MOXA WHITE PAPER

Five Reasons Why Your IoT Application Needs Fog Computing

Ryan Teng
Moxa Product Manager

Abstract

Industry experts have warned that the cloud-computing models deployed in many IoT systems today are ill equipped to deal with the volume of data generated by the billions of IoT devices that are slated to go online in the next couple of years. To add to this, these devices generate data in a multitude of formats using a variety of protocols, making their acquisition and real-time processing difficult. In this white paper, we look at the fog computing model and why it is required in the today's IoT applications.

Cloud Computing vs. Fog Computing

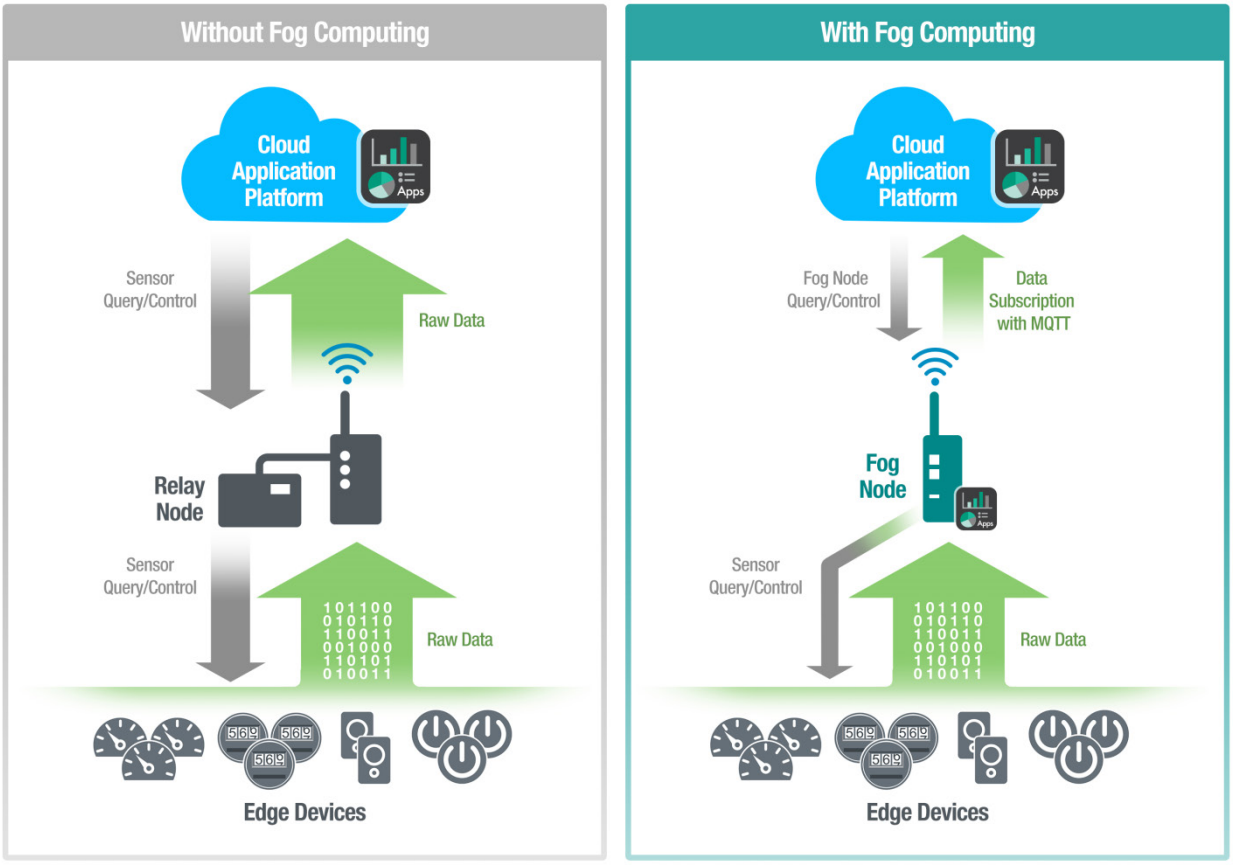
Cloud computing in the IoT is about centralized data processing. In contrast, fog computing focuses on moving computational power, storage capacity, device-control capability, and networking power closer to the devices.

Fog computing is a term created by Cisco that is used to describe computing on devices in an intermediate layer called the fog layer between the cloud and the IoT edge devices. The fog layer consists of fog nodes, which are essentially industrial controllers, gateway computers, switches, and I/O devices that provide computing power, storage, and connectivity services. The fog computing model extends the cloud closer to the edge of your network where the devices reside, and facilitates edge intelligence.

The explosive growth of the IoT is built on the premise of the availability of unlimited computing power and resources, which only cloud services can provide. In spite of its power and reach, the cloud computing model is not suitable for applications that are time-critical and applications where internet connectivity is poor.

Released on March 15, 2018

Moxa is a leading provider of edge connectivity, industrial networking, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 30 years of industry experience, Moxa has connected more than 50 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.



Fog computing works best in IoT-based systems with geographically dispersed end devices, where connectivity to cloud-based systems is irregular but low latency is a key requirement. IoT applications that periodically generate data in the order of terabytes, where sending data to the cloud and back is not feasible, are also good candidates for the fog computing model.

Cloud computing is recommended for:	**Fog computing is recommended for:**
Application that are not time sensitive and do not require real-time responses such as: ○ Big data analytics and dashboards ○ Data/pattern analysis and machine learning ○ Simulation and optimization ○ Predictive maintenance ○ Long-term data storage	Critical applications that are time-sensitive and require real-time responses such as: ○ Data acquisition and preprocessing ○ Condition monitoring ○ Rule-based decision making ○ Short-term data storage

IoT applications that process large volumes of data at distributed on-site locations and require quick response times are better served by a hybrid model that consists of both cloud and fog resources.

Why Your IoT Application Needs Fog Computing

The promotors of the fog computing model acknowledge that the cloud computing is here to stay and some functions in the IoT are better served by the cloud computing model. However, there are some distinct benefits that the fog computing model can bring to your IoT applications.

1. Latency

Sending all of your device data to the cloud for processing and analytics can take anywhere between a quick few minutes to several days at a stretch. For example, if your IoT devices are generating one terabyte (TB) of data per day, it could take you a couple of days to transfer this data to the cloud, process it, and generate actionable items from the data. By this time, the window of opportunity to act on the conclusions drawn from the data may have passed. Today's business applications demand a response time in the order of seconds or milliseconds. Time-sensitive applications, such as Industrial IoT, need immediate processing of device data to be able to take timely corrective actions. The fog computing model can minimize latency and enable quick decision making when compared to the cloud computing model.

2. Security

Sending sensitive operational data from the edge to the cloud puts the data and your edge devices at risk. Multiple levels of security need to be put in place in an IoT system to ensure that the data is securely transferred to cloud storage systems. Processing data at the edge helps prevent data breaches and enables faster responses.

3. Data Integrity

The cloud model has outsourced the storage and processing of data. Data integrity is a key concern in the IoT because sensitive day from various critical applications is stored on a public cloud. Cloud storage providers typically do not disclose the physical location of the storage. In addition, sending data from the device to a gateway and then to a cloud over the Internet puts the data at risk of corruption or unauthorized access.

4. Data-Transfer and Bandwidth Cost

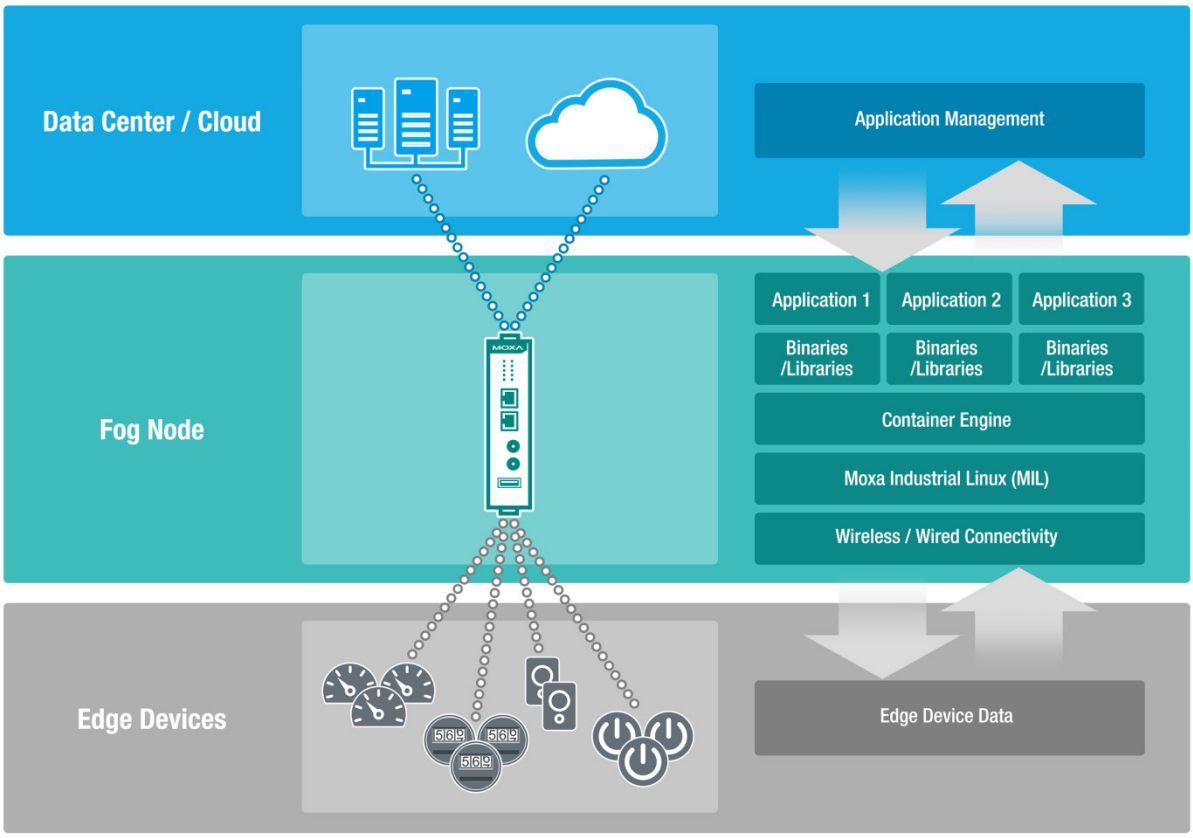
Transferring large volumes of data from the edge of the network to a cloud server can be prohibitively expensive. For example a typical offshore oil platform can generate 1 to 2 TB of data per day. The most common way for offshore oil platforms to transfer data is via a satellite connection, where data speeds range from 64 Kbps to 2 Mbps. With these data speeds, it would take more than 12 days to transfer one day's worth of data from the oil platform to a central repository. Furthermore, the cost of transferring this data on a daily basis could lead to unsustainable communication costs in the long run.

5. Independent Operation in Remote Locations

The fog computing model enables remote locations to reduce downtime and operate independently when the central system is inaccessible. For example, if there is a network outage and connectivity to the cloud system is lost, field sites can use local computing power to process and analyze data. Processed data can then be sent to the cloud for long-term storage when the connection is restored.

The Role of the Fog Nodes in Fog Computing

At the heart of the fog computing model are fog nodes. Fog nodes are geographically-dispersed resource-rich devices that can be deployed anywhere in a network. As the IoT evolves and proliferates into virtually every business domain, high-speed data processing, big-data analytics, and shorter response times are becoming the norm. Meeting these requirements through the current centralized cloud-based model is proving to be difficult, whereas the decentralized architecture of the fog computing model can bring computing resources and application services closer to the edge, thereby enabling faster response times. The fog nodes are bridging the gap between the OT (operation technology) and the IT (information technology) worlds.



Discussion on what the ideal profile of a fog node should be is ongoing, but the critical responsibilities of a fog node are:

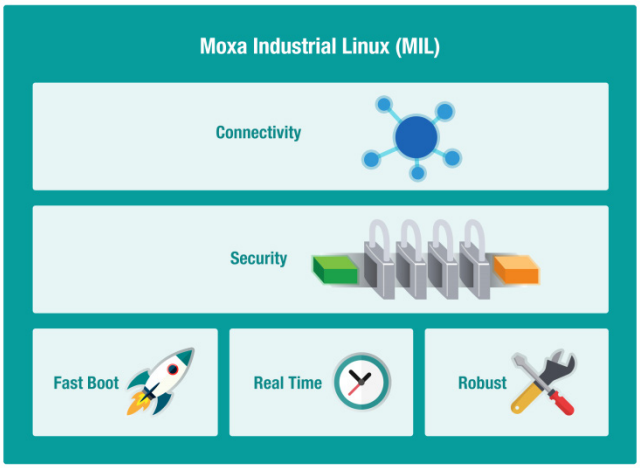
- Receive real-time data from IoT devices
- Run IoT-enabled applications for real-time analytics
- Can typically respond to requests in milliseconds
- Provide temporary data storage until the necessary data is transferred to the cloud
- Send periodic summaries of the data collected from the devices to the cloud
- Deploy applications from the cloud to the devices distributed across multiple locations

A framework that is based on a smart gateway (computer or router) with industrial-strength reliability, running a combination of open Linux and Docker container, and embedded with vendor's own proprietary application, is being touted as an ideal solution for fog computing. The Linux open platform enables easy porting of IoT applications to the IT infrastructure, while providing multi-vendor support and programmability. Some solution providers are proposing a layer of abstraction between the OS and the applications to facilitate easy deployment and management of applications on the fog node. Powered by these features, a fog node can intelligently process large volumes of data received from the sensors and field monitors and send only critical data or a summary of the data to the cloud.

Moxa's Solution

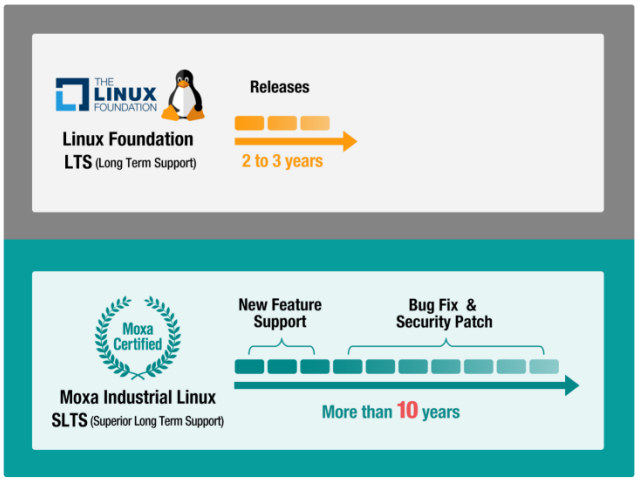
Moxa's fog computing solution consists of a powerful data-acquisition and device-control platform that includes Moxa Industrial Linux. To address the need for a long-term solution for civil infrastructure projects, such as power generation and distribution, water, oil and gas, transportation, and building automation, Moxa joins industry leaders, such as Codethink, Hitachi, Plat'Home, Renesas, Siemens, and Toshiba, to create a reliable and secure Linux-based embedded software platform that can be sustained for more than 10 years through the Civil Infrastructure Platform (CIP) project hosted by The Linux Foundation. The goal is to create an open-source platform for managing and monitoring IoT-enabled civil infrastructure and make it safe, secure, reliable, scalable, and sustainable. For additional information on the CIP, visit https://www.cip-project.org/.

Moxa Industrial Linux



Moxa Industrial Linux (MIL) is small footprint, high-performance, industrial-grade Linux distribution developed by Moxa with the aim of accelerating the development of embedded and IoT applications. To provide a reliable IoT platform to customers, Moxa will support MIL in its next-generation IIoT gateways and ARM-based computers. Moxa's IoT platform comes with a 5-year hardware warranty and supports a wide range of wireless modules, including Wi-Fi, Bluetooth, and 3G/LTE, for connecting various devices. The MIL provides a container-based virtual machine like middleware abstraction layer between the OS and the applications. The flexible software middleware allows you to run multiple isolated systems on a single control host so that you can easily change the behavior of the fog node without worrying about software compatibility. Armed with MIL, Moxa's next-generation IIoT gateways offer an efficient, flexible, and robust platform for diverse fog computing environments and scenarios.

Superior Long Term Support



Moxa's IIoT platform comes with a 10-yr long-term Linux support. As a leading provider of RISC computers with Linux solutions, Moxa ensures that our customers are kept up-to-date with the latest bug and security fixes via the MIL security service. Moxa Industrial Linux is regularly maintained with security patches and critical Linux updates that are delivered through a secure channel from a Moxa certified repository.