FOG COMPUTING

VOLUME 5, ISSUE 6
OFFICE OF INFORMATION AND TECHNOLOGY (OIT)

INTRODUCTION

According to the Global System for Mobile Communications (GSMA Intelligence), by 2025, there will be 25 billion connections to the Internet of Things (IoT). That giant network of Internet connected "things" and people will be roughly five times greater than the five billion IoT that existed at the beginning of 2018! With two out of three people in the world connected to a mobile device in March of 2018, among a world population of 7.4 billion people, it can seem unimaginable that in less than two years, there is expected to be 2.5 IoT devices per person among a world population that reaches 8 billion. These statistics explain the basis for the drive for Federal agencies, businesses, and organizations to evaluate how IoT devices will be connected to existing networks, and the risks associated with those connections.

In this Tech Insight, we provide an overview of fog computing—a term The National Institute of Standards and Technology (NIST) reminds us is often erroneously confused as a synonym to edge computing. We will examine their key differences and differentiate a third concept, mist computing, as we define fog computing, its applications, and its utility in the proliferation of IoT. Lastly, we will assess fog computing's potential impact to the Department of Veterans Affairs (VA), as VA continues its move to the cloud.

ORIGINS OF FOG COMPUTING

It is surely no surprise to those who have lived amidst the shallow fog that engulfs San Fran*cisco* that it was a *Cisco* fellow who created the term ***fog computing*** in 2014. Fog computing describes an extension of cloud computing to the edge of an enterprise's network. Just as the weather phenomenon, fog, is known as the edge of the cloud when it forms at ground level at the time air on the ground cools; fog computing is known to bring IoT, 5G, and embedded artificial intelligence (AI) to the "bleeding edge" of cloud computing by allowing massive amounts of data to be processed quicker as things, apps, and devices connect at a rapid pace.

The National Institute of Standards and Technology (NIST) recently released the NIST Special Publication 500-325 that provides definitions and contextual information to help researchers and engineers better understand fog computing from the U.S. Government's perspective and

application. According to NIST, "Fog computing runs applications in a multi-layer architecture that decouples and meshes the hardware and software functions, allowing for dynamic reconfigurations for different applications while performing intelligent computing and transmission services. Edge computing runs specific applications in a fixed logic location and provides a direct transmission service." The NIST definition explains that fog computing is hierarchical, where edge computing tends to be limited to a small number of peripheral devices. Fog computing addresses computation, networking, storage, control, and data-processing acceleration.

OUT OF THE CLOUD AND INTO THE FOG

A public infrastructure-as-a-service (IaaS) cloud vendor can be thought of as a high-level, global endpoint for data; the edge of the network is where data from IoT devices are created. Fog computing, on the other hand, provides a distributed network that connects these two environments. Although there are many similarities between cloud and fog computing, including as-a-service models and deployment options, NIST outlines several characteristics of fog computing that makes it better suited to IoT applications than a cloud platform:

- *Contextual location awareness and low latency*: Because the nodes are often co-located with edge devices, they are aware of their physical and logical locations, making analysis and response faster than with cloud computing.
- *Geographical distribution*: Fog computing can better handle the streaming services required by geographically distributed IoT devices.
- *Heterogeneity*: Fog computing supports collection and processing of different data form factors, acquired through multiple types of networks.
- *Real-time interactions*: Fog computing applications involve real-time interactions rather than batch processing.
- *Scalability and agility*: Fog computing supports elastic compute, resource pooling, data-load changes, and variable network conditions.
- *Wireless access*. Fog computing works well with wireless IoT access networks and mobile devices.

One of the greatest challenges when deploying an IoT system is managing the data generated by IoT sensors and actuators. Traditional cloud-based IoT systems are challenged by the large scale, heterogeneity, and high latency witnessed in some cloud ecosystems. One solution is to decentralize applications, management, and data analytics into the network itself, using fog computing as a distributed and federated computing model.

THE FOG, MIST, AND EDGE

Moreover, NIST outlines the characteristics of mist computing. Mist computing is defined as a "lightweight" or sub-fog layer that resides in the network fabric, with its nodes placed closer to edge devices. It uses microcomputers and microcontrollers to feed data into fog computing nodes and potentially, into centralized computing services. Edge computing applications, by contrast, have fixed logical locations and directly transmit data between a small number of peripheral devices.

SECURITY FOR CLOUD AND FOG SERVICES

An emerging challenge to cloud data storage is that fissures are beginning to show in the existing system as more and more data is poured into the cloud. In February 2017, Amazon Web Service (AWS) cloud computing department suffered a four-hour outage that either was knocked offline or significantly slowed down as hundreds of thousands of websites experienced outages because AWS was used for hosting their databases, images, videos, and web services.

Safely securing IoT devices was the focus of a Forrester Research in a report titled Predictions 2018: IoT Moves from Experimentation to Business Scale. The report indicates more and more of IoT connectivity and integrations will happen in the cloud. However, in an effort to cut costs and trim latency, IoT data processing and analysis will also move from the core to the edge of the network. Forrester predicts even more damaging cyber-attacks across a wide swath of IoT implementations. The report is not optimistic about improvements in IoT security, predicting more successful attacks on IoT devices and the platforms they run on.

In late 2017, the Federal Trade Commission (FTC) noted the importance of taking reasonable steps to safeguard privacy and security for IoT devices. The Agency submitted public comments to a working group convened by the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) that is developing guidance about ways for IoT device manufacturers to better inform consumers about security updates related to the devices.

IOT IMPACT ON VA

Charles Worthington, VA's Chief Technology Officer (CTO), indicated a VA roadmap for VA's estimated 70,000 IoT-connected devices already in use across the VA enterprise. Additionally, VA concerns about security and safety was codified in a November 2016 VA OIT Enterprise Design Pattern (EDP) entitled Mobility and Internet of Things. The document indicated that VA will refrain from enabling or using fog computing or endpoint-to-endpoint analytics capabilities, due to security concerns. "VA-owned endpoint devices will only communicate with designated

gateways, and not directly with each other." The EDP noted that this restriction may be lifted in subsequent versions of this EDP as IoT security matures."

NIST has already provided a roadmap to future IoT cybersecurity concerns to Federal agencies and private industries. Its interagency report on the state of IoT cyber standards warned that without a standardized set of cybersecurity requirements in place, many IoT devices — from smart cars to the energy-efficiency sensors in the General Service Administration (GSA) headquarters building — could be vulnerable to cyber-attack.

CONCLUSION

Digital Journal reports that fog networking supports the *Internet of Everything* (IoE) concept, wherein most daily-use devices will be interconnected with each other, phones, connected vehicles, consumer appliances, and virtual reality (VR), using Google glass as prime examples. VR devices work under a 5K environment and at network edge with dynamic feeds (Google glass, tablets, and phones) in a cloud/fog scenario to reduce latency times and improve audio/video compression ratios that catch camera feeds in multi-camera systems. Autonomous vehicles for safe, easy transportation; subsurface geophysical imaging for fossil fuel detection; and process manufacturing alteration for improved product variation are just some of the benefits that well-networked fog nodes can bring about in industry, according to Computer Business Review.

Since fog computing enables the analysis of data at the edge of devices, its adoption among healthcare organizations is further estimated to increase to stem latency issues in the operation of healthcare apps requiring real-time analysis.

The purpose of healthcare IoT is to make it easier for patients to stay connected to their providers, and for their providers to deliver accountable, value-based care to their populations. Fog computing may be the foundational infrastructure for transforming healthcare IoT from novelty to reality. In order to accomplish this, the healthcare industry must overcome three of its major big data obstacles: (1) the challenge of turning big data into smart data, (2) the geographical distribution of providers and their lack of interoperability, and (3) the challenge of stringent patient privacy and security rules that govern the flow of sensitive health data.

Are you keeping up with technology topics like fog computing and its probable impact on the VA? Information about EDPs, Tech Insights, and What's New in Tech can be found at VA Pulse. Click here to register.

TECH INSIGHT SERIES

The monthly Tech Insight series aims to help readers make better decisions and be more informed customers of OIT products and services by providing them with high-level overviews of technologies that impact or will impact VA's IT environment. Tech Insights introduce topics in an easily digestible fashion by presenting background information on the topic, clearly explaining its importance within VA, and providing recommendations for success from OIT. All Tech Insights are available here.

DISCLAIMER: This document includes links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.