Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are

What You Will Learn

The Internet of Things (IoT) is generating an unprecedented volume and variety of data. But by the time the data makes its way to the cloud for analysis, the opportunity to act on it might be gone. This white paper, intended for IT and operational technology professionals, explains a new model for analyzing and acting on IoT data. It is called either edge computing or Fog computing:

- Analyzes the most time-sensitive data at the network edge, close to where it is generated instead of sending vast amounts of IoT data to the cloud.
- Acts on IoT data in milliseconds, based on policy.
- Sends selected data to the cloud for historical analysis and longer-term storage.

What IoT Means to Your Business

The IoT speeds up awareness and response to events. In industries such as manufacturing, oil and gas, utilities, transportation, mining, and the public sector, faster response time can improve output, boost service levels, and increase safety.

Imagine it: On a factory floor, a temperature sensor on a critical machine sends readings associated with imminent failure. A technician is dispatched to repair the machine in time to avoid a costly shutdown. In oil and gas exploration, sensors on oil pipelines register a pressure change. In response, pumps automatically slow down to avert a disaster. In utilities, ruggedized cameras at remote field substations detect an intruder and alert security officers. Almost instantaneous analysis reveals similar events at other substations, automatically raising the alert to the highest level.

Connecting new kinds of things to the Internet also creates new business opportunities. Examples include pay-as-you-drive vehicle insurance, lighting-as-a-service, and machine-as-a-service (Maas).

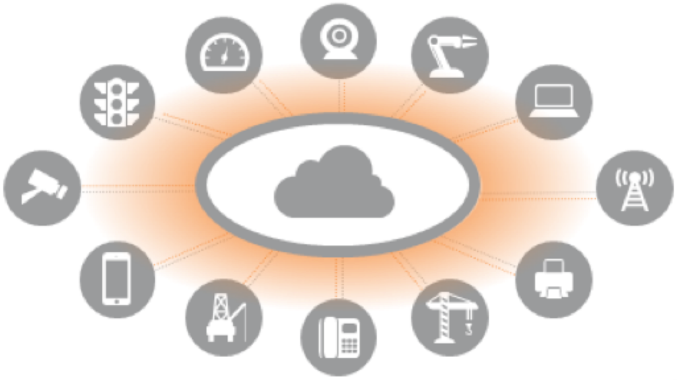
What IoT Means to Your Infrastructure

Capitalizing on the IoT requires a new kind of infrastructure. Today’s cloud models are not designed for the volume, variety, and velocity of data that the IoT generates. Billions of previously unconnected devices are generating more than two exabytes of data each day. An estimated 50 billion “things” will be connected to the Internet by 2020. Moving all data from these things to the cloud for analysis would require vast amounts of bandwidth.

> Today’s cloud models are not designed for the volume, variety, and velocity of data that the IoT generates.

These billions of new things also represent countless new **types** of things (Figure 1). Some are machines that connect to a controller using industrial protocols, not IP. Before this information can be sent to the cloud for analysis or storage, it must be translated to IP.

Figure 1. Connecting More and Different Kinds of Things Directly to the Cloud Is Impractical



Compounding the challenge, IoT devices generate data constantly, and often analysis must be very rapid. For example, when the temperature in a chemical vat is fast approaching the acceptable limit, corrective action must be taken almost immediately. In the time it takes for temperature readings to travel from the edge to the cloud for analysis, the opportunity to avert a spoiled batch might be lost.

Handling the volume, variety, and velocity of IoT data requires a new computing model. The main requirements are to:

- **Minimize latency:** Milliseconds matter when you are trying to prevent manufacturing line shutdowns or restore electrical service. Analyzing data close to the device that collected the data can make the difference between averting disaster and a cascading system failure.

> Analyzing data close to the device that collected the data can make the difference between averting disaster and a cascading system failure.

- **Conserve network bandwidth:** Offshore oilrigs generate 500 GB of data weekly. Commercial jets generate 10 TB for every 30 minutes of flight. It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the cloud. Nor is it necessary, because many critical analyses do not require cloud-scale processing and storage.
- **Address security concerns:** IoT data needs to be protected both in transit and at rest. This requires monitoring and automated response across the entire attack continuum: before, during, and after.
- **Operate reliably:** IoT data is increasingly used for decisions affecting citizen safety and critical infrastructure. The integrity and availability of the infrastructure and data cannot be in question.
- **Collect and secure data across a wide geographic area with different environmental conditions:** IoT devices can be distributed over hundreds or more square miles. Devices deployed in harsh environments such as roadways, railways, utility field substations, and vehicles might need to be ruggedized. That is not the case for devices in controlled, indoor environments.

- **Move data to the best place for processing:** Which place is best depends partly on how quickly a decision is needed. Extremely time-sensitive decisions should be made closer to the things producing and acting on the data. In contrast, big data analytics on historical data needs the computing and storage resources of the cloud.

Traditional cloud computing architectures do not meet all of these requirements. The prevailing approach—moving all data from the network edge to the data center for processing—adds latency. Traffic from thousands of devices soon outstrips bandwidth capacity. Industry regulations and privacy concerns prohibit offsite storage of certain types of data. In addition, cloud servers communicate only with IP, not the countless other protocols used by IoT devices. The ideal place to analyze most IoT data is near the devices that produce and act on that data. We call it Fog computing.

Fog Computing 101

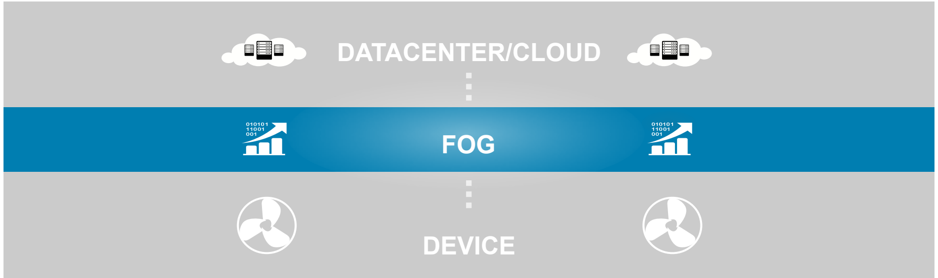
What Is It?

The fog extends the cloud to be closer to the things that produce and act on IoT data (Figure 2). These devices, called fog nodes, can be deployed anywhere with a network connection: on a factory floor, on top of a power pole, alongside a railway track, in a vehicle, or on an oil rig. Any device with computing, storage, and network connectivity can be a fog node. Examples include industrial controllers, switches, routers, embedded servers, and video surveillance cameras.

IDC estimates that the amount of data analyzed on devices that are physically close to the Internet of Things is approaching 40 percent.[1] There is good reason: analyzing IoT data close to where it is collected minimizes latency. It offloads gigabytes of network traffic from the core network, and it keeps sensitive data inside the network.

Analyzing IoT data close to where it is collected minimizes latency. It offloads gigabytes of network traffic from the core network. And it keeps sensitive data inside the network.

Figure 2. The Fog Extends the Cloud Closer to the Devices Producing Data



Examples of Fog Applications

Fog applications are as diverse as the Internet of Things itself. What they have in common is monitoring or analyzing real-time data from network-connected things and then initiating an action. The action can involve machine-to-machine (M2M) communications or human-machine interaction (HMI). Examples include locking a door, changing equipment settings, applying the brakes on a train, zooming a video camera, opening a valve in response to a pressure reading, creating a bar chart, or sending an alert to a technician to make a preventive repair. The possibilities are unlimited.

[1] IDC FutureScape: Worldwide Internet of Things 2015 Predictions.

Production fog applications are rapidly proliferating in manufacturing, oil and gas, utilities, transportation, mining, and the public sector.

When to Consider Fog Computing

- Data is collected at the extreme edge: vehicles, ships, factory floors, roadways, railways, etc.
- Thousands or millions of things across a large geographic area are generating data.
- It is necessary to analyze and act on the data in less than a second.

How Does Fog Work?

Developers either port or write IoT applications for fog nodes at the network edge. The fog nodes closest to the network edge ingest the data from IoT devices. Then—**and this is crucial**—the fog IoT application directs different types of data to the optimal place for analysis, as shown in Table 1:

- The most time-sensitive data is analyzed on the fog node closest to the things generating the data. In a Cisco Smart Grid distribution network, for example, the most time-sensitive requirement is to verify that protection and control loops are operating properly. Therefore, the fog nodes closest to the grid sensors can look for signs of problems and then prevent them by sending control commands to actuators.
- Data that can wait seconds or minutes for action is passed along to an aggregation node for analysis and action. In the Smart Grid example, each substation might have its own aggregation node that reports the operational status of each downstream feeder and lateral.
- Data that is less time sensitive is sent to the cloud for historical analysis, big data analytics, and long-term storage (see sidebar). For example, each of thousands or hundreds of thousands of fog nodes might send periodic summaries of grid data to the cloud for historical analysis and storage.

Table 1. Fog Nodes Extend the Cloud to the Network Edge

	Fog Nodes Closest to IoT Devices	Fog Aggregation Nodes	Cloud
Response time	Milliseconds to subsecond	Seconds to minutes	Minutes, days, weeks
Application examples	M2M communication Haptics[2], including telemedicine and training	Visualization Simple analytics	Big data analytics Graphical dashboards
How long IoT data is stored	Transient	Short duration: perhaps hours, days, or weeks	Months or years
Geographic coverage	Very local: for example, one city block	Wider	Global

[2] Haptics is controlling technology using the sense of touch. A realistic experience requires feedback in less than 1 millisecond.

What Happens in the Fog and the Cloud

Fog nodes:

- Receive feeds from IoT devices using any protocol, in real time
- Run IoT-enabled applications for real-time control and analytics, with millisecond response time
- Provide transient storage, often 1–2 hours
- Send periodic data summaries to the cloud

The cloud platform:

- Receives and aggregates data summaries from many fog nodes
- Performs analysis on the IoT data and data from other sources to gain business insight
- Can send new application rules to the fog nodes based on these insights

Benefits of Fog Computing

Extending the cloud closer to the things that generate and act on data benefits the business in the following ways:

- **Greater business agility:** With the right tools, developers can quickly develop fog applications and deploy them where needed. Machine manufacturers can offer MaaS to their customers. Fog applications program the machine to operate in the way each customer needs.
- **Better security:** Protect your fog nodes using the same policy, controls, and procedures you use in other parts of your IT environment. Use the same physical security and cybersecurity solutions.
- **Deeper insights, with privacy control:** Analyze sensitive data locally instead of sending it to the cloud for analysis. Your IT team can monitor and control the devices that collect, analyze, and store data.
- **Lower operating expense:** Conserve network bandwidth by processing selected data locally instead of sending it to the cloud for analysis.

Conclusion

Fog computing gives the cloud a companion to handle the two exabytes of data generated daily from the Internet of Things. Processing data closer to where it is produced and needed solves the challenges of exploding data volume, variety, and velocity.

Fog computing accelerates awareness and response to events by eliminating a round trip to the cloud for analysis. It avoids the need for costly bandwidth additions by offloading gigabytes of network traffic from the core network. It also protects sensitive IoT data by analyzing it inside company walls. Ultimately, organizations that adopt fog computing gain deeper and faster insights, leading to increased business agility, higher service levels, and improved safety.

For More Information

Fog computing is here today, as part of the Cisco IoT system. It can make your business more agile, faster to respond, and more innovative.

To learn more, visit: www.cisco.com/go/iot.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-734435-00 04/15