applied sciences

MDPI

Article

Future of IoT Networks: A Survey

Suk Kyu Lee [1], Mungyu Bae [2] and Hwangnam Kim [2,*]

[1] LG Electronics Inc., Seoul 06772, Korea; skjl25@gmail.com
[2] School of Electrical Engineering, Korea University, Seoul 02841, Korea; nardyen@korea.ac.kr
* Correspondence: hnkim@korea.ac.kr; Tel.: +82-2-3290-4821

Received: 13 September 2017 ; Accepted: 10 October 2017; Published: 16 October 2017

Abstract: The introduction of mobile devices has changed our daily lives. They enable users to obtain information even in a nomadic environment and provide information without limitations. A decade after the introduction of this technology, we are now facing the next innovation that will change our daily lives. With the introduction of the Internet of Things (IoT), our communication ability will not be restricted to only mobile devices. Rather, it will expand to all things with which we coexist. Many studies have discussed IoT-related services and platforms. However, there are only limited discussions about the IoT network. In this paper, we will thoroughly analyze the technical details about the IoT network. Based on our survey of papers, we will provide insight about the future IoT network and the crucial components that will enable it.

Keywords: Internet of Things; Internet of Everything; IoT network; future network

1. Introduction

The age of the Internet of Things (IoT) is forthcoming [1]. It will give objects and even generated contents to the ability to communicate with other mediums. With the generated data from every object, the data will not remain raw as they are today but will be customized to the users based on their needs and even converge with other data. The concept of IoT is simple, although its capability is unlimited and its usage can change the entire paradigm of legacy technology. It is based on embedding a network interface into objects, enabling communications among them to provide various services for users. Consequently, each object will have its own identifier, such as an Internet Protocol address (IP address) in the current Internet that can connect and communicate with other objects through the IoT networking environment. Unlike the era before IoT, when the users could obtain data only from the service provider, the users can directly access the sensors and give commands to the actuators. With this capability, data from IoT applications will be utilized to provide a novel service to industry, academia, and even personal use.

To successfully manage IoT services, the IoT infrastructure must be well-designed. However, there are some limitations in the current research and development plan to create a complete IoT environment. First, the applications and services for IoT are sporadically developed from numerous vendors without the usage of the standard technology [2]. Second, there is no standard networking protocol for IoT applications. Even today, there are diverse networking protocols such as Wi-Fi, Bluetooth, ZigBee, Z-wave, and Long Term Evolution (LTE). Nonetheless, there is no device that can communicate with all existing networking protocols. To overcome this issue, the gateway, or the IoT device that can support heterogeneous networks, is crucial to create one complete IoT network. Additionally, the increasing number of IoT devices and the necessity of Big Data processing will expand the number of packets, where this issue can be a critical problem to the legacy network architecture.

In this paper, we focus on the network layer of the IoT. Although many studies have already conducted surveys on IoT, some survey papers primarily focused on the service aspect of IoT. Moreover, surveys in [3–7] present results on each focused subject. Nevertheless, many papers consider to

maintain the legacy network infrastructure, since the modification of existing network infrastructure costs highly. Obviously, the concept of future network for IoT should be researched in a national scale, and this consideration is an essential prerequisite to realize IoT environment. Therefore, we will discuss the reason why the current network is insufficient as an IoT network. Furthermore, we will describe the needs for modification and argue in favor of creating a novel network infrastructure to support the IoT environment.

Structure of This Article

IoT is not limited to include the communication functionality of the things; rather, it is an integrated solution to share all manner of information among devices, users and services to provide user-preferred service. However, current research on the IoT network varies. In this paper, we specifically focus on the network issues in the IoT because the IoT network is the fundamental component that can enable IoT services. We categorize this paper as follows:

- Overview of IoT,
- Current market and research trend of IoT,
- Research challenges of the IoT network,
- Insights for the future IoT network.

In Section 2, we introduce the overview of IoT and categorize it in terms of its technology. We introduce the market overview of IoT and its potential in Section 3. We then investigate various world wide research programs on IoT and future network architectures of various nations. In addition, we analyze the current status and the limitations of the IoT network, such as SDN, heterogeneity, and service-oriented networking, in Section 4. Finally, diverse inspirations that can solve the limitations of the current IoT network research described in the previous sections will be derived and analyzed in Section 5. Specifically, we will introduce novel concepts for a flawless future IoT network. Finally, we conclude the paper in Section 6.

2. IoT Overview

In this section, we briefly describe the overview of the IoT structure, which Figure 1 presents. The structure of the IoT consists of four layers: service layer, platform layer, network layer, and device layer. Many research institutions adopt the IoT classification standard shown in Figure 1 to maintain specialty and consistency for IoT development.

The service layer, which is on the surface, provides the interface and communicates with the users. Examples of the service layer are autonomous driving, health care, smart industry, personal devices, and door security. These services are connected with a platform layer to provide customized services to the users.

The next layer of the IoT structure is the platform layer. The platform layer is located under the service layer and supports the IoT applications and services. There are many types of platforms, including the device platform, data analysis platform, service development platform, and service platform. For instance, the device platform provides an execution environment of services and development for users. Context awareness and prediction, cooperation among things, and connection between the service layer and other layers with the translation of natural language to machine language are examples of the data analysis platform. Furthermore, the service development platform provides development toolkits to users for them to easily develop IoT services. Finally, the service platform supports the generation and execution of a variety of applications.

Along with the service and platform layers, one of the core layers of the IoT environment is the network layer. It serves to transmit the data among devices, contents, services and users. The network layer should be able to process, control, and manage enormous amounts of network traffic. A detailed elaboration of the network layer will be further described later in this paper.

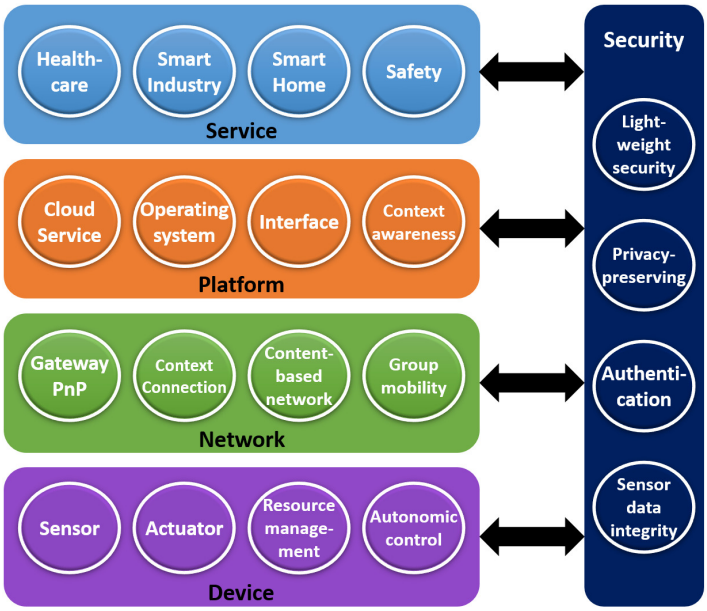

Figure 1. The overview of IoT structure.

Finally, the device layer is a layer that perceives the environment with various sensing devices, processes it to send to the sink node or gateway, and responds to it if necessary. The device itself must be smart by applying autonomic actuation and a smart control algorithm. The device layer should be able to acquire and control the IoT devices.

In addition to the four layers, security and privacy are important in IoT. Instead of identifying security as its own layer, each layer should incorporate a security solution to protect it from threats. Security issues should be handled as an important functional entity for each layer, and their current or prospective solutions should be customized according to specific properties and operations of each layer.

Each layer is important and has its own roles and capability to enable IoT. Although each layer of IoT is important and should be discussed in depth, the aim of this paper is to describe the IoT network in detail. We will primarily focus on the IoT network in terms of its challenges and provide insights for the future IoT network.

2.1. IoT Service

The features of the IoT services can be formulated in different ways. Many papers have proposed internal modeling of IoT services [8–11]. These studies proposed a semantic modeling approach to integrate the IoT framework into the IoT services by automatically obtaining the data from the mobile devices and the sensors [9,10]. Furthermore, the mechanism to interact between the IoT services and the sensors is discussed [8]. However, the core components within the domain of IoT services are tacking behavior, achievement of real-time awareness of the physical environment, and assistance with human decision making through deep analysis and data visualization [12]. IoT not only links sensor devices and generates the data for a purpose; rather, it focuses on the automation and optimization within the current systems [12]. For example, automated control of closed systems, control of optimizing resource usage across the network, and automated control in an open environment with great uncertainty. In addition, the data must be searched in a manner of semantic modelling approach by understanding the meaning of the data. Consequently, the proposed IoT services, such as smart homes, smart cities, health monitoring, smart grids, and smart traffic systems, have already incorporated these fundamental models of automation and resource optimization for any environment.

2.2. IoT Platform

The role of the IoT platform is to support and execute IoT services. In the past, the platform was developed in a closed manner. However, industries and governments are developing assorted IoT platforms as open source platforms. One of the reasons for this trend is to enhance the speed to enter the market, reduce the development cost, and improve the quality of the software [13]. By opening up the software platform, many developers are given the opportunity to contribute their work. This will eventually expedite the development process and reduce the cost. Specifically, Qualcomm developed the Alljoyn platform and is now under the process of turning it into as an open platform under the AllSeen Alliance [14,15]. Additionally, the European Union (EU) is operating the OpenIoT project to develop an open platform for IoT [16].

Another notable aspect of the IoT platform is the way in which the services were developed. In the past, the services were executed and developed independently. Now, they are being transformed into one platform that can support various services. For example, Cisco, International Business Machines Corporation (IBM), Qualcomm, Intel, and Google are developing their home, environment, energy, and traffic supporting services as a cross-platform network that can support various services [14]. Furthermore, the EU's Seventh Framework Programme (FP7) project and the Horizon 2020, International Telecommunication Union Telecommunication Standardization Sector (ITU-T), and oneM2M platforms standardize the IoT platform as a cross-platform network.

In addition, internal modeling of the IoT platform has been proposed [17,18]. The core idea of the internal modeling of the IoT platform is the publisher/subscriber model. For example, MAGIC Broker 2 is an IoT platform that provides a programming interface based on the publisher/subscriber model [17]. The authors created this platform by utilizing the mobile devices, public displays, and a Web-based sensor actuator named Sense Tecnic [17].

Finally, interaction between the platform and the devices is crucial to construct and design an IoT platform. Application Programming Interfaces (APIs) are the key components with which IoT devices can interact with the IoT platform. For example, an exemplary API for IoT platform has been developed [19]. The authors proposed an API based on TinyOS [20] named the Constrained Application Protocol (CoAP) that can enable both client and server to be integrated into the IoT environment.

Overall, the trend for the IoT platform is primarily based on the open source platform, cross-platform, publisher/subscriber model, and well-suited APIs.

2.3. IoT Devices

The role of IoT devices is not limited to collecting data; rather, they should also interact with heterogeneous networks to provide a broad variety of services. For instance, IoT devices need the ability to interact either node-to-node or node-to-Web based on whether the target node is in their own network [21]. In addition, the same philosophy as the IoT platform is also applied to IoT devices. The trend for developing an IoT device is in open-source and/or open-hardware approaches for developers and manufacturers. For example, IoT device manufacturing companies such as Arduino, ioBridge iota, and ARM provide the baseline architecture. With the baseline architecture, users and developers can develop their own IoT devices.

3. Current Market and Research Trend of IoT

In this section, we describe the overview of the current market and the research overview of IoT. We believe that solely explaining the IoT network is insufficient. It is important to know the current viewpoint of IoT from both market and research perspectives to understand the future IoT network. Thus, we believe that it is worthwhile to discuss the market and the research overview of IoT.

3.1. Market Overview

IoT is expected to change human life and open a larger and even more innovative market than its predecessor [22]. Although the number of devices that are currently connected to the Internet may look large given the population, we should note that the number of devices that are actually connected is small compared with the things with which we coexist in our daily lives. IoT is not limited to creating devices that can connect to the Internet it can provide novel services, applications, and even software toolkits to support its operations. The entities in the IoT market is not limited to the data providers; rather, it can expand to consumers, intermediaries and service providers and further change the pricing schemes [23]. Additionally, the service will further expand to open the data market and customize services for users, industry, and academia [22].

Furthermore, the IoT environment is not specifically considered at the device level. It should concentrate on the infrastructure side, such as gateways for billions of devices, services, user-centric information sharing services, Big Data, and customized data for the users. This will eventually induce improvements to both legacy communications and even service markets. For example, IoT services in the industry can be applied to manufacturing, the supply chain, energy, health, automotive, and insurance fields [24]. Moreover, it can provide novel toolkits in terms of software, hardware, and data [25]. Consequently, the technological paradigm will be shifted and further applied to a larger connected network with IoT.

3.2. Research Programs

Many research projects are currently operating in the field of IoT [26–38]. We will focus on introducing IoT research in Europe, the United States, and Asia.

3.2.1. European Union

To expedite collaboration in the EU research and development program, Europe established the Cluster of European Research Projects on the Internet of Things (CERP-IoT) in 2010 to conduct research on IoT. The primary vision of the EU's IoT is based on smart things and objects. Starting from the interactions with the smart objects and things, the committee extended the IoT vision to accommodate the domain of smart energy, smart buildings, smart living, smart health, smart cities, and smart transport [26] and proposed a roadmap of IoT in 2011 [26]. Based on this roadmap, the EU government initiated the Horizon 2020 program in 2011 by announcing multiple IoT R&BD programs that were focused on implementing IoT smart life service [27]. Specific details of Europe's Horizon 2020's research goals are as follows. First, the program is not limited to IoT but also focuses on the future Internet, cloud computing, Big Data, and 5G networking. Each specific item of the program is designed not to work independently but to interact with each other. Second, the EU's research programs mostly fund small and medium enterprises (SME). With the funding emphasis on SME, many companies can discover innovative IoT business models and IoT applications to invigorate IoT services. Finally, to distinguish itself from the previous disseminated research and services, Europe's Horizon 2020 encouraged large global collaboration with other research institutions. Each specific member of Horizon 2020 should interact with the others and let the industry develop the business model, application, and services to enable IoT as a whole. The result [28] for first two years is that the number and the quality of applications about IoT had been rapidly increased. This results mean that the Horizon 2020 project is on a cruise to close its purpose.

3.2.2. United States

The National Intelligence Council (NIC) of the United States selected IoT as one of six technologies that has potential impacts on national interests through 2025 [31]. Specifically, industry giants such as Cisco and Qualcomm primarily focus on extending the current network infrastructure into the IoT and construct the hyper-connected infrastructure. Further, legacy sensor devices and radio frequency

identification (RFID) are based on seamless connection. In terms of the government aspect, the National Institute for Standards and Technology (NIST) regards IoT as a basis technology for smart grid implementation. Moreover, the National Science Foundation has selected IoT as one of the technology areas in the Small Business Technology Transfer (STTR) program [32].

3.2.3. Asia

In terms of Asia, China and Japan are the major nations that are currently investigating IoT vigorously.

China has gathered 5 billion Yuan as a fund for Chinese IoT investment. The Chinese government's latest five-year plan primarily chose the smart grid, transportation, logistics, the home, environment and security, industry and automation, health, agriculture, finance, and military as principal service areas for developing IoT technologies [33,34]. In addition, the Chinese government has placed emphasis on a nation wide standardization strategy. Moreover, the Chinese government is establishing a demonstration test bed and IoT database. The Chinese government established a project named as "Internet Plus" strategy [35], which is a plan to collaborate between IoT technology and manufacturing business.

Along with the Chinese government, Japan is currently conducting the "i-Japan Strategy 2015" research program as a part of IoT research [36]. The Ministry of Internal Affairs and Communications (MIC) of Japan created a consortium that is based on mobile carrier service providers and system vendors [37]. The Japanese government is concentrating on remote health-care and earthquake monitoring to enable a secure future digital society. The Ministry of Education, Culture, Sports, Science and Technology ordered the new project, "The Research Project for Information & Communication Technology (ICT) System Architecture in the Era of IoT" [38] to get a foothold in IoT environment.

3.3. Current Research on Future Network Architecture

In this subsection, we present a survey on the future network architecture for IoT, in contrast to the IP-based conventional network architecture. The current network is based on the server-client model, and the number of nodes in the network has not been as enormous as it is today. In the server-client model, it is difficult to change the network functions and control the network with ease owing to an increase in network complexity. However, this will eventually become a larger problem in the era of IoT because the number of devices that will be connected to the IoT network is expected to increase exponentially.

Fortunately, some nations have recognized this problem and proposed novel network architectures [39]. For instance, there are many research projects about the future network architecture under FP7 and Horizon 2020 in the EU. Specifically, the 4WARD and Scalable & Adaptive Internet Solutions (SAIL) project studies the future network architecture. Additionally, Future Internet Research and Experimentation (FIRE) is intended to construct the initiative test bed infrastructure for the future Internet technology. In Horizon 2020, FIRE+ [40] is proposed to expand previous FIRE project by enabling experiments in any size, complexity, or networking technology. In addition to the EU, the Future INternet Design (FIND) project had been researched under the National Science Foundation (NSF) in the United States. Future Internet Architecture (FIA), which is the successor of FIND, has four main research topics to build the Internet architecture: Named Data Networking (NDN), MobilityFirst, NEBULA, and eXpressive Internet Architecture. Along with FIA, NSF sponsors the Global Environment for Network Innovation (GENI) project to construct the test bed environment. Currently, the Future Internet Architecture-Next Phase (FIA-NP) project is in progress to realize the research results of FIA. The overview of the future network architecture projects from the European Union is presented in Table 1, and Table 2 elaborates the research projects in the United States.

Table 1. The projects of the future network in the EU.

Projects	Contents
4WARD & SAIL	• 4WARD: an ultra-scale future Internet research project, which inject 20 million euro to work together in different and specialized network architectures. • Scalable & Adaptive Internet Solutions (SAIL) project: the successor of 4WARD to develop a high network architecture. • Research challenges: network virtualization, network management, information-centric networking, and routing in the core network.
FIRE [41]	• Future Internet Research & Experimentation (FIRE): the test bed development project that is similar to GENI, whose purpose is to narrow the gap between visionary research and large-scale experimentation. • New projects started in January 2016, focusing on networking and networked services. • Federation for FIRE (Fed4FIRE): a real federation of experimentation facilities that focus on the simple, efficient, and cost-effective experimental environment. • Research challenges: federated test-bed and implementing controlled experiments.
FIRE+ [40]	• FIRE+ (2014): to implement a reliable experimental infrastructure with independence in terms of the size of experimental, geographical constraint, and tools. • Integrating experiments and facilities in FIRE+ (2015): a large-scale and real life experimental infrastructure to design and deploy services for the future internet. • Future Internet Experimentation: Building a European experimental Infrastructure (2016): Focus on the experimental capability, which can cover variety of networking areas and standardization and interoperability of experimental facilities.

Table 2. The projects of the future network in the United States.

Projects	Descriptions
FIND	• The purpose of Future INternet Design (FIND) is to develop an innovative Internet architecture that excludes existing Internet technology. • Research challenges: network architecture and transmission structure.
Future Internet Architecture (FIA)	Named Data Networking (NDN) • It focuses on the contents of the future network, and the purpose is to change the communication paradigm from "where" to "what" and focus on the contents and the user rather than the address or the server. • The main architecture of this project is that a user receives the contents from the network node, which caches it in the network, rather than making a request to the content server and providing the contents. • Research challenges: creating NDN, including routing scalability and fast forwarding. MobilityFirst [42] • It focuses on the mobility issues in the future network, and the purposes are to provide mobility to the device, satisfying location-aware service for the user, and to design the effective communication structure between the mobile nodes. • It assumes that mobility is a general situation rather than the exception, which is in case in the current network system. • Research challenges: fast global naming service, Generalized Delay-Tolerant Network (GDTN) routing, connection-less transport, etc. NEBULA [43] • It focuses on cloud computing in the future network, and the purpose is to provide the cloud computing model, which can serve an always-available network service. • Research challenges: reliability and security among the users and data centers and data center-to-data center, extensible network design, trustworthiness, etc. eXpressive Internet Architecture [44] • It focuses on secure communication in the future network, and research challenges are trustworthiness, different interfaces between network actors, intrinsic security, etc.

Table 2. *Cont.*

FIA-NP	• It is the "Next Phase" of the FIA project, in which the objective is to deploy the designs in large-scale and realistic environments. • Research challenges: enhancement of existing FIA design and developing a prototype that is adequate for the relevant environment.
GENI	• The purpose of Global Environment for Network Innovation (GENI) is to build a national scale network infrastructure that can provide an environment that is similar to reality, and research challenges are programmability for all layers, end-to-end virtualization, federation with different networks, and test bed.

4. Research Challenges of the IoT Network

In this section, we will discuss the current research challenges in the IoT network. Even if many researchers and governments have focused on implementing environment for IoT network, we think that there are some issues, which are important to IoT network but relatively unknown to major researches. The following contents will handle such important issues. Firstly, we will review various studies in terms of the IoT network. Afterwards, we will present the components that may be contained in the IoT network. Finally, we will analyze the research challenges in the IoT network.

4.1. Literature Review

In [45], the authors proposed two network models, the man-like nervous (MLN) model and the social organization framework (SOF) model. The idea of MLN model is similar to a reverse tree, in which the sensors are in the low rank of the model, and it becomes a distributed node to send sensing data to the centralized data center. Additionally, the SOF model consists of local IoT, industrial IoT, and national IoT that manages the distributed nodes in the specific region and the data center. The theme of [45] is that IoT is based on the data center and manages the data from the sensors based on the MLN model. However, the specific usage of the IoT network is not provided yet.

Another architecture of the IoT network was described by Catellani et al. [46]. In this work, the authors created a test bed for an IoT environment by utilizing the legacy sensors and actuators by modifying it with TinyOS. The authors envisioned that the future IoT network would be based on Internet Protocol version 6 (IPv6), and every communication will be conducted with IP addresses. Moreover, instead of enumerating the future networking protocol, the authors categorized the nodes in terms of base station node (BSN), mobile node (MN), and specialized node (SN). BSN refers to the IPv6 sink and router, MN refers to wireless dongle to add wireless sensor network (WSN) connectivity to a standard laptop, and SN refers to nodes offering services such as temperature readings or actuation.

Finally, Gubbi et al. [47] claimed that future IoT network will be based on the current WSN technology. The nodes are expected to be deployed in an ad-hoc manner, and a novel cyber infrastructure is based on a service-oriented architecture (SOA) and sensor networks to acquire the data from the sensors and the devices. Furthermore, the addressing schemes will be based on IPv6 and possible adaptation with the uniform resource name (URN) system for development of the IoT network. The authors claimed that cloud-based centralized storage is required to support the storage and analysis for IoT. Consequently, the authors noted that the future IoT network will be based on current WSN technology with the middleware to support heterogeneous devices and a centralized storage for the data.

In all, the current proposals for the IoT network are mostly based on WSN networks without creating a novel network architecture. Many studies have noted that there should be a centralized data center to store and provide customized data to the users. As we have already introduced in the previous sections, a network architecture of IoT environment has to be changed due to the amount of devices and different service type.

4.2. Service-Oriented Network

The service-oriented network (SON) is an important component of the IoT network, in which content distribution network (CDN) is one of the most discussed models to enable SON [48,49]. Figure 2 presents the concept of the CDN. The CDN is a system that stores the copies of contents in many distributed servers to deliver the content effectively [50]. The CDN has an advantage that it can provide content and services to the user rapidly. Nonetheless, it is required to synchronize and distribute content [51]. Currently, the CDN institutes a Peer-to-Peer network (P2P) technology to let nearby users directly exchange content with one another [52] to improve the data exchange throughput. However, the CDN uses legacy network technology, and there are shortcomings that require an extra service to obtain the information of the content [53]. Table 3 represents the comparison of introduced SON technologies.

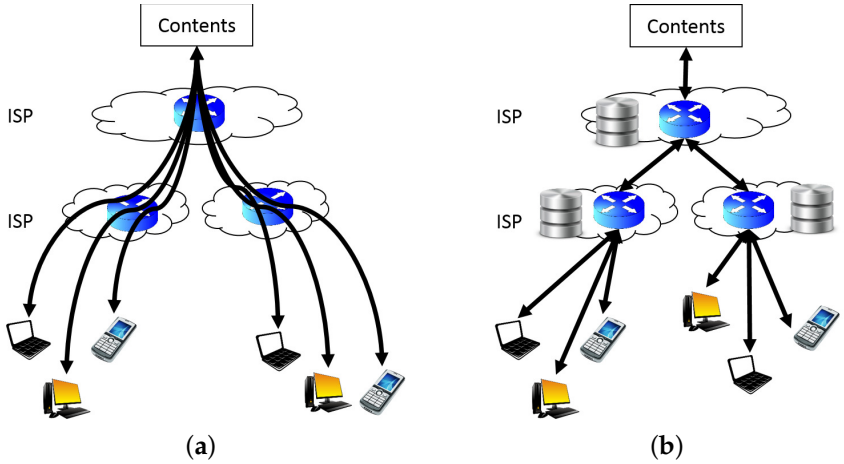

Figure 2. The concept of content distributed network. (**a**) The procedure of current content request; (**b**) The procedure of content-distributed network.

Table 3. Comparison of service-oriented network technologies.

References	CDN [1]	IP-Based	User-Demand	Synchron-Ization	Replica Placement	Additional
[48]	server-farm	O	O	X	O	QoE-based [2], machine-learning
[51]	hybrid	O	X	O	X	synchronizing CDN edge server
[52]	hybrid	O	X	X	O	economic modeling-based
[50]	server-farm	O	X	X	O	popularity-based

[1] Content Distribution Network (CDN); [2] Quality-of-Experience (QoE).

4.3. Heterogeneity of Network Technologies

In IoT, it is prevalent that the devices are installed with different types of network protocols. Each network protocol has different service types and network conditions. To overcome the challenge of integrating different network protocols, there have been efforts to integrate heterogeneous networks [54–56]. Further, direct communication among the devices is not always supported even if the devices are collocated and use the same radio technology [57]. The IoT-A communication protocol model was proposed by [58] and accepts standards such as Constrained Application Protocol (CoAP), User Datagram Protocol (UDP), Internet Engineering Task Force IPv6 Routing Protocol for Low-Power and Lossy Networks (IETF RPL), IPv6 over Low-Power Wireless Personal Area Networks. (6LoWPAN), IEEE 802.15.4e, and IEEE Std 802.15.4-2006. However, there is no standard or exemplary technology that can support different network protocols. Inter-operability encompassing these network protocols is expected be a major challenge for constructing the IoT network. Generally, a network translation gateway is required to connect devices that employ different communication

protocols [59,60]. Nonetheless, forcing all communication through the gateway may result in overhead problems. These issues with integrating various network protocols must be addressed within the IoT network. Table 4 compares the techniques related to support heterogeneity.

Table 4. The comparison of heterogeneity technologies.

References	Integration	Coupling	Translation Gateway Required	Additional
[54]	CDMA2000 [1]/WLAN	loosely coupled	O	
[55]	3GPP [2]/WLAN	loosely coupled	O	
[56]	3G/WLAN	tightly coupled	O	
[57]	various protocols	X	X	
[60]	non-IP/IP	tightly coupled	O	embedding IPv6 layer

[1] Code-Division Multiple Access 2000 (CDMA2000); [2] 3rd Generation Partnership Project (3GPP).

4.4. Software-Defined Network & Network Function Virtualization

In an IoT environment, devices and services have their own policies. To seamlessly operate the devices, services, and platforms, the network must manage the network flow. Specifically, the network manager must control and apply flow rules to the devices and platforms. One of the solutions for this issue is to modify the devices and improve the networking capability. Nonetheless, this approach may increase the cost, and it is time consuming. Specific functions of network equipment are not opened to the network manager, so the network manager cannot easily modify the existing flow rules as the manager wants. For instance, the network manager must access each of the devices to customize the network flow rule. Furthermore, in a conventional network configuration, the router or switch has customized hardware parts or chips that are suited for the network environment. To modify the network environment, all chips and parts of the switch must also be modified, and this process requires many efforts and costs to replace the hardware parts of a router or switch.

To overcome these challenges, the concept of the programmable network has been introduced as the software defined network (SDN). The fundamental idea of SDN is to provide a feature to manage the traffic of the network in a software manner. SDN can be an essential technical feature of IoT, and research related to institute SDN into an IoT environment is currently underway [61,62]. SDN separates the control plane and data plane from the network flow to enable programming of the network. SDN can substitute control software for hardware parts. Additionally, the network manager can modify the network configuration according to the current network status.

It is certain that the size of the IoT network will increase. In this particular case, a plurality of network equipment is needed to cover the network. When the network managers want to add network functions, they must buy the functions or new equipment to embed the wanted functions into the current network. To overcome this challenge, the concept of network virtualization [63] was introduced to easily connect different clients without making a new physical connection. Further, network function virtualization (NFV) supports various services in the network device [64,65]. The concept of NFV is to virtualize various functions such as the firewall, DNS, and caching and operate these functions in a software manner. The NFV can provide a different service to each flow with ease, which reduces the network manager's overhead and cost to change the network service.

4.5. Network Security

IoT devices may obtain visual and the sound information of the user without notice. This phenomenon is not limited to the private sector but also affects the public sector. Devices that monitor car traffic, surveillance, and mass transportation will be capable of communicate with one another. Thus, it is crucial to have a secure environment, in which personal information should not be leaked to other users, even if the user does not have malicious intent. Further, it is necessary to devise a scheme that can protect the devices from malicious attacks.

In [66], IoT security can be summarized as follows: (i) resilience to attacks that may lead to system failure, (ii) data authentication to defend from forgery attacks such as changing sensor data

modification, (iii) access control algorithm for information provider to control the access level of data, and (iv) user privacy preservation to protect the issue in which the server easily infers the user's private information through the user's data. With this in mind, the devices themselves should be equipped with a mechanism to protect their operations, and the network itself should be protected. In terms of networking, a security challenge may exist with the tight resource constraints in IoT devices, Distributed Denial-Of-Service attack (DDoS) resistance, and protocol translation and end-to-end security among multiple heterogeneous devices [67]. It is necessary to devise a security scheme that can protect both the devices and the network to provide secure IoT services to the users.

4.6. Reconfigurable Networking Group

IoT devices should have the ability to devise a network based on their proximity and logical operation of the IoT service. Although the current network is based on the service provider, the future IoT network should have the capability of composing and maintaining a network that is based on location. For example, the devices must provide information that is based on that specific location. Based on the juxtaposed data from various devices, data from the devices in a specific location can provide information that is specific to the physical location of the user. Thus, grouping of the devices based on the specific location is needed. However, if the user wants a service that is not based on the specific location, the devices should be grouped based on the logical operation of the service.

4.7. IoT Gateway

The IoT gateway [68] is believed to be an important component of the IoT network. The main functionality of the conventional gateway or router is to forward packets to the destination node. The main purpose of the IoT gateway is similar to that of a conventional gateway, but there are some additional features as follows.

First, heterogeneous network connectivity [69,70] must be guaranteed. A short-range communication technology is definitely required to provide connectivity to small sensors or devices. These nodes must send packets to the IoT gateway first, so the IoT gateway must support all of these short-range communication protocols. Further, the IoT gateway must support wired communications, high-performance communication protocols including Wi-Fi and LTE, and existing short-range communication protocols including ZigBee, Bluetooth, and Z-wave. Second, network manageability is crucial for the IoT gateway. A conventional gateway manages the nodes in the subnet. However, the concept of network manageability is larger in an IoT gateway than in a conventional gateway. The IoT gateway is not limited to supporting conventional network management functions; rather, it should even update the affiliated devices' firmware or system. Consequently, the concept of manageability of the IoT gateway has expanded, and techniques to empower the network management is essential for the IoT gateway.

Finally, the IoT gateway must support the protocol or platform interworking. Many novel network concepts such as platforms and protocols, are developed to make IoT environment settle into traditional networks. Nonetheless, these can cause compatibility problems with conventional devices because legacy devices, such as household appliances, are not equipped with platforms and protocols. Thus, compatibility with the conventional platform and standard competition issues must be solved by allowing the IoT gateway to support platform interworking. Table 5 shows the current research and implementations of the IoT gateway.

Table 5. The technological comparison of IoT gateway.

References	IP-Based	Multiple Communication Card	Extra Storage	Focusing
[71]	O	O	X	supports various communication cards
[72]	O	O	X	supports various communication cards
[70]	O	O	X	priority-based scheduling algorithm
[73]	X	O	O	Machine-to-Machine communication

4.8. Discussions

The current research on the IoT network can be summarized as follows: Service-oriented network based on CDN and P2P, Platform-centric heterogeneity support, SDN, Object-to-object security, Location- and proximity-based grouping, IoT gateway. The similarity among current IoT network research is that they assume the IP-based client-server model for communication. These studies are essential components to realize the IoT on the current network. However, the existing research direction has some limitations. Most devices are still based on IPv4, which has the issue of a limited number of available addresses. As a result, IPv6 takes the spotlight for next-generation network addressing, and many research and development effort are underway based on IPv6. However, IP-based networking is based on one-to-one communication, in which a device attempts to connect with nearby devices one by one when it wants to receive content. This retrieval procedure may require additional resources and time. Therefore, a service provider with plenty of content is required to reduce this effort. In this case, the users must send the queries to access a content-providing server, which may lead to an overhead problem for the content server. Moreover, the availability of the content is related on the status of a server that has the content, despite the fact that the user has legitimate authority. An ID-based networking concept such as NDN is necessary to solve these limitations and realize a veritable service-oriented network. It is a great challenge to institute this concept into the real network infrastructure. Furthermore, novel technologies such as SDN, content-based routing, context-based multi-connection, naming management, and gateway-based communication that are suitable for the IoT environment are required because satisfaction of ID-based networking does not imply that it can satisfy the IoT environment.

5. Future IoT Network

In this section, we describe and provide insights on our envisioned future IoT network in detail. Figure 3 illustrates our vision of the future IoT network. Each component in the IoT network will be explained in detail in this section.

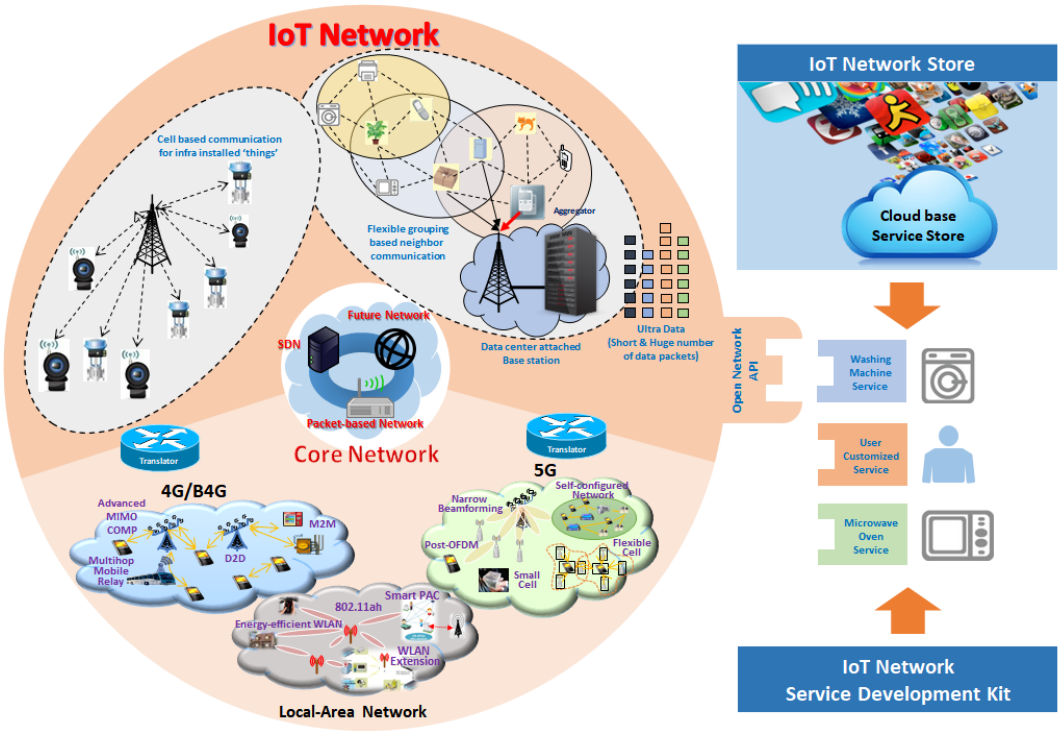

Figure 3. Overview of future IoT network.

5.1. Software-Defined Network

The advantage of SDN is to enable the users to program the switch. As described previously, SDN has a technical feature that can enable programming of the network service devices [74–79]. One of the well-known SDNs is OpenFlow [76]. It is a programmable network in which the users can program the switch to change the protocol and test a new protocol. There are various functionalities in OpenFlow, but it can be summarized in at least three parts: (i) a flow table with an action associated with each flow entry and to tell the switch how to process the flow, (ii) a secure channel that connects the switch to a remote control process and allows commands and packets to be sent between the controller and the switch, (iii) a protocol that can provide an open and standard way for a controller to communicate with any switch. Instead of relying on a vendor-specific switch, the SDN protocol can provide the feature to program the switch based on the service that the user wants to provide to the other users. Moreover, IoT service providers can use APIs to operate IoT services with SDN-enabled devices. Finally, SDN can be equipped with virtualization, with which the users can differentiate the service by virtualizing the router or the switch. Consequently, SDN can enable physical and virtual object control for IoT.

5.2. Management of IoT Devices on IoT Network

For IoT devices to access the IoT network, the IoT network itself should support a mechanism of plug-and-play for the IoT devices [80]. Current devices are primarily controlled by users in terms of turning on the device and connecting the device to the network. However, the IoT device should not be configured manually by the users and should be automatically configured. To support this feature, the plug-and-play mechanism is crucial for the IoT network because it can automatically connect the IoT devices to the IoT network. For example, the authors in [81] proposed plug-and-work to orchestrate numerous devices to automatically connect within industrial and production systems. Plug-and-work concentrates on self-configuration mechanisms by enabling a secure plug-and-work environment for IoT. Nonetheless, the IoT network should be able to provide a connectivity mechanism for connecting trillions of devices and managing networking addresses regardless of the type of network connection.

Furthermore, there are issues with assigning IP addresses to IoT devices and data. To efficiently manage IoT devices, an efficient and scalable addressing scheme for connecting IoT devices to the Internet is needed. One of the solutions to handle the addressing issue in the IoT network is to employ the IPv6 address allocation scheme [82,83]. The IPv6 addressing architecture defines two scopes for a unicast address, link-local and global. The link-local address is used for auto-discovery and auto-configuration. It is used for the local network and does not guarantee uniqueness in a larger network. Moreover, it will not be forwarded by the routers to the other links. The global scope address is expected to be used as a globally unique address. Thus, the device can utilize a global IP address to communicate over the Internet and utilize the link-local address to connect to the local area network. Specifically, the Unique Local Address (ULA) is designed for local networks larger than a single link but not for communication with the Internet [84]. Globally unique addresses (GUA) are administered to provide a unique and routable address for the Internet communication. For devices that do not require Internet communication, the address schemes can be employed as a ULA. However, in case the IoT devices need to communicate in the global network, it can employ the GUA address. Consequently, the IPv6 will not only ease the issue of scalability of the networking address, but it can also be configured in an adaptive manner to increase the efficiency of the IoT network [85]. Further, with the IPv6 technologies to maintain and allocate IP addresses for IoT devices, the IoT network can handle connectivity management from a local network to a global network.

5.3. Supporting Heterogeneity of Network Technologies

Many network protocols, including radio-frequency identification (RFID), Wi-Fi, Bluetooth, ZigBee, 3G, and LTE, work independently. A unifying architecture that can support heterogeneity of networking protocols, interoperability among network protocols and the devices is needed to enable

the IoT network [86]. In [58], the authors proposed six layers for the IoT network, which are listed as follows : physical layer, link layer, ID layer, network layer, end-to-end layer, and data layer. This is different from the legacy networking stack, but the main problem with this protocol stack is that it is focused only on the LoWPAN networking technology. In terms of wide-range communications, a large proportion of the communication features of IoT is concentrated on wide-range coverage as stated in the Weightless open standard [87]. It is true that IoT devices should support wide coverage; however, the current commodity network protocol requires additional technical features and chips that can support low power and yet increase communication coverage to support this feature. This will represent an additional cost for the manufacturers. To reduce the additional cost to enable IoT, the future IoT network should incorporate the idea of supporting interoperability among various network protocols. To encompass the feature to support different network protocols, the IoT network should be able to acquire the data from different networking protocols. Furthermore, the gateway for the IoT network should also support acquisition of various network protocols and connect the devices to the IoT network.

5.4. Connection Management

Each device may have different a communication protocol, so the connection management object may support different standards to nodes that belong to the user. The IoT home gateway or access point (AP) may manage the different standards, but there is a problem when the nodes are out of the communication range. For example, cellular communication, which provides a wide-range connection to the device, cannot be installed in the small sensors owing to the problems of price and battery consumption. Further, communication management is required in both the static and nomadic environment because a guest node that temporarily visits the network area may exist. The concept of grouping [88,89] can be a good candidate to manage the connectivity of the devices. For instance, grouping devices can be categorized as follows: physical grouping and logical grouping.

Figure 4 and Table 6 elaborate the concept of physical and logical grouping in the IoT environment. In terms of physical grouping, devices can be grouped based on their physical proximity. Meanwhile, connection among equal IoT service task devices is needed to support the service-oriented network without establishing direct connections with one another. In this case, a new manager, which is the main agent of the service or network management-available device, must manage this group of devices, which can be classified as logical grouping. With these two categories of device grouping, any IoT service can provide effective services for users.

Table 6. Grouping techniques.

Technique	Attributes
Physical grouping	• It is similar to the concept of a subnet. • Each node in the same physical group exists near the connection management object to communicate directly. • A node can be included in the physical group that can communicate the connection management object through multi-hop.
Logical grouping	• It contains the devices that use same service or application even if they are connected to different physical networks. • The devices that belong to the same logical group are managed from each communication management object in its physical group. • A new manager is needed to manage the network connection for all devices in the logical group.

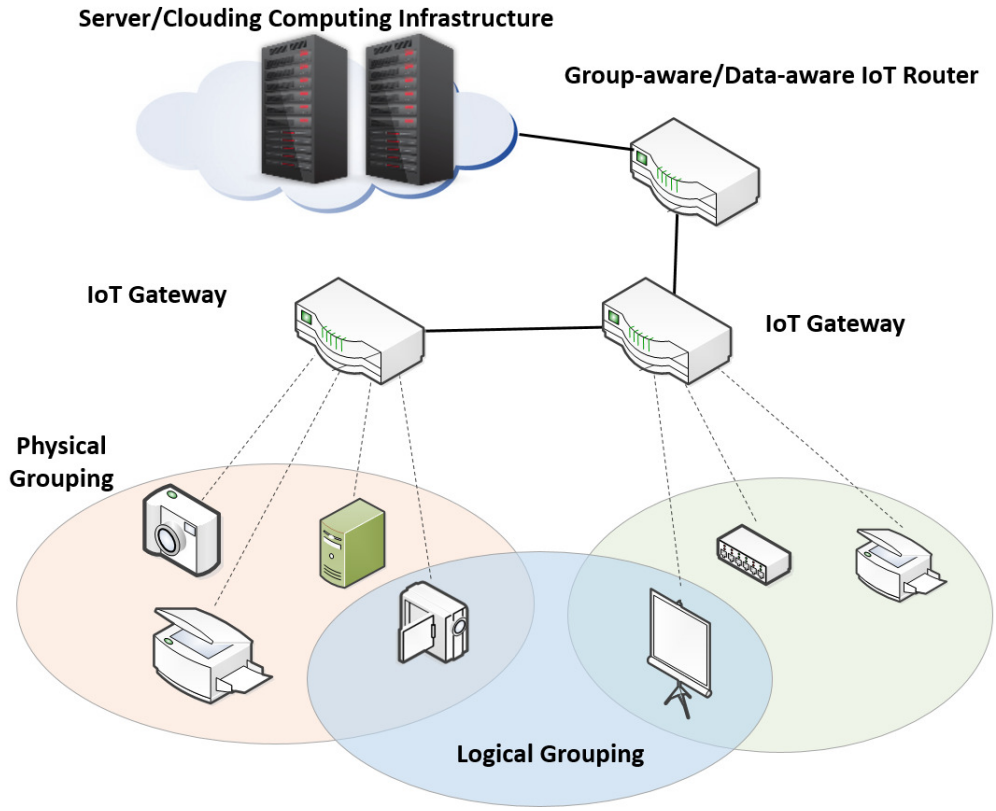

Figure 4. The concept of physical grouping and logical grouping.

5.5. Network Security

Guaranteeing network security and privacy in the IoT network is an important component. In this subsection, we describe the security issue of the future IoT network [90].

5.5.1. Data Security

Data security is one of the important issues in the security area. The confidentiality of the IoT data may not be regarded significantly because many IoT data can contain simple data such as temperature, humidity, and others. However, some of the data such as credit data or request data to control IoT devices may indirectly contain the user's private information and affect the user's daily patterns. For instance, when these data are forged or falsified, a malicious attacker can easily control the user's IoT devices. In this situation, a malicious user can easily connect the user's IoT device and obtain information without any restrictions. Furthermore, the attacker can easily change the user's device to use it as an attack by utilizing the user's cheap and disposable IoT device to conduct a DDoS attack [91]. With IoT devices, DDoS attack can harmfully affect the IoT network and services. Consequently, a malicious attempt to control the things of the user can affect the user's life and even the industry.

One of the simplest solutions to effectively secure data can be to utilize the existing techniques such as Public Key Infrastructure (PKI) or Elliptic Curve Cryptography (ECC) [92,93]. However, these techniques require enormous amounts of computational power and battery resources. Although current mobile devices may support the security schemes, many IoT devices have limited power and computational resources. Therefore, a light weight encryption algorithm [94] and key management protocol are needed for IoT devices. Additionally, there are some DDoS-preventing algorithms [95], which use null routing or unauthorized packet filtering. However, these solutions cannot defend the reduced throughput because the router must receive the DDoS packet and filter it. Furthermore, data requests from various light weight sensors may lead to similar behavior to a DDoS

attack in the IoT environment. Specifically, if the user requests tremendous amounts of data from various light weight sensors, even if the data may be temperature or other light density data, receiving these data can cause behavior similar to a DDoS attack for the user. Thus, even if the user has not intended to receive a DDoS attack, similar behavior to a DDoS attack may occur if the data security and control algorithm is not researched.

5.5.2. Privacy

Privacy is a critical issue [96,97] in the IoT environment. Many users will realize that IoT can improve and even change their daily patterns. Nonetheless, most users are also concerned with the privacy issue of IoT. This concern is appropriate because anyone can connect to another user's devices and collect information. In this case, user s' private information can be leaked to the information collector. For example, when an application server wants to collect the temperature from all users in a specific area, this server sends a temperature collection query to all nodes in the area. The nodes that respond to this query may reply with their IP address, location information, and temperature data. Although some of the data may not be related to the privacy issue, other data, such as the user's location, may violate the user's privacy. Because the server can handle all types of user data, it can easily see the private information of the user. If this server acts maliciously, this information can be abused, and the replied user's privacy is not guaranteed.

To overcome this challenge, we consider two simple methods that can use current privacy preservation techniques to prevent the leakage of users' private data. In the first method, the user's device ignores the query that needs privacy-sensitive data. This method can easily prevent privacy invasion, but it may not be suitable for the purpose of IoT. The second method is to construct the network architecture, in which the user's device returns only the requested data without including privacy-sensitive data. However, essential data, such as IP address or location information in the location-based service, cannot be hidden or ignored to receive this service. From the server side, the integrity of the received data from the user's device cannot be guaranteed with the second method. Therefore, research on a privacy-preserving cryptography solution that can maintain the concept of a service-based architecture and content-based networking, is required. Recently, work in [98,99] has attempted to follow this method with a fully decentralized anonymous authentication protocol [98] or a novel framework for privacy preservation [99]. However, it is difficult to implement them in the IoT environment because such algorithms do not consider content-based networking. Consequently, it is crucial to protect the user's privacy in the IoT environment.

5.6. IoT Gateway

The IoT gateway is the core component in the future IoT network. Figure 5 presents the overview of the IoT gateway.

In this subsection, we describe the key features to compose the IoT gateway.

5.6.1. Network-to-Network (N2N) Communication Support

In the IoT environment, it is crucial to manage the information such as affiliated node attributes, identification of holding contents, and network status, in the group by the network management object to successfully utilize an information-centric network (ICN) [100,101] or content-distributed network (CDN). Further, these types of information should be shared by the content management server or neighbor network management object to effectively conduct context-based multi-connection or content-based routing. We believe that network-to-network (N2N) communication is needed to share non-real-time data from the network to other networks without configuring an end-to-end connection across two or more networks. A network management object may become a good candidate to share the network information, and it can directly connect with the core network to share other network management objects. However, sharing this information through a newly constructed network connection may cause overhead problems, which can lead to throughput degradation at the core

network side. A technique that can transmit the data without reconfiguring new networks among the networks is necessary to solve this problem. Consequently, an N2N communication protocol is needed for the IoT gateway, which can act as a network management object.

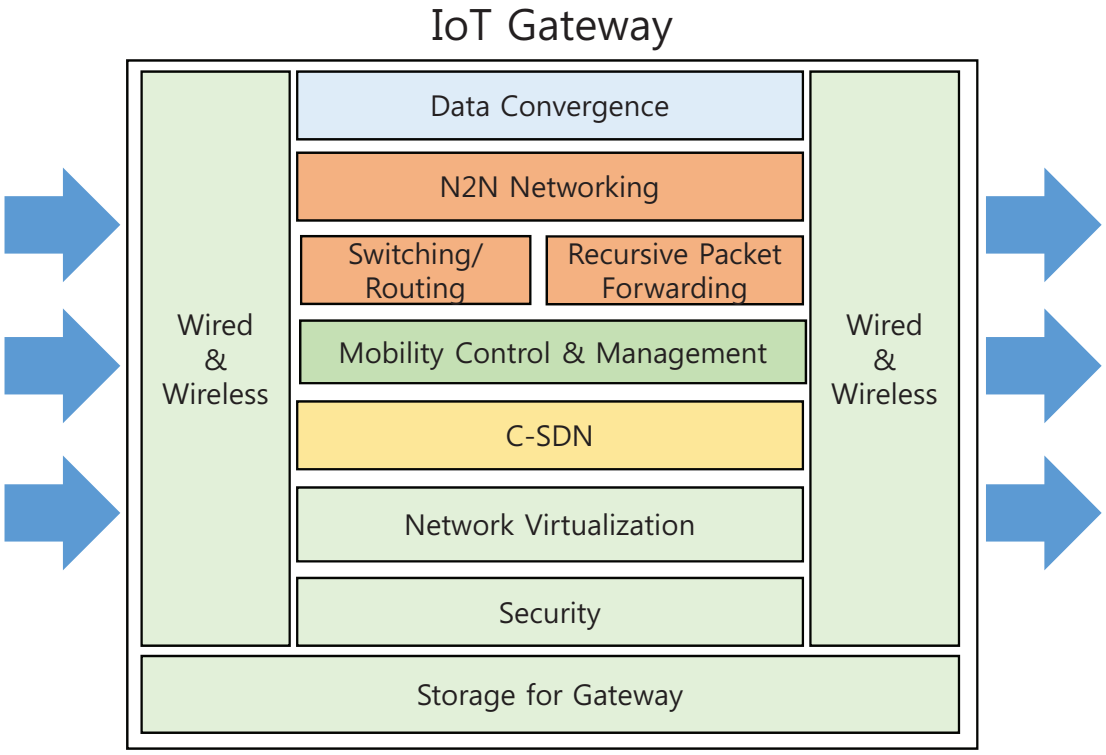

Figure 5. Overview of the IoT gateway.

5.6.2. Routing

One of the important features of the IoT gateway is the routing algorithm, which includes not only the routing for the sub-network of the IoT gateway but also the routing for the affiliated core network. The routing for the internal network, which is the group of nodes in the same subnet, is based on a multi-hop network such as a sensor network [102,103]. This method seems to be sufficient because IoT nodes are primarily composed of the sensors. Nonetheless, it is still a problem to apply in the IoT environment. First, the IoT environment assumes that many sensors or devices may have high mobility. Following this property, devices that belong to the user will probably be connected to the near network management object when the user is in transit. Especially, some types of devices, such as sensors, have a higher probability than the other devices to connect to the nearby network management object owing to limited battery resources. A physical network group may break when a device attempts to connect to the nearby network management object, and managing the network is impossible. Thus, to prevent devices from connecting to different physical groups, a routing algorithm for the nodes attached to the IoT gateway is needed.

Regarding the routing issue within the core network, most of the existing routing algorithms are based on the target node's IP address because a sender transmits to a specific destination node in the existing network. However, targetless requests to acquire information and connection availability is increasing in the IoT environment, as we introduced in Section 4.2. There have already been some researches [104–106] to overcome this challenge. A solution of Bhowmik et al. uses workload-based indexing technique to provide bandwidth-efficiency. Jin et al. [105] selects reliable communication links to node to reduce redundant communication traffic, and Vural et al. [106] caches transient data in the routers to reduce the delay by data item lifetime. However, we propose a new following algorithm,

which utilizes the ID of the things rather than IP address-based routing from the core network, and it can be an example of possible suggestion to overcome this challenge.

Figure 6 presents this scenario when an ID-based routing algorithm is needed.

We assume that device #1 needs some content, whose IDs are *C* and *D*. Device #1 sends a request to IoT gateway #2 that it needs content *C* and *D*. Gateway #2 then knows that device #2 has content *C*, so it sends a message to device #2 to obtain content *C*. However, it does not know the location of content *D*. There are three solutions by which gateway #2 can act to obtain content *D*.

The first method is that gateway #2 performs N2N communication with IoT gateway #1; it may know that gateway #1 has content *D*. Therefore, it sends a request to gateway #1 for content *D*. However, this solution is unavailable when gateway #1 is too far from gateway #2 to perform N2N communication. Another method is that gateway #2 sends a request to a name resolution server that has numerous IDs and locations of content. Gateway #2 can obtain the information that gateway #1 knows the location of content *D*. This solution is simple to realize, but the overhead of maintaining the server is high. The last idea is that gateway #2 performs ID-based routing to find the location of content *D*. In this case, gateway #2 forwards the request packets to nearby networks. When gateway #1 receives the request packet, it replies with the messages and content to gateway #2 using a backward technique. This example is simple to directly embed in the core network, so many novel studies are needed for the content-based routing algorithm.

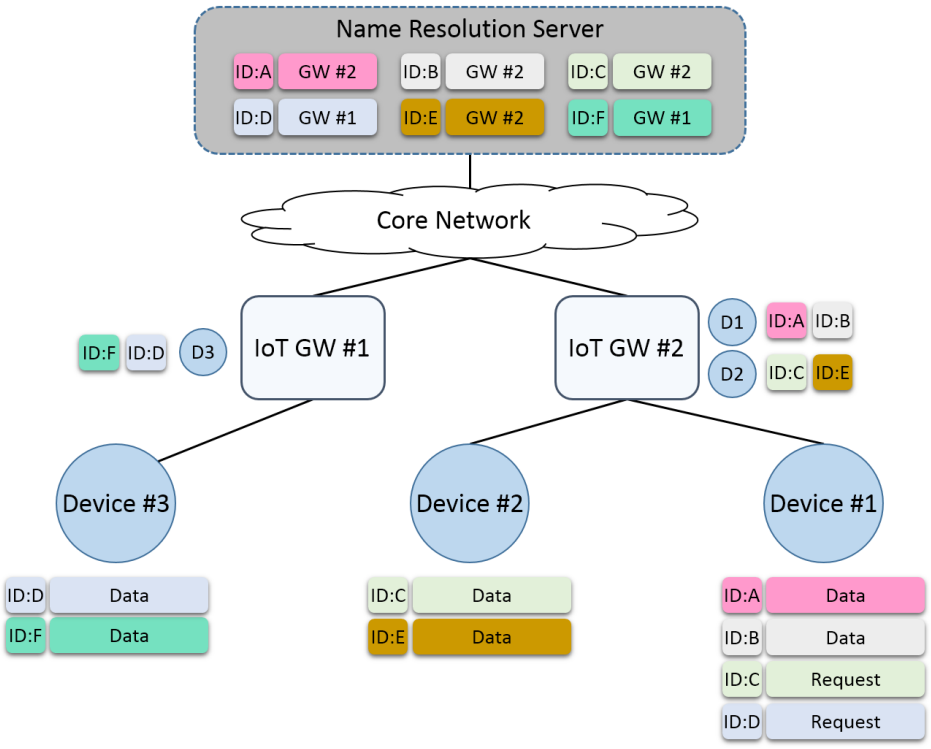

Figure 6. The concept of ID-based routing.

5.6.3. Mobility Control

Mobility is already an important issue in legacy networking and communications. Various devices including cell phones have attributes of mobility, and many studies have proposed mobility control in both the cellular network and IP network. The cellular network, which is proposed to provide plenary communication anywhere, solves some critical problems by reporting its location to the mobility management server. Nonetheless, a cellular network is based on mobility control, which is possible only with an enormous number of servers and extra-large infrastructure. In addition, there is a problem that cellular-based devices consume significant battery resources to maintain connectivity.

In terms of IP networking, some solutions [107,108] such as mobile IP, have been proposed to support mobility. These solutions are difficult to adopt because of message authentication, connection delay, and the complicated management of IP. Thus, mobility control in an IP network is performed only when the client attempts to reconnect when the connection is broken. Although it is a very simple solution, seamless handover and connectivity are not guaranteed. Further, this may lead to degradation of network performance and Quality Of Service (QoS) in the end.

Therefore, a novel concept of mobility support is required. Moreover, it is advantageous to support mobility control by the network management object in terms of reliability instead of constructing a mass server or new infrastructure such as a cellular network. Because the device normally maintains continuity when it moves except during power-off, the nearby network management object can control the mobile devices with ease. For example, when a mobile device identifies that it is moved, it sends the mobility message to its network management object. The network management object then forwards the server's data to nearby objects, and the mobile device can receive the data seamlessly.

5.6.4. Packet Forwarding

As we previously mentioned, searching an appropriate node for content and sending a connection request may cause a considerable delay in a targetless connection. For example, if the user wants to adjust the temperature of the room, every sensor in the room must check the temperature and the number of people within the room. With this information, the sensors send the sensing data to the administrator server in the existing network. Further, the administrator server analyzes the received data to select the rooms in which temperature control is requested and establishes every connection to send the temperature control order. This process is time consuming because it requires numerous steps to merely control the temperature of the time.

To reduce the time delay and improve the efficiency to control the sensors, a targetless connection is required to solve the delay problem in the IoT environment. Additionally, packet forwarding [109,110] or a multi cast technique is appropriate for this type of connection because these algorithms can send multiple data to multiple destinations simultaneously. However, these techniques basically generate many packets for communication, and some technique to improve network efficiency is needed.

5.6.5. SDN for Convergence (C-SDN)

In the IoT environment, SDN is needed from the end-level because each device needs a different traffic rate to satisfy QoS, and guest devices that demand a connection to the IoT gateway must be managed. Further, the content not only uses the data of the local area's sensors or actuators but also needs the data from various networks. In this case, the IoT gateway must provide the data convergence concept to rapidly collect required data and not maintain the expired data or content. For the IoT gateway to be deployed, it is crucial that it have a data convergence unit to process the tremendous volume of data and provide the customized data to the users. It is crucial to have a feature of data aggregation to collect multi modal data, converge with the legacy sensor network's information, and transform the acquired data into transmittable data. However, it is not limited only to collecting the data; rather, it should be able to filter and analyze the data based on the aggregated data to enable the users receive accurate and comfortable service.

5.6.6. Security of IoT gateway

Basically, the IoT gateway manages the IoT devices that are connected to the gateway. The IoT gateway can serve to reply to the query because it has already saved and collected the data from the connected IoT devices. In this case, the IoT device is not required to consider the confidentiality of its data. However, data confidentiality must be considered between the IoT gateway and the requester [111]. The IoT gateway has better computational performance and battery power than the IoT device, so employing a well-known security algorithm is possible. To guarantee privacy, a novel privacy-preserving security algorithm seems to be the best candidate, which can hide private data but

allow the receiver to operate without revealing it. As we previously introduced, this algorithm still does not exist.

Further, the communication medium of the IoT gateway and the IoT device is usually based on wireless communication, where eavesdropping can be possible. Nonetheless, the IoT device is based on a battery, so adoption of a security algorithm can be an overhead. Therefore, a simple and light weight security algorithm or adaptive encryption scheme that can distinguish the data to be encrypted is needed to protect the IoT data.

Node registration and authentication [112] is also an important issue in the security of the IoT gateway. Basically, owing to the mobility of the node and to guarantee connectivity with all devices, there may be many registration types, such as guest, master, and so on. For instance, a guest node is a foreigner of the group with limited communication. The master node can manage all nodes in the group and control the networking of the group even if it is out of the home network. Finally, a member node can be a user's thing and can utilize the network in general. Therefore, flexible node authentication is required to support the various devices that have a connection with the gateway.

6. Conclusions

Current IoT research has been classified in terms of layers of service, platform, network, and device. In this paper, we focused on the network layer, which we believe is the most important part of realizing the IoT environment. We surveyed the IoT network and presented insights about the future IoT network. The success of IoT will be based on the novel architecture of the IoT network. Without a well-designed network architecture for the IoT, IoT services and devices will not seamlessly operate and provide necessary services to the users. To give insight to researchers, we introduced a novel architecture for the IoT network and some techniques that are predictable or certain in such an architecture, such as IoT network management, connection management, grouping and privacy.

Acknowledgments: This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2015R1D1A1A01059151), and Unmanned Vehicles Advanced Core Technology Research and Development Program through the Unmanned Vehicle Advanced Research Center(UVARC) funded by the Ministry of Science, ICT and Future Planning, the Republic of Korea (NRF-2016M1B3A1A01937599).

Author Contributions: Suk Kyu Lee and Mungyu Bae reviewed the articles and wrote the paper. Suk Kyu Lee and Mungyu Bae contributed equally to this work. Hwangnam Kim governed the overall procedure of this research.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

References

1. Yan, Z.; Niemi, V.; Yang, L.T. Key technologies for 5G, the next generation of mobile networks and services. *Int. J. Commun. Syst.* **2016**, *29*, 2328–2329.
2. Zhao, M. Discrete Control in the Internet of things and Smart Environments through a Shared Infrastructure. Ph.D. Thesis, Université Grenoble Alpes, Grenoble, France, 15 September 2015.
3. Chen, L.; Thombre, S.; Jarvinen, K.; Lohan, E.S.; Alen-Savikko, A.K.; Leppakoski, H.; Bhuiyan, M.Z.H.; Bu-Pasha, S.; Ferrara, G.N.; Honkala, S.; et al. Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey. *IEEE Access* **2017**, *5*, 8956–8977.
4. Singh, K.J.; Kapoor, D.S. Create Your Own Internet of Things: A survey of IoT platforms. *IEEE Consum. Electron. Mag.* **2017**, *6*, 57–68.
5. Alam, F.; Mehmood, R.; Katib, I.; Albogami, N.; Albeshri, A. Data Fusion and IoT for Smart Ubiquitous Environments: A Survey. *IEEE Access* **2017**, *5*, 9533–9554.
6. Verma, S.; Kawamoto, Y.; Fadlullah, Z.; Nishiyama, H.; Kato, N. A Survey on Network Methodologies for Real-Time Analytics of Massive IoT Data and Open Research Issues. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1457–1477 .

7. Ngu, A.H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, Q.Z. IoT middleware: A survey on issues and enabling technologies. *IEEE Internet Things J.* **2017**, *4*, 1–20.
8. Thoma, M.; Meyer, S.; Sperner, K.; Meissner, S.; Braun, T. On iot-services: Survey, classification and enterprise integration. In Proceedings of the 2012 IEEE International Conference on Green Computing and Communications (GreenCom), Besancon, France, 20–23 November 2012; pp. 257–260.
9. De, S.; Barnaghi, P.; Bauer, M.; Meissner, S. Service modelling for the Internet of Things. In Proceedings of the 2011 Federated Conference on Computer Science and Information Systems (FedCSIS), Szczecin, Poland, 18–21 September 2011; pp. 949–955.
10. Mayer, S.; Hodges, J.; Yu, D.; Kritzler, M.; Michahelles, F. An Open Semantic Framework for the Industrial Internet of Things. *IEEE Intell. Syst.* **2017**, *32*, 96–101.
11. Dziak, D.; Jachimczyk, B.; Kulesza, W.J. IoT-Based Information System for Healthcare Application: Design Methodology Approach. *Appl. Sci.* **2017**, *7*, 596.
12. Chui, M.; Löffler, M.; Roberts, R. The internet of things. *McKinsey Q.* **2010**, *2*, 1–9.
13. Cha, S.; Ruiz, M.P.; Wachowicz, M.; Tran, L.H.; Cao, H.; Maduako, I. The role of an IoT platform in the design of real-time recommender systems. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 448–453.
14. Qualcomm Connected Experiences, Inc. *A Common Language for the Internet of Everything*; Qualcomm Connected Experiences, Inc.: Cambridge, MA, USA, 2014.
15. AllSeen Alliance. *Open Source IoT to advance the Internet of Everything*; AllSeen Alliance: Beaverton, OR, USA, 2014.
16. OpenIoT Project. Available online: http://openiot.eu/ (accessed on 14 October 2017).
17. Blackstock, M.; Kaviani, N.; Lea, R.; Friday, A. MAGIC Broker 2: An open and extensible platform for the Internet of Things. In Proceedings of the 2010 Internet of Things (IOT), Tokyo, Japan, 29 November–1 December 2010; pp. 1–8.
18. Happ, D.; Karowski, N.; Menzel, T.; Handziski, V.; Wolisz, A. Meeting IoT platform requirements with open pub/sub solutions. *Ann. Telecommun.* **2017**, *72*, 41–52.
19. Jan, S.R.; Khan, F.; Ullah, F.; Azim, N.; Tahir, M. Using CoAP Protocol for Resource Observation in IoT. *Int. J. Emerg. Technol. Comput. Sci. Electron.* **2016**, *21*, 385–388.
20. Levis, P.; Madden, S.; Polastre, J.; Szewczyk, R.; Whitehouse, K.; Woo, A.; Gay, D.; Hill, J.; Welsh, M.; Brewer, E.; et al. TinyOS: An operating system for sensor networks. In *Ambient intelligence*; Springer: Berlin, Germany, 2005; pp. 115–148.
21. Samie, F.; Bauer, L.; Henkel, J. IoT technologies for embedded computing: A survey. In Proceedings of the 2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS), Pittsburgh, PA, USA, 2–7 October 2016; pp. 1–10.
22. McKinsey & Company. *Ten IT-Enabled Business Trends for the Decade Ahead*; McKinsey Company: New York, NY, USA, 2013.
23. Niyato, D.; Alsheikh, M.A.; Wang, P.; Kim, D.I.; Han, Z. Market model and optimal pricing scheme of big data and Internet of things (IoT). In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6.
24. Chang, Y.C.P.; Chen, S.; Wang, T.J.; Lee, Y. Fog Computing Node System Software Architecture and Potential Applications for NB-IoT Industry. In Proceedings of the 2016 International Computer Symposium (ICS), Chiayi, Taiwan, 15–17 December 2016; pp. 727–730.
25. Lee, I. An Exploratory Study of the Impact of the Internet of Things (IoT) on Business Model Innovation: Building Smart Enterprises at Fortune 500 Companies. In *The Internet of Things: Breakthroughs in Research and Practice*; IGI Global: Hershey, PA, USA, 2017; pp. 423–440.
26. Vermesan, O.; Friess, P.; Guillemin, P.; Gusmeroli, S.; Sundmaeker, H.; Bassi, A.; Jubert, I.S.; Mazura, M.; Harrison, M.; Eisenhauer, M.; et al. *Internet of Things Strategic Research Roadmap*; River Publishers: Gistrup, Denmark, 2011; pp. 9–52.
27. Commission of the European Communities. Specific programme implementing horizon 2020: The framework programme for research and innovation (2014–2020). *Off. J. Eur. Union* **2011**, *811*, 965–1041.
28. Horizon 2020: Two Years on. Available online: https://ec.europa.eu/programmes/horizon2020/en/news/horizon-2020-two-years (accessed on 14 October 2017).

29. European Commission. Seventh Framework Programme. In *European Research Cluster on the Internet of Things*; European Commission: Brussels, Belgium, 2010.
30. Coetzee, L.; Eksteen, J. The Internet of Things-promise for the future: An introduction. In Proceedings of the 2011 IST-Africa Conference, Gaborone, Botswana, 11–13 May 2011; pp. 1–9.
31. Council, N. *Disruptive Civil Technologies: Six Technologies with Potential Impacts on Us Interests Out to 2025*; Conference Report; National Intelligence Council: Washington, DC, USA, 2008.
32. Small Business Technology Transfer Program Phase I. Available online: https://www.nsf.gov/pubs/2016/nsf16600/nsf16600.htm/ (accessed on 14 October 2017).
33. KPMG. *China's 12th Five-Year Plan: Overview*; KPMG China: Beijing, China, 2011.
34. Hogan Lovells. *Internet of Things: Innovation with Chinese Characteristics*; Hogan Lovells: London, UK, 2013.
35. Internet Plus. Available online: http://english.gov.cn/2016special/internetplus/ (accessed on 14 October 2017).
36. Headquarters, I.S. *I-Japan Strategy 2015*; National Intelligence Council: Washington, DC, USA, 2009.
37. European Commission—DG INFSO. *ICT-EU Japan Coordinated Call: Objective ICT-2013.10.1*; European Commission—DG INFSO: Auderghem, Belgium, 2013.
38. The Research Project for ICT System Architecture in the Era of IoT. Available online: http://www.mext.go.jp/ (accessed on 14 October 2017).
39. Zhang, H.; Quan, W.; Chao, H.C.; Qiao, C. Smart identifier network: A collaborative architecture for the future internet. *IEEE Netw.* **2016**, *30*, 46–51.
40. European Commission. *Future Internet Research and Experimentation (FIRE+)*; European Commission: Brussel, Belgium, 2014.
41. Future Internet Research and Experimentation (FIRE). Available online: https://www.ict-fire.eu/ (accessed on 14 October 2017).
42. Raychaudhuri, D.; Nagaraja, K.; Venkataramani, A. Mobilityfirst: A robust and trustworthy mobility-centric architecture for the future internet. *ACM SIGMOBILE Mob. Comput. Commun. Rev.* **2012**, *16*, 2–13.
43. Anderson, T.; Birman, K.; Broberg, R.; Caesar, M.; Comer, D.; Cotton, C.; Freedman, M.J.; Haeberlen, A.; Ives, Z.G.; Krishnamurthy, A.; et al. *The Nebula Future Internet Architecture*; Springer: Berlin, Germany, 2013.
44. Naylor, D.; Mukerjee, M.K.; Agyapong, P.; Grandl, R.; Kang, R.; Machado, M.; Brown, S.; Doucette, C.; Hsiao, H.C.; Han, D.; et al. XIA: Architecting a more trustworthy and evolvable internet. *ACM SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 50–57.
45. Ning, H.; Wang, Z. Future Internet of things architecture: Like mankind neural system or social organization framework. *IEEE Commun. Lett.* **2011**, *15*, 461–463.
46. Castellani, A.P.; Bui, N.; Casari, P.; Rossi, M.; Shelby, Z.; Zorzi, M. Architecture and protocols for the internet of things: A case study. In Proceedings of the 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mannheim, Germany, 29 March–2 April 2010; pp. 678–683.
47. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660.
48. Mellouk, A.; Hoceini, S.; Tran, H.A. Quality of experience vs. quality of service: Application for a CDN Architecture. In Proceedings of the 2013 21st International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Primosten, Croatia, 18–20 September 2013; pp. 1–8.
49. Zhiyan, L.; Bao, X.; Xin, W.; Lvtian, W. A Service-Oriented Structure Model of Internet of Things. *J. Converg. Inf. Technol.* **2012**, *7*, 33–40.
50. Cho, K.; Lee, M.; Park, K.; Kwon, T.T.; Choi, Y.; Pack, S. Wave: Popularity-based and collaborative in-network caching for content-oriented networks. In Proceedings of the 2012 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Orlando, FL, USA, 25–30 March 2012; pp. 316–321.
51. Nam, Y.; Lee, C.; Kang, S.; Park, J. Synchronization among CDN edge severs using P2P networking. In Proceedings of the 2015 International Conference on Information and Communication Technology Convergence (ICTC), Cheju-do, Korea, 28–30 October 2015; pp. 466–468.
52. Garmehi, M.; Analoui, M.; Pathan, M.; Buyya, R. An economic replica placement mechanism for streaming content distribution in Hybrid CDN-P2P networks. *Comput. Commun.* **2014**, *52*, 60–70.
53. Suarez, J.; Quevedo, J.; Vidal, I.; Corujo, D.; Garcia-Reinoso, J.; Aguiar, R.L. A Secure IoT Management Architecture Based on Information-Centric Networking. *J. Netw. Comput. Appl.* **2016**, *63*, 190–204.

54. Buddhikot, M.M.; Chandranmenon, G.; Han, S.; Lee, Y.W.; Miller, S.; Salgarelli, L. Design and implementation of a WLAN/CDMA2000 interworking architecture. *IEEE Commun. Mag.* **2003**, *41*, 90–100.
55. Ahmavaara, K.; Haverinen, H.; Pichna, R. Interworking architecture between 3GPP and WLAN systems. *IEEE Commun. Mag.* **2003**, *41*, 74–81.
56. Salkintzis, A.K. Interworking techniques and architectures for WLAN/3G integration toward 4G mobile data networks. *IEEE Wirel. Commun.* **2004**, *11*, 50–61.
57. De Poorter, E.; Moerman, I.; Demeester, P. Enabling direct connectivity between heterogeneous objects in the internet of things through a network-service-oriented architecture. *EURASIP J. Wirel. Commun. Netw.* **2011**, *2011*, 1–14.
58. Internet of Things-Architecture IoT-A Deliverable D1. 3–Updated Reference Model for IoT v1. 5. Available online: http://www.meet-iot.eu/deliverables-IOTA/D1_3.pdf (accessed on 14 October 2017).
59. Gill, M.S. Network Address Translation for Inbound Connections in Paradigm of Private Network. *Int. J. Adv. Res. Comput. Sci.* **2015**, *6*, 40–41.
60. Mayer, K.; Fritsche, W. IP-enabled wireless sensor networks and their integration into the internet. In Proceedings of the First International Conference on Integrated Internet Ad-Hoc and Sensor Networks, Nice, France, 30–31 May 2006; p. 5.
61. Vilalta, R.; Mayoral, A.; Pubill, D.; Casellas, R.; Martínez, R.; Serra, J.; Verikoukis, C.; Muñoz, R. End-to-End SDN orchestration of IoT services using an SDN/NFV-enabled edge node. In Proceedings of the 2016 Optical Fiber Communications Conference and Exhibition (OFC), Anaheim, CA, USA, 20–24 March 2016; pp. 1–3.
62. Volkov, A.; Khakimov, A.; Muthanna, A.; Kirichek, R.; Vladyko, A.; Koucheryavy, A. Interaction of the IoT Traffic Generated by a Smart City Segment with SDN Core Network. In Proceedings of the International Conference on Wired/Wireless Internet Communication, St. Petersburg, Russia, 21–23 June 2017; pp. 115–126.
63. Guo, Y.; Zhu, H.; Yang, L. Service-oriented network virtualization architecture for internet of things. *China Commun.* **2016**, *13*, 163–172.
64. Mijumbi, R.; Serrat, J.; Gorricho, J.L.; Bouten, N.; De Turck, F.; Boutaba, R. Network function virtualization: State-of-the-art and research challenges. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 236–262.
65. European Technical Standards Institute . *Network Functions Virtualisation—Network Operator Perspectives on Industry Progress*; European Technical Standards Institute: Valbonne, France, 2014.
66. Weber, R.H. Internet of Things–New security and privacy challenges. *Comput. Law Secur. Rev.* **2010**, *26*, 23–30.
67. Wurm, J.; Hoang, K.; Arias, O.; Sadeghi, A.R.; Jin, Y. Security analysis on consumer and industrial iot devices. In Proceedings of the 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macao, China, 25–28 January 2016; pp. 519–524.
68. Datta, S.K.; Bonnet, C.; Nikaein, N. An IoT gateway centric architecture to provide novel M2M services. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 514–519.
69. Zachariah, T.; Klugman, N.; Campbell, B.; Adkins, J.; Jackson, N.; Dutta, P. The internet of things has a gateway problem. In Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications, Santa Fe, NM, USA, 12–13 February 2015; pp. 27–32.
70. Min, D.; Xiao, Z.; Sheng, B.; Quanyong, H.; Xuwei, P. Design and implementation of heterogeneous IOT gateway based on dynamic priority scheduling algorithm. *Trans. Inst. Meas. Control* **2014**, *36*, 924–931.
71. Guoqiang, S.; Yanming, C.; Chao, Z.; Yanxu, Z. Design and Implementation of a Smart IoT Gateway. In Proceedings of the IEEE International Conference on and IEEE Cyber, Physical and Social Computing Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), Beijing, China, 20–23 August 2013; pp. 720–723.
72. Chang, C.T.; Chang, C.Y.; Martinez, R.D.B.; Chen, P.T.; Chen, Y.D. An IoT Multi-Interface Gateway for Building a Smart Space. *Open J. Soc. Sci.* **2015**, *3*, 56.
73. Datta, S.K.; Bonnet, C. Smart M2M gateway based architecture for M2M device and Endpoint management. In Proceedings of the 2014 IEEE International Conference on Internet of Things (iThings), and Green Computing and Communications (GreenCom), and Cyber, Physical and Social Computing (CPSCom), Taipei, Taiwan, 1–3 September 2014; pp. 61–68.
74. Wang, Y.; Zhang, Y.; Chen, J. SDNPS: A Load-Balanced Topic-Based Publish/Subscribe System in Software-Defined Networking. *Appl. Sci.* **2016**, *6*, 91.

75. Lantz, B.; Heller, B.; McKeown, N. A network in a laptop: Rapid prototyping for software-defined networks. In Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, Monterey, CA, USA, 20–21 October 2010; p. 19.
76. McKeown, N.; Anderson, T.; Balakrishnan, H.; Parulkar, G.; Peterson, L.; Rexford, J.; Shenker, S.; Turner, J. OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Comput. Commun. Rev.* **2008**, *38*, 69–74.
77. Reitblatt, M.; Canini, M.; Guha, A.; Foster, N. FatTire: Declarative fault tolerance for software-defined networks. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, New York, NY, USA, 12–16 August 2013; pp. 109–114.
78. Kobayashi, M.; Seetharaman, S.; Parulkar, G.; Appenzeller, G.; Little, J.; Van Reijendam, J.; Weissmann, P.; McKeown, N. Maturing of OpenFlow and software-defined networking through deployments. *Comput. Netw.* **2014**, *61*, 151–175.
79. Mendonca, M.; Nunes, B.A.A.; Nguyen, X.N.; Obraczka, K.; Turletti, T. A Survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 1617–1634.
80. Yang, F.; Hughes, D.; Matthys, N.; Man, K.L. The PnP Web Tag: A plug-and-play programming model for connecting IoT devices to the web of things. In Proceedings of the 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Jeju, Korea, 25–28 October 2016; pp. 452–455.
81. Houyou, A.M.; Huth, H.P. Internet of Things at Work: Enabling Plug-and-Work in Automation Networks. In Proceedings of Embedded World Conference 2011, Nuremberg, Germany, 1–3 March 2011.
82. Baron, L.; Klacza, R.; Rahman, M.Y.; Scognamiglio, C.; Friedman, T.; Fdida, S.; Saint-Marcel, F. OneLab: On-demand deployment of IoT over IPv6 Infrastructure as a service for IEEE INFOCOM community. In Proceedings of the IEEE Infocom 2016 Live/Video Demonstration, San Francisco, CA, USA, 10–15 April 2016.
83. Mulligan, G. IPv6 for IoT and gateway. In *Internet of Things and Data Analytics Handbook*; John Wiley Sons: Hoboken, NJ, USA, 2016; pp. 187–196.
84. Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE). Available online: https://www.rfc-editor.org/info/rfc8105 (accessed on 14 October 2017).
85. Savolainen, T.; Soininen, J.; Silverajan, B. IPv6 Addressing Strategies for IoT. *IEEE Sens. J.* **2013**, *13*, 3511–3519.
86. Aloi, G.; Caliciuri, G.; Fortino, G.; Gravina, R.; Pace, P.; Russo, W.; Savaglio, C. Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. *J. Netw. Comput. Appl.* **2017**, *81*, 74–84.
87. Weightless SIG. *Weightless SIG for M2M and Internet of Things (IoT)*; Weightless SIG: Cambridge, UK, 2014.
88. Feng, X.; Liu, X.; Yu, H. A new internet of things group search optimizer. *Int. J. Commun. Syst.* **2016**, *29*, 535–552.
89. Said, O. Analysis, design and simulation of Internet of Things routing algorithm based on ant colony optimization. *Int. J. Commun. Syst.* **2017**, *30*, 1–20.
90. Li, S.; Tryfonas, T.; Li, H. The internet of things: A security point of view. *Internet Res.* **2016**, *26*, 337–359.
91. Lyu, M.; Sherratt, D.; Sivanathan, A.; Gharakheili, H.H.; Radford, A.; Sivaraman, V. Quantifying the reflective DDoS attack capability of household IoT devices. In Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Boston, MA, USA, 18–20 July 2017; pp. 46–51.
92. Doukas, C.; Maglogiannis, I.; Koufi, V.; Malamateniou, F.; Vassilacopoulos, G. Enabling data protection through PKI encryption in IoT m-Health devices. In Proceedings of the 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE), Larnaca, Cyprus, 11–13 November 2012; pp. 25–29.
93. Ma, M.; He, D.; Kumar, N.; Choo, K.K.R.; Chen, J. Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2017**, *PP*, 1, doi:10.1109/TII.2017.2703922.
94. Lee, J.Y.; Lin, W.C.; Huang, Y.H. A lightweight authentication protocol for Internet of Things. In Proceedings of the 2014 International Symposium on Next-Generation MISCs (ISNE), Taoyuan, Taiwan, 7–10 May 2014; pp. 1–2.
95. Yoon, S.; Park, H.; Yoo, H.S. Security issues on smarthome in IOT environment. In *Computer Science and Its Applications*; Springer: Berlin, Germany, 2015; pp. 691–696.
96. Privacy of Big Data in the Internet of Things Era. IEEE IT Special Issue Internet of Anything. Available online: http://arxiv.org/abs/1412.8339 (accessed on 14 October 2017).

97. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134.
98. Alcaide, A.; Palomar, E.; Montero-Castillo, J.; Ribagorda, A. Anonymous authentication for privacy-preserving IoT target-driven applications. *Comput. Secur.* **2013**, *37*, 111–123.
99. Bernabe, J.B.; Hernández, J.L.; Moreno, M.V.; Gomez, A.F.S. Privacy-preserving security framework for a social-aware internet of things. In *Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services*; Springer: Berlin, Germany, 2014; pp. 408–415.
100. Quevedo, J.; Corujo, D.; Aguiar, R. A case for ICN usage in IoT environments. In Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM), Austin, TX, USA, 8–12 December 2014; pp. 2770–2775.
101. Zhang, M.; Luo, H.; Zhang, H. A survey of caching mechanisms in information-centric networking. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1473–1499.
102. Karaboga, D.; Okdem, S.; Ozturk, C. Cluster based wireless sensor network routing using artificial bee colony algorithm. *Wirel. Netw.* **2012**, *18*, 847–860.
103. Goyal, D.; Tripathy, M.R. Routing protocols in wireless sensor networks: A survey. In Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies (ACCT), Rohtak, India, 7–8 January 2012; pp. 474–480.
104. Bhowmik, S.; Tariq, M.A.; Grunert, J.; Rothermel, K. Bandwidth-efficient content-based routing on software-defined networks. In Proceedings of the 10th ACM International Conference on Distributed and Event-based Systems, Irvine, CA, USA, 20–24 June 2016; pp. 137–144.
105. Jin, Y.; Gormus, S.; Kulkarni, P.; Sooriyabandara, M. Content centric routing in IoT networks and its integration in RPL. *Comput. Commun.* **2016**, *89*, 87–104.
106. Vural, S.; Wang, N.; Navaratnam, P.; Tafazolli, R. Caching Transient Data in Internet Content Routers. *IEEE/ACM Trans. Netw.* **2017**, *25*, 1048–1061.
107. Fu, Y.; Yang, L. Sensor mobility control for multitarget tracking in mobile sensor networks. *Int. J. Distrib. Sens. Netw.* **2014**, *2014*, 278179.
108. Jalin, F.A.; Othman, N.E. A review of mobile IP protocol for the implementation on dual stack mobility management. *J. Theor. Appl. Inf. Technol.* **2016**, *87*, 527.
109. Antonini, M.; Cirani, S.; Ferrari, G.; Medagliani, P.; Picone, M.; Veltri, L. Lightweight multicast forwarding for service discovery in low-power IoT networks. In Proceedings of the 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 17–19 September 2014; pp. 133–138.
110. Hail, M.A.M.; Amadeo, M.; Molinaro, A.; Fischer, S. On the Performance of Caching and Forwarding in Information-Centric Networking for the IoT. In *Wired/Wireless Internet Communications*; Springer: Berlin, Germany, 2015; pp. 313–326.
111. Han, J.H.; Jeon, Y.; Kim, J. Security considerations for secure and trustworthy smart home system in the IoT environment. In Proceedings of the 2015 International Conference on Information and Communication Technology Convergence (ICTC), Cheju-do, Korea, 28–30 October 2015; pp. 1116–1118.
112. Dhillon, P.K.; Kalra, S. Secure multi-factor remote user authentication scheme for Internet of Things environments. *Int. J. Commun. Syst.* **2017**, doi:10.1002/dac.3323.