Future Generation Computer Systems 88 (2018) 606–613

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Toward integrated Cloud–Fog networks for efficient IoT provisioning: Key challenges and solutions

Limei Peng [a], Ahmad R. Dhaini [b], Pin-Han Ho [c,*]

[a] School of Computer Science and Engineering, Kyungpook National University, Daegu 41566, Republic of Korea
[b] Department of Computer Science, American University of Beirut, P.O. Box: 11-0236, Riad El Solh, Beirut, 1107-2020, Lebanon
[c] Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue W., Waterloo, ON N2L 3G1, Canada

HIGHLIGHTS

- We first provide a literature review of the work related to the integration of Cloud–Fog networks.
- We then present iCloudFog, a scalable and agile integrated Cloud–Fog architecture that provisions Fog and IoT networks dynamically based on the Cloud and IoT nodes' availability and capability, and network requirements.
- We identify the key challenges that emerge in the process of constructing the iCloudFog framework, such as network dimensioning, security and IoT job scheduling, and indoor localization, and suggest viable approaches to address these challenges.

ARTICLE INFO

Article history:
Received 19 March 2018
Received in revised form 30 April 2018
Accepted 9 May 2018
Available online 12 May 2018

Keywords:
Cloud computing
Edge computing
Fog computing

ABSTRACT

Fog computing has been proposed as one of the promising technologies for the construction of a scalable network infrastructure in the user's vicinity, with the purpose of serving the tremendous amount of daily generated latency-sensitive Internet-of-Things (IoT) data. In provisioning the emerging IoT data in addition to the legacy Cloud services, the Cloud and Fog form a natural continuum of one another and the integration of these two key technologies would offer a promising infrastructure full with IoT resources for IoT data provisioning.

In this article, we present iCloudFog, a reconfigurable architecture that enables an agile integration of Fog and Cloud networks. iCloudFog allows to construct different Fog types (i.e., wireless, wired, or hybrid) to fit the different characteristics of IoT devices and data, and Fog nodes. Due to its nature, iCloudFog presents several unique key research challenges that have not yet been addressed in existing literatures, such as network dimensioning and configuration, resource management/QoS, security/privacy, and positioning/localization. We discuss these challenges and suggest promising approaches to resolve them. Effective design and implementation of solutions based on the suggested approaches would allow iCloudFog to play a salient role towards the successful provisioning of future IoT applications and services.

1. Introduction

The era of Internet Technology (IT) has unconsciously migrated to Data Technology (DT) with the proliferation of mobile devices such as smart phones, tablets, wearable devices, etc., the total number of which is predicted to approach 50 billion by 2020 [1]. Billions of these "things" are generating more than two Exabytes of everyday Internet-of-Things (IoT) data featured by *3Vs*, i.e. *volume*, *variety*, and *velocity* [2–5]. Provisioning the *3Vs* IoT data in the Cloud datacenter networks (DCNs) could be subject to serious technical difficulties, mostly due to the fact that moving all generated IoT data at the devices to the Cloud for analysis would saturate the network capacity and cause unbearable latency, eventually failing the premises of the IoT services.

Specifically, Cloud datacenters (DCs) have been widely deployed by leading IT companies such as Cisco, Google, Microsoft, Amazon, etc., to provide the computing/storage resources to enterprises/individuals under the leasing models of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS), etc., [6,7]. Even though Cloud DCs under these leasing models work well for heavyweight and latency-tolerant service requests, they are inherently inappropriate to serve the pervasive *3Vs* IoT data with stringent real-time requirements [8,9], mainly due to the long distance between DCs and end-users, in addition to the centralized control and management on DCs. Nonetheless, it

* Corresponding author.
E-mail addresses: auroraplm@knu.ac.kr (L. Peng), ahmad.dhaini@aub.edu.lb (A.R. Dhaini), p4ho@uwaterloo.ca (P.-H. Ho).

https://doi.org/10.1016/j.future.2018.05.015
0167-739X/

was forecasted that by year 2020, up to 92% of workloads should still be processed by Cloud DCs [7]. Cloud DCs will continue to be a significant infrastructure in provisioning the legacy Cloud and the emerging IoT applications.

It becomes apparent that an additional control layer in between the Cloud and the IoT devices situated in the vicinity of the IoT devices for governing the data locality and mobility will be necessary toward the success of provisioning the *3Vs* IoT data. With this regard, we have seen extensive research interest shifted from the network core to the edge in the past a few years, generally termed Edge Computing (EC). Based on the concept, many vendor-specific control platforms emerged, including mobile Cloud Computing (MCC), mobile Edge Computing (MEC), cloudlet, etc. [10–12]. As a similar alternative, Fog Computing (FC) has been coined for IoT services by Cisco in 2012 and since then, it has been receiving tremendous attention from academia and industry [1,13].

The key concept behind FC is to take advantage of the end-user devices located at (or near) the edge, which would be rich in IoT resources, i.e. storage, compute, and bandwidth, to process the real-time data of neighboring Things in a one-hop manner so as to minimize the latency. The Cloud and Fog (which is a "Cloud closer to the ground") are not binary options, in contrast, they are an interdependent and mutually beneficial continuum [14]. For instance, Cloud still coordinates the Fogs and the devices in a Fog as well as handles heavyweight data, nonetheless, the delay-sensitive data can be processed and responded by Fog nodes that are in the vicinity of the IoT devices [15,16].

Even though significant industrial and/or academic progresses have been achieved on either the Cloud or the Edge, respectively, very little progress has been witnessed on an integrated Cloud–Fog framework. Researchers have become aware of this missing piece and have realized the significance of such an integrated architecture, which can optimize the power of both Cloud and Fog to speed up the development of IoT. Research in this field has just recently kicked off, with very little progress being made [17].

In this article, we first provide a literature review of the studies related to the integration of Cloud–Fog networks. We then present iCloudFog, a scalable and agile integrated Cloud–Fog architecture that provisions IoT resources of Cloud and/or Fog to IoT data requests dynamically based on the Cloud/Fog nodes' availability and capability as well as the IoT data requirements. In the process of constructing the iCloudFog framework, we identify the key challenges being network dimensioning, IoT job scheduling with consideration on QoS, security/privacy, and indoor localization/positioning, and suggest viable approaches to address these challenges.

The remainder of the article is organized as follows. In Section 2, we discuss the differences between Cloud Computing (CC), Edge Computing (EC), and Fog Computing (FC), and then present a literature review. In Section 3, we present the proposed iCloudFog architecture. In Section 4, we discuss they key challenges in iCloudFog such as network dimensioning, resource management/job scheduling, security, and indoor localization/positioning, and present viable solutions. In Section 5, we summarize the article and present the conclusions.

2. Literature review

In this section, we first briefly discuss the differences between CC, EC, and FC, and then present an overview of the related works. Finally, we discuss the key challenges and issues need to be addressed.

2.1. Cloud vs. edge vs. fog computing

It is important to note the differences between EC and FC, and how FC stands in relation to CC. In fact, there are essential differences between EC and FC. Firstly, different from existing EC paradigms, FC can be expanded into the core network such that both the edge and core components (e.g., core routers, regional servers, switches, remote nodes, etc.) can become a computational infrastructure in FC [16,18]. Secondly, unlike EC, FC can extend Cloud-based services like IaaS, PaaS, and SaaS to the edge of network as well. Therefore, FC is foreseen to be more promising for supporting IoT in the future.

Meanwhile, CC and FC form a mutual beneficial continuum; namely, CC would still be the main enabler for legacy services, which are heavyweight and latency-tolerant, whereas FC takes charge of the lightweight and latency-sensitive IoT data such as Tactile services and applications [19]. In this continuum, the front-end process, which includes a collection of data from the IoT devices mainly relies on wireless technologies such as WiFi, Bluetooth, ZigBee. Conversely, the back-end process, which provides the collected IoT data with compute/storage/bandwidth resources on a Fog node or a Fog network for analysis, may rely on either a wireless, a wired, or a hybrid technology. Therefore, wired nodes in the Cloud may also be part of the Fog. As such, constructing efficient integrated Cloud–Fog networks is essential for provisioning legacy Cloud data and emerging IoT data in a more efficient way.

2.2. Related works

An integrated Fog and Cloud archetype, namely IFCIoT, was proposed in [17] to address the architectural challenges associated with the realization of scalable IoT/CPS (cyber–physical systems) applications leveraging FC.

Aazam et al. proposed a layered architecture for FC to address resource management challenges, such as resource prediction, allocation, and pricing in Fog servers [20]. Here, a probability-based model was presented, which considers the type, traits, and characteristics of Fog customers to make resource management decisions.

N. Wang et al. developed a framework for edge node resource management (ENORM) which addressed the resource management problems of provisioning edge nodes for cloud applications. A provisioning mechanism has been proposed by considering handshaking, deployment of workloads and termination of edge services. The results showed that when compared to a cloud-only model, the application latency is reduced between 20%–80% in a given location for the fog computing based use-case employing ENORM [21].

Bittencourt et al. proposed a layered architecture to facilitate mobility of connected IoT nodes [22]. In their approach, a virtual machine (VM) instance is created for each IoT node connected to the Fog server. When an IoT device crosses the radio boundary of the Fog server, it is handed-off to another Fog server by exchanging a snapshot of the IoT device's VM instance.

Jalali et al. showed that FC may help to save energy in CC [23]. They compared the energy consumption of applications using centralized DCs in CC with applications using nano data-centers (nDCs) in FC. They also showed that the best energy savings using nDCs is achieved for applications that generate and distribute a large amount of data at the end-user premises, which is not frequently accessed (e.g., home video surveillance).

Vatanparvar et al. investigated the energy management-as-as-service over the FC platform in different domains, by implementing two prototypes for home energy management (HEM) and micro-grid-level energy management, respectively [24].

Table 1
Taxonomy of key research.

iCloudFog research	Related work
Resource management	[20,21]
Mobility/handover	[22]
Energy efficiency	[23,24]
Network virtualization: SDN, NFV	[25–28]
Network dimensioning	N/A
Security	N/A
Localization/positioning	N/A

The authors in [25–28] discussed the role of technologies such as software defined networking (SDN) and network function virtualization (NFV) in EC and FC for supporting IoT services. Specifically, *Liang et al.* focused on SDN in radio access networks (RANs) with FC [26], whereas *Baktir et al.* gave an overall review on how EC can benefit from SDN [27]. *Ojo et al.* proposed an SDN-IoT architecture with NFV implementation with specific choices for where and how to adopt SDN and NFV approaches to meet the requirements of IoT [28]. Finally, *Paglieranni et al.* proposed in [25] to add hardware accelerators and SDN/NFV in the network nodes to support FC, which could significantly improve the network performance.

2.3. Challenges

A taxonomy of the key research challenges in integrated Cloud–Fog networks and the related works are illustrated in Table 1. As noticed, most existing literatures, which assume pre-constructed Fog networks, focused on addressing the issues of energy efficiency, resource management, the application of SDN/NFV, and mobility. There are still many features and problems to be explored and addressed.

For instance, no research has ever considered the important feature that a Fog node can either be wired or wireless and how Fogs can be dynamically dimensioned and constructed by incorporating the IoT data features and Cloud/Fog node capabilities. In addition, even though some literature did address resource management challenges in FC, none has considered how to optimize the IoT resources while maximally satisfying the quality-of-service (QoS) of IoT data requirements simultaneously.

Similarly, research on resource management/job scheduling with considerations on privacy preservation is still blank. In addition, very little work that addresses user mobility and security can be found, except the one addressing it from the architecture perspective based on virtual machine [22]. Finally, no work considered the indoor localization/positioning for supporting the IoT data locality and user mobility in Fog.

The above aspects of the integrated Cloud and Fog framework are critical to boost the IoT development and thus require urgent investigation. In this article, we touch upon these missing pieces, and suggest viable approaches for solving them.

3. Proposed iCloudFog architecture

3.1. Overview of iCloudFog framework

The proposed iCloudFog architecture is illustrated in Fig. 1. The physical network architecture is composed of the optical backbone interconnect, an access network, and the IoT end-user devices. The abstraction of the physical architecture comprises three layers, namely Cloud, Fog and IoT. With iCloudFog, three types of communication are defined: Cloud-to-Fog (C2F), Fog-to-Fog (F2F), and Fog-to-Thing (F2T).

To ensure high efficiency of the iCloudFog operations, particularly in dealing with data locality in the presence of user mobility and traffic variations, it is essential to devise an effective approach for dynamically constructing small-scale Fogs by which the four types of communication can be efficiently initiated and provisioned. different from the Cloud, which is equipped with fixed DCs that intercommunicate on top of the optical backbone network, a Fog network is ad-hoc and heterogeneous in nature due to the diversity of the Fog nodes (i.e., could be wired, wireless, or hybrid fiber-wireless) and dynamic ability of the IoT devices to sporadically join and leave the Fog. Thus, the scale of each Fog network is highly adaptive to the data characteristics of the IoT devices in terms of *3Vs* IoT data, which are further used to determine the Fog nodes and their connectivity.

3.2. Dynamic fog construction

With iCloudFog, the diverse IoT end-devices collect different types of IoT data of different requirements such as latency-sensitive or not, heavyweight or lightweight, the security level, bandwidth-hungry or not, etc. Therefore, a Fog is expected to support multiple IoT data types. A Fog is not likely to work well for all kinds of IoT data types and thus we can feature a Fog for one or more specific IoT data type(s) so as to achieve optimal IoT resource utilization and good quality of service (QoS).

Secondly, since the mobility and velocity of changes in IoT data's entrance/exit are dynamic, Fogs should have their own lifetime and should be dynamically dimensioned and (re)configured. To maximize the power of a Fog node in a given Fog type, a timely threshold value for the lifetime a Fog node can be configured, and then its performance can be tracked to adjust the threshold accordingly.

Finally, to provision the huge volume of IoT data using the limited IoT resources efficiently, the Fog scale/size should be carefully defined. A sizable Fog may generate long communication latency, while a very small Fog may lack sufficient IoT resources for compute and storage. This issue can be addressed by performing effective network dimensioning that takes into account the capabilities and requirements of all Fog nodes and IoT devices.

Fig. 2 illustrates the different Fog types that can be constructed in iCloudFog. Namely, three types are defined: 1) Wireless Fog consisting of wireless nodes only (i.e., *Fog* 1); 2) Wired Fog consisting of wired nodes only (i.e., *Fog* 3); and 3) Hybrid wireless-wired Fog consisting of both wired and wireless nodes (i.e., *Fog* 2). For tasks with stringent latency requirement, a suitable Fog network would be one with low communication delay and rich IoT resources. For heavyweight tasks without strict latency requirement, the wired type such as *Fog* 3 can be employed.

Fig. 2 also shows how a pool of Fog nodes can be shared with the Cloud to enable distributed storage, computing and processing of IoT latency-insensitive data, thereby exploiting the Cloud–Fog continuum. It also shows how some IoT devices, can act as Fog nodes once deemed capable of acting as computing, bandwidth and storage providers for handling real-time delay-sensitive IoT data. Meanwhile, DCs in the Cloud continue to handle heavyweight, computation intensive and delay-tolerant data.

3.3. Communication types

Once the Fogs are constructed, defining the C2F, F2F, and F2T communications would be essential to enable seamless operation of iCloudFog. For instance, C2F and F2F can be based on existing legacy communication technologies in optical networks such as wavelength division multiplexing (WDM). The F2T communication would be based on existing integrated technologies such as Fiber-Wireless networks, since a lot of Fogs are expected to consist of both wired and wireless Fog nodes. Here, SDN can be used to control the C2F and F2F since a wired Fog node is more likely to be selected as a gateway for communications with Cloud or other

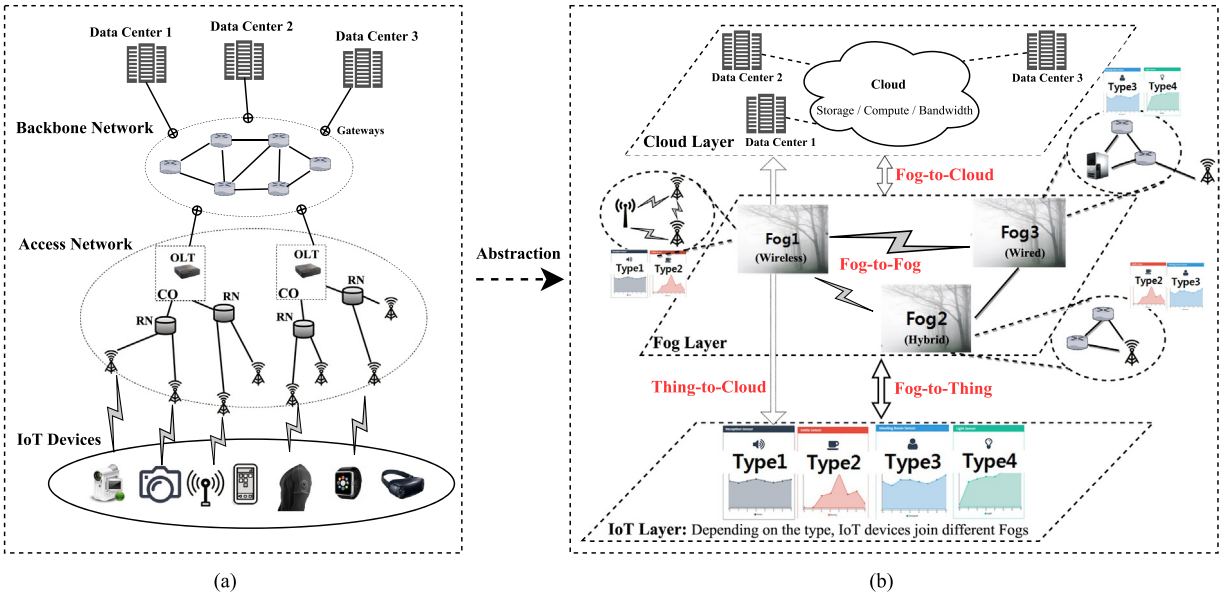

Fig. 1. (a) Physical network connection; (b) Illustration of iCloudFog.

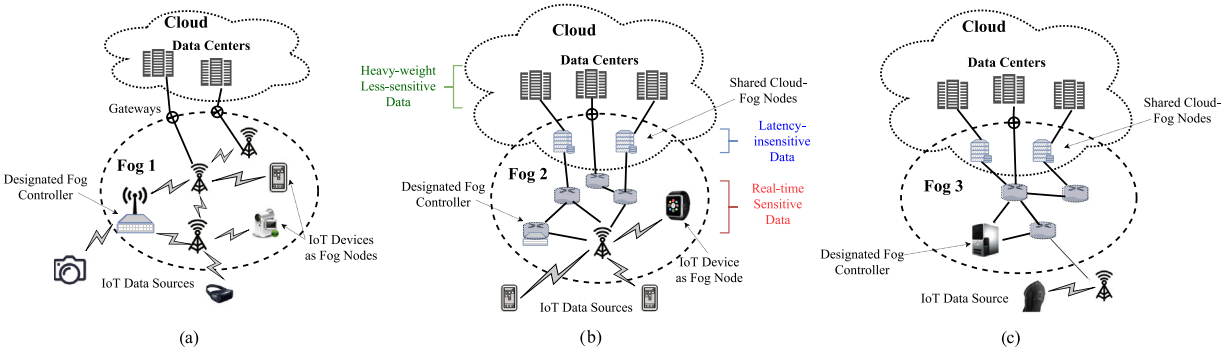

Fig. 2. Fog types in iCloudFog: (a) Wireless; (b) Hybrid Wired-Wireless; (c) Wired.

Fogs; in which case, the control is similar to that of the existing SDN technologies required for backbone networks.

For F2T, which is kind of an intra-Fog communication, dedicated Fog controllers can be employed at some wireless point or as additional control function in exiting wired Fog nodes. In case the operator prefers to have all Fog nodes with control ability, a wired node can be designated as a centralized controller based on models such as Master/Slave, Cluster, or peer-to-peer. For a Fog consisting of similar Fog nodes as shown in Figs.2a and 2c, the round-robin scheme can be employed to designate a Fog controller, with its efficiency in controlling Fogs being evaluated to decide whether or not to employ it again in the future.

4. Key challenges and promising solutions in iCloudFog

The integrated Cloud–Fog (iCloudFog) architecture requires addressing several research challenges so as to enable effective operation. In this section, we focus on four primary ones, namely network dimensioning and configuration, QoS and privacy-aware resource management and job scheduling, security, and positioning/localization. We discuss potential approaches to effectively address these challenges.

4.1. Network dimensioning and configuration

The dynamic nature of Fog networks requires an effective network dimensioning mechanism that takes into account the availability of resources and salient network parameters such as transmission bandwidth need and contribution, computing/storage need and contribution, energy efficiency, security, and mobility. This mechanism must also be computationally fast to adapt to the dynamic nature of Fog networks, where nodes (i.e., IoT devices) join and leave in small timespans.

Fig. 3 illustrates the Fog dimensioning problem and the steps taken to solve it. First, the set of current Fog nodes (i.e., fixed Fog nodes, shared Cloud–Fog nodes) and candidate ones (i.e, IoT devices) are abstracted and classified based on their type and proximity to one another. This step helps determine the network size and the constraints imposed (e.g., fixed versus wireless, range of coverage for the wireless node, etc.). Second, the eligibility of a node to be part of the Fog network is determined based on its demand and contribution. Namely, let the set of m Fog networks to be constructed be denoted as $F = \{F_1, F_2, \ldots, F_i, \ldots, F_m\}$, such that a Fog network F_i comprises n current/fixed and candidate Fog nodes, defined as $F_i = \{f_{i,1}, f_{i,2}, \ldots, f_{i,j}, \ldots, f_{i,n}\}$. Every Fog node $f_{i,j} \in F_i$ has a demand $D(f_{i,j})$ and a network contribution $C(f_{i,j})$, such that $D(f_{i,j})$ and $R(f_{i,j})$ are a function of the bandwidth, computing, storage, and energy consumption/battery life. Thus, assuming that node $f_{i,j}$ is "interested" in being a Fog service provider, it is taken as

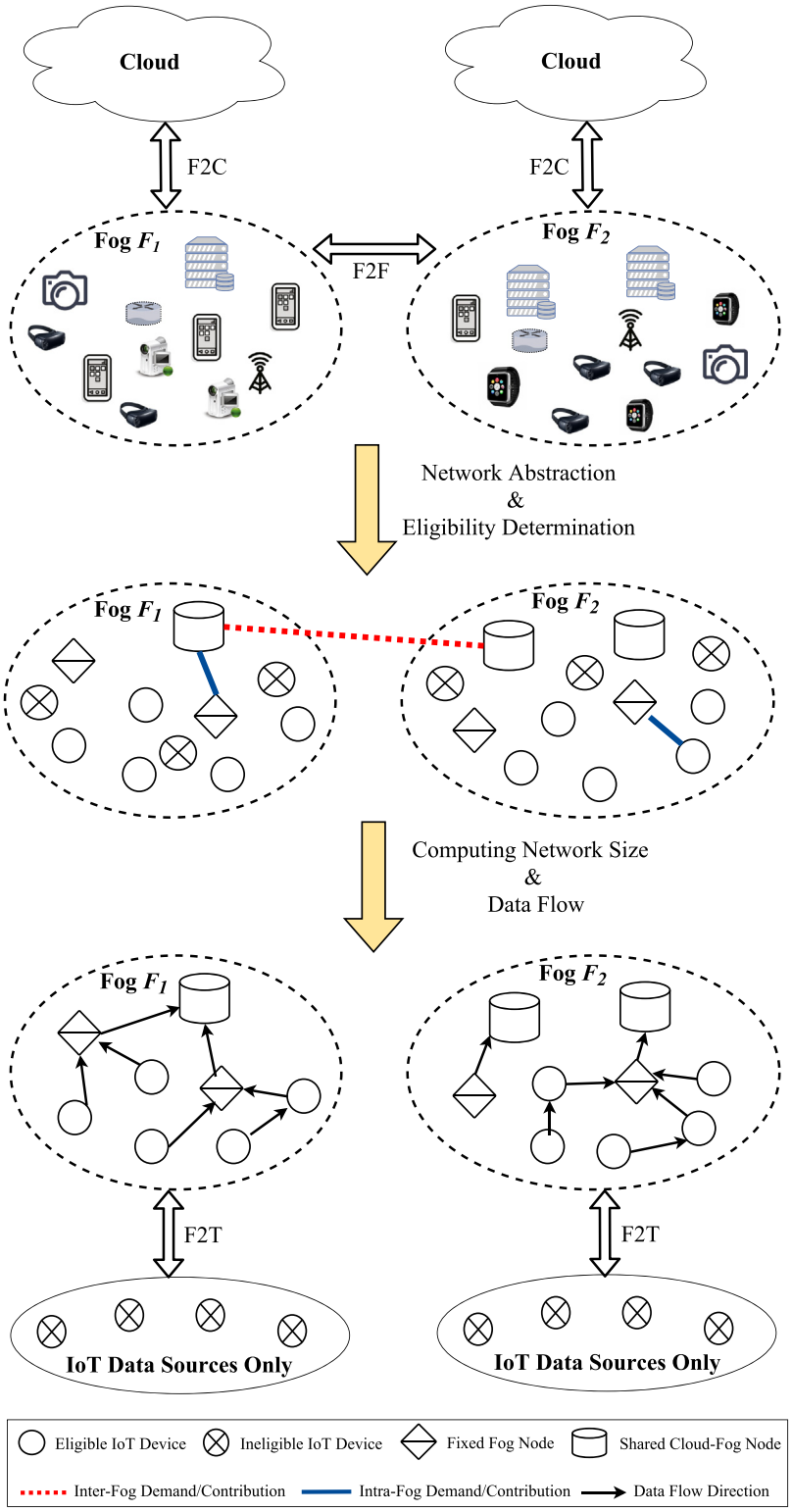

Fig. 3. Illustration of the networking dimensioning problem in iCloudFog, and the steps taken by the proposed approach.

eligible if $C(f_{i,j}) - D(f_{i,j}) > 0$; otherwise, if it is of type of IoT, it will be taken as an IoT data source only; whereas if it is a fixed node, it is not included in the constructed network (e.g., it may be running at maximum capability). The IoT device information related to its interest in being a Fog provider, and its demand/contribution are sent to the designated controller every time the IoT device is hooked into the network.

The demand and contribution can be classified into two types: 1) "inter-Fog" where a current Fog node (fixed or shared Cloud–Fog) in say Fog F_1, requires to serve a neighboring Fog network, say Fog F_2 (e.g., if an IoT device roams from one Fog network to another, a request is placed between Fog nodes, which adds communication overhead), or with its corresponding Cloud (e.g., when the shared

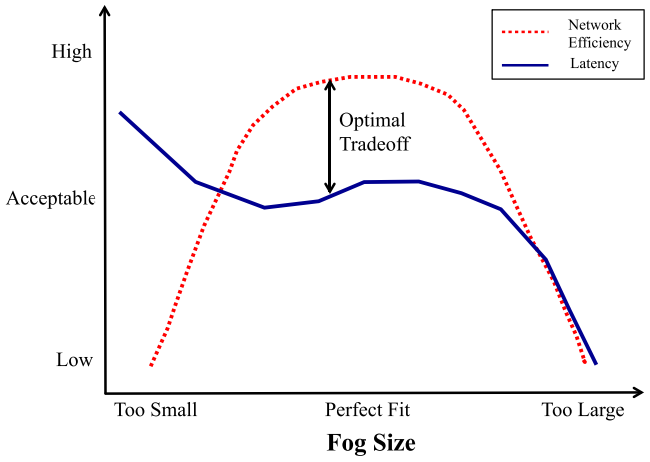

Fig. 4. Relationship between Fog size, latency, and network efficiency.

Cloud–Fog server requires to serve or be served by a DC); 2) "intra-Fog" where any two Fog nodes require to serve and be served by another node within the same Fog.

Once the set of eligible nodes are selected, a network is dimensioned according to the overall network demand. In general, there is a tradeoff between network size, network efficiency and latency. As illustrated in Fig. 4, network efficiency significantly downgrades when the network size increases beyond its optimal value; this can be due to the high messaging overhead, and/or low network utilization due to the allocation of extra unnecessary resources. Thus, not all eligible nodes may be necessary included in the constructed network, especially if they cannot serve the IoT data requests (e.g., delay-sensitive applications require provisioning IoT nodes due to their proximity to the users, etc.), and vice versa. Dimensioning the Fog size also presents a trade-off between network efficiency and IoT data latency; thus, the Fog network must be sized according to the foregoing best trade-off.

Finally, the route of data flows among the Fog nodes is provisioned based the QoS, mobility and security requirements of each IoT request (as we will see next). The devised algorithm can be implemented at the designated Fog controller, which will broadcast the network configuration to all nodes after every (re)configuration run.

4.2. Resource management/job scheduling

For C2F and F2F, which are a kind of inter-Fog communication, most of the legacy strategies on resource management/job scheduling for the core networks can be used directly. Thus, we will focus on the issues related to intra-Fog communication, i.e., F2T.

Let each Fog node $f_{i,j}$ within the constructed Fog F_i be featured by $f_{i,j} = \{(fm_{i,j}, fl_{i,j}, fp_{i,j}), (fs_{i,j}, fc_{i,j}, fb_{i,j})\}$. The first tuple $(fm_{i,j}, fl_{i,j}, fp_{i,j})$ represents the invisible attributes of Fog node $f_{i,j}$ such as mobility (i.e., ability to move, and approximate range), latency (which is the estimation of communication delay with the Cloud, other Fogs or other Fog nodes), and privacy (i.e., the credit of its privacy ability when serving IoT data which can be scored based to its performance history), respectively. The second tuple $(fs_{i,j}, fc_{i,j}, fb_{i,j})$ represents the available IoT resources, where $fs_{i,j}$, $fc_{i,j}$, and $fb_{i,j}$ represent the available storage, compute, and bandwidth resources of Fog node $f_{i,j}$, respectively. Meanwhile, there is a set of k tasks classified according to the IoT data collected in F_i, denoted as $T_i = \{t_{i,1}, t_{i,2}, \ldots, t_{i,j}, \ldots, t_{i,k}\}$. Each task is represented by $t_{i,j} = \{(tl_{i,j}, tq_{i,j}), (ts_{i,j}, tc_{i,j}, tb_{i,j})\}$. The first tuple $(tl_{i,j}, tq_{i,j})$ indicates the latency requirement $tl_{i,j}$, and security level $tq_{i,j}$, respectively. The second tuple $(ts_{i,j}, tc_{i,j}, tb_{i,j})$ indicates the requirements on the IoT resources, namely the storage $ts_{i,j}$, compute $tc_{i,j}$, and bandwidth $tb_{i,j}$, required to complete $tl_{i,j}$, respectively. As such, the resource management/job scheduling problem can be then normalized to an optimization problem of mapping F_i to T_i with satisfactory QoS and IoT resources.

As illustrated in Fig. 5, a Fog can be taken as a virtual pool of resources with different attributes. Meanwhile, the IoT data of a Fog is represented by an array of tasks waiting to be served, such that each task has different latency, security and network demands. If each task is divided into multiple sub-tasks, which can be executed on different Fog nodes, then either a Fog node or a set of Fog nodes can be selected to execute the task. However, the latter can only occur if the sum of available IoT resources provided by all the selected Fog nodes can satisfy the task's demands.

Different from most of the existing work which only consider a single resource type (i.e., either storage, computing, or bandwidth) with very limited to no consideration on QoS, each IoT task in a Fog has multiple dimensions since it requires all the foregoing resources; meanwhile, the Fog node attributes such as communication delay, security reputation, and mobility should be considered as inputs to satisfy the QoS demands. This makes the problem much more complicated, yet it enables a higher degree of network flexibility than the existing solutions currently considered for the CC and EC paradigms.

4.3. Security and data privacy

Instant user authentication is a highly desired feature in IoT data transmission where power conservation is a critical requirement. Thus, physical-layer assisted message authentication schemes over the public key infrastructure (PKI) can be employed to achieve light-weighed communication in the F2T interface. Here, fast authentication can be performed for each message by identifying the uniqueness regarding the time-space characteristics of the channel responses. This can be achieved by employing a confidence degree (CD) based framework that defines how likely the currently received signal is launched by the same transmitter as in the previously received ones via the sensed channel responses.

The CD is an estimation on whether two received signals should be considered from a common transmitter, mostly based on the two-dimensional (i.e., time and space) channel response values sensed at the receiver side. Normally, two signals could travel along the same (or very similar) channels while at different time points, and in this case the two signals would be taken as from a common transmitter. As such, a received packet can be authenticated in sub-microseconds instead of going through additional software/hardware processing.

Consequently, a secure authentication protocol according to the trust model and the conventional PKI can be implemented in the IoT devices. The proposed trust model would provide the estimated CD values of two signals of different time points, which will be used to assist the authentication process. For example, the development of the trust model can take the two signals as input, and use statistical signal processing techniques mostly based on convolutional correlation functions that will yield CD, for evaluating the similarity of the two inputs. Finally, the integration of the trust model with the PKI can help develop a physical-layer assisted authentication (PAA) scheme.

4.4. Positioning and localization

Capturing the instant precise positions of all IoT devices is a salient building block for enabling a ubiquitous and seamless iCloudFog operation. This is particularly critical when the Things

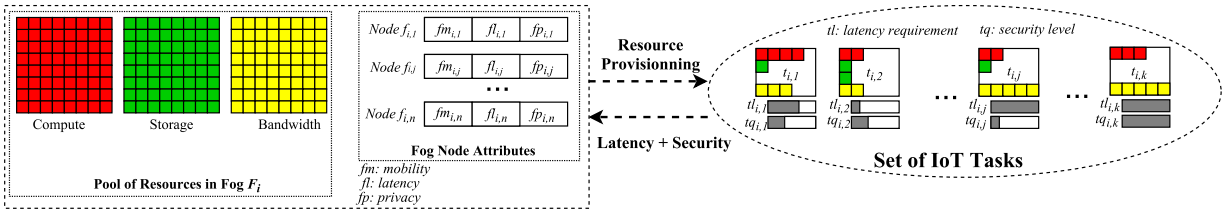

Fig. 5. QoS and Security-aware resource allocation in iCloudFog.

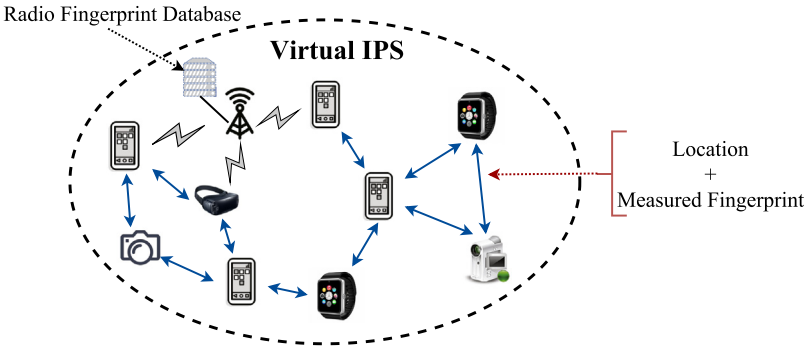

Fig. 6. Virtual Indoor Positioning System construction in iCloudFog.

are located indoor, shaded from GPS and cellular signals. Fortunately, several promising indoor positioning solutions already exist; these can be exploited to serve that goal. For instance, Google's Indoor Positioning System (IPS) is characterized by a traditional site survey process as an offline training phase [29], in order to build a radio fingerprint database at every location of the indoor area.

Subsequently, the IPS would provide a user's location by retrieving the matched fingerprints from the database. Similarly, Nokia's High Accuracy Indoor Positioning (HAIP) system [29,30], manipulates the directional position beacons in the coverage area using the Bluetooth Low Energy (BLE) technology, so as to achieve up to 0.3m position accuracy for indoor users, at the expense of extra equipment and accurate installation in the training phase. The training effort is sometimes too expensive or even impossible.

An alternative solution for achieving the indoor positioning capability would be to take advantage of the Inertial Navigation System (INS), which is already available in current smartphones. INS can be enabled via a digital compass, a gyroscope, and/or an accelerometer. With INS-based solutions, the training phase can be waived; however, this strongly depends on the employed motion model and the precision of the sensor(s), which could be in turn affected by the sensor's noise. This may lead to a measurement error, thereby making the dead-reckoned trajectories less accurate when the imprecision is accumulated over time.

As noticed, every existing scheme has its pros and cons. Thus, to enable a seamless iCloudFog operation, a graceful integration of multiple technologies may be required. As such, novel IPS-based platforms should be developed to achieve joint localization and simultaneous positioning of mobile Things within each Fog, via INS and a dynamically correlated fingerprint database.

As illustrated in Fig. 6, mobile devices could share their location estimates and measured fingerprints with nearby users using short-range wireless communication, in order to simultaneously calibrate their position estimation processes, and help construct the radio fingerprint database at minimal training cost. Hence, collaborative IoT devices in a Fog would collect the received landmark signatures from each other, to form a virtual IPS that can provide to all the Things within the Fog network, the indoor positioning functionality. Eventually, any collaborating and/or newly arriving Thing can issue a query to the virtual IPS to obtain its own predicted location with high accuracy. One or multiple servers can be optionally situated in the area of interest, responsible for continuously calibrating their fingerprint database(s). It may also be critical to equip each Thing with sufficient intelligence to determine how to calibrate its current location according to the analysis on all the collected fingerprints over time.

5. Conclusions

Fog computing has been taken as a promising technology for enabling low-latency, flexible and scalable future edge network operation to support intensive IoT data. In this article, we discussed the integration of Fog with the Cloud, which has been shown to have several merits. We then proposed iCloudFog, an integrated Cloud–Fog architecture that enables the construction of different Fog types to fit the different characteristics of IoT devices and data, and Fog nodes. Key research challenges such as network dimensioning and configuration, resource management, data privacy and security, and localization have been discussed. Promising approaches were also presented to address these challenges. If these challenges are efficiently addressed, we expect iCloudFog networks to be an exciting solution for the successful provisioning of future IoT data, which has been growing at an immense rate in the last few years.

Acknowledgment

This work is supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (Grand No. 2015R1C1A1A02036536 and Grand No. 2018R1D1A1B07051118).

References

[1] Cisco fog computing solutions: Unleash the power of the Internet of Things, white paper, Cisco, 2015.
[2] Yin. Zhang, et al., SOVCAN: safety-oriented vehicular controller area network, IEEE Commun. 55 (8) (2017) 94–99.
[3] Yin Zhang, et al., TempoRec: temporal-topic based recommender for social network services, Mobile Netw. Appl. 22 (6) (2017) 1182–1191.

[4] M. Chen, et al., Deep features learning for medical image analysis with convolutional autoencoder neural network, IEEE Trans. Big Data (June) (2017).
[5] S. Xiao, et al., Self-evolving trading strategy integrating internet of things and big data, IEEE Internet Things J. (Oct.) (2017).
[6] M. Armbrust, et al., A view of cloud computing, Commun. ACM 53 (4) (2010) 50–58.
[7] Cisco Global Cloud Index: Forecast and Methodology, 2015–2020, 2016.
[8] M. Al-Fares, et al., Hedera: dynamic flow scheduling for data center networks, ACM Proc. Netw. Syst. Des. Implementation (2010).
[9] K. Kitayama, et al., Torus-topology data center network based on optical packet/agile circuit switching with intelligent flow management, IEEE/OSA J. Lightwave Technol. 33 (5) (2015) 1063–1071.
[10] M. Qiu, et al., Energy-Aware data allocation for mobile cloud systems, IEEE Syst. J. (2014).
[11] E. Borcoci, et al., Fog computing, mobile edge computing, cloudlets-whichone? SoftNet (2016).
[12] M.R. Mahmud, et al., Maximizing quality of experience through context-aware mobile application scheduling in cloudlet infrastructure, Sotfw. Pract. Exp. 46 (11) (2016) 1525–1545.
[13] Cisco, Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are, White Paper, 2015.
[14] Openfog consortium.
[15] M. Chiang, et al., Fog Networking: An Overview on Research Opportunities, 2016.
[16] S. Yi, et al., Fog computing: platform and applications, in: HotWeb, 2015.
[17] A. Munir, et al., Ifciot: integrated fog cloud iot: a novel architectural paradigm for the future internet of things, IEEE Consumer Electron. Mag. 6 (2017) 74–82.
[18] M.R. Mahmud, et al., Fog Computing: A Taxonomy, Survey and Future Directions, 2016.
[19] The Tactile Internet. ITU-T, Report, August 2014.
[20] M. Aazam, et al., Fog computing micro datacenter based dynamic resource estimation and pricing model for iot, in: AINA, 2015.
[21] N. Wang, et al., ENORM: a framework for edge node resource manamgent, IEEE Trans. Service Comput. (January) (2017).
[22] L. Bittencourt, et al., Towards virtual machine migration in fog computing, in: 3PGCIC, 2015.
[23] F. Jalali, et al., Fog computing may help to save energy in cloud computing, IEEE J. Sel. Areas Commun. 34 (2016) 1728–1739.
[24] K. Vatanparvar, et al., Energy management as a service over fog computing platform, in: ACM/IEEE International Conference on Cyber-Physical Systems, 2015.
[25] P. Paglierani, et al., High performance computing and network function virtualization: a major challenge towards network programmability, in: BlackSeaCom, 2015.
[26] K. Liang, et al., Integrated architecture for software defined and virtualized radio access networks with fog computing, IEEE Netw. (2016).
[27] A.C. Baktir, et al., How can edge computing benefit from software-defined networking: a survey, use cases and future directions, IEEE Commun. Surv. Tutorials (June) (2017).
[28] M. Ojo, et al., A SDN-IoT Architecture with NFV Implementation, in: Globecom Workshops, 2016.
[29] S. He, et al., Wi-Fi fingerprint-based indoor positioning: recent advances and comparisons, IEEE Commun. Surv. Tutorials 18 (2016) 466–490.
[30] K. Kalliola, High Accuracy Indoor Positioning Based on BLE, Nokia Research Center, 2011.

Limei Peng received the M.S. and Ph.D. degrees from the Chonbuk National University,South Korea, in 2006 and 2010, respectively. In 2011, she was a Research Professor with Grid Middleware Research Center, Korea Advanced Institute of Science and Technology, South Korea. She has been an Associate Professor with the School of Electronic and Information Engineering, Soochow University, China, for more than two years. She has been an Assistant Professor with the Department of Industrial Engineering, Ajou University, South Korea. She is now an assistant professor with the School of Computer and Engineering, Kyungpook National University, South Korea. Her research interests fall in optical communication networks and protocols, datacenter networks, software de_ned networks, and cloud computing networks.

Ahmad R. Dhaini is currently an assistant professor of Computer Science at the American University of Beirut (AUB), and a visiting assistant professor at University of Waterloo, while on leave from AUB. He received his B.Sc. in computer science from AUB in 2004; his M.Sc. degree in electrical and computer engineering from Concordia University, Canada in 2006 with a best thesis award nomination. In 2006–2007, he was a software analyst and consultant at TEKSystems, Canada; and in 2007–2008, a software designer at Ericsson, Canada. He obtained his Ph.D. in electrical and computer engineering from University of Waterloo, Canada in 2011, and was granted several awards such as the Ontario Graduate Scholarship in Science and Technology (OGSST), and other various teaching and research awards at University of Waterloo. In 2011–2012, he worked as a research associate at University of Waterloo, Canada, and as a consultant at KAUST, Saudi Arabia. In 2012–2014, he was a postdoctoral scholar at Stanford University, working in the Photonics and Networking Research Laboratory (PNRL), after being awarded the prestigious NSERC postdoctoral fellowship. He also completed the Stanford Ignite program for entrepreneurship and innovation, which teaches scientists how to convert an idea into a business. Dr. Dhaini is a co-inventor of two US patents. He has also authored/coauthored more than 40 highly cited research articles in top IEEE journals and conferences. He is a reviewer for NSF, NSERC, and several US universities' internal grants. He also serves as Editor for Springer's Photonics Networks Communications journal, and reviewer and technical program committee (TPC) member for several major IEEE journals and conferences. His research interests cover several themes of integrated networks such as fiber-wireless (FiWi) broadband access networks, mission-critical networks, green communications, edge computing, and software-defined networking. He has also co-PIed several projects related to biotechnology, more specifically in the areas of mobile health and medical image analysis. Pin-Han Ho received the B.Sc. and M.Sc. degrees at the Electrical Engineering Department, National Taiwan University, in 1993 and 1995, respectively, and the Ph.D. degree from Queens University, Kingston, Canada, in 2002. He is currently an Full Professor in the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He is the author/coauthor of more than 150 refereed technical papers, several book chapters, and the coauthor of a book on optical networking and survivability. His current research interests cover a wide range of topics in broadband wired and wireless communication networks, including survivable network design, fiber-wireless network integration, edge computing, and network security. Dr. Ho is the recipient of the Distinguished Research Excellent Award in the Electrical and Computer Engineering Department of University of Waterloo, Early Researcher Award (Premier Research Excellence Award) in 2005, the Best Paper Award in International Symposium on Performance Evaluation of Computer and Telecommunication Systems in 2002, International Conference on Communication Optical Networking Symposium in 2005, and International Conference on Communication Security and Wireless Communications symposium in 2007, and the Outstanding Paper Award in International Conference on High Performance Switching and Routing in 2002

Pin-Han Ho received the B.Sc. and M.Sc. degrees at the Electrical Engineering Department, National Taiwan University, in 1993 and 1995, respectively, and the Ph.D. degree from Queens University, Kingston, Canada, in 2002. He is currently an Full Professor in the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He is the author/coauthor of more than 150 refereed technical papers, several book chapters, and the coauthor of a book on optical networking and survivability. His current research interests cover a wide range of topics in broadband wired and wireless communication networks, including survivable network design, fiber-wireless network integration, edge computing, and network security. Dr. Ho is the recipient of the Distinguished Research Excellent Award in the Electrical and Computer Engineering Department of University of Waterloo, Early Researcher Award (Premier Research Excellence Award) in 2005, the Best Paper Award in International Symposium on Performance Evaluation of Computer and Telecommunication Systems in 2002, International Conference on Communication Optical Networking Symposium in 2005, and International Conference on Communication Security and Wireless Communications symposium in 2007, and the Outstanding Paper Award in International Conference on High Performance Switching and Routing in 2002.