Future Generation Computer Systems 88 (2018) 16–27

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Security and trust issues in Fog computing: A survey

PeiYun Zhang [a], MengChu Zhou [b,c,*], Giancarlo Fortino [d]

[a] School of Computer and Information, Anhui Normal University, Wuhu 241003, China
[b] Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102, USA
[c] The Institute of Systems Engineering, Macau University of Science and Technology, Macau 999078, China
[d] Department of Informatics, Modeling, Electronics, and Systems, University of Calabria, Italy

HIGHLIGHTS

- We discuss and analyze the architectures of Fog computing, and indicate the related potential security and trust issues.
- We analyze how such issues have been tackled in the existing investigations.
- We indicate the open challenges, research trends and future topics of security and trust in Fog computing.

ARTICLE INFO

Article history:
Received 27 December 2017
Received in revised form 3 March 2018
Accepted 8 May 2018
Available online 15 May 2018

Keywords:
Fog computing
Cloud computing
Trust
Security

ABSTRACT

Fog computing uses one or more collaborative end users or near-user edge devices to perform storage, communication, control, configuration, measurement and management functions. It can well solve latency and bandwidth limitation problems encountered by using cloud computing. First, this work discusses and analyzes the architectures of Fog computing, and indicates the related potential security and trust issues. Then, how such issues have been tackled in the existing literature is comprehensively reported. Finally, the open challenges, research trends and future topics of security and trust in Fog computing are discussed.

1. Introduction

Cloud computing (the Cloud in brief) has drastically changed the landscape of information technology (IT) by providing some major benefits to IT users, including eliminating upfront IT investment, scalability, proportional costs, and so on [1–5]. However, as more and more devices are connected, latency-sensitive applications seriously face the problem of large latency. In addition, Cloud computing is unable to meet the requirements of mobility support and location awareness. To overcome these problems, a new paradigm called Fog computing (the Fog in brief) was proposed in 2012 [6,7].

According to Bonomi et al. [8], the Fog is a highly virtualized platform that provides storage, computing and networking services between the Cloud data centers and end devices. Both Cloud and Fog provide data, computation, storage and application services to end users [9]. However, the latter is distinguished from the former by its decentralization, processing large amounts of data locally, software installation on heterogeneous hardware [10], proximity to end-users, dense geographical distribution, and support for mobility [11].

Here, we show an example of a traffic light system to discuss the relationship between them when dealing with latency. In a traffic light system without the Fog, there may be 3∼4 hops from the monitoring probe to the server in the Cloud. Hence, real-time decisions cannot be made immediately and the system faces the challenge of network latency. However, by using the Fog, the monitoring probe acts as a sensor, and the traffic lights act as an actuator. The Fog node can send conventional compressed video that may endure some time latency to the Cloud. When the Fog node detects an ambulance's headlight flashing, it makes an immediate decision to turn on the corresponding traffic lights, so as to let the ambulance go through without any delay. However, the Fog cannot replace the Cloud but supplements it.

Many companies and institutes, such as ARM, Cisco, Dell, Intel, Microsoft Corp., Cloudlet, Intelligent Edge by Intel and the Princeton University Edge Laboratory are devoted to research and development of the Fog. OpenFog (Found in 2015) Consortium workgroups are working towards creating an open architecture for the Fog to enable its interoperability and scalability [12].

* Corresponding author.
E-mail address: zhou@njit.edu (M.C. Zhou).

https://doi.org/10.1016/j.future.2018.05.008
0167-739X/

Network equipment like switches and gateways is provided by Cisco, Huawei, Ericsson, etc. The current research trends reflect the tremendous potential of the Fog.

The Fog features with location awareness, low latency and edge location [13]. It fits to a scenario where a huge number of heterogeneous ubiquitous and decentralized devices communicate, need to cooperate, and perform storage and processing tasks [6]. Users can visit their Fog anytime by using any device that can be connected to the Fog network. The Fog has many applications in such areas as smart city [14–16] and healthcare [17–20]. It can also provide better Quality of Service (QoS) in terms of fast response and small energy consumption [21,22].

The Fog uses network devices (named Fog nodes in this paper) for latency-aware processing of data collected from Internet of Thing (IoT) [23]. Fog nodes are denoted as heterogeneous components deployed in an edge network in Fog environments. They include gateways, routers, switchers, access points, base stations, and specific Fog servers [24]. The Fog facilitates uniform and seamless resource management including computation, networking and storage allocation [25]. Fog nodes are often the first set of processors that data encounter in IoT, and have the resources to implement a full hardware root of trust. This root of trust can be extended to all the processes and applications running on them, and then to the Cloud [26]. Without a hardware root of trust, various attack scenarios can compromise the software infrastructures of the Fog, allowing hackers to gain a foothold. The requirements of life safety-critical systems mandate the sorts of security capabilities available on the Fog [27]. Hence, new security and trust challenges emerge with the rise of the Fog. The existing methods cannot be directly applied to the Fog because of its mobility, heterogeneity, large-scale geo-distribution [12]. This work reviews these concerns in the Fog and the existing solutions. Differing from other survey papers about Fog computing, this paper focuses on its security and trust issues, especially in the region of the Fog.

The rest of this paper is organized as follows. Section 2 reveals a Fog architecture as well as related security and trust issues. Section 3 summarizes the related work to cope with security and trust issues. Section 4 presents open research problems. Section 5 discusses the future work. Finally, Section 6 concludes this survey paper.

2. Fog computing architecture

2.1. General architecture

Based on the modern computing architecture with three layers [11,21]: the Cloud, the Fog and the Edge, we provide a comprehensive fog architecture as shown in Fig. 1. Between the Cloud and the Fog lies a core network to offer network services. From it we can see that the Cloud lies at the upper core level and is far away from edge devices. The Fog lies at the middle level and is closer to edge devices than the Cloud. Each Fog node is connected to the Cloud. Each edge device is connected to a Fog node [28]. In addition, we can see that Fog nodes can be connected to each other. Communications between Fog–Fog, Fog–Cloud, and Fog–Edge are all bi-directional.

The Cloud: It includes high-performance servers and storage devices for broadcasting, data warehousing and big data analysis [19]. It is the remote control and management center that can store large data, and process highly complex but often non-urgent tasks. The data is sent to the Cloud through high-speed wireless or wired communications. The Cloud provides ultimate and global coverage. As a repository, it provides data storage to meet users' long-term needs and intelligent data analysis.

The Fog: It consists of a network of interconnected Fog nodes [19,24]. It provides geo-distributed, low latency and urgent computation as well as location awareness. Each Fog node is a resource

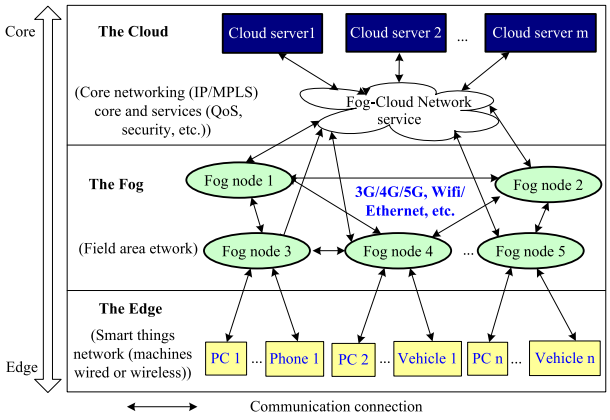

Fig. 1. A comprehensive Fog architecture.

center for ephemeral storage. Its functions include network transform, data collection, communications, data upload, data storage, computation and management. Compared with the edge devices, Fog nodes have more memory or storage ability for computing, which makes it possible to process a significant amount of data from edge devices. On the other hand, when needing a more complex and longtime computation, the computation work should be sent to the Cloud by Fog nodes through various available communications technologies, e.g., 3G/4G/5G cellular networks and WiFi. Fog nodes are bridges between Cloud and edge devices.

Fog nodes are independent and can be interconnected for collaboration. Management and collaborative procedures are applied on Fog nodes to implement management and control. The collaboration among Fog nodes can be executed via remote or local communications among them.

The Edge: It consists of several physical devices (edge devices) enabled with their ubiquitous identification, sensing, and communication capacity [19], such as vehicles, machines and cell phones. Each edge device is connected to one of the Fog nodes. Edge devices have a large variety of sensors and local data. It is very expensive and time-consuming to send all the data from terminal edge devices to the Cloud through a network. Hence, by connecting them to Fog nodes, one can deal with the urgent data but not transfer from edge devices to the cloud immediately.

Some easily misunderstood concepts are discussed in the following.

Edge computing vs. the Fog: Edge computing is different from the Fog in that the latter is a highly virtualized platform that provides computation, storage, and networking services between end devices and Cloud computing data centers [11]. Both of them need to push intelligence and processing capabilities out of centralized data centers and down closer to edge devices, such as IoT sensors, relays, and motors. The key difference between them is where intelligence and computing power are placed [12]. The Fog pushes intelligence down to the local area network (LAN) level, processing data in Fog nodes. While Edge computing pushes the intelligence, processing power, and communication capabilities further down to edge devices [29]. More details between them are discussed in [24]. In [30], Endpoint computing is regarded as Edge computing. Other similar concepts such as Cloudlets and Micro-data centers are discussed in [31].

Wireless sensor networks (WSNs) vs. the Fog: WSNs are designed to operate at very low power to extend battery life or use energy harvesting to sustain themselves. Most of them face the problems of small memory motes, low processing power, and