TORBZ - FOTOLIA

EVALUATE

3 OTA architectures for IoT devices

Organizations must pick the right OTA update architecture to ensure IoT devices receive the latest changes more efficiently and with less of an effect on your organization.

By **Julia Borgini,** Spacebarpress Media

Published: **04 Mar 2020**

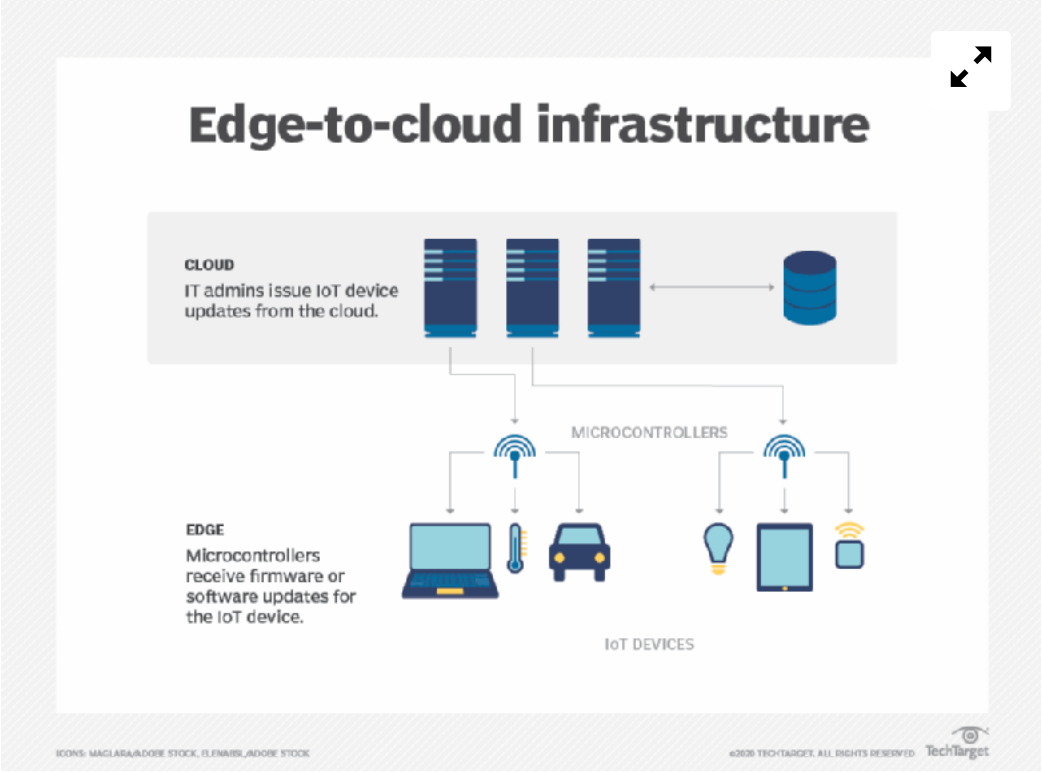
No matter how many IoT devices an organization uses, it's crucial to choose the OTA update approach that best fits the organization's needs to save time, effort and money.

Updating IoT devices becomes more critical as organizations integrate more devices into every phase of work on the network and depend more on IoT data gathering and processing. The correct over-the-air (OTA) update architecture for an organization depends the devices themselves, the business processes, and the availability and skill of the IT team. OTA updates are a scalable way to ensure IoT devices in the field have the latest settings, software and firmware. This method can keep the devices secure and maintain a high level of performance.

IT teams can use three different OTA architectures to ensure their IoT devices receive regular updates: edge-to-cloud, gateway-to-cloud and edge-to-gateway-to-cloud. The architecture an organization chooses depends on the required hardware, network architecture, IT team's skills and the IoT device itself.

Edge-to-cloud updates

With edge-to-cloud updates, an internet-connected microcontroller receives the update from the cloud that can patch the microcontroller's firmware or device software. The microcontroller acts as an update dispatcher and processor on the edge of the network and is positioned close to the IoT device.



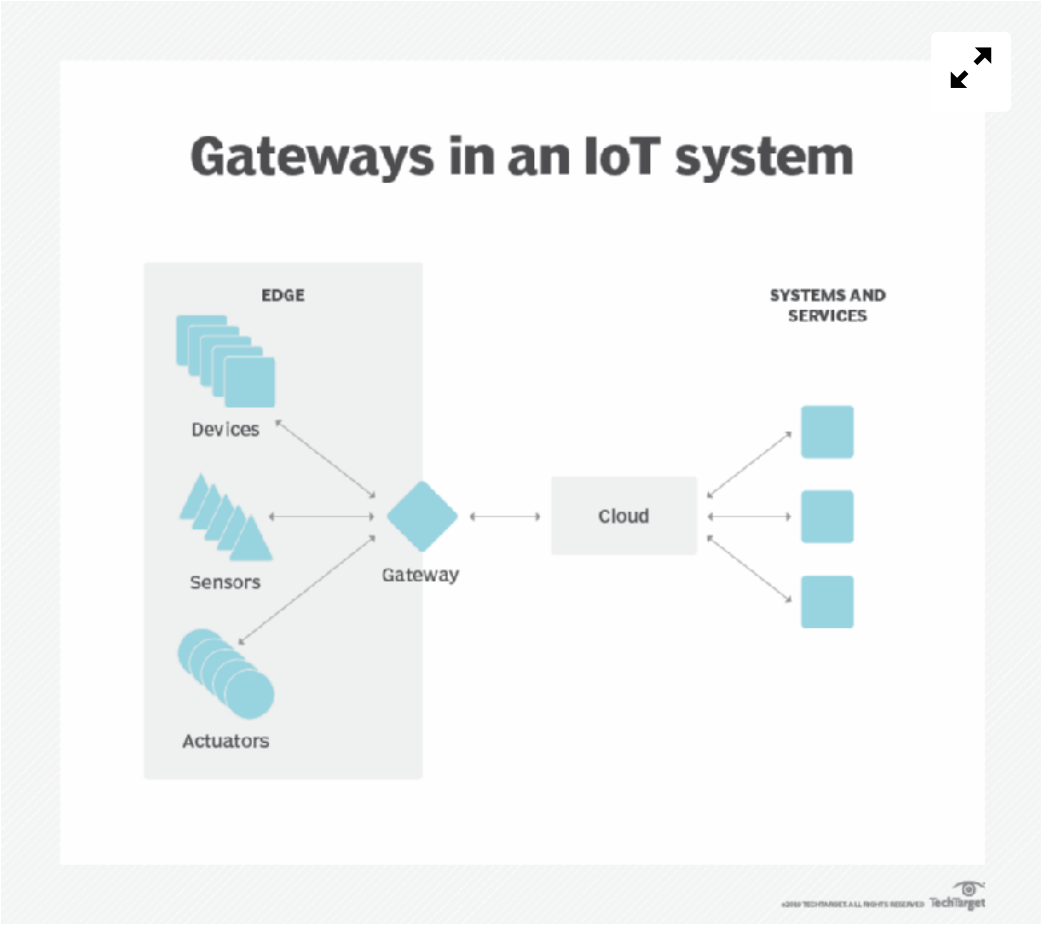
Benefits: The edge-to-cloud OTA architectures for IoT allow devices to receive updates separately based on function or need while leaving other devices alone. This prevents update issues from affecting the entire fleet of devices. For example, isolating updates in a healthcare setting would decrease the risk to patients whose lives may depend on the devices. IT staff could schedule updates during device downtime to minimize a decline in performance and business processes that use the device.

Drawbacks: Not updating all devices at the same time could introduce new risks.

Devices could miss critical security updates that expose them to hackers, as well as hardware and software failures, because they miss incremental fixes and patches. IT staff must also have a clear understanding of the devices that will be affected during each update so that they can inform business leaders before updating. Separate device updates increase the risk of bricking a device if the update is not completed correctly, unless it can recover automatically from a failed or interrupted update.

Gateway-to-cloud updates

The gateway-to-cloud OTA architectures for IoT have an internet-connected gateway that manages a fleet of IoT devices and receives updates from the cloud to patch its software application, the host environment or the gateway's firmware.



Benefits: The IoT devices remain untouched by gateway-to-cloud updates but enjoy the benefits of transmitting data through always-updated gateways. Gateways work to connect devices to systems that don't match device requirements. Some devices use low energy and don't support energy-intensive protocols such as Wi-Fi or Bluetooth to connect directly to the cloud. Other devices do not have enough processing power to handle the updates or are single use and not meant to handle updates, such as ones that only gather data to transmit to analytic services in the cloud.

Drawbacks: Updating only the gateway introduces a single point of failure for the entire fleet of devices. If the gateway update fails or is interrupted, any processes handled by the fleet behind it is at risk because data transmissions become inconsistent. If the gateway does not have automatic recovery from a failed update, it could fail completely, cutting off the entire fleet and reducing productivity. Problems could be compounded if multiple gateways have the same issue and it's not caught in time.

Depending on the gateway being updated and the roles of the IoT devices connected to it, there may never be a good time to update it. While updates can be sent to gateways at any time, the scheduling of the update could negatively affect the fleet if it's done during a high-traffic or heavy-processing time for the devices. Business processes may be negatively affected without warning if gateway updates are scheduled at inopportune times.

Edge-to-gateway-to-cloud updates

In edge-to-gateway-to-cloud architecture, the IoT gateway acts as a dispatcher for updating the fleet of IoT devices attached to it. The gateway downloads the IoT updates and transmits them to the devices.

Benefits: This architecture always updates devices based on individual needs, which reduces security risks and maintains high performance for each device. It also reduces the risk to the entire fleet in the case of a failed or interrupted update, because the rest of the fleet is isolated from it. Devices do not need to have a microcontroller to handle the update, nor do they need to be connected to the

internet. They get updates through a wired or wireless connection to the gateway device alone.

Drawbacks: The edge-to-gateway-to-cloud OTA architectures for IoT are useful in scenarios where internet connections are weak or budgetary restraints prevent sophisticated individual IoT devices, but it does have drawbacks. It creates a single point of failure if the gateway does not receive the update properly. The gateway will be unable to transmit updates to the individual devices. Hardware failures in the cabling between the gateway and device could prevent or interrupt the update. Devices may not have the ability to indicate when an update failed, leading to a mismatch in update schedules. The gateway might not be configured to identify devices with failed updates or devices that are bricked after an update, leading to a mismatch in updates. This would adversely affect business processes and cause time-consuming troubleshooting.

Next Steps

How to build an effective edge IoT architecture

Dig Deeper on IoT APIs, Applications and Software

Command tech conversations with IoT terminology you must know

By: **Kristen Gloss**

6 steps to prioritize IoT gateway security

By: **Julia Borgini**

Why so many enterprise IoT projects fail

By: **Thomas Ryd**

OTA update (over-the-air update)

By: **Erica Mixon**

Latest TechTarget resources

CIO

SECURITY

NETWORKING

DATA CENTER

DATA MANAGEMENT

SearchCIO

Amazon GDPR fine signals expansion of regulatory focus

Amazon's $887 million GDPR fine likely stems from consumer consent and may indicate the EU is moving beyond data breaches and ...

Inside look at Equifax's $1.5B digital transformation journey

A massive digital transformation effort at Equifax is gaining momentum. CTO Bryson Koehler talks about overhauling data ...