Chapter 8
Security Challenges in Fog Computing

Anshu Devi
Kurukshetra University, India

Ramesh Kait
Kurukshetra University, India

Virender Ranga
National Institute of Technology Kurukshetra, India

ABSTRACT

Fog computing is a term coined by networking giant Cisco. It is a new paradigm that extends the cloud computing model by conferring computation, storage, and application services at the periphery of networks. Fog computing is a gifted paradigm of cloud computing that facilitates the mobility, portability, heterogeneity, and processing of voluminous data. These distinct features of fog help to reduce latency and make it suitable for location-sensitive applications. Fog computing features raise new security concerns and challenges. The existing cloud security has not been implemented directly due to mobility, heterogeneity of fog nodes. As we know, IoT has to process large amount of data quickly; therefore, it has various functionality-driven applications that escalate security concerns. The primary aim of this chapter is to present the most recent security aspects such as authentication and trust, reputation-based trust model, rogue fog node and authentication at different level, security threats, challenges, and also highlights the future aspects of fog.

INTRODUCTION

Security is the topmost concern for government, business organizations and every individual in this digital world. As billions and millions of device get connected and it is estimated that around 2020, 40 percent of world data will come from sensors and 90 percent of world data generated from last 2 years. It is also estimated that every day 2.5 quintillion of data is generated. Hackers found new vulnerabilities to exploit and increasingly sophisticated attacks and making more susceptible system. These systems are prone to

DOI: 10.4018/978-1-5225-7335-7.ch008

attacks due to their inability to identify, protect and respond to threats. Hackers gets privilege with the help of entry point that allow them to access and damage the systems of physical world as well as pose security threats to business entities, factories, critical infrastructure, transportation system. But now Fog computing which is an open architecture that enables innovation for 5g, IoT and AI have been emerged as a solution to medicate such threats. Fog distributed architecture safeguards connected system from cloud to devices, forming additional layer system security in which compute, control, and navigate and communication are closer to the surfaces and data sources to protect. Let's take a closer look: Fog nodes protect cloud based IoT's and Fog based services by implementing wide range of security functions on any number of interconnected devices and even smallest constraints include providing trusted digital distributed platform, applications, services and managing as well as updating security potential, malware detection. Fog ensures trustworthy communication by detecting, invalidating and reporting attacks.

Fog can monitor the security status through new devices that quickly detect and isolate threats. If a security breach is detected, Fog provides a foundation that enable real time incident response directly or within local context minimizing disruption of services through its capability, marginality, capacity and resource distribution. Fog allows block chain of low cost IoTs end points.

Let's took an example: Multiple power generators are infected with malware, Fog allow operation manager to remotely operate and shut down the generator which are infected keeping service distribution to minimum . During the attacks the Fog nodes continue to operate simultaneously using local intelligence and local storage data to manage permission and data accessibility for building the services in showing the utility fire-alarm, elevator, security system and other critical services remain active.

Hackers seek out and take over the smart factor by targeting vulnerabilities in assembly learn equipment. Fog node protect OT domain by monitoring traffic from internet into distributed Fog network and leverage machine learning in the local context to detect probable attack. Once the attack detected by Fog node that act as a gateway, will block the traffic generated by attackers and protect critical factory network.

NECESSITY OF FOG

Total expenditure on IoT's device will be 1.7 trillion dollar by 2020.So according to given statistics now we can think about architecture of IoT where we can use all these devices in scalable manner so that processing can happen in a quicker and efficient manner. The total number of connected vehicles worldwide will be 250 million by 2020. There will be more than 30 billion IoT devices. So amount of data that will be generated will be huge. Now In order to reduce processing time of data Fog can be used.

Since Fog computing is the extension of cloud computing, therefore it should be important to define cloud computing, as it is not easy to comprehend Fog without knowing cloud. As we know cloud are important things in IoT devices as it senses so much of data and finally those data need to be handled. Now main problem with cloud in IoT environment is of latency. As cloud has certain inefficiency about handling the requirements of IoT.

There are certain issues with volume of data generated by IoT devices, latency and bandwidth (Abdelshkour).

In terms of **Data Volume**: It is estimated that 50 billion or millions of devices may be on-line by 2020. Presently everyday billions of devices produce terabytes of data. As the devices density are increasing everyday so the current cloud model is unable to process this amount of data. Private firms, factories,