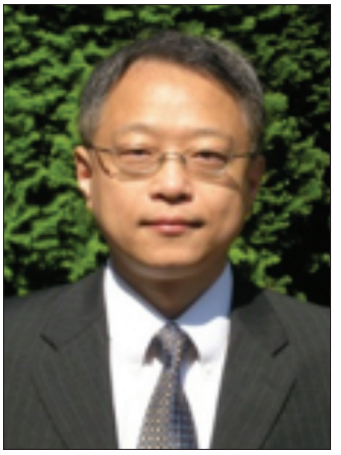
THE EMERGING ERA OF FOG COMPUTING AND NETWORKING

Harvey Freeman



Tao Zhang

Over the past decade, moving computing, control, and data storage into the Cloud has been the trend. However, today Cloud computing is encountering growing challenges in meeting many new requirements in the emerging Internet of Things (IoT). Such challenges include:

Latency Constraints: The stringent latency and delay requirements of many IoT systems fall far outside what mainstream Cloud services can support. For example, industrial control systems often demand end-to-end latencies to be within a few milliseconds. Many connected vehicle, virtual reality, gaming, and real-time financial trading applications may require latencies to stay below a few tens of milliseconds.

Network Bandwidth Constraints: The vast and rapidly growing number of connected things is creating data at an exponential rate. Sending all data to the Cloud will demand prohibitively high network bandwidth. This is often unnecessary. Sometimes, it is prohibited due to regulations and data privacy concerns.

Resource-Constrained Devices: IoT will support a vast number and variety of resource-constrained devices. Many such devices will not be able to rely solely on their own resources to fulfill all their computing needs. Requiring all of them to rely on Cloud services will be unrealistic and cost-prohibitive as well, because interacting with the Cloud often requires heavy processing and complex protocols. For example, the multitude of microcomputers on a car need firmware updates, but requiring each of these resource-constrained devices to perform the heavy cryptographic processing and run the complex procedures and protocols required for direct contact with the Cloud can be cost-prohibitive and also result in a system that is excessively difficult to manage.

Uninterrupted Services without Internet Access: Many IoT devices and systems, such as vehicles, drones, and oil rigs, may have intermittent network connectivity to the Cloud, but will require non-interrupted services.

New Security Challenges in IoT: Cloud and host computing alone have difficulty meeting many new security challenges in IoT. Such challenges include, for example, keeping the security credentials and software on the vast number and variety of resource-constrained devices up to date, authenticating and protecting these devices from security attacks, and assessing the security status of large distributed systems in a trustworthy manner.

Filling these and many additional gaps in today's computing models will require a new computing and networking paradigm. This new paradigm is Fog, which distributes computing, control, storage, and networking services closer to end users. Fog is a natural extension of the Cloud, bridging the Cloud and the endpoints to make computing possible anywhere along the continuum from the Cloud down to the end users. A Fog computing platform will allow the same application to run anywhere, reducing the need for specialized applications dedicated just for the Cloud or just for the edge devices. It will enable applications from different suppliers to run on the same physical platform without mutual interference. It will provide a common lifecycle management framework for all applications, offering capabilities for composing, configuring, dispatching, activating and deactivating, adding and removing, and updating applications. It will further provide a secure execution environment for Fog services and applications. This emerging Fog computing and networking era will represent a fundamental advancement in the state-of-the-art of computing and networking.

Fog provides effective ways to overcome many limitations of the existing Cloud and host computing models. Table 1 shows, for illustration, how Fog can help address the challenges we discussed at the beginning of this column.

Fog will also enable new and potentially highly disruptive business models for computing and networking. With Fog computing and networking, routers, switches, and application servers will converge into Fog nodes. Such a transformation can significantly reshape the landscape of the networking, server, and software industries. Fog-as-a-service will enable new models to deliver services to customers. Unlike Clouds that are mostly operated by large companies who can afford to build and operate huge data centers, Fog-as-a-service will enable companies, big and small, to deliver computing, storage, and control services at different scales to meet the needs of a wide variety of customers.

Proof-of-Concept (POC) trials are demonstrating the business value and technology necessity of Fog computing. For example, Cisco recently conducted a successful POC in Barcelona, where Fog computing made smart city applications more cost-effective and manageable. Barcelona envisions deploying thousands of roadside cabinets throughout the city to optimize traffic management, energy management, and water and waste management. Before they could turn this vision into reality, the city faced two major challenges. First, the traditional approach of adding new applications by adding dedicated new gateways and servers in every roadside cabinet is no longer feasible due to limited cabinet space. Second, the siloed applications have

IoT challenges	How Fog can help
Latency constraints	Store and process data, carry out control and other time-sensitive tasks near end users.
Network bandwidth constraints	Enable hierarchical data processing along the endpoint-to-Cloud continuum, hence reducing the amount of data that needs to be sent to the Cloud.
Resource-constrained devices	Perform resource-intensive tasks on behalf of resource-constrained devices when such tasks cannot be moved to the Cloud due to any reason.
Uninterrupted service with intermittent Internet access	A local Fog system can function autonomously to ensure non-interrupted services even with intermittent network connectivity to the Cloud.
New security challenges in IoT	Provide services to, for example: 1) manage and update security credentials and software on resource-constrained devices; and 2) protect devices that cannot adequately protect themselves.

Table 1. Fog provides capabilities to address IoT challenges.

been using siloed application management systems, which made the system excessively expensive to deploy and operate. Fog computing provided a solution. A single Fog node provided a common platform at each cabinet for all services and allowed applications from different suppliers to coexist without mutual interference. It provided a unified platform to support networking, security, and lifecycle management for all applications, reducing the system costs and allowing application providers to focus on developing applications rather than dedicated hardware and software for hosting and managing their applications.

On the journey to realize the full promise of Fog computing and networking, we will encounter many new challenges. For instance:

- What will Fog architectures look like?
- What new networking capabilities will Fog enable?
- How should the Fog interact with the Cloud?
- How to support the development and lifecycle management of Fog networks, services and applications?
- How to enable scalable and manageable Fog systems and networks?
- How to secure Fog computing and networking?
- How to enable users to control their Fog services?

Addressing these challenges necessitates rethinking of the end-to-end computing and networking paradigm, and will provide a fertile ground for innovation and disruption.

To that end, major industry movers and leading academic institutions joined forces to found a global Open Fog Consortium (OpenFog) in November 2015. The objective is to develop an open Fog reference architecture and to accelerate market adoption of Fog solutions. Championed by ComSoc, IEEE has entered into a strategic affiliation with OpenFog. We will co-create and co-promote Fog computing and networking concepts and architectures. We plan to jointly sponsor an annual Fog industry event. We will also co-sponsor events, journals and their special issues on Fog. Furthermore, we will jointly identify needs for new standards required to enable Fog computing and networking, and be ready to take leadership in developing these crucial standards.

At this historic moment, as we witness the emergence of the Fog computing and networking era, please join our efforts to enable and shape this new trend. The work and fun have just begun.

BIOGRAPHY

DR. TAO ZHANG, an IEEE Fellow, is a distinguished engineer/senior director of Cisco's Corporate Strategic Innovation Group. He joined Cisco in 2012 as the chief scientist for smart connected vehicles. Since then, he has also been leading initiatives to create strategies, architectures, technology, and eco-systems for the Internet of Things (IoT) and Fog Computing. Prior to Cisco, he was chief scientist and director of Mobile and Vehicular Networking at Telcordia Technologies (formerly Bell Communications Research or Bellcore). For more than 25 years he has been in various technical and executive positions, directing research and product development for vehicular, mobile, and broadband networking. He is a co-founder and a Board director of the Open Fog Consortium, the CIO of the IEEE Communications Society (2016-17), and a founding Board director of the Connected Vehicle Trade Association (CVTA). He holds more than 50 U.S. patents and has co-authored two books: *Vehicle Safety Communications: Protocols, Security, and Privacy* (2012) and *IP-Based Next Generation Wireless Networks* (2004), both published by John Wiley & Sons.