inventions

MDPI

Review

Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges

Alireza Ghasempour

Department of Information and Communication Technology, University of Applied Science and Technology, Tehran 1391637111, Iran; alireza_ghasempour@yahoo.com

Received: 12 February 2019; Accepted: 21 March 2019; Published: 26 March 2019

Abstract: Internet of Things (IoT) is a connection of people and things at any time, in any place, with anyone and anything, using any network and any service. Thus, IoT is a huge dynamic global network infrastructure of Internet-enabled entities with web services. One of the most important applications of IoT is the Smart Grid (SG). SG is a data communications network which is integrated with the power grid to collect and analyze data that are acquired from transmission lines, distribution substations, and consumers. In this paper, we talk about IoT and SG and their relationship. Some IoT architectures in SG, requirements for using IoT in SG, IoT applications and services in SG, and challenges and future work are discussed.

Keywords: Internet of Things; smart grid; advanced metering infrastructure; distributed energy resources; smart meters; meter data management system; demand response; cybersecurity

1. Introduction

Before talking about the Internet of Things (IoT), it is worthy to explore the evolution of the Internet. The first experimental network of two computers was created between the TX-2 computer by Lincoln Labs of Massachusetts Institute of Technology (MIT) and the Q-32 mainframe operated by the RAND corporations via a dedicated telephone line in 1965 [1]. The Internet was invented by Vinton Cerf in 1973 [2]. Commercial use of the Internet started in the late 1980s [1]. The World Wide Web (WWW) was invented by Tim Berners-Lee in 1989 [2] and became available in 1991 [3]. The first mobile phone with Internet connectivity was the Nokia 9000 Communicator, launched in Finland in 1996 [4]. Thus, the mobile-Internet was formed. In June 2000, Friends Reunited as the first online social network to achieve prominence in Britain was launched [5]. By emerging social networks, peoples' identities are added to the Internet. In the next step in the IoT, objects can connect and communicate with each other via the Internet.

The research in the IoT is in the beginning stages, and researchers provided different definitions for it. Thus, there isn't only one definition for IoT. The IoT is composed of two words: "Internet" and "Thing." The "Internet" can be defined as "The interconnection of computers in the world based on TCP/IP protocols" and the "Thing" is "an object that is not precisely identifiable" Thus, "Internet of Things" semantically means a worldwide network of interconnected objects uniquely addressable, based on Transmission Control Protocol (TCP) and Internet Protocol (IP). Thus, it is reasonable to define the IoT as "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts" [6].

Also, IoT can be defined as a connection of people and things at any time, in any place, with anything and anyone, using any path and any service [7,8]. This implies addressing elements such as convergence, content, collections (repositories), computing, communication, and connectivity in the context where there is a seamless interconnection between people/humans and things and/or between things (see Figure 1) [9]. Thus, IoT is a huge dynamic global network infrastructure of Internet-enabled physical and virtual objects/entities with web services which contains embedded technologies and all types of information devices such as global positioning system (GPS), infrared devices, scanners, radio frequency identification (RFID) tags/devices, sensors, actuators, smartphones, and the Internet to sense, identify, locate, track, connect, monitor, manage, communicate/interact, cooperate, and control of objects/things in physical, digital, and virtual world. It uses computing and self-configuring capabilities (based on interoperable communication protocols) and software tools to process information, achieve data mining, and extract knowledge.

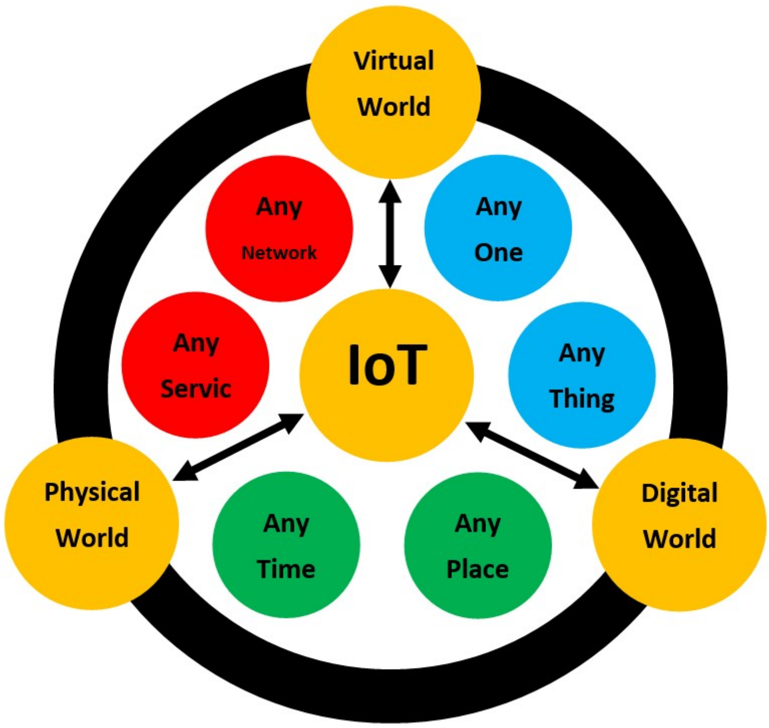

Figure 1. Internet of Things (IoT) with its connections and related entities.

One of the most important applications of IoT is the Smart Grid (SG). SG is a data communications network which is integrated with the power grid to collect and analyze data that are acquired from transmission lines, distribution substations, and consumers. Based on these data, SG can provide predictive information to its suppliers and customers on how to best manage power [10]. In this paper, different layers of IoT architecture will be discussed. We will investigate technologies which are essential to apply IoT to SG. Several IoT applications and services in SG will be introduced. Finally, challenges that must be addressed and future work are discussed.

The rest of the paper is organized as follows. In Section 2, IoT, its history and development are reviewed. Smart grid and its components are discussed in Section 3. Section 4 presents how IoT can be used in SG to accomplish reliable data transmission. The architecture of IoT is discussed in Section 5. In Section 6, several key technologies to enable applying IoT to SG are introduced. The challenges which must be addressed in future research directions are presented in Section 7. The conclusion is given in Section 8.

2. Internet of Things

IoT is a multidisciplinary field that covers many subjects from technical issues (such as routing protocols) to a combination of social and technical problems (e.g., security). IoT represents a vision in which the Internet extends into the real world encompassing every uniquely identifiable object.

This vision is ubiquitous computing. Initially, Mark Weiser [11] in 1991 coined the term "Ubiquitous Computing" that can be truly realized by IoT. Kevin Ashton [12] proposed the term "IoT" in his presentation at Procter & Gamble (P&G) in 1999. Also, Neil Gershenfeld [13] used the same notion in his book in 1999. The IoT first became popular through Sarma et al. [14] (from MIT Auto-ID center) in 2000. LG announced its first Internet refrigerator plans in 2000. During 2002–2004, IoT was mentioned in mainstream publications such as Forbes [15], the Guardian [16], Scientific American [17] and the Boston Globe [18]. International Telecom Union (ITU) published an annual report of the IoT [19], which extended the concept of the IoT in 2005. In that report, there are four key enablers to the IoT:

1. Feeling Things (such as sensors and wireless sensor networks)
2. Tagging Things (using Radio Frequency Identification (RFID))
3. Thinking Things (such as smart materials, smart clothing and wearable computing, smart homes and vehicles, and robotics)
4. Shrinking Things (using nanotechnology to make products smaller and smaller)

In 2005, Fleisch and Mattern [20] published their book in IoT topic. European politicians initially used IoT in the context of RFID technology, e.g., in the titles of some RFID conferences such as "From RFID to the IoT, Pervasive networked systems" (2006) and "RFID: Towards the IoT" (2007). In March 2008, the first scientific conference [21] was held in IoT. In 2008, a group of high-tech companies launched the Internet Protocol for Smart Objects (IPSO) Alliance for the following goals [22]:

1. Interoperability: Organize interoperability tests that will allow members and interested parties to show that products and services using IP for Smart Objects can work together and meet industry standards for communication.
2. Invest in Innovation: Help innovators in small companies who are making IP devices and web objects to gain visibility in the industry.
3. Promote IP: Promote the use of IP as the premier solution for access and communication for Smart Objects - in print, in public, and in the media.
4. Uphold Standards: Support Internet Engineering Task Force (IETF) and other standards development organizations in the development of standards for Smart Objects.

In April 2008, U.S. National Intelligence Council listed the Internet of Things as one of the 6 "Disruptive Civil Technologies" (Biogeotechnology, Energy Storage Materials, Biofuels and Bio-Based Chemicals, Clean Coal Technologies, Service Robotics, and The Internet of Things) with potential impacts on US interests out to 2025 [23].

In Jan 2009, President Obama promoted the idea of a smarter planet as a developing national strategy and consequently gave worldwide concern. A dedicated European Union committee published an action plan for Europe which sought to create a new and broad paradigm: the transition from a network of interconnected computers and people, to a network of interconnected people with things or things with each other (IoT) in 2009 [24]. Andrew Milroy at Frost and Sullivan [25] anticipated that year 2014 would be the year of the Internet of things and the focus of both IT buyers and sellers shifts to IoT. Also, more data would be generated by machines ('things') than by human beings in 2014.

Today, the IoT is used to denote advanced connectivity of devices and services that go beyond the traditional machine to machine and covers a variety of protocols and applications. Connectivity will take on an entirely new dimension, and future global networks will consist of not only humans and devices, but also all sorts of things. Physical items can connect to the virtual world, be controlled remotely and act as physical access points to Internet services. Currently, IoT can be viewed as a network of networks.

There are three visions for IoT [26]:

- Internet-oriented: In the internet-oriented vision, it is needed to make smart objects. The objects must use the specification of IP protocols.
- Semantic-oriented: In Semantic-oriented vision, the number of available sensors will be vast, and their collected data will be huge. Thus, the raw data needs to be managed and processed for better representations and understanding.

- Things-oriented: In the things-oriented vision, we can track any object using sensors and pervasive technologies. Any object can be identified uniquely using an electronic product code (EPC). EPC is extended using sensors.

IoT has three important characteristics [27]:

1. Comprehensive sense: Using sensors to collect information from any objects anytime and anywhere.
2. Intelligent processing: Using techniques such as cloud computing to analyze huge amounts of data to control objects.
3. Reliable transmission: Accurate and real-time data transmission via communications networks and the Internet.

Cisco has created a dynamic connections counter to track the estimated number of connected things from December 2012 until July 2020 [28]. In Dec. 2012, there were 8.7 billion connected objects globally while in May 2014, the number is exceeding 12.3 billion. Cisco has conducted analysis on the potential economic impact of the Internet of Everything, and their analysis indicates that there is as much as $14.4 trillion of potential economic "value at stake" for global private-sector businesses over the next decade, as a result of the emergence of the Internet of Everything [29]. Looking to the future, Cisco Internet Business Solutions Group (IBSG) predicts there will be 25 billion devices connected to the Internet by 2015 and 50 billion by 2020 [30]. A separate analysis from Morgan Stanley predicts that number can be as high as 75 billion and claims that there are 200 unique consumer devices or equipment that could be connected to the Internet that have not yet done so [31]. Michael Mandel [32] in his report in Progressive Policy Institute describes how technological innovation, particularly as it relates to the Internet of Everything (IoE), could lead America's economy out of a "slow-growth rut." The European Commission (Information Society and Media DG) predicted 50 to 100 billion devices to be connected by 2020 [33]. Future technological developments in IoT and its research needs that have been foreseen for the next 20 years are outlined in Tables 1 and 2 [33]. Since there is a growing interest in using IoT technologies, the number of industrial IoT projects and the number of IoT publications is quickly growing.

3. Smart Grid

The smart grid is proposed to solve the issues of electricity grid (e.g., low reliability, high outages, high greenhouse gas and carbon emission, economics, safety, and energy security) [34]. One of the definitions for the smart grid is that the smart grid is a communication network on top of the electricity grid to gather and analyze data from different components of a power grid to predict power supply and demand which can be used for power management [8]. For comprehensive details and information about characteristics and benefits of the SG, comparison between a power grid and SG, and general requirements of a communication network in a SG, the readers can see chapter 3 of [35].

In a proposed model for the smart grid by the national institute of standards and technology, the smart grid has 7 domains and roles of these domains are defined so that required information can be exchanged and necessary decisions can be made [7]. Some of the required functionalities to deploy the smart grid are as follows [10]:

1. Communication networks: Public, private, wired, and wireless communication networks that can be used as the communication infrastructure for smart grid [36].
2. Cybersecurity: Determining measures to guarantee availability, integrity, and confidentiality of the communication and control systems which are required to manage, operate, and protect smart grid infrastructures [37].
3. Distributed energy resources: Using different kinds of generation (e.g., renewable energies) and/or storage systems (batteries, plug-in electric cars with bi-directional chargers) that are connected to distributed systems [38].
4. Distribution grid management: Trying to maximize the performance of components in distribution systems such as feeders and transformers and integrate them with transmission systems,

increase reliability, increase the distribution system efficiency, and improve management of distributed renewable energy sources [39].

5. Electric transportation: Integrating plug-in electric vehicles in a large-scale [40].

6. Energy efficiency: Providing mechanisms for different kinds of customers to modify their energy usage during peak hours and optimizing the balance between power supply and demand [41].

7. Energy storage: Using direct or indirect energy storage technologies such as pumped hydroelectric storage technology [42].

8. Wide-area monitoring: Monitoring of power system components over a large geographic area to optimize their performance and preventing problems before they happen [43].

9. Advanced metering infrastructure (AMI): AMI as one of the key components of SG creates a bidirectional communication network between smart meters (SMs) and utility system to collect, send, and analyze consumer energy consumption data [44–46].

AMI is an improved and modified version of automatic meter reading. In an automatic meter reading, data from different types of meters were collected automatically and were sent to a central system through a one-way communication network for future analysis and billing purpose. Since the automatic meter reading couldn't provide bidirectional communications, AMI was introduced.

AMI has many tasks such as the ability to self-heal, adaptive power pricing, demand-side management, energy efficiency enhancement, improving the reliability of SG, interoperability with other systems, monitoring and control of power quality, outage management, providing communications between central system and SMs, saving energy, and updating the software of SMs [44].

AMI components are a central system, two-way communication networks, data concentrators, and smart meters. SMs are installed at customers' locations or other positions in smart grid to measure consumption data and send them to the central system via communication networks for billing, informing consumers for their consumptions, etc. In direct load control, SMs can give power consumption overviews and schedule times for turning on and off devices to shift the load in SG. Also, direct load control can add distributed energy resources to SG to supply higher load when the power grid produces extra power [7].

Distributed energy resources, electric vehicles, gateways, home energy display, smart devices, SMs, and tools for power consumption control can connect to each other via a home area network. Bluetooth, IEEE 802.11b, IEEE 802.11s, IEEE 802.3az-2010, power line communication, and ZigBee technologies can be used for home area network [45].

Several SMs send their data to the corresponding data concentrator through a neighborhood area network (NAN) [34]. For example, several homes that are supplied by one transformer create a NAN. Thus, NAN should carry a large volume of data and satisfy their quality of service requirements. The following technologies and networks are some candidates for NAN: family standards of IEEE 802.11, the third and the fourth generations of wireless cellular networks (e.g., long-term evolution (LTE), worldwide interoperability for microwave access (WiMAX), wideband code-division multiple access), and optical networks (e.g., passive optical networks or Ethernet passive optical networks). Also, equipment in the field should be managed by a field area network (FAN). The geographical coverage of a FAN is like NAN. Therefore, similar communication networks and technologies can be used for FAN too.

Data concentrator aggregates and compresses data from SMs in uplink connection and relays data to SMs in downlink connection. Data concentrator enhances scalability and reliability of SG, reduces power consumption of SMs, and decreases data collision between SMs' transmitted data. But it increases the delay in transmitting SMs' data somewhat. Some data concentrators are connected to the central system via a wide area network (WAN). Long-range and high-bandwidth communication technologies such as fiber optic and wireless cellular networks (e.g., WiMAX, LTE, and LTE advanced can be used in WAN [46].

The central system collects and analyzes SMs' data. It can have several components (connected via a local area network) such as a meter data management system [47], geographic information system, outage management system, consumer information system, power quality management, and load forecasting systems. As an example, a meter data management system gets SMs' data, stores them in databases, and processes them [45].

4. IoT Applications and Services in SG

IoT can support technologies in SG. Comprehensive sensing and processing abilities of IoT can improve SG abilities such as processing, warning, self-healing, disaster recovery, and reliability. Combining IoT and SG can greatly promote the development of smart terminals, meters and sensors, information equipment, and communication devices. IoT can be used to accomplish reliable data transmission in wire and wireless communication infrastructures in different parts of SG (electricity generation, transmission lines, distribution, and consumption/utilization) as follows:

1. In electricity generation, IoT can be used to monitor electricity generation of different kinds of power plants (such as coal, wind, solar, biomass), gas emissions, energy storage, energy consumption, and predict necessary power to supply consumers.
2. IoT can be used to acquire electricity consumption, dispatch, monitor and protect transmission lines, substations, and towers, manage and control equipment.
3. IoT can be used in customer side in smart meters to measure different types of parameters, intelligent power consumption, interoperability between different networks, charging and discharging of electric vehicles, manage energy efficiency and power demand.

The main IoT application scenarios are as follows:

1. AMI with high reliability: AMI is a key component in SG. IoT can be used in AMI to collect data, measure abnormality in SG, exchange information between smart meters, monitor electricity quality and distributed energy, analyze user consumption pattern.
2. Smart home: A smart home can be used to interact with users and SG, enhance SG services, meet marketing demand, improve QoS, control smart appliances, read power consumption information which is gathered by smart meters, and monitor renewable energy.
3. Transmission line monitoring: By using wireless broadband communication technologies, the transmission lines can be monitored to discover fault issues and eliminate them.
4. Electric Vehicle (EV) assistant management system: EV assistant management systems comprise of charging station, EV, and monitoring center. With GPS, users can inspect nearby charging stations and their parking information. The GPS will automatically guide drivers to the most suitable charging station. The monitoring center manages car batteries, charging equipment, charging stations and optimize resources.

5. Integrated IoT Architectures in Smart Grid

Several IoT architectures have been proposed to be integrated into SG. They can be categorized to architectures with three layers or four layers [48–53] (see Table 1). In [48], three layers are proposed. Layer 1 includes smart meters, network devices, and communication protocols. Layer 2 contains devices which are responsible for receiving data at the central system. Layer 3 includes artificial intelligent systems to provide information to decision and billing systems.

Table 1. Three-layer and four-layer models which are proposed for IoT architecture in a smart grid.

	[48–50]	[51]	[52]	[53]
Layer 4		Application	Social	Master station system
Layer 3	Application	Cloud management	Application	Remote communication
Layer 2	Network	Network	Network	Field network
Layer 1	Perception	Perception	Perception	Terminal

In [49,50], a three-layer structure is presented that contains perception layer, network layer, and application layer. Perception layer (or device layer) uses different kinds of sensors (e.g., power sensor), tags and readers (e.g., RFID tags/readers), or sensor equipment (such as GPS devices or cameras) to collect information. The network layer contains different kinds of wired and wireless industry-specific or public communication networks (such as 2G, 3G, 4G, cable broadband, public switched telephone networks, private networks, Wi-Fi, ZigBee) and the Internet to map the information gathered by sensors in the perception layer to communication protocols. It is used to route and transmit these mapped data to the application layer for processing, control, and access to the core network. It includes management and information centers. The application layer processes the information received from the network layer to monitor IoT devices in real time. It uses a variety of IoT technologies to realize an extensive set of IoT applications and contains application structure. Application structure is responsible for information processing and computing, and interface to resources. IoT can accomplish the integration of information technologies via the application layer.

In [51], the authors proposed four layers: device layer, network layer, cloud management layer, and application layer. Device layer contains two sub-layers: (1) thing layer (which contains different types of sensors, smart meters, smart tags, and actuators) to sense environment, collect data, and control home appliances, (2) gateway layer (which contains microcontrollers, communication modules, and local display and storage) that controls how to connect to elements of thing layer. The network layer sends the data from the device layer to the application layer. The cloud management layer is responsible for data storage and analysis and data and user management. The application layer provides services to end users such as homeowners or utilities and includes demand response management, dynamic pricing, or energy management.

The authors in [52] reviewed previous three-layer and four-layer models. The 4th layer in the four-layer model is the supporting layer which integrates some common IoT technologies. Then, they proposed a four-layer model that includes the previous three layers (perception layer, network layer, and application layer) and add an additional social layer on top of these three layers. The social layer regulates IoT applications.

The proposed four-layer model in [53] has a terminal layer, field network layer, remote communication layer, and master station system layer. The terminal layer comprises remote terminal units, smart meters, and smart devices. The field network layer includes wired communications such as fiber optics or wireless communication technologies such as Wi-Fi, ZigBee, or RFID. The remote communication layer contains wired and wireless wide area networks such as 3G or 4G wireless cellular networks. Master station system layer includes the control systems for different parts of a smart grid, e.g., generation, transmission, and distribution.

6. Requirements for Using IoT in SG

To use IoT in SG, we should have some technologies and satisfy some requirements which are listed as follows:

1. Communication technologies: Communication technologies can be used to receive and transmit acquired information about the state of SG's devices. We have short-range and long-range communication technology standards. ZigBee, Bluetooth, and ultra-wideband technologies are examples of short-range communication technologies. For long-range communications, power line communications [54], optical fiber, wireless cellular networks such as 3G and 4G, and satellite communications can be used.

2. Data fusion techniques: Since the resources of IoT terminals (such as batteries, memory, and bandwidth) are limited, it is not possible to send all information to the destination. Thus, to increase the efficiency of information gathering, data fusion techniques can be utilized to collect and combine data.

3. Energy harvesting process: Since most of the IoT devices use battery as one of their primary power sources, energy harvesting process is very important for IoT applications, e.g., using different sensors and cameras to monitor different parts of a smart grid.

4. Operating in harsh environments: IoT devices which are installed in high-voltage transmission lines and substations must work in harsh environments. Thus, to extend the lifetime of their sensors in these conditions, we should have sensors should be high or low temperature resistant, anti-electromagnetic, or waterproof.

5. Reliability: IoT applications in different environments need to satisfy different requirements such as reliability, self-organization, or self-healing. Thus, based on the actual environment, suitable IoT device must be selected to overwhelm environmental issues. For example, when some devices cannot send data due to lack of energy, a new route for the data must be found so that the network reliability remains at the required level.

6. Security: Security methods must be implemented in all IoT layers to transmit, store, and manage data, avoid information leakage and losses, and protect data.

7. Sensors: Sensors measure quantities such as current, voltage, frequency, temperature, power, light, and other signals and deliver the raw information for processing, transmitting, and analyzing. Recently, nanotechnology is used to provide high-performance material which covers different sensor applications and enhances the growth of sensor industry.

7. Challenges and Future Research Directions

To achieve technical goals in applying IoT in SG, there are many challenges which must be addressed in future research directions. Since IoT devices must work in different environments that may have harsh conditions (e.g., high or low temperatures, high voltages, exposure to electromagnetic waves, working in water, etc.), therefore, they must satisfy requirements at those conditions such as reliability or compatibility.

In many applications, IoT devices and sensors operate on batteries (e.g., different types of sensors which are used to monitor transmission lines), so suitable energy harvesting techniques should be used or designed. We have several communication networks in different parts of the SG, so, IoT devices should support necessary communication protocols so that transferring data from smart meters to the central system is possible and guaranteed.

Since IoT devices in SG have limited resources and capabilities such as batteries, processing power, storage, or bandwidth, so data fusion processes should be used to compress and aggregate useful data so that we have more efficient energy and bandwidth usage and data collection.

Delay and packet loss are important parameters that determine the performance of smart gird. Since congestion causes delay and packet loss, it degrades system performance (because IoT devices and/or gateways IoT devices must resend data which causes more delay and increases the probability of congestion again) and SG cannot satisfy predetermined requirements, e.g., maximum tolerable delay. Therefore, it is necessary to minimize delay, optimize network design by finding an optimum number of gateways and IoT devices, and minimize the number of connections to each gateway.

Since the smart grid contains many different gateways and IoT devices with different specifications and resources, interoperability between these devices to exchange information is very critical. One solution to achieve interoperability is to use IP-based networks. Another solution is that IoT devices should support different communication protocols and architectures.

Sensors, smart meters, and other similar devices that measure and collect information in a smart grid create big data that can consume a lot of energy and other resources and create a bottleneck. We should design the smart grid in such a way that can efficiently store and process this huge amount of collected data.

There are many separate standards for IoT devices, but there is no unified standard for IoT devices in the smart grid. This may cause security, reliability, and interoperability issues for IoT devices in SG. Therefore, standardization efforts should be unified.

To monitor and control IoT devices in SG, we should use the Internet which is very vulnerable, and attackers can manipulate measured data by sensors and smart meters and cause a lot of financial losses. Therefore, we should develop secure communications for IoT devices in the smart grid by considering resource limitations of IoT devices and determine some security measures for these devices. For example, IoT devices have limitations in computation and storage. Thus, we should design or use security solutions so that IoT devices are able to run them. From the collected data by smart meters, it is possible to extract some information about consumers' habits (e.g., wake up times, etc.), therefore it must be guaranteed that this private information will not be used without consumers' permission. Also, suitable mechanisms for security measures such as trust management (between IoT devices which are owned by different parties, e.g., customers and utilities), authentication, authorization, data integrity, maintaining confidentiality, and detecting identity spoofing should be devised.

8. Conclusions

In this paper, we discussed the Internet of Things as a network of networks and talked about its history, three visions and developments. The smart grid, as one of the most important applications of IoT, is studied. Architecture and elements of a smart grid are discussed. Then, IoT architectures for SG, requirements for using IoT in SG, IoT applications and services in SG, and challenges and future work are investigated.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Internet History of 1960s. Available online: https://www.computerhistory.org/internethistory/1960s/ (accessed on 14 January 2019).
2. Zhou, H. *The Internet of Things in the Cloud: A Middleware Perspective*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2008.
3. History of the World Wide Web. Available online: http://en.wikipedia.org/wiki/History_of_the_World_Wide_Web (accessed on 14 January 2019).
4. History of the Internet. Available online: http://en.wikipedia.org/wiki/History_of_the_Internet (accessed on 14 January 2019).
5. Friends Reunited. Available online: https://en.wikipedia.org/wiki/Friends_Reunited (accessed on 14 January 2019).
6. Towards a Definition of the Internet of Things (IoT). Available online: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (accessed on 16 January 2019).
7. Ghasempour, A.; Moon, T.K. Optimizing the Number of Collectors in Machine-to-Machine Advanced Metering Infrastructure Architecture for Internet of Things-based Smart Grid. In Proceedings of the IEEE Green Technologies Conference (IEEE GreenTech 2016), Kansas City, MO, USA, 7–8 April 2016; pp. 51–55. [CrossRef]
8. Ghasempour, A. Optimum Number of Aggregators based on Power Consumption, Cost, and Network Lifetime in Advanced Metering Infrastructure Architecture for Smart Grid Internet of Things. In Proceedings of the IEEE Consumer Communications and Networking Conference (IEEE CCNC 2016), Las Vegas, NV, USA, 9–12 January 2016. [CrossRef]
9. Internet of Things Strategic Research Roadmap. Available online: http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf (accessed on 16 January 2019).
10. NIST Releases Final Version of Smart Grid Framework. Available online: https://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf (accessed on 16 January 2019).
11. Weiser, M. The Computer for the 21st Century. *Sci. Am.* **1991**, *265*, 66–75. [CrossRef]
12. That 'Internet of Things' Thing. Available online: https://www.rfidjournal.com/articles/view?4986 (accessed on 16 January 2019).
13. Gershenfeld, N. *When Things Start to Think*, 1st ed.; Henry Holt and Company: New York, NY, USA, 1999.
14. Sarma, S.; Brock, D.L.; Ashton, K. *The Networked Physical World*; Auto-ID Center White Paper MIT-AUTOID-WH-001: Cambridge, MA, USA, 2000; pp. 1–16.
15. Schoenberger, C.R. The Internet of things. *Forbes*, 18 March 2002; 155160.

16. The Internet of Things. Available online: http://www.theguardian.com/technology/2003/oct/09/shopping.newmedia (accessed on 16 January 2019).
17. Gershenfeld, N.; Krikorian, R.; Cohen, D. The Internet of things. *Sci. Am.* **2004**, *291*, 76–81. [CrossRef] [PubMed]
18. The Internet of things: Start-ups Jump into Next Big Thing: Tiny Networked Chips. Available online: http://www.boston.com/business/technology/articles/2004/10/25/the_internet_of_things/ (accessed on 16 January 2019).
19. The Internet of Things. Available online: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf (accessed on 16 January 2019).
20. Fleisch, E.; Mattern, F. (Eds.) *Das Internet der Dinge—Ubiquitous Computing und RFID in der Praxis*, 1st ed.; Springer: Berlin/Heidelberg, Germany, 2005.
21. First International Conference for Industry and Academia on the Internet of Things. Available online: http://www.iot-conference.org/iot2008/ (accessed on 16 January 2019).
22. Castanier, F. Reduce Cost and Complexity of M2M and IoT Solutions via Embedded IP and Application Layer Interoperability for Smart Objects. In Proceedings of the M2M Forum, Milan, Italy, 20 May 2014.
23. Disruptive Civil Technologies: Six Technologies with Potential Impacts on US Interests out to 2025. Available online: https://fas.org/irp/nic/disruptive.pdf (accessed on 16 January 2019).
24. Internet of Things—An action plan for Europe. *Off. J. Eur. Union* **2009**, *278*, 116–120.
25. 2014: Ubiquitous Connectivity and the Internet of Things. Available online: http://www.frost.com/reg/blog-display.do?id=3161648 (accessed on 17 January 2019).
26. Singh, D.; Tripathi, G.; Jara, A.J. A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 287–292.
27. Miao, Y.; Bu, Y. Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid. In Proceedings of the International Conference on Advances in Energy Engineering (ICAEE), Beijing, China, 19–20 June 2010; pp. 69–72.
28. Connections Counter: The Internet of Everything in Motion. Available online: https://newsroom.cisco.com/feature-content?articleId=1208342 (accessed on 17 January 2019).
29. The Possibilities of the Internet of Everything Economy #IoE. Available online: https://blogs.cisco.com/news/the-possibilities-of-the-internet-of-everything-economy (accessed on 17 January 2019).
30. Evans, D. The Internet of Things: How the Next Evolution of the Internet is Changing Everything. Available online: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed on 17 January 2019).
31. Morgan Stanley: 75 Billion Devices Will Be Connected to The Internet Of Things By 2020. Available online: https://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10 (accessed on 17 January 2019).
32. Can the Internet of Everything Bring Back the High-Growth Economy? Available online: https://www.progressivepolicy.org/issues/economy/can-the-internet-of-everything-bring-back-the-high-growth-economy/ (accessed on 17 January 2019).
33. Vision and Challenges for Realizing the Internet of Things. Available online: https://publications.europa.eu/en/publication-detail/-/publication/ed079554-72c3-4b4e-98f3-34d2780c28fc/language-en (accessed on 17 January 2019).
34. Ghasempour, A. Optimized Advanced Metering Infrastructure Architecture of Smart Grid based on Total Cost, Energy, and Delay. In Proceedings of the 2016 IEEE Conference on Innovative Smart Grid Technologies (IEEE ISGT 2016), Minneapolis, MN, USA, 6–9 September 2016; pp. 1–6. [CrossRef]
35. Ghasempour, A. Advanced Metering Infrastructure in Smart Grid: Requirements, Challenges, Architectures, technologies, and Optimizations. In *Smart Grids: Emerging Technologies, Challenges and Future Directions*, 1st ed.; Lou, J., Ed.; Nova Science Publishers: Hauppauge, NY, USA, 2017.
36. Mouftah, H.T.; Erol-Kantarci, M.; Rehmani, M.H. Communication Architectures and Technologies for Advanced Smart Grid Services. In *Transportation and Power Grid in Smart Cities: Communication Networks and Services*, 1st ed.; Mouftah, H.T., Erol-Kantarci, M., Rehmani, M.H., Eds.; Wiley: Hoboken, NJ, USA, 2019; pp. 217–245. [CrossRef]

37. Zhao, Z.; Chen, G. An Overview of Cyber Security for Smart Grid. In Proceedings of the 2018 IEEE 27th International Symposium on Industrial Electronics, Cairns, Australia, 13–15 June 2018; pp. 1127–1131. [CrossRef]
38. Refaat, S.S.; Abu-Rub, H.; Trabelsi, M.; Mohamed, A. Reliability evaluation of smart grid system with large penetration of distributed energy resources. In Proceedings of the 2018 IEEE International Conference on Industrial Technology (ICIT), Lyon, France, 20–22 February 2018; pp. 1279–1284. [CrossRef]
39. Refaat, S.S.; Mohamed, A.; Kakosimos, P. Self-Healing control strategy; Challenges and opportunities for distribution systems in smart grid. In Proceedings of the 2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018), Doha, Qatar, 10–12 April 2018; pp. 1–6. [CrossRef]
40. Jarvis, R.; Moses, P. Smart Grid Congestion Caused by Plug-in Electric Vehicle Charging. In Proceedings of the 2019 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 7–8 February 2019; pp. 1–5. [CrossRef]
41. Rafiei, S.; Bakhshai, A. A review on energy efficiency optimization in Smart Grid. Proceedings of 38th Annual Conference on IEEE Industrial Electronics Society, Montreal, QC, Canada, 25–28 October 2012; pp. 5916–5919. [CrossRef]
42. Akaber, P.; Moussa, B.; Debbabi, M.; Assi, C. Automated Post-Failure Service Restoration in Smart Grid through Network Reconfiguration in the Presence of Energy Storage Systems. *IEEE Syst. J.* **2019**, 1–10. [CrossRef]
43. Qi, F.; Yu, P.; Chen, B.; Li, W.; Zhang, Q.; Jin, D.; Zhang, G.; Wang, Y. Optimal Planning of Smart Grid Communication Network for Interregional Wide-Area Monitoring Protection and Control System. In Proceedings of the 2018 IEEE International Conference on Energy Internet (ICEI), Beijing, China, 21–25 May 2018; pp. 190–195. [CrossRef]
44. Ghasempour, A. Optimum Packet Service and Arrival Rates in Advanced Metering Infrastructure Architecture of Smart Grid. In Proceedings of the 2016 IEEE Green Technologies Conference (IEEE GreenTech 2016), Kansas City, MO, USA, 6–8 April 2016; pp. 1–5. [CrossRef]
45. Ghasempour, A.; Gunther, J.H. Finding the Optimal Number of Aggregators in Machine-to-Machine Advanced Metering Infrastructure Architecture of Smart Grid based on Cost, Delay, and Energy Consumption. In Proceedings of the 2016 13th IEEE Annual Consumer Communications & Networking Conference (IEEE CCNC 2016), Las Vegas, NV, USA, 9–12 January 2016; pp. 960–963. [CrossRef]
46. Ghasempour, A. Optimized Scalable Decentralized Hybrid Advanced Metering Infrastructure for Smart Grid. In Proceedings of the 2015 IEEE International Conference on Smart Grid Communications (IEEE SmartGridComm 2015), Miami, FL, USA, 2–5 November 2015; pp. 223–228. [CrossRef]
47. Sarwat, A.I.; Sundararajan, A.; Parvez, I. Trends and Future Directions of Research for Smart Grid IoT Sensor Networks. In *Proceedings of International Symposium on Sensor Networks, Systems and Security, Advances in Computing and Networking with Applications*, 1st ed.; Rao, N., Brooks, R., Wu, C., Eds.; Springer: New York, NY, USA, 2018; pp. 45–61.
48. Lloret, J.; Tomas, J.; Canovas, A.; Parra, L. An Integrated IoT Architecture for Smart Metering. *IEEE Commun. Mag.* **2016**, *54*, 50–57. [CrossRef]
49. Wang, C.; Li, X.; Liu, Y.; Wang, H. The research on development direction and points in IoT in China power grid. In Proceedings of the 2014 International Conference on Information Science, Electronics and Electrical Engineering, Sapporo City, Hokkaido, Japan, 26–28 April 2014; pp. 245–248. [CrossRef]
50. Chen, X.; Sun, L.; Zhu, H.; Zhen, Y.; Chen, H. Application of Internet of Things in Power-Line Monitoring. In Proceedings of the 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Sanya, China, 10–12 October 2012; pp. 423–426. [CrossRef]
51. 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. [CrossRef]
52. Ning, H.; Hu, S. Technology classification, industry, and education for Future Internet of Things. *Int. J. Commun. Syst.* **2012**, *25*, 1230–1241. [CrossRef]

53. Wang, Y.F.; Lin, W.M.; Zhang, T.; Ma, Y.Y. Research on application and security protection of Internet of Things in Smart Grid. In Proceedings of the IET International Conference on Information Science and Control Engineering, Shenzhen, China, 7–9 December 2012; pp. 1–5. [CrossRef]
54. Yang, Q.; Wang, H.; Wang, T.; You, L.; Lu, L.; Liew, S.C. Powerline-PNC: Boosting throughput of powerline networks with physical-layer network coding. In Proceedings of the IEEE International Conference on Smart Grid Communications, Miami, FL, USA, 2–5 November 2015; pp. 103–108. [CrossRef]