Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 12, Issue 4

Fog Computing: Intelligence for IoT

By Tony Merenda

The Internet of Things promises to be a transformative technology, potentially replacing or augmenting nearly every item in our daily lives (and likely introducing others not even dreamed of yet). The Fitbits and Nest thermostats of today are merely the beginning – Gartner foresees that as soon as 2020, the IoT may already include 26 billion connected units. The world to come is one in which every home, office, and place of business will be dense with IoT devices, from smart appliances to smart products to RFID tags and sensors, not to mention that each individual may be covered in IoT wearables everywhere they go. By their functions, these soon-to-be ubiquitous devices provide streams that are data rich and bandwidth hungry. Just as if in your home you suddenly began using hundreds of different smartphones to stream YouTube and then saw your Wi-Fi signal buckle under the pressure, this new IoT technology will require a new, more robust, network to support it.

Internet of Things devices will require always-on connections

Additionally, IoT devices are not only data intensive but require constant connectivity. Whereas with current connected devices, going offline may not totally impair functionality or have a major impact on the user's life (an offline tablet is inconvenient but still an app machine, a Fitbit still records data for later), many soon-to-come IoT devices like tags and sensors will lose their core functionally when not able to connect. Smart appliances and household controls will revert to their current non-smart input methods; and once users have become accustomed to the convenience of controlling the lights and doors and pre-heating the oven with their smartphones or voice commands, going back to the old ways will feel like having to stand up to change the channel on the television feels now. There's the possibility of more serious implications as well – say, for devices that perform vitally important medical monitoring. In the retail sector, already most storefronts are so Internet-dependent that they cannot complete transactions without an online connection – with more adoption of IoT solutions, loss of connectivity could produce slow downs and other issues throughout supply chains and enterprise business pipelines as well. Gartner finds that, even today, network downtime can cost an organization up to $300,000 every hour, and this can only be expected to increase as more IoT solutions are incorporated into enterprise processes.

Centralizing cloud data processing at a single site is currently a highly popular approach to satisfying data processing needs, largely because it offers lower costs and robust application security. The cloud itself has effectively slashed infrastructure costs for enterprises in recent years, trouncing traditional on-premises approaches with much cheaper and simpler-to-scale cloud delivery of on-demand computing, storage, and network services. It's this infrastructure – cloud computing at remote Internet data centers where the flow of data is governed by network gateways – that is utilized in realizing much of the IoT as it is today. However, this infrastructure will not suffice under the demands of a fully-realized IoT-enabled world without some significant reinforcement.

Fog computing bridges IoT and cloud for more dependable networks

Fog computing is a method for bridging the distance between IoT devices and remote data centers; by analogy, bringing the cloud down to earth and nearer to where all that raw data is being collected, and to where processed data in the form of device feedback or information is being returned to. In order to produce a less strained and more resilient system, fog computing selects the portion of the vast data sets created by IoT devices which would benefit most from fast response times and handles their processing load using computing resources placed at the network edge. In fog computing, data is filtered and summarized in order to reduce its volume, and to select the data of maximum importance and value to the task at hand. This filtered cream-of-the-crop data is caught and

processed by these nearer-by fog computing resources, not unlike a shortstop in baseball, and relayed back to the user with the lowest possible amount of latency. Meanwhile, those data processing tasks that are not as time sensitive or important are allowed to bounce into the outfield to be handled and relayed back by a remote data center (the center fielder, if you will). For IoT devices providing services that execute time-sensitive tasks and rely upon low-latency data processing, fog computing acts as an essential extension of the cloud that supports the performance quality that such devices require. As Gartner research director, Fabrizio Biscotti, observes: "IoT deployments will generate large quantities of data that need to be processed and analyzed in real time. Processing large quantities of IoT data in real time will increase as a proportion of workloads of data centers, leaving providers facing new security, capacity and analytics challenges."

By absorbing the most demanding strains and passing on the rest, fog computing reinforces the entire IoT infrastructure, from device to fog to cloud. As far as there are infrastructural issues providing reasons to doubt the implementation of a successful IoT future, conceptually, fog computing goes a long way to putting these fears to rest. Among vendors, Cisco is a proponent that has proposed a functional fog computing framework, which would use industrial-strength routers to safeguard the dependability of resources at the fog level. These routers would run open Linux and JVM platforms embedded with Cisco's own IOS, making it possible to leverage these open platforms in allowing applications to be ported to Cisco's infrastructure via code supported by an array of different vendors. To achieve the recognized goals of a fog computing design (low latency delivered at the edge, and high-volume traffic stemmed through smart filtering and reduced transmission of just summary and exception information to the cloud level), it falls upon smart gateways at the edge to successfully process or redirect those millions of tasks flying in from the vast constellation of IoT devices they are responsible for.

Fog computing's success depends on smart network gateways

Those smart gateways will require every bit of resilience they can muster to take on the magnitude of the task at hand, and guarantee the network uptime upon which there will be such a premium. As stated above, downtime is already expensive enough – in a future world permeated by IoT functionality that it takes for granted, any kind of network downtime could be as disabling as a power outage is today. For enterprises of any kind to maintain business continuity and customer loyalty while utilizing IoT solutions, uptime must be kept at the maximum. This can be achieved through the industry's bag of best tricks: redundant

Building an infrastructure that can support an exponential rise in the volume of connected devices is quite the undertaking, but one that can be achieved with fog computing.

connections with automatic failover, top of the line security, and most importantly, intelligence within the gateway devices that enables them to monitor their environment, power supply and other factors and to automatically deal with common threats to uptime (and wisely send alerts for help when advanced issues arise). At the same time, implementation of these smart gateways, and fog computing for the IoT in the first place, depends upon factors such as rapid deployment, scaling, simplicity of management without extravagant resources, and ultimately cost. These needs can be met by the technology, through smart gateways that feature cost-effective out-of-band access for full control of remote devices when primary connections fail, automated outage detection and recovery, resilient 4G LTE cellular connectivity with 3G failback, military-grade FIPS 140-2 security but, most importantly, the built-in intelligence to recognize and overcome causes of network downtime.

Building an infrastructure that can support an exponential rise in the volume of connected devices is quite the undertaking, but one that can be achieved with fog computing. To realize the countless benefits of the IoT at its full potential, that infrastructure will rely upon the intelligence and steadfastness of devices at the network edge.