An Introduction and Comparison of the Application of Cloud and Fog in IoT

Zheng Li(✉) and Yilin Wang

Jiangsu Collaborative Innovation Center of Atmospheric Environment
and Equipment Technology (CICAEET), Nanjing University of Information Science
and Technology, Nanjing 210044, China
20171344068@nuist.edu.cn

Abstract. This paper mainly introduces the definitions of cloud computing and fog computing, and expounds their differences. Firstly, the new problems encountered by the Internet of Things (IoTs) are put forward. It also points out the shortcomings of cloud computing in solving these problems. Then it explains the advantages of fog computing over cloud computing in solving these problems, and finally introduces the new challenges fog computing encounters.

Keywords: Cloud computing · Fog computing · IoT

1 Introduction

Over the past few years, cloud computing has gained tremendous popularity from the applications of IoTs. The main reasons are that the cloud computing technology is relatively mature, and it is possible to access and utilize the cloud information and resources at anytime and anywhere. Overall, cloud computing provides users with many advantages, such as low-cost, convenient access to information, rapid deployment, data backup and recovery, and automatic software integration [8]. However, with the emergence of new requirements of the emerging IoTs (such as low latency and high security), the traditional centralized cloud computing is insufficient to support the complex edge network of the interconnection of all things.

At the same time, the number and types of heterogeneous user terminals and IoTs access devices are also increasing sharply: smart headphones, smart phones, mobile computers, smart appliances, on-board networking systems, intelligent traffic control lights and more networking public facilities. In addition, more and more new networking devices are emerging [4]. These billions of devices and heterogeneous data constitute a variety of complex systems. How to effectively manage these systems has become the focus of the cloud and IoT research fields [15].

Supported by National Natural Science Foundation of China (Grants No 61702274) and the Natural Science Foundation of Jiangsu Province (Grants No BK20170958), and PAPD.

X. Zhang et al. (Eds.): CloudComp 2019/SmartGift 2019, LNICST 322, pp. 63–75, 2020.
https://doi.org/10.1007/978-3-030-48513-9_5

In 2012, Cisco proposed an emergency architecture and solution. Instead of using centralized cloud computing servers, the architecture moves the computing servers to data sources and user terminals to overcome the shortcomings of cloud computing, which is the fog computing paradigm [15]. Fog computing has some advantages, such as low latency, low network bandwidth requirements, low performance requirements of terminal devices, stable services and better security and privacy.

However, due to the immaturity of fog computing technology, there are few examples of using fog computing in real life. If we want to truly implement the application and better prospects of fog computing, we must understand fog's complex network system, including complex heterogeneous hardware, software and the process of accessing network [15]. In addition, we have to solve fog's problems, such as a large number of data management, heterogeneous equipment management, the lack of specific processes and technology, and the lack of fog equipment security.

The above issues will be discussed in detail in the following chapters.

2 Cloud Computing

2.1 Definition of Cloud Computing

Cloud is a computing model that supports convenient, ubiquitous and on-demand network access to a shared pool of configurable computing resources like the networks, storage space, servers, applications and services. These resources can be supplied and released with minimal management effort and minimal interaction among service providers [1]. Figure 1 shows an example of a cloud model:

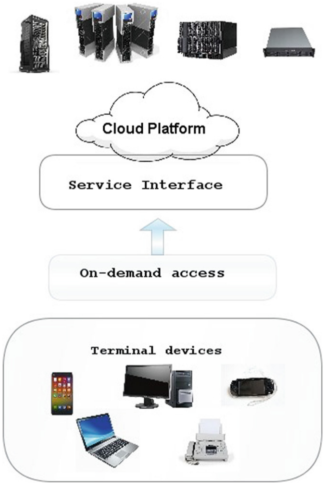

Fig. 1. The cloud model.

2.2 Characteristics of Cloud Computing

Cloud computing is attractive because it has the following four characteristics [10]:

1. Cloud computing does not require pre-investment because it is a pay-on-demand pricing model that allows service providers to benefit from the cost of leasing resources in the cloud without investing in infrastructures.
2. Operating cost is low. Resources in cloud environment can be quickly released based on users' requirements. Service providers can release some idle resources when the service demand is low, instead of providing unnecessary capacities at the peak load.
3. Infrastructure providers can collect a large amount of resources from data centers, and service providers can easily access these data, so as to judge service growth needs according to data trends, and then accurately expand the scale of their services.
4. Cloud services support the access to various devices via the Internet, which is very convenient.

3 Fog Computing

3.1 Definition of Fog Computing

Fog computing is a layered model which supports ubiquitous and convenient access to a shared continuum of extensible computing resources. The model promotes the deployment of distributed and delay-aware applications and services, and consists of fog nodes which are either physical or virtual. Fog nodes reside between intelligent terminal equipments and cloud services. Fog node have context-aware functions and support general data management and communication systems. The organizational form of fog nodes in the cluster is based on the specific working mode. Separation is supported by vertical distribution and association is supported by horizontal distribution. They can also be distributed according to the delay distance to the smart terminal. Fog computing minimizes request response time with applications, provides local computing resources for terminal equipment, and provides network connections to centralized services [2].

Figure 2 shows a fog system, which has three layers: cloud layer, fog layer and IoTs/end user layer. The fog layer can be formed by one or more fog domains and they may be controlled by the same or different service providers. A fog domain covers a number of fog nodes that include the edge routers, gateways, PCs, smart phones, switches and set-top boxes. The IoTs/end-user layer consists of two domains. The first domain includes the end-user devices, and the second domain includes the IoT devices [3].

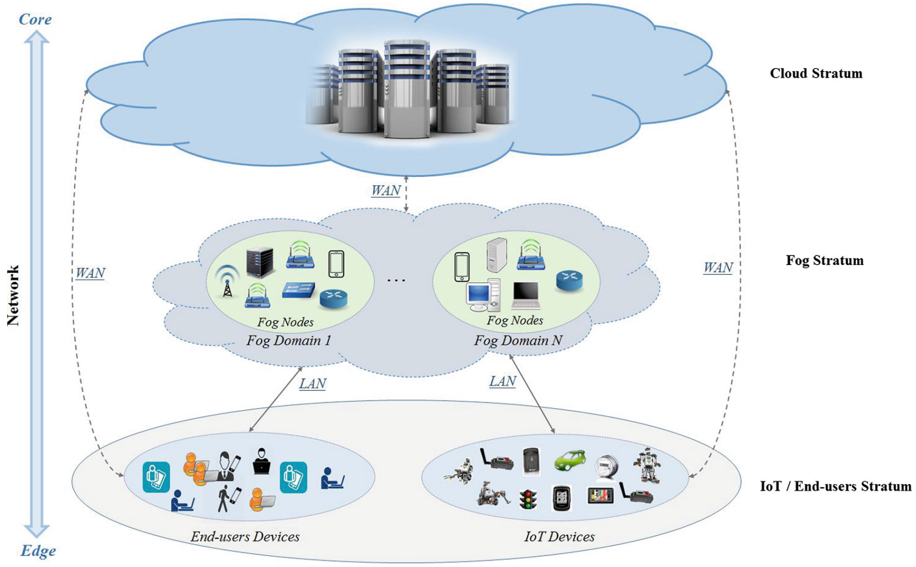

Fig. 2. The fog system [3].

3.2 Characteristics of Fog Computing

Fog computing has several different features from cloud computing [2]. Cloud computing is based on IT operator services and social public clouds. Fog computing is based on the small clouds, such as the personal clouds, the private clouds and the enterprise clouds. Cloud computing emphasizes overall computing power and is usually composed of clusters of high-performance computing devices. Fog computing is composed of more dispersed functional computers, and each computing node needs to play a role. Fog computing extends cloud computing by extending the computing power from the network center to the network edge, and has been widely used in various services.

Location Awareness and Low Latency. Fog nodes are tightly coupled with intelligent terminal devices or access networks and provide computing resources for these devices. And because fog nodes are aware of their logical location in the whole system and the delay cost of communicating with other nodes, fog computing can provide as low a delay as possible by providing services nearby. Because fog nodes usually coexist with smart terminal devices, data generated by these devices can be analyzed and responded much faster than data generated from centralized cloud services or data centers [2].

Geographical Distribution. Fog computing requires a wide deployment of target services and applications which can identify geographic location. Fog nodes provide some form of data management and communication services between the network edge layer where the terminal equipment is located and fog computing services or centralized (cloud) computing resources (if needed) [4]. In order to deploy a given fog computing capability, fog nodes operate in a centralized or decentralized manner and can be configured as separate fog nodes. For example, by locating fog nodes along tracks and highways, fog computing provides high-quality streaming media services to mobile vehicles and achieves a good result [2].

Heterogeneity. In fog computing, fog nodes interact with various types of network terminal devices on the edge of the network, which will generate data of various shape factors [2]. Therefore, fog must have the characteristics of accommodating heterogeneous data and be able to collect, aggregate and process these heterogeneous data.

Scalability and Agility. In nature, fog computing is adaptive. Because contacting with the network edge layer, the amount of data, resource conditions and network environment which fog computing faces may change constantly. Fog computing can support flexible computing, data load change, network condition and resource pool change at the cluster level to list some supporting adaptive functions [2].

Interoperability and Federation. Fog is distributed, and the functions and services provided by each node are not as powerful as those provided by a centralized cloud transport center. A single service provided by fog may require joint support from multiple nodes. Therefore, fog supports cross-domain cooperation among nodes and interoperability of fog computing components. In addition, fog has a unified specification to achieve seamless support for services [2].

Real-Time Interactions. The interaction between fog and data source is real-time, which does not have long waiting and delay. Fog nodes receive data from terminal devices and respond immediately after finishing analysis, rather than sending data as batch processing to the distant cloud center [2].

4 Cloud and Fog Computing

4.1 Comparison of Cloud and Fog Computing

Fog computing is an extension of cloud computing. It has many similarities and differences with cloud computing. We compare cloud and fog from the following aspects, which can intuitively reflect their similarities and differences.

Reaction Time and Latency. The most time-sensitive data will be sent to the nearest fog node for analysis and processing, so as to minimize the reaction time as far as possible. When the fog node closest to the IoT device is used to process data, the recovery time can be reduced to milliseconds or even sub-seconds. Data that is not particularly urgent can wait to be sent to the aggregation area of the fog node for processing, possibly for a few seconds or minutes. But the response time for interacting with the cloud may be a few minutes, days or even weeks [13,14]. So it is not hard to see that fog has more flexible choices and faster responses than clouds. That's why fog has a much lower delay than clouds.

Node Location Distribution. Cloud is in the network while fog nodes are distributed on the edge of the network and interact with IoT devices. Cloud occurs in the form of dense central servers, but fog exists not only in scattered nodes near IoT terminals, but also in dense data centers [14].

Service Scope and Location Perception. Cloud computing has few nodes and can't perceive location, but its service coverage covers the whole world. Unlike cloud computing, the number of fog nodes is very large, and they have the capability of location awareness. In terms of service scope, fog nodes which are very close to the IoT terminal equipment have a generally local service scope, such as a city block. But the service scope of node-intensive area can cover a wider area [13,14].

Vulnerability and Security. In the cloud, the user data is stored in the cloud computing center, and the possibility of damage is very high. Users often worry about the security of their data. Because fog is geographically dispersed, the possibility of damage is very low. Moreover, data processing in fog is closer to users, so users can have control over data security and privacy [8].

4.2 Collaboration Between Cloud and Fog Computing

Cloud is far away from user terminals, and there will be some problems in the application of the emerging IoTs. When we use fog to extend the cloud to terminal devices on the edge of the network, we can fill the new demand. So how can data be processed and analyzed in the collaboration of cloud and fog? Fig. 3 shows an example of a cloud-fog interaction model:

Next, we describe the tasks that cloud and fog nodes need to accomplish in the interaction.

The Things Fog Nodes Need to Do. At the edge of the network, that is, near the data source, the fog nodes at the edge receive data from the terminal devices of IoT in real time. The fog nodes can also receive the heterogeneous dynamic data. Then the real-time control and analysis of the data are carried out by running the application supported by the IoTs to achieve the millisecond

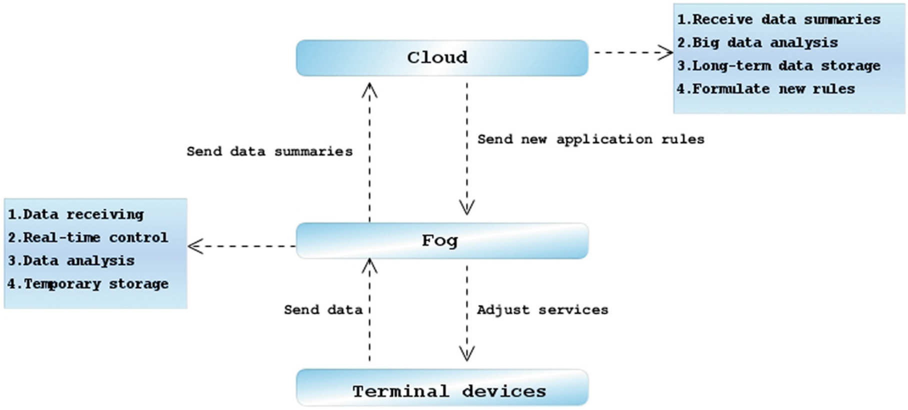

Fig. 3. Interaction model of cloud and fog.

response time. At the same time, fog nodes provide temporary data storage. This storage usually lasts about 1 to 2 h. After processing and analyzing the data, fog nodes should send data summaries to the cloud regularly, and report the overall information of the data [14].

The Things Cloud Needs to Do. When cloud platforms receive data digests sent by various fog nodes, they need to be collected and aggregated by cloud platforms. Then, the cloud platform makes an overall analysis and evaluation of these data to obtain service growth trends and determine the direction of business development. Finally, the cloud platform formulates new application rules based on the results of business evaluation, so as to achieve the goal of adjusting service balance [14].

5 Fog Computing Help on the New Challenges of IoT

Moving computing, control and storage tasks to the cloud has been a trend in the past decade. However, today, with the upgrading of devices and technologies, the emerging IoTs has generated many new demands. Cloud computing faces great challenges in meeting these requirements. At this time, it is a new trend to expand the cloud to the edge of the network. Let us focus on the new challenges of the cloud-based IoTs and the advantages fog has over cloud computing in these new challenges.

5.1 Low Latency Requirements

Nowadays, many industrial systems and life applications require end-to-end communication between devices with low latency, such as, unmanned vehicles, flight control of unmanned aerial vehicles, virtual reality applications and smart home applications, especially those requiring rapid response at high speed and delays of less than tens of milliseconds. It is also necessary to have a low latency processing capability in order to analyze the road conditions and control the duration of the lights according to the changing traffic conditions. In order to eliminate the delay in data transmission, fog deploys nodes on the edge of the network, allowing data to be analyzed, processed and stored near the end user. In [12], the researchers set up a proof-of-concept platform. They tested the face recognition application and reduced the response time from 900 ms to 169 ms by moving the computing program from the cloud to the edge. Fog also supports time-sensitive control functions in local physical systems [4]. This may be ideal and often the only option for meeting low latency requirements.

5.2 Network Bandwidth Constraints

With the advent of the age of interconnection, the speed of data creation is increasing exponentially [5]. For example, networked cars can create tens of megabytes of data per second. This will include a variety of data, including vehicle mobility (e.g. driving routes and speeds), vehicle status (e.g. wear and tear of vehicle components), vehicle surroundings (e.g. road conditions and weather conditions) and videos recorded by vehicle travel recorders. A driverless car will generate more data [6]. The American Smart Grid generate 1,000 gigabytes of data per year. Google trades 1 Gigabyte a month and the Library of Congress generates about 2.4 gigabytes of data each month. In 2010, AT&T's network used up 200 gigabytes [7]. If all the different types of data are sent to the cloud for processing, there will be a very high bandwidth requirement. This will impose a heavy burden on the existing bandwidth, and even lead to congestion, which is obviously not advisable. ABI Research estimates that 90% of the data generated by endpoints will be stored and processed locally, not in the cloud [5].

Fog processes the data between the cloud and the terminal, which can filter out some inappropriate or irrelevant data and prevent them from transmitting over the whole network [8]. Data generated from user terminals can be allocated to the nearest data center for processing without having to transfer all source data to the cloud, because many critical analyses do not require cloud computing processing and storage. Fog's processing method will greatly reduce the amount of data sent to the cloud, greatly reduce the bandwidth pressure and reduce the bandwidth requirements.

5.3 Resource Constraints of Devices

In IoT systems, some devices cannot directly interact with the cloud due to resource constraints (e.g. network, computing and storage resources), so they cannot transfer tasks to the cloud. It is unrealistic to upgrade and update resources for each device at a high cost.

In this case, the cloud will not be able to perform its functions, while fog can replace these devices to perform tasks that require intensive resources [4]. The core components of the fog computing architecture are fog nodes, which are either physical components (such as routers, switches, gateways, and servers) or virtual components (such as virtualized switches and virtual machines). Fog nodes are tightly coupled to intelligent user terminals or access networks and provide these terminal devices with computing resources [2]. Therefore, the complexity of terminal devices and resource requirements are reduced.

5.4 Stability of Service

When the connection to the cloud is not stable and continuous, the cloud can not provide stable and continuous services to users or devices. For example, when a vehicle enters an area that is not covered by the Internet, many necessary applications are unavailable in on-board and personnel equipment, and then the cloud service will be disconnected, so there will be unstable cloud services [4].

But unlike clouds, fog has a dense geographical distribution. Edge networks created by fog computing are located at different points to extend the infrastructure for cloud geographic isolation. Forming a continuous coverage of the service scope helps to process the analysis data more quickly and steadily. And administrators can support mobility requirements which is based on location [8].

5.5 Security and Privacy

Because of the rapid development of the IoTs, more and more data are connected to the network, including a large number of privacy information. For example, people's work and rest rules can be excavated from real-time information generated by intelligent household appliances, and important privacy information such as property can be eavesdropped from chat data. Therefore, both the transmission process and the static state of data in the IoTs need to be well protected, which requires the monitoring and automatic response of malicious attacks in the whole process [11].

In cloud computing, private and corporate data, and even confidential information, are stored in the cloud. Users must rely on cloud service providers to ensure their data security and privacy, which will cause users to worry [8]. For example, a user does not have complete control over his/her data, his/her privacy is maliciously exploited, and cloud computing centers may cause data loss in the process of expansion.

In fog, sensitive data is processed locally rather than sent to the cloud for analysis. Our own administrators can monitor and inspect the devices that collect, analyze, process and store data so that we can control the data by ourselves [11]. In some devices that cannot adequately protect data due to resource constraints, the fog system can act as a proxy for these devices to help manage and update the security credentials and software of these devices to compensate for their security vacancies. Fog system can also use local information to monitor the security status of nearby devices and detect threats immediately to ensure security [4].

6 Problems in Fog Computing

6.1 Data Management

In order to reduce the delay and let users control the data, fog will process and store most of the data locally near the terminal. The Internet Data Center (IDC) points out that by 2020, about 44 zetabytes of data are expected to be generated [18]. How can such a large amount of data generated by heterogeneous devices be managed? Therefore, appropriate data selection and transmission protocols must be considered [14].

In addition, accessing the fog network from the outside is very tedious, and the addition of a new service provider will greatly increase the complexity of the fog network. Therefore, it is pressing to look for the gap as soon as possible, determine the method of data governance and implement it scientifically to achieve data integrity constraints and confidentiality requirements [15].

6.2 Heterogeneous Equipment Management

In the fog, billions of different devices must be distributed. Various heterogeneous devices may produce different faults in many locations. It is a complex task to monitor and track the fault information of hardware and provide software patches for updating and maintenance.

Faced with these possible unknown faults, open fog suggests using machine learning technology to develop a framework with fault comprehensive feature detection and fault tolerance [17,21]; especially in systems involving critical applications of life, such as anomaly detection in the medical field. Only by solving this problem can fog be truly applied to IoT on a wide range of network edges [15].

6.3 Lack of Concrete Processes and Technologies

Fog can be used to support edge network. Fog serves as a local data storage and application server for the edge networks, providing services for end-user devices, and helping these network devices and end-user devices (e.g., vehicles, commercial or industrial intelligent robots, UAVs, smart phones and computers) to form local networks. To help these local devices build trustworthy communications, fog also provides them with temporary security credentials [4].

To achieve this, we have to consider how our fog function connects to the hardware and operating system of the local device. In this context, a lot of research has been done, but the fog-based implementation methods of the IoTS are rarely studied. Most of them focus on embedded devices, protocols, principles, security, QoS and applications [19,20]. The use of D4D to pool idle edge resources is mentioned in [16], but a new protocol stack may also be needed for end-user devices to support fog edge networks. So far, we still lack specific processes and tools to realize the connection between fog computing and IoTs applications [15].

6.4 Security and Privacy

As we mentioned in the section of security challenges of IoT, fog acts as a node for traffic encryption and access control, aggregating and controlling privacy-sensitive data before data leaves the edge. Fog also acts as a proxy for resource-constrained terminal devices, providing them with the choice of security functions to ensure the security of resource-constrained devices [4].

But many studies have also shown that fog devices lack safety [22,23]. Fog is dispersed, it needs to work in places where the environment is much more fragile than the cloud. Cloud servers are in the cloud center, and many fog devices are in public places, lack of security monitoring, and are very vulnerable to be damaged. Moreover, fog systems do not have the powerful resources to protect themselves like centralized cloud systems, so fog systems are more vulnerable to attacks, such as session riding, session hijacking and SQL injection [15].

In [9], fog security and privacy challenges are divided into the following points: 1) The security and reliability of fog network need a trust model to be ensured. Fog nodes and IoTs devices need to establish mutual authentication trust mechanism. 2) It is difficult for resource-constrained IoTs devices to use traditional certificate and public key infrastructure (PKI) authentication mechanisms. 3) The messages sent by IoTs devices can not be encrypted symmetrically. In addition, asymmetrical encryption technology has great challenges, including resource and environment constraints, overhead constraints and maintenance of the PKI. 4) Privacy protection in fog is challenging, because fog is more likely than cloud to collect location information of user equipment and usage data of facilities, which may lead to the disclosure of important location privacy. The scattered fog nodes may be attacked because of the different security protection intensity. And frequent interaction among the three layers of fog architecture will increase the possibility of privacy disclosure. The last point is that fog is more vulnerable to malicious attacks. The performance of the network may be seriously damaged without proper security measures.

7 Conclusion

In this paper, we first introduced the background of fog generation and the development of fog field. Then we introduced the concept and characteristics of cloud computing based on the cloud computing definition given by NIST, which has the highest recognition at present. We introduced the concept and characteristics of fog computing. We pointed out the difference between cloud computing and fog computing through comparative analysis from different perspectives. The interaction workflow between cloud and fog was also described from two perspectives of fog and cloud. We described the new challenges faced by IoT in today's new application requirements, and briefly described the disadvantages of cloud computing on these issues and the advantages of fog computing in solving this problem. Finally, we introduced the problems that need to be solved in fog computing, and provided some suggestions for future research.

References

1. Mell, P.M., Grance, T.: SP 800–145. The NIST Definition of Cloud Computing. National Institute of Standards & Technology (2011)
2. Iorga, M.: Fog Computing Conceptual Model. Special Publication (NIST SP)- 500–325. https://doi.org/10.6028/NIST.SP.500-325
3. Mouradian, C., Naboulsi, D., Yangui, S., et al.: A comprehensive survey on fog computing: state-of-the-art and research challenges. IEEE Commun. Surv. Tutor. **20**, 416–464 (2017)
4. Chiang, M., Zhang, T.: Fog and IoT: an overview of research opportunities. IEEE Internet Things J. **3**(6), 854–864 (2016)
5. Kelly, R.: Internet of Things Data to Top 1.6 Zettabytes by 2022. https://campustechnology.com/articles/2015/04/15/internet-of-thingsdata-to-top-1-6-zettabytes-by-2020.aspx. Accessed 7 Apr 2016
6. Mearian, L.: Self-driving cars could create 1GB of data a second. http://www.computerworld.com/article/2484219/emergingtechnology/self-driving-cars-could-create-1gb-of-data-a-second.html. Accessed 7 Apr 2016
7. Cochrane, N.: US smart grid to generate 1000 petabytes of data a year, 23 March 2010. http://www.itnews.com.au/news/us-smart-grid-to-generate-1000petabytes-of-data-a-year-170290#ixzz458VaITi6. Accessed 7 Apr 2016
8. Kumar, A., Saharan, K.P., Saharan, K.P., et al.: Fog in comparison to cloud: a survey. Arch. Intern. Med. **141**(13), 1771–1776 (2015)
9. Hong, Y., Liu, W.M., Wang, L.: Privacy preserving smart meter streaming against information leakage of appliance status. IEEE Trans. Inf. Forensics Secur. **12**, 2227–2241 (2017)
10. Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: state-of-the-art and research challenges. J. Internet Serv. Appl. **1**(1), 7–18 (2010)
11. Pande, V., Marlecha, C., Kayte, S.: A review-fog computing and its role in the Internet of Things. Int. J. Eng. Res. Appl. **6**, 7–11 (2016)
12. Shi, W., et al.: Edge computing: vision and challenges. IEEE Internet Things J. **3**(5), 637–646 (2016)
13. Firdhous, M., Ghazali, O., Hassan, S.: Fog computing: will it be the future of cloud computing? In: Proceedings of the Third International Conference on Informatics & Applications, Kuala Terengganu, Malaysia (2014)
14. Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. https://www.innovation4.cn/library/r1490
15. Dasgupta, A., Gill, A.Q.: Fog computing challenges: a systematic review. In: Australasian Conference on Information Systems, Hobart, Australia (2017)
16. Zhang, Z., Zhang, J., Ying, L.: Multimedia streaming in cooperative mobile social networks. Preprint
17. Dastjerdi, A.V., Buyya, R.: Fog computing: helping the Internet of Things realize its potential. Computer **49**(8), 112–116 (2016)
18. MacGillivray, C., et al.: IDC futurescape: worldwide Internet of Things 2017 predictions (2016)
19. Vaquero, L.M., Rodero-Merino, L.: Finding your way in the fog: towards a comprehensive definition of fog computing. SIGCOMM Comput. Commun. Rev. **44**(5), 27–32 (2014)
20. Yi, S., Li, C., Li, Q.: A survey of fog computing: concepts, applications and issues. Paper presented to the proceedings of the 2015 workshop on mobile big data, Hangzhou, China (2015)

21. Consortium, O: Openfog Reference Architecture for Fog Computing (2017). OPFRA001.020817
22. Stojmenovic, I., Wen, S.: The fog computing paradigm: scenarios and security issues. In: 2014 Federated Conference on Computer Science and Information Systems, pp. 1–8 (2014)
23. Li, J., Jin, J., Yuan, D., Palaniswami, M., Moessner, K.: EHOPES: data-centered fog platform for smart living. In: 2015 International Telecommunication Networks and Applications Conference (ITNAC), pp. 308–313. IEEE (2015)