Chapter 90
Confidentiality and Safekeeping Problems and Techniques in Fog Computing

Nida Kauser Khanum
Ramaiah Institute of Technology, India

Pankaj Lathar
Chaudhary Brahm Prakash Government Engineering College, India

G. M. Siddesh
M. S. Ramaiah Institute of Technology, India

ABSTRACT

Fog computing is an extension of cloud computing, and it is one of the most important architypes in the current world. Fog computing is like cloud computing as it provides data storage, computation, processing, and application services to end-users. In this chapter, the authors discuss the security and privacy issues concerned with fog computing. The issues present in cloud are also inherited by fog computing, but the same methods available for cloud computing are not applicable to fog computing due to its decentralized nature. The authors also discuss a few real-time applications like healthcare systems, intelligent food traceability, surveillance video stream processing, collection, and pre-processing of speech data. Finally, the concept of decoy technique and intrusion detection and prevention technique is covered.

INTRODUCTION

The Internet of things (IoT) will be the "Internet of future" due to its growth rate in massive domains like wearable technology, smart city, smart transportation, smart grid. These smart applications require certain amount of resources like storage, battery, computation power and bandwidth. The IoT devices are not configured with so much resources. Therefore, they are generally assisted by robust server ends. Cloud

DOI: 10.4018/978-1-7998-5339-8.ch090

is considered as an auspicious solution to deliver services to end users, and for its adaptable resources at very low cost. The server ends used by IoT are deployed in Cloud for its fair benefits provided to the users.

Even though cloud has several advantages, it cannot solve all problems due to its own drawbacks. Latency is one of the major issue in cloud because the data centers are located near the core network. The real-time applications like gaming, augmented reality and real-time streaming are subtle to latency and cloud is not a feasible choice for the application deployment that require very quick response and avoid round-trip latency during transmission of data from/to terminal nodes to/from cloud servers for processing. The data is sent through multiple gateways during transmission. In addition, there are also unresolved glitches that regularly need agility support, geo-distribution and location-alertness in IoT applications (Shanhe et al., 2015).

However, the state-of-the-art technology in computing standard is to impulse computation and storage resources to the control of networks. This results in growth of an auspicious computing architype called fog computing that provides services to the edge devices instead of relying on cloud services. Fog computing eradicates many issues arising in cloud computing service. It retains computation and data local to end users by providing low latency, location-awareness and high bandwidth. It gets the title as fog because it is a cloud present close to the ground. The devices that provide fog services to the edge devices are named as fog nodes. Fog nodes can not only be resource-rich devices but they can also be resource-poor devices like end devices, smart TVs/set-top-boxes and gateways. Usually cloud computing is collaborated with fog computing by forming a three-layered architecture comprising of end users, fog and cloud service as shown in Figure 1.

Cloud computing and fog computing share many similar characteristics like adaptable resources (computation, storage and networking). There resources are building blocks for both cloud and fog computing, signifying that utmost cloud computing technologies can be pragmatic to fog computing. Nevertheless, the new paradigm fog has quite a few exclusive features that makes it diverse from other present computing architectures. One of the imperative feature is maintaining close distance to end users. To support applications that are latency-sensitive, it is vigorous to preserve computing resources at the core of the network. The other stimulating feature is that the fog nodes which are geographically distributed can infer its own position and keep a track of all the end devices by providing mobility. It also provides reduced delay and bandwidth by dropping data volume to great extent at primary stage by preprocessing the data at fog nodes before sending it to cloud for further analytics. This property yields many benefits for stream mining and edge analytics. This has a significant role in the era of big data (Bonomi et al., 2012).

There are many features that are enhanced in fog computing when compared to cloud. It provides mobility, large IoT device support, extensibility, reduced delay, decentralization and many more. Along with vast benefits, fog computing welcomes many issues in security and privacy of devices and information stored. The main concern of this chapter is understanding the security and privacy issues in fog computing. It also includes the architecture of fog computing and its interaction with other counterparts (cloud and IoT) that gives an overview of differences among the different layers. The present techniques that are employed to make fog secure is also discussed. Real-time applications are discussed that face security and privacy issues. At the end of the chapter an intrusion detection and prevention technique is proposed.