail. On the other hand, system security will be affected by the large amount of information [97]. Despite challenges introduced by BD analysis, advanced machine learning algorithms can enjoy large scale information for better training in their process [95,96,98].

Assume that there is an Advanced Metering Infrastructure (AMI) to collect data of the system. The very first step after gathering the data is to use a method to extract information. This can be done through cluster-based computing systems. For example, in 2004, Google introduced a solution based on the Google File System, which used different methods to process data. In 2012, Hadoop with an Apache license introduced another method to deal with BD, and used Spark SQL as a database system. Later, this BD processing framework became the most dominant one [99].

After useful knowledge extraction from BD, the system should be able to further classify the information and provide certain services (such as sending signals to the actuators or alerting systems). As an example, in energy systems, data collected from electricity and heat consumption can be subjected to consumers' type like industrial and residential, and each of the consumption level can be further classified into off, standby, and active operating mode. Based on this argumentation, a BD architecture is introduced in [100].

3.4. Privacy and Security

The concepts of privacy and security are tied together; as the level of security becomes lower, the system would be more threatened by unauthorized manipulation and so the privacy may be affected. On the other hand, privacy could be violated in a secure system. As an example, assume that noise pollution is aimed to determine on streets in an IoT framework; hence, sound sensors should be installed on the streets. While the system may be designed in a secure manner and no unauthorized third party may have the access to consumers' information, the very first question arise about privacy is that: "Is it legal to record people's voice?" Another example is that in IoT framework for smart buildings, a procedure could be detected for what people watch on television, or when they are awake. Although an appropriate security protocols may be used in such system, the question is that who can access this information, and do people feel pleasant to share this information? This challenge makes IoT processing slow and is extensively reported in the literature [101,102].

Generally, there are three main categories for privacy challenges: personal privacy, privacy-preserving data mining, and underlying technologies' privacy. Considering these aspects of privacy, legal regulations, which are globally accepted by governments, are strongly needed. In addition, human rights should be considered in all actions that are done in this regard [103]. Generally speaking, limitations in IoT sensors' capability make challenges in privacy and security issue more complex. This means that they cannot handle complicated security protocols. This challenge is mentioned in [104], and a small cryptographic key size is designed for IoT security.

3.5. Standards

IoT covers a large range of technologies and use cases that range from a single device to massive cross-platform deployments of embedded systems connecting in real-time while following different standards [105]. The mismatch among IoT devices using different standards and protocols is a major problem. Assume that some information needs to be sent from an Apple iPhone device to some other

mobile devices via Bluetooth. This may not be possible as Apple devices can only be connected to Apple devices via Bluetooth.

The very first step in standardization of IoT-based energy system is to define a system of systems with a common sense of understanding. In this manner, it is worth mentioning some of the organizations' definitions of IoT are as follows:

- IEEE: The IoT is the integration of things, equipped with sensors, via the internet.
- The European Telecommunications Standards Institute (ETSI): This institute does not provide a direct definition of the IoT. However, it brings a definition for M2M communication. M2M communications is a kind of communication among devices for which there is no need of human direct manipulations.
- The International Telecommunication Union (ITU): the IoT is a ubiquitous network, which means that it is available anywhere, anytime, by anything and anyone. This definition does not answer specific questions like what is the range of availability of an IoT system, yet generally, it brings a great presentation of an IoT system. In addition, ITU Telecommunication Standardization Sector (ITU-T) mentioned the IoT system as an infrastructure for information society that connect physical and virtual things together. This definition includes all inanimate objects.

Aside from the mentioned institutes, some companies provide definitions about the IoT. Some of them are mentioned as follows:

- The Systems, Applications, and Products in Data Processing (SAP): The IoT is a world where physical things are defined in the information network, hence they can participate in business activities.
- The CISCO: this company defines the Internet of everything as gathering people, data, and things in order to provide a network, which is capable of exchanging information into actions.
- The Hewlett-Packard Company (HP): the IoT is a system, for which every object is defined on the internet. This means that human can manipulate and control objects from any place; and devices can communicate with each other without human interactions [106].

What is explicitly obvious from the comparison of IoT definitions provided by a non-profit institute and companies is that they all define the IoT in a same manner, yet companies try to provide a definition for which its benefit for the people is bold. In summary, the IoT is an infrastructure including sensors, communication system, data processing system, and objects that are connected via the Internet, in order to bring services and applications for people with minimum human intervention. Based on this definition, related standards should be addressed for communication systems, data processing, the Internet protocols, services, and applications.

In case of communication systems, for example, IEEE 802.15.4-based (ZigBee) is one of the mostly adopted standards about low-rate wireless networks [107]. Based on this standard, data can be transferred at 800/900 MHz and 2.4 GHz. Other standards like IEEE 802.11p have also been developed for wireless communications. IEEE 802.11 is the standard about Wireless Local Area Networks (WLANs) in a vehicular environment. Communication bandwidth in the mentioned standard is 10 MHz and 5.9 GHz frequency band [108]. It is worth mentioning that technologies like LoRa and Sigfox present long range, low power consumption data transmission, and are used widely in IoT-driven systems [109,110]. The range of frequency accepted by the aforementioned technologies is in 863–870 MHz [110]. Main advantages of LoRa and Sigfox technologies are their free-license availability. In addition to their long-range data transmission, which makes it possible to be utilized for many applications such as agriculture processing, energy management systems, smart homes, smart parking, etc. Regarding LoRa technology, LoRaWAN is a protocol designed for low-powered devices specifically for the LoRa technology. This is suitable for some applications in which a small amount of data need to be transferred, such as in electric vehicles [111]. These features lead to the

integration of the LoRaWAN protocol with cellular communication technologies such as 4G in the IoT-driven systems [112]. The LoRa technology has been widely accepted by the related organizations.

In Sigfox technology, however, ultra-narrow band technology is employed in order to transmit information in long-distance communication [109]. Considering the bandwidth dedicated to the Sigfox technology, only a small amount of data may be transferred. While LoRa technology may be used in bidirectional communication links, for instance, grid monitoring, network density needs to be higher in Sigfox technology. Apart from this difference, these technologies are very similar [113]. Considering characteristics of the Sigfox technology, it is widely used in remote devices that need to transfer small amounts of data in a long distance.

In a similar way, several attempts have been done by many organizations such as oneM2M and IEEE to define a global standard that fits every IoT system [100,114]. For instance, in the OneM2M organization, several partners participate in defining a standard for Machine-to-Machine (M2M) with more focus on the service layer. On the other hand, IEEE organization is developing a standard for IoT focusing on communication layer. In [115], a great attempt is done to collect standards for IoT introduced by organizations to make a coordination among them. A complete list of communication standards regarding to the IoT is mentioned in Table 1.

Table 1. Communication technologies and standards.

Technology Name	Standard Name	Frequency Band	Coverage Range	Data Rate
ZigBee	ZigBee	2.4 GHz	100 m	250 Kbps
WiFi	IEEE 802.11	2.4 GHz, 5 GHz	150 m	1 Gbps
WiMAX	IEEE 802.16	10–66 GHz	50 km	75 Mbps
Thread	IEEE 802.15.4	2.4 GHz	30 m	250 Kbps
Z-Wave	Z-Wave	900 MHz	30 m	100 Kbps
Bluetooth	IEEE 801.15.1	2.4 GHz	10 m	1 Mbps
Cellular	4G	1.4–20 MHz	50 km	100 Mbps
LoRa	LoRa	863, 915 MHz	+10 km	100 Kbps
Sigfox	Sigfox	863, 915 MHz	+10 km	10, 100 Kbps
PLC	IEEE 1901	500 kHz	3 km	10–500 kbps
Ethernet	IEEE 802.3	100 MHz	100 m	100 Mbps–10 Gbps
Fiber optic	IEEE 802.3	500 MHz	100 km	40 Gbps
Satellite	IEEE 521	30–300 GHz	6000 km	1 Mbps

3.6. Global Architecture for Energy Internet

Architecture design is another challenge in IoT-enabled energy systems. System architectures are designed based on its applications and use. A basic architecture for an IoT system includes three layers: application layer, network layer, and perception layer [116]. The application layer is the top layer in which transferred data from network layer are proceed and used to provide services. Network layer is the middle layer, which is responsible to receive information from perception layer and transmit it application layer. Most IoT components such as communication systems' components and protocols are categorized in this layer. The lowest layer in three-layer IoT architecture is the perception layer. Collecting information from sensors and processing of data are considered in this layer. The three-layer architecture is introduced by standards, like IEEE P2413 [114]. This architecture is also recommended for health care systems and smart grids [117,118].

The three-layer architecture is well known because of its simplicity, and it is easy to apply. However, some details may be missed by defining the IoT system through three layer. In this regard, some other architectures are introduced in the literature, including more layers with more details in each layer, or targeting a goal and introducing it as an additional layer. In this regard, security as one of the most important features in every IoT systems is considered as another perspective of the architecture [119]. In [120], a generic architecture is introduced to deal with an interoperability challenge in IoT where a distributed architecture is designed to deal with heterogeneity, scalability,

interoperability, security and privacy, etc. In this attempt, a three-layer architecture is presented, and an extra distributed module, called security management, is presented. This module is distributed among the main three layers, and by doing so, modeling and enforcement of security, policies are supported. In [121], a five-layer architecture is introduced including objects layer, object abstraction layer, service management layer, application layer, and business layer. In the business layer, BD analysis and end-user privacy is mentioned. In the application layer, services are presented to consumers. The service management layer plays the role of the middleware layer. Hence, in this layer, processing of data received from the object abstraction layer will be done. In the object abstraction layer, transferring the information between sensors and the service layer is handled. This layer acts as communication layer, so different communication technologies like WiFi, ZigBee, etc. are categorized in this layer. The very basic layer is objects layer in which things are presented as physical sensors. In this layer, information are collected from objects. IoT-based energy system's architecture is illustrated in Figure 3.

What is evident by reviewing IoT architectures introduced in literature is that every team tries to follow its goal by defining an architecture for an IoT-based system. For instance, to improve the security of the system, a security layer may be added to the system architecture, while this may affect data quality as a result. Designing a general architecture for IoT-based system leads to a trade-off among system goals, physical and virtual components, system size, etc.

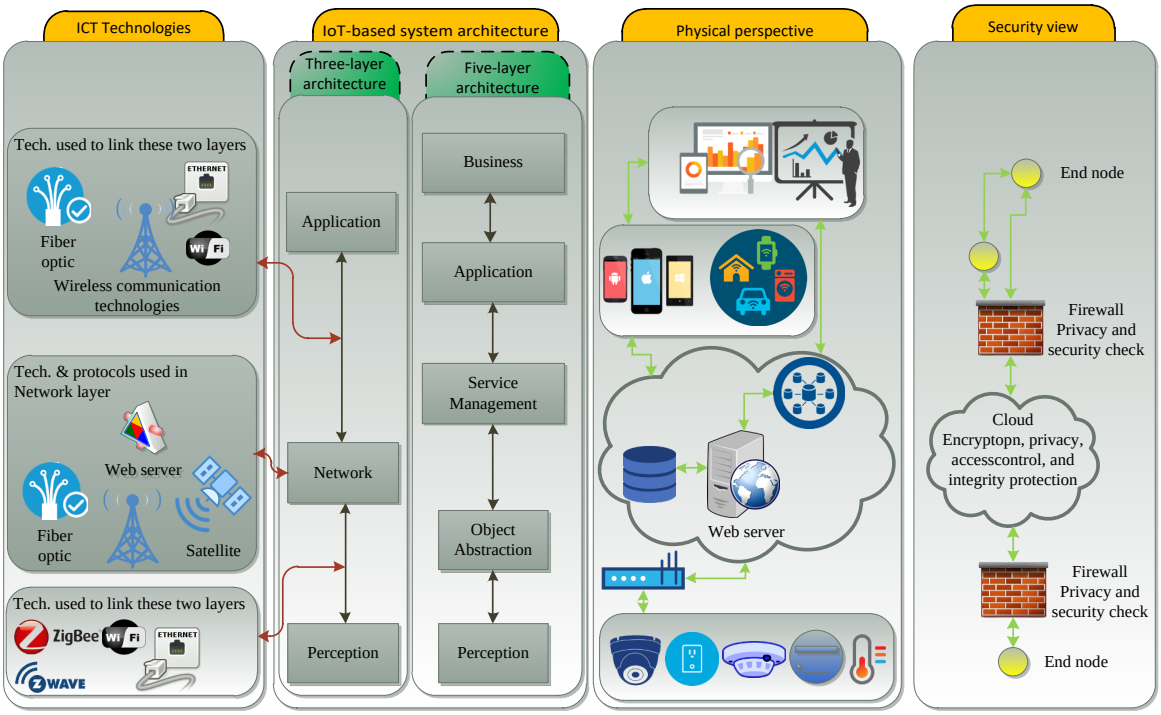

Figure 3. IoT-based system architecture.

4. Illustrative Examples

In this section, some examples of energy internet are indicated to show different applications of IoT systems in smart buildings, smart cities, and smart grids, which vary greatly in terms of system structure and scale, information scale, privacy and security level, etc.

4.1. Smart Buildings

The very basic feature of an energy system using IoT can be introduced as a consumer of energy sending information to a data collector via a communication system. This appears in a smart building.

In this case, the number of components is limited, and they are close to each other. Hence, short-range communication systems like ZigBee is suitable for this application.

In designing of an IoT-based smart building, the very first step is to address every physical object by a virtual one [122–124]. In this manner, a virtual environment will map every object related to the real-world environment. For developing smart energy systems in buildings, the three main issues should be considered: energy consumption monitoring using smart meters and smart devices, designing a model to analysis it, and implementing an appropriate IoT-based system considering the designed model to analyze energy and needs. For example, using LAN is more appropriate in comparison with a WAN for a small house. The latter one needs attention to every detail including how to manage BD, determine location-based energy management, etc., and all of the IoT-based smart buildings are studied. In order to make the information secure, some policies should be agreed on by energy consumers. As an example, details about the location of end-users must be available to authorities, and security constraints should not negatively affect this accessibility.

The main motivator of employing IoT for Buildings is reducing sensors' prices and developing applications that are user friendly [125]. This means that, by using a mobile device, every component that is connected to the IoT system can be monitored and controlled. In [126], an example of IoT-based smart home is presented. In this attempt, data sense by some sensors, and then information is sent to a network using ZigBee technology in JavaScript Object Notation (JSON) format. Then, applications like monitoring home conditions, managing home conditions, and controlling home access are applied through the Internet. Physical components are equipped by RFID tags, and, in this manner, physical objects are introduced into the cloud as virtual objects.

One of the main applications in IoT-based smart buildings is the internet-based demand response, which can be introduced as incentive-based or price-based schemes [127]. Communication infrastructure is mentioned as the key feature in developing DR in smart buildings.

4.2. Power IoT

The issue of implementing IoT in smart grids is dissimilar from smart building in different aspects of security, data mining, etc. One of the main reasons that can be addressed is the scale of the system. As the size of the system increases in smart grids, wireless communication is mostly chosen for communication infrastructure. This leads to a great attention to ICT in IoT-based smart grids [18].

Another matter in IoT-based smart grids that is worth a great amount of attention is a variety of applications and services, provided by either the grid or third parties. In this manner, a higher level of standards, protocols, architecture, etc. should be followed, which is called industrial IoT (IIoT) [128]. At the same time, as the systems' scale become larger, the need and importance of real-time applications increases. This is introduced as a Knowledge Discovery in Database (KDD) in the literature, as online monitoring is a desirable capability in smart grids [129]. To overcome this challenge, new technologies, protocols, and architectures should be developed. In [130], a new technology called Software Defined Networking (SDN) is developed to make data system more robust. By using SDN technology, real-time monitoring and control of the energy systems are available. To do so, an architecture including infrastructure, control, and application layers is presented based on the IIoT paradigm for energy systems. Talking about IoT-based smart grid architecture, a four-layer architecture for residential smart grids including device, network, cloud management, and application layer is presented in [131]. In this effort, the network layer connects device and application layer using IP-based protocols like Representational State Transfer (RESTful) based on Hypertext Transfer Protocol (HTTP). On the other hand, in the device layer, some other IP-based protocols like Bluetooth may be used for connecting things to gateways, as most devices have limitations from a communication point of view.

To apply the IoT system into smart grid systems, some technologies should be considered: (1) Sensor technologies; (2) Communication technologies, like Bluetooth, ZigBee, etc.; (3) Data Mining technologies: as IoT nodes are limited in many aspects such as bandwidth, it is inappropriate to

exchange all unstructured data. Hence, data fusion technologies may be hired in order to exchange useful data. In [132], necessary technologies to implement IoT into power systems are discussed in detail.

4.3. IoT-Driven Smart Cities

To apply IoT systems in smart cities, some fundamentals need to be defined in advance. The first indispensable necessity is communication infrastructure. Then, people interaction with the system should be enabled. In smart cities, IoT is not only for energy management purposes, but also for many different goals, such as smart parking, transportation and vehicular traffic, healthcare, etc.—all of which can be monitored and controlled via a unified IoT system, while a different level of accessibility, privacy, security, BD, and even communication technologies must be enabled based on the services' specifications [133]. To apply IoT in smart cities, still an architecture must be used to categorize every component in a category and to define their connections. In [106], a three-layer architecture including perception, network, and application layer is used in order to implement IoT systems into smart cities. Many of the implemented IoT systems in smart cities are reported in [106,134], which include Amsterdam, Barcelona, Fujisawa, etc. In all of the mentioned attempts, one or two services like controlling streetlights are implemented. Although these attempts are appreciated, a global IoT system including most IoT services mentioned in the literature with different control and monitor level, and real-time accessibility for consumers is a matter of research and has not been implemented yet.

5. Discussion and Conclusions

In this paper, a general overview of the IoT-enabled energy systems was presented. IoT key features, different specifications, such as energy consumers, communication infrastructures, and privacy were also outlined in the context of energy systems, which could be an integration of different domains such as electrical and thermal grids and communication networks. Then, some challenges in IoT-based energy systems like BD analysis and are discussed. Finally, some examples of IoT-based systems in three levels of smart homes, smart power grids, and smart cities are discussed, so a general view of how to implement IoT systems in real work can be comprehended.

One of the main challenges of enabling IoT in energy systems is to map every single object into one unique virtual object. This challenge can be overcome via standard communication protocols like IPv6 standards. On the other hand, as IoT-based systems contain many components, they can raise concerns from different points of view like security and energy saving. In this regard, every system designer may include his/her own concerns to design an architecture for the system, which leads to different architectures. Therefore, a unified architecture for IoT-based energy systems is still a concern for researchers.

It is true that every piece of useful information from system components can enhance monitoring or controlling the system. However, adding information to controlling systems as an input can make it more complex. Moreover, this needs financial support. The development of IoT-based systems increases dramatically as the price of sensors decreases during the last decade. It is anticipated that sensors become smaller in size and cheaper in price. Changes in wireless sensor network and the maturation of sensor systems, improvement in performance of data processing systems, and the progress in solving communication systems drawbacks, such as communication delays and data loss, will affect the future of IoT-based system.

One of the main objectives of the integration of the IoT with energy systems is to involve more people's cooperation with system operators, in addition to involving more interaction with the energy components. By doing so, it is expected to operate the system in more reliable and stable conditions. Improving system performance is always desired from the viewpoint of system operators, while this may face challenges from some perspectives like cloud computing, data management, infrastructures, and social network.

Author Contributions: All authors contributed to the preparation of the manuscript. B.S. made a comprehensive review of the existing literature and wrote the manuscript. A.A.-M., J.C.V., and J.M.G. guided the whole work, edited the language, and provided their comments on the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mohanty, S.P.; Choppali, U.; Kougianos, E. Everything you wanted to know about smart cities. *IEEE Consum. Electron. Mag.* **2016**, *5*, 60–70, doi:10.1109/MCE.2016.2556879. [CrossRef]
2. Chelloug, S.A.; El-Zawawy, M.A. Middleware for Internet of Things: Survey and Challenges. *Intell. Autom. Soft Comput.* **2015**, *3*, 70–95, doi:10.1080/10798587.2017.1290328. [CrossRef]
3. Boroojeni, K.; Amini, M.H.; Nejadpak, A.; Dragicevic, T.; Iyengar, S.S.; Blaabjerg, F. A Novel Cloud-Based Platform for Implementation of Oblivious Power Routing for Clusters of Microgrids. *IEEE Access* **2016**, *5*, 607–619, doi:10.1109/ACCESS.2016.2646418. [CrossRef]
4. Bouzid, A.M.; Guerrero, J.M.; Cheriti, A.; Bouhamida, M.; Sicard, P.; Benghanem, M. A survey on control of electric power distributed generation systems for microgrid applications. *Renew. Sustain. Energy Rev.* **2015**, *44*, 751–766, doi:10.1016/j.rser.2015.01.016. [CrossRef]
5. Giustina, D.D.; Dedè, A.; Invernizzi, G.; Valle, D.P.; Franzoni, F.; Pegoiani, A.; Cremaschini, L. Smart Grid Automation Based on IEC 61850: An Experimental Characterization. *IEEE Trans. Instrum. Meas.* **2015**, *64*, 2055–2063, doi:10.1109/TIM.2015.2415131. [CrossRef]
6. John, T.; Ping Lam, S. Voltage and frequency control during microgrid islanding in a multi-area multi-microgrid system. *IET Gener. Transm. Distrib.* **2017**, *11*, 1502–1512, doi:10.1049/iet-gtd.2016.1113. [CrossRef]
7. Parhizi, S.; Lotfi, H.; Khodaei, A.; Bahramirad, S. State of the art in research on microgrids: A review. *IEEE Access* **2015**, *3*, 890–925, doi:10.1109/ACCESS.2015.2443119. [CrossRef]
8. Setiawan, M.A.; Shahnia, F.; Rajakaruna, S.; Ghosh, A. ZigBee-Based Communication System for Data Transfer within Future Microgrids. *IEEE Trans. Smart Grid* **2015**, *6*, 2343–2355, doi:10.1109/TSG.2015.2402678. [CrossRef]
9. Das, S.; Singh Sidhu, T. Application of compressive sampling in synchrophasor data communication in WAMS. *IEEE Trans. Ind. Inform.* **2014**, *10*, 450–460, doi:10.1109/TII.2013.2272088. [CrossRef]
10. Bou-Harb, E.; Fachkha, C.; Pourzandi, M.; Debbabi, M.; Assi, C. Communication security for smart grid distribution networks. *IEEE Commun. Mag.* **2013**, *51*, 42–49, doi:10.1109/MCOM.2013.6400437. [CrossRef]
11. Karlsson, D.; Hemmingsson, M. Terminology, phenomena, and solution implementation strategies. *IEEE Power Energy Mag.* **2004**, *2*, 68–76, doi:10.1109/MPAE.2004.1338124. [CrossRef]
12. Mao, R.; Li, H.; Xu, Y.; Li, H. Wireless communication for controlling microgrids: Co-simulation and performance evaluation. In Proceedings of the 2013 IEEE Power and Energy Society General Meeting, Vancouver, BC, Canada, 21–25 July 2013; doi:10.1109/PESMG.2013.6673056. [CrossRef]
13. Mirtaheri, H.; Chicco, G.; del Razo, V.; Jacobsen, H.A. A framework for control and co-simulation in distribution networks applied to electric vehicle charging with Vehicle-Originating-Signals. In Proceedings of the 2016 IEEE International Energy Conference (ENERGYCON), Leuven, Belgium, 4–8 April 2016; pp. 1–6, doi:10.1109/ENERGYCON.2016.7513941. [CrossRef]
14. Kounev, V.; Tipper, D.; Lévesque, M.; Grainger, B.M.; Mcdermott, T.; Reed, G.F. A Microgrid Co-simulation Framework. In Proceedings of the Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Seattle, WA, USA, 13 April 2015.
15. Wong, T.Y.; Shum, C.; Lau, W.H.; Chung, S.H.; Tsang, K.F.; Tse, C.F. Modeling and co-simulation of IEC61850-based microgrid protection. In Proceedings of the 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm 2016), Sydney, NSW, Australia, 6–9 November 2016; pp. 582–587, doi:10.1109/SmartGridComm.2016.7778824. [CrossRef]
16. Wang, X.; Yaz, E.E. Smart Power Grid Synchronization with Fault Tolerant Nonlinear Estimation. *IEEE Trans. Power Syst.* **2016**, *31*, 4806–4816, doi:10.1109/TPWRS.2016.2517634. [CrossRef]
17. Wang, S.; Gao, W.; Wang, J.; Lin, J. Synchronized sampling technology-based compensation for network effects in WAMS communication. *IEEE Trans. Smart Grid* **2012**, *3*, 837–845, doi:10.1109/TSG.2012.2183902. [CrossRef]

18. Sajid, A.; Abbas, H.; Saleem, K. Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access* **2016**, *4*, 1375–1384, doi:10.1109/ACCESS.2016.2549047. [CrossRef]
19. Samuel, S.S.I. A review of connectivity challenges in IoT-smart home. In Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC 2016), Muscat, Oman, 15–16 March 2016; pp. 364–367, doi:10.1109/ICBDSC.2016.7460395. [CrossRef]
20. Georgiou, K.; de Souza, S.X.; Eder, K. The IoT energy challenge: A software perspective. *IEEE Embed. Syst. Lett.* **2017**, *1*, doi:10.1109/LES.2017.2741419. [CrossRef]
21. Bedi, G.; Venayagamoorthy, G.K.; Singh, R.; Brooks, R.R.; Wang, K.C. Review of Internet of Things (IoT) in Electric Power and Energy Systems. *IEEE Internet Things J.* **2018**, *5*, 847–870, doi:10.1109/JIOT.2018.2802704. [CrossRef]
22. Bedi, G.; Venayagamoorthy, G.K.; Singh, R. Navigating the challenges of Internet of Things (IoT) for power and energy systems. In Proceedings of the 2016 Clemson University Power Systems Conference (PSC), Clemson, SC, USA, 8–11 March 2016; pp. 1–5, doi:10.1109/PSC.2016.7462853. [CrossRef]
23. Zhou, K.; Yang, S.; Shao, Z. Energy Internet: The business perspective. *Appl. Energy* **2016**, *178*, 212–222, doi:10.1016/j.apenergy.2016.06.052. [CrossRef]
24. Shahnia, F.; Ghosh, A.; Rajakaruna, S.; Chandrasena, R.P. Primary control level of parallel distributed energy resources converters in system of multiple interconnected autonomous microgrids within self-healing networks. *IET Gener. Transm. Distrib.* **2014**, *8*, 203–222, doi:10.1049/iet-gtd.2013.0126. [CrossRef]
25. Mohan, V.; Suresh, R.; Singh, J.G.; Ongsakul, W.; Madhu, N. Microgrid Energy Management Combining Sensitivities, Interval and Probabilistic Uncertainties of Renewable Generation and Loads. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2017**, *7*, 262–270, doi:10.1109/JETCAS.2017.2679030. [CrossRef]
26. Tahanan, M.; van Ackooij, W.; Frangioni, A.; Lacalandra, F. Large-scale Unit Commitment under uncertainty. *4OR* **2015**, *13*, 115–171, doi:10.1007/s10288-014-0279-y. [CrossRef]
27. Arefifar, S.A.; Ordonez, M.; Mohamed, Y.A.R.I.; Member, S. V–I Controllability-Based Optimal Allocation of Resources in Smart Distribution Systems. *IEEE Trans. Smart Grid* **2016**, *7*, 1378–1388. [CrossRef]
28. Karimi-Davijani, H.; Ojo, O. Controllability Analysis of Renewable Energy Systems. In *Power Electronics for Renewable Energy Systems, Transportation and Industrial Applications*; John Wiley & Sons, Ltd.: Chichester, UK, 2014; pp. 199–230, doi:10.1002/9781118755525.ch8. [CrossRef]
29. Pankaj, A. *Short-Term Energy Outlook (STEO) Forecast Highlights*; Technical Report; U.S. Energy Information Administration: Washington, DC, USA, 2017.
30. Louw, A.; Boyle, R.; Strahan, D.; Collins, B.; Stopforth, K.; Becker, L. *Global Trends in Renewable Energy Investment 2017*; Technical Report; Frankfurt School-UNEP Centre/BNEF: Frankfurt, Germany, 2017.
31. Gupta, S.K.; Mukherjee, T.; Varsamopoulos, G.; Banerjee, A. Research directions in energy-sustainable cyber–physical systems. *Sustain. Comput. Inform. Syst.* **2011**, *1*, 57–74. [CrossRef]
32. Shi, W.; Li, N.; Chu, C.C.; Gadh, R. Real-Time Energy Management in Microgrids. *IEEE Trans. Smart Grid* **2017**, *8*, 228–238, doi:10.1109/TSG.2015.2462294. [CrossRef]
33. Luna, A.C.; Diaz, N.L.; Graells, M.; Vasquez, J.C.; Guerrero, J.M. Mixed-integer-linear-programming-based energy management system for hybrid PV-wind-battery microgrids: Modeling, design, and experimental verification. *IEEE Trans. Power Electron.* **2017**, *32*, 2769–2783, doi:10.1109/TPEL.2016.2581021. [CrossRef]
34. Good, N.; Ellis, K.A.; Mancarella, P. Review and classification of barriers and enablers of demand response in the smart grid. *Renew. Sustain. Energy Rev.* **2017**, *72*, 57–72, doi:10.1016/j.rser.2017.01.043. [CrossRef]
35. Anvari-Moghaddam, A.; Monsef, H.; Rahimi-Kian, A. Cost-effective and comfort-aware residential energy management under different pricing schemes and weather conditions. *Energy Build.* **2015**, *86*, 782–793, doi:10.1016/j.enbuild.2014.10.017. [CrossRef]
36. Antunes, C.H.; Soares, A.; Gomes, A. An energy management system for residential demand response based on multiobjective optimization. In Proceedings of the 2016 IEEE Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 21–24 August 2016; pp. 90–94, doi:10.1109/SEGE.2016.7589506. [CrossRef]
37. Soares, A.; Gomes, A.; Antunes, C.H.; Oliveira, C. A Customized Evolutionary Algorithm for Multiobjective Management of Residential Energy Resources. *IEEE Trans. Ind. Inform.* **2017**, *13*, 492–501, doi:10.1109/TII.2016.2628961. [CrossRef]
38. Mohsenian-Rad, H. Optimal demand bidding for time-shiftable loads. *IEEE Trans. Power Syst.* **2015**, *30*, 939–951, doi:10.1109/TPWRS.2014.2338735. [CrossRef]

39. Van der Meer, D.; Chandra Mouli, G.R.; Morales-Espana, G.; Ramirez Elizondo, L.; Bauer, P. Energy Management System with PV Power Forecast to Optimally Charge EVs at the Workplace. *IEEE Trans. Ind. Inform.* **2016**, *14*, 311–320, doi:10.1109/TII.2016.2634624. [CrossRef]
40. Mahmud, K.; Town, G.E.; Morsalin, S.; Hossain, M. Integration of electric vehicles and management in the internet of energy. *Renew. Sustain. Energy Rev.* **2017**, *82*, 4179–4203, doi:10.1016/j.rser.2017.11.004. [CrossRef]
41. McKenna, K.; Keane, A. Residential Load Modeling of Price-Based Demand Response for Network Impact Studies. *IEEE Trans. Smart Grid* **2016**, *7*, 2285–2294, doi:10.1109/TSG.2015.2437451. [CrossRef]
42. Chuan, L.; Ukil, A. Modeling and Validation of Electrical Load Profiling in Residential Buildings in Singapore. *IEEE Trans. Power Syst.* **2015**, *30*, 2800–2809, doi:10.1109/TPWRS.2014.2367509. [CrossRef]
43. Youssef, K.H. Power Quality Constrained Optimal Management of Unbalanced Smart Microgrids during Scheduled Multiple Transitions between Grid-Connected and Islanded Modes. *IEEE Trans. Smart Grid* **2017**, *8*, 457–464, doi:10.1109/TSG.2016.2577643. [CrossRef]
44. Frankfurt School-UNEP Centre/BNEF. *Global Trends in Renewable Energy Investment*; Technical Report; Frankfurt School-UNEP Centre/BNEF: Frankfurt, Germany, 2016.
45. Wang, K.; Hu, X.; Li, H.; Li, P.; Zeng, D.; Guo, S. A Survey on Energy Internet Communications for Sustainability. *IEEE Trans. Sustain. Comput.* **2017**, *2*, 231–254, doi:10.1109/TSUSC.2017.2707122. [CrossRef]
46. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Comput. Netw.* **2014**, *67*, 74–88, doi:10.1016/j.comnet.2014.03.029. [CrossRef]
47. Bauschert, T.; Büsing, C.; D'Andreagiovanni, F.; Koster, A.M.C.A.; Kutschka, M.; Steglich, U. Network planning under demand uncertainty with robust optimization. *IEEE Commun. Mag.* **2014**, *52*, 178–185, doi:10.1109/MCOM.2014.6736760. [CrossRef]
48. Fadlullah, Z.M.; Fouda, M.M.; Kato, N.; Takeuchi, A.; Iwasaki, N.; Nozaki, Y. Toward Intelligent Machine-to-Machine Communications in Smart Grid Towards Intelligent Machine-to Machine Communications in Smart Grid. *IEEE Commun. Mag.* **2011**, *49*, 60–65. [CrossRef]
49. Jiang, J.; Qian, Y. Distributed Communication Architecture for Smart Grid Applications. *IEEE Commun. Mag.* **2016**, *54*, 60–67, doi:10.1109/MCOM.2016.1600321CM. [CrossRef]
50. Xu, L.D.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243, doi:10.1109/TII.2014.2300753. [CrossRef]
51. Patil, K.; Lahudkar, P.S.L. A Survey of MAC Layer Issues and Application layer Protocols for Machine-to-Machine Communications. *IEEE Internet Things J.* **2015**, *2*, 175–186.
52. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 5–20, doi:10.1109/SURV.2012.021312.00034. [CrossRef]
53. Draft International Standard ISO/IEC DIS 17821. *Information Technology—Specification of Low Power Wireless Mesh Network over Channel-Hopped TDMA Links*; International Organization for Standardization: Geneva, Switzerland, 2014.
54. Lin, G.Y.; Chang, S.R.; Wei, H.Y. Estimation and adaptation for bursty LTE random access. *IEEE Trans. Veh. Technol.* **2016**, *65*, 2560–2577, doi:10.1109/TVT.2015.2418811. [CrossRef]
55. Nielsen, J.J.; Kim, D.M.; Madueno, G.C.; Pratas, N.K.; Popovski, P. A tractable model of the LTE access reservation procedure for machine-type communications. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM 2015), San Diego, CA, USA, 6–10 December 2015; pp. 1–6, doi:10.1109/GLOCOM.2014.7417529. [CrossRef]
56. Lin, X.; Bergman, J.; Gunnarsson, F.; Liberg, O.; Razavi, S.M.; Razaghi, H.S.; Rydn, H.; Sui, Y. Positioning for the Internet of Things: A 3GPP Perspective. *IEEE Commun. Mag.* **2017**, *55*, 179–185, doi:10.1109/MCOM.2017.1700269. [CrossRef]
57. Zayas, A.D.; Merino, P. The 3GPP NB-IoT system architecture for the Internet of Things. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops 2017), Paris, France, 21–25 May 2017; pp. 277–282, doi:10.1109/ICCW.2017.7962670. [CrossRef]
58. Liberg, O.; Sundberg, M.; Wang, Y.P.E.; Bergman, J.; Sachs, J. The Cellular Internet of Things. In *Cellular Internet of Things*; Academic Press: London, UK, 2018; pp. 1–13, doi:10.1016/B978-0-12-812458-1.00001-0. [CrossRef]

59. Zdraveski, V.; Mishev, K.; Trajanov, D.; Kocarev, L. ISO-Standardized Smart City Platform Architecture and Dashboard. *IEEE Pervasive Comput.* **2017**, *16*, 35–43, doi:10.1109/MPRV.2017.31. [CrossRef]
60. Nielsen, J.J.; Ganem, H.; Jorguseski, L.; Alic, K.; Smolnikar, M.; Zhu, Z.; Pratas, N.K.; Golinski, M.; Zhang, H.; Kuhar, U.; et al. Secure Real-Time Monitoring and Management of Smart Distribution Grid using Shared Cellular Networks. *IEEE Wirel. Commun.* **2017**, *24*, 10–17, doi:10.1109/MWC.2017.1600252. [CrossRef]
61. Li, Z.; Shahidehpour, M.; Aminifar, F. Cybersecurity in Distributed Power Systems. *Proc. IEEE* **2017**, *105*, 1367–1388, doi:10.1109/JPROC.2017.2687865. [CrossRef]
62. Roman, R.; Najera, P.; Lopez, J. Securing the Internet of Things. *Computer* **2011**, *44*, 51–58, doi:10.5480/1536-5026-34.1.63. [CrossRef]
63. Phom, H.S.; Kuntze, N.; Rudolph, C.; Cupelli, M.; Liu, J.; Monti, A. A user-centric privacy manager for future energy systems. In Proceedings of the 2010 International Conference on Power System Technology: Technological Innovations Making Power Grid Smarter (POWERCON2010), Hangzhou, China, 24–28 October 2010; pp. 1–7, doi:10.1109/POWERCON.2010.5666447. [CrossRef]
64. Henze, M.; Hermerschmidt, L.; Kerpen, D.; Häußling, R.; Rumpe, B.; Wehrle, K. A comprehensive approach to privacy in the cloud-based Internet of Things. *Future Gener. Comput. Syst.* **2016**, *56*, 701–718, doi:10.1016/j.future.2015.09.016. [CrossRef]
65. Groopman, J.; Etlinger, S. *Consumer Perceptions of Privacy in the Internet of Things: What Brands Can Learn from a Concerned Citizenry*; Altimeter Group: San Francisco, CA, USA, 2015; pp. 1–25.
66. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-Physical Systems Security—A Survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831, doi:10.1109/JIOT.2017.2703172. [CrossRef]
67. Song, T.; Li, R.; Mei, B.; Yu, J.; Xing, X.; Cheng, X. A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. *IEEE Internet Things J.* **2017**, *4*, 1844–1852, doi:10.1109/JIOT.2017.2707489. [CrossRef]
68. Jayaraman, P.P.; Yang, X.; Yavari, A.; Georgakopoulos, D.; Yi, X. Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation. *Future Gener. Comput. Syst.* **2017**, *76*, 540–549, doi:10.1016/j.future.2017.03.001. [CrossRef]
69. Roman, R.; Lopez, J. Security in the distributed internet of things. In *International Conference on Trusted Systems*; Lecture Notes in Computer Science (LNCS); Springer: Berlin/Heidelberg, Germany, 2012; Volume 7711, pp. 65–66, doi:10.1007/978-3-642-35371-0_6. [CrossRef]
70. Buczak, A.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 1153–1176, doi:10.1109/COMST.2015.2494502. [CrossRef]
71. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Netw.* **2012**, *10*, 1497–1516, doi:10.1016/j.adhoc.2012.02.016. [CrossRef]
72. Roman, R.; Alcaraz, C.; Lopez, J.; Sklavos, N. Key management systems for sensor networks in the context of the Internet of Things. *Comput. Electr. Eng.* **2011**, *37*, 147–159, doi:10.1016/j.compeleceng.2011.01.009. [CrossRef]
73. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164, doi:10.1016/j.comnet.2014.11.008. [CrossRef]
74. Hu, C.; Zhang, J.; Wen, Q. An identity-based personal location system with protected privacy in IOT. In Proceedings of the 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT 2011), Shenzhen, China, 28–30 October 2011; pp. 192–195, doi:10.1109/ICBNMT.2011.6155923. [CrossRef]
75. Yoon, S.G.; Choi, Y.J.; Park, J.K.; Bahk, S. Stackelberg-Game-Based Demand Response for At-Home Electric Vehicle Charging. *IEEE Trans. Veh. Technol.* **2016**, *65*, 4172–4184, doi:10.1109/TVT.2015.2440471. [CrossRef]
76. Luna, A.C.; Diaz, N.L.; Graells, M.; Vasquez, J.C.; Guerrero, J.M. Cooperative energy management for a cluster of households prosumers. *IEEE Trans. Consum. Electron.* **2016**, *62*, 235–242, doi:10.1109/TCE.2016.7613189. [CrossRef]
77. Falahi, M.; Lotfifard, S.; Ehsani, M.; Butler-Purry, K. Dynamic model predictive-based energy management of dg integrated distribution systems. *IEEE Trans. Power Deliv.* **2013**, *28*, 2217–2227, doi:10.1109/TPWRD.2013.2274664. [CrossRef]
78. Zafar, R.; Mahmood, A.; Razzaq, S.; Ali, W.; Naeem, U.; Shehzad, K. Prosumer based energy management and sharing in smart grid. *Renew. Sustain. Energy Rev.* **2018**, *82*, 1675–1684, doi:10.1016/j.rser.2017.07.018. [CrossRef]

79. Ejaz, W.; Naeem, M.; Shahid, A.; Anpalagan, A.; Jo, M. Efficient Energy Management for Internet of Things in Smart Cities. *IEEE Commun. Mag.* **2017**, *55*, 84–91, doi:10.1109/MCOM.2017.1600218CM. [CrossRef]
80. Olivares, D.E.; Canizares, C.A.; Kazerani, M. A centralized energy management system for isolated microgrids. *IEEE Trans. Smart Grid* **2014**, *5*, 1864–1875, doi:10.1109/TSG.2013.2294187. [CrossRef]
81. Vandoorn, T.L.; Vasquez, J.C.; De Kooning, J.; Guerrero, J.M.; Vandevelde, L. Microgrids: Hierarchical control and an overview of the control and reserve management strategies. *IEEE Ind. Electron. Mag.* **2013**, *7*, 42–55, doi:10.1109/MIE.2013.2279306. [CrossRef]
82. Li, Q.; Chen, F.; Chen, M.; Guerrero, J.M.; Abbott, D. Agent-Based Decentralized Control Method for Islanded Microgrids. *IEEE Trans. Smart Grid* **2016**, *7*, 637–649, doi:10.1109/TSG.2015.2422732. [CrossRef]
83. Wang, Z.; Chen, B.; Wang, J.; Kim, J. Decentralized Energy Management System for Networked Microgrids in Grid-Connected and Islanded Modes. *IEEE Trans. Smart Grid* **2016**, *7*, 1097–1105, doi:10.1109/TSG.2015.2427371. [CrossRef]
84. Shi, W.; Xie, X.; Chu, C.C.; Gadh, R. Distributed Optimal Energy Management in Microgrids. *IEEE Trans. Smart Grid* **2015**, *6*, 1137–1146, doi:10.1109/TSG.2014.2373150. [CrossRef]
85. Iannello, F.; Simeone, O.; Spagnolini, U. Energy Management Policies for Passive RFID Sensors with RF-Energy Harvesting. In Proceedings of the 2010 IEEE International Conference on Communications, Cape Town, South Africa, 23–27 May 2010; pp. 1–6, doi:10.1109/ICC.2010.5502035. [CrossRef]
86. Zhao, W.; Homma, H.; Toshiyoshi, H. Power management system of a MEMS vibrational energy harvesting sensor node under low vibration conditions. In Proceedings of the 2017 Symposium on Design, Test, Integration and Packaging of MEMS/MOEMS (DTIP), Bordeaux, France, 29 May–1 June 2017; pp. 1–4, doi:10.1109/DTIP.2017.7984499. [CrossRef]
87. Nitti, M.; Pilloni, V.; Colistra, G.; Atzori, L. The Virtual Object as a Major Element of the Internet of Things: A Survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1228–1240, doi:10.1109/COMST.2015.2498304. [CrossRef]
88. Reynolds, J.; Braden, R.; Ginoza, S.; De, A. *Internet Official Protocol Standards*; Technical Report; The Internet Society: Reston, VA, USA, 2002; doi:10.17487/rfc3300. [CrossRef]
89. Savolainen, T.; Soininen, J.; Silverajan, B. IPv6 addressing strategies for IoT. *IEEE Sens. J.* **2013**, *13*, 3511–3519, doi:10.1109/JSEN.2013.2259691. [CrossRef]
90. Rose, K.; Eldridge, S.; Lyman, C. The internet of things: An overview. *Internet Soc.* **2015**, 1–50, doi:10.1017/CBO9781107415324.004. [CrossRef]
91. Kaur, N.; Sood, S.K. An Energy-Efficient Architecture for the Internet of Things (IoT). *IEEE Syst. J.* **2017**, *11*, 796–805, doi:10.1109/JSYST.2015.2469676. [CrossRef]
92. Umut Akgül, Ö.; Canberk, B. Self-Organized Things (SoT): An energy efficient next generation network management. *Comput. Commun.* **2016**, *74*, 52–62, doi:10.1016/j.comcom.2014.07.004. [CrossRef]
93. Kamalinejad, P.; Mahapatra, C.; Sheng, Z.; Mirabbasi, S.; Leung, V.C.M.; Guan, Y.L. Wireless energy harvesting for the Internet of Things. *IEEE Commun. Mag.* **2015**, *53*, 102–108. [CrossRef]
94. Stojmenovic, I. Machine-to-Machine Communications With In-Network Data Aggregation, Processing, and Actuation for Large-Scale Cyber-Physical Systems. *IEEE Internet Things J.* **2014**, *1*, 122–128, doi:10.1109/JIOT.2014.2311693. [CrossRef]
95. Akusok, A.; Bjork, K.M.; Miche, Y.; Lendasse, A. High-Performance Extreme Learning Machines: A Complete Toolbox for Big Data Applications. *IEEE Access* **2015**, *3*, 1011–1025, doi:10.1109/ACCESS.2015.2450498. [CrossRef]
96. Baccarelli, E.; Naranjo, P.G.; Scarpiniti, M.; Shojafar, M.; Abawajy, J.H. Fog of Everything: Energy-Efficient Networked Computing Architectures, Research Challenges, and a Case Study. *IEEE Access* **2017**, *5*, 9882–9910, doi:10.1109/ACCESS.2017.2702013. [CrossRef]
97. Ragothaman, B.; Prabha, S.; Jose, E.; Sarojini, B. A Survey on Big Data and Internet of Things. In Proceedings of the UGC Sponsored Two Day National Conference on Internet of Things, Tamilnadu, India, 18–19 February 2016; pp. 174–179, doi:10.1109/MASS.2016.38. [CrossRef]
98. Tang, B.; Chen, Z.; Hefferman, G.; Pei, S.; Wei, T.; He, H.; Yang, Q. Incorporating Intelligence in Fog Computing for Big Data Analysis in Smart Cities. *IEEE Trans. Ind. Inform.* **2017**, *13*, 2140–2150, doi:10.1109/TII.2017.2679740. [CrossRef]
99. Meng, X.; Bradley, J.; Yavuz, B.; Sparks, E.; Venkataraman, S.; Liu, D.; Freeman, J.; Tsai, D.; Amde, M.; Owen, S.; et al. MLlib: Machine Learning in Apache Spark. *CoRR* **2015**, *17*, 1–7, doi:10.1145/2882903.2912565. [CrossRef]

100. Lloret, J.; Tomas, J.; Canovas, A.; Parra, L. An Integrated IoT Architecture for Smart Metering. *IEEE Commun. Mag.* **2016**, *54*, 50–57, doi:10.1109/MCOM.2016.1600647CM. [CrossRef]
101. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623, doi:10.1109/PERCOMW.2017.7917634. [CrossRef]
102. Federal Trade Commission (FTC). *IoT Privacy & Security in a Connected World*; FTC Staff Report; Federal Trade Commission: Washington, DC, USA, 2015; p. 71.
103. Dong, R.; Ratliff, L.J. The quest for Privacy in the Internet of Things. *IEEE Cloud Comput.* **2016**, *3*, 36–45, doi:10.1109/MCC.2016.28. [CrossRef]
104. Premnath, S.N.; Haas, Z.J. Security and privacy in the internet-of-things under time-and-budget-limited adversary model. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 277–280, doi:10.1109/LWC.2015.2408609. [CrossRef]
105. Brooks, T.T. List of IEEE Internet of Things Standards. In *Cyber-Assurance for the Internet of Things*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2016; pp. 283–318, doi:10.1002/9781119193784.app1. [CrossRef]
106. Talari, S.; Shafie-khah, M.; Siano, P.; Loia, V.; Tommasetti, A.; Catalão, J. A Review of Smart Cities Based on the Internet of Things Concept. *Energies* **2017**, *10*, 421, doi:10.3390/en10040421. [CrossRef]
107. IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011). *IEEE Standard for Low-Rate Wireless Networks*; IEEE Standards Association: Piscataway, NJ, USA, 2016; pp. 1–709, doi:10.1109/IEEESTD.2016.7460875. [CrossRef]
108. IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012). *IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*; IEEE Standards Association: Piscataway, NJ, USA, 2016.
109. Reynders, B.; Meert, W.; Pollin, S. Range and coexistence analysis of long range unlicensed communication. In Proceedings of the 2016 23rd International Conference on Telecommunications (ICT), Thessaloniki, Greece, 16–18 May 2016; pp. 1–6, doi:10.1109/ICT.2016.7500415. [CrossRef]
110. Lauridsen, M.; Vejlgaard, B.; Kovacs, I.Z.; Nguyen, H.; Mogensen, P. Interference Measurements in the European 868 MHz ISM Band with Focus on LoRa and SigFox. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 19–22 March 2017; pp. 1–6, doi:10.1109/WCNC.2017.7925650. [CrossRef]
111. Ouya, A.; Aragon, B.M.D.; Bouette, C.; Habault, G.; Montavont, N.; Papadopoulos, G.Z. An efficient electric vehicle charging architecture based on LoRa communication. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 381–386, doi:10.1109/SmartGridComm.2017.8340723. [CrossRef]
112. Navarro-Ortiz, J.; Sendra, S.; Ameigeiras, P.; Lopez-Soler, J.M. Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things. *IEEE Commun. Mag.* **2018**, *56*, 60–67, doi:10.1109/MCOM.2018.1700625. [CrossRef]
113. Lauridsen, M.; Nguyen, H.; Vejlgaard, B.; Kovacs, I.Z.; Mogensen, P.; Sorensen, M. Coverage Comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km^2 Area. In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, Australia, 4–7 June 2017; pp. 1–5, doi:10.1109/VTCSpring.2017.8108182. [CrossRef]
114. IEEE P2413. *Standard for an Architectural Framework for the Internet of Things (IoT) IEEE P2413*; IEEE Standards Association: Piscataway, NJ, USA, 2016.
115. Gazis, V. A Survey of Standards for Machine-to-Machine and the Internet of Things. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 482–511, doi:10.1109/COMST.2016.2592948. [CrossRef]
116. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142, doi:10.1109/JIOT.2017.2683200. [CrossRef]
117. Lei-hong, L.; Yue-shan, H.; Xiao-ming, W. A Community Health Service Architecture Based on the Internet of Things on Health-Care. In Proceedings of the World Congress on Medical Physics and Biomedical Engineering, Beijing, China, 26–31 May 2012; Volume 39, pp. 1317–1320, doi:10.1007/978-3-642-29305-4_345. [CrossRef]

118. Zheng, L.; Chen, S.; Xiang, S.; Hu, Y. Research of architecture and application of internet of things for smart grid. In Proceedings of the 2012 International Conference on Computer Science and Service System (CSSS 2012), Nanjing, China, 11–13 August 2012; pp. 938–941, doi:10.1109/CSSS.2012.238. [CrossRef]
119. Taj Dini, M.; Yu Sokolov, V. Internet of Things Security Problems. *Mod. Inf. Secur.* **2017**, *1*, 120–127.
120. Sarkar, C.; Akshay, A.U.; Prasad, R.V.; Rahim, A.; Neisse, R.; Baldini, G. DIAT: A scalable distributed architecture for IoT. *IEEE Internet Things J.* **2015**, *2*, 230–239, doi:10.1109/JIOT.2014.2387155. [CrossRef]
121. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376, doi:10.1109/COMST.2015.2444095. [CrossRef]
122. Gracanin, D.; Matkovic, K.; Wheeler, J. An approach to modeling internet of things based smart built environments. In Proceedings of the 2015 Winter Simulation Conference, Huntington Beach, CA, USA, 6–9 December 2015; pp. 3208–3209.
123. Pan, J.; Jain, R.; Paul, S.; Vu, T.; Saifullah, A.; Sha, M. An Internet of Things Framework for Smart Energy in Buildings: Designs, Prototype, and Experiments. *IEEE Internet Things J.* **2015**, *2*, 527–537, doi:10.1109/JIOT.2015.2413397. [CrossRef]
124. Pappachan, P.; Degeling, M.; Yus, R.; Das, A.; Bhagavatula, S.; Melicher, W.; Naeini, P.E.; Zhang, S.; Bauer, L.; Kobsa, A.; et al. Towards Privacy-Aware Smart Buildings: Capturing, Communicating, and Enforcing Privacy Policies and Preferences. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), Atlanta, GA, USA, 5–8 June 2017; doi:10.1109/ICDCSW.2017.52. [CrossRef]
125. Mandula, K.; Parupalli, R.; Murty, C.; Magesh, E.; Lunagariya, R. Mobile based Horne Automation using Internet of Things (IoT). In Proceedings of the 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, India, 18–19 December 2015; doi:10.1109/ICCICCT.2015.7475301. [CrossRef]
126. Soliman, M.; Abiodun, T.; Hamouda, T.; Zhou, J.; Lung, C.H. Smart Home: Integrating Internet of Things with Web Services and Cloud Computing. In Proceedings of the 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), Bristol, UK, 2–5 December 2013; doi:10.1109/CloudCom.2013.155. [CrossRef]
127. Haider, H.T.; See, O.H.; Elmenreich, W. A review of residential demand response of smart grid. *Renew. Sustain. Energy Rev.* **2016**, *59*, 166–178, doi:10.1016/j.rser.2016.01.016. [CrossRef]
128. Jeschke, S.; Brecher, C.; Song, H.; Rawat, D.B. *Industrial Internet of Things*; Springer International Publishing: Basel, Switzerland, 2017; doi:10.1007/978-3-319-42559-7. [CrossRef]
129. Gamarra, C.; Guerrero, J.M.; Montero, E. A knowledge discovery in databases approach for industrial microgrid planning. *Renew. Sustain. Energy Rev.* **2016**, *60*, 615–630, doi:10.1016/j.rser.2016.01.091. [CrossRef]
130. Al-Rubaye, S.; Kadhum, E.; Ni, Q.; Anpalagan, A. Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency. *IEEE Internet Things J.* **2017**, *99*, 1–11, doi:10.1109/JIOT.2017.2734903. [CrossRef]
131. Viswanath, S.K.; Yuen, C.; Tushar, W.; Li, W.T.; Wen, C.K.; Hu, K.; Chen, C.; Liu, X. System design of the internet of things for residential smart grid. *IEEE Wirel. Commun.* **2016**, *23*, 90–98, doi:10.1109/MWC.2016.7721747. [CrossRef]
132. Qu, Q.; Zhen, Y.; Li, X.; Zhang, Y.; Zeng, L. Application of Internet of Things in Smart Grid Power Transmission. In Proceedings of the 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC), Vancouver, BC, Canada, 26–28 June 2012.
133. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. *IEEE Internet Things J.* **2014**, *1*, 22–32, doi:10.1109/JIOT.2014.2306328. [CrossRef]
134. Hancke, G.P.; de Carvalho e Silva, B.; Hancke, G.P. The role of advanced sensing in smart cities. *Sensors* **2013**, *13*, 393–425, doi:10.3390/s130100393. [CrossRef] [PubMed]