What is IoT Edge?

Azure IoT Edge is a combination of a cloud service running in the cloud and a runtime that runs on the device. IoT Edge is managed by the IoT Hub

Azure IoT Hub enables secure and reliable communication between your IoT solution and the devices it manages. **IoT Hub** provides a cloud-hosted solution backend to connect devices with per-device authentication, device management, and scaled provisioning

IoT Edge enables you to:

React in near real time to local changes and it is reliable to operate in offline or intermittent mode.

Manage edge devices and data to reduce costs.

Deploy using containers and secure and certified hardware.

Distribute AI and analytics workloads to the edge.

Use existing developer skillsets and code: IoT Edge code supports languages such as C, C#, Java, Node.js, and Python.

Provide security for edge deployments and ensures a privacy for IoT deployments.

Act as a gateway: IoT Edge can function as a protocol gateway and thus provide connectivity and edge analytics to IoT devices that would otherwise not have these capabilities.

Availability of third-party modules: Users can use third-party modules from the Azure marketplace to reduce time to market and enhance the robustness of software solution at the edge.

Azure IoT Edge comprises three components:

1. IoT Edge modules

The units of execution are implemented as Docker compatible containers. IoT Edge modules can run Azure services, third-party services, or user's own code and it can also run business logic in IoT Edge devices. The execution can run offline if needed by the users; can configure modules to communicate with each other to create a pipeline for data processing locally.

2. IoT Edge runtime

It manages the runtime and communication for the modules deployed to each device and ensures that the modules are always running and report module health to the cloud.

3. IoT Edge cloud interface

It enables users to monitor and manage IoT Edge devices remotely. Its cloud interface allows you to manage this overall lifecycle at scale for a diverse set of devices, which could be geographically scattered.

When to use IoT Edge?

Decision criteria

Near real-time response to local changes

Does your application need to react quickly to local changes in near real time? IoT Edge can run modules locally on IoT Edge devices to enable faster response to local changes.

Deploy and manage using Containers to IoT Edge devices

Does your application need to be deployed in docker compatible containers to IoT Edge devices? IoT Edge enables you to use containers to run your logic at the IoT Edge. Containers help to manage software dependencies such as runtimes and libraries, ensuring that the application runs consistently wherever it's deployed.

Security for IoT Edge deployments

The lack of security for IoT devices is a significant barrier to entry for many enterprises. IoT Edge provides security in several ways. These include integrating with Azure Security Center and by making use of any hardware security modules to provide strong authenticated connections for confidential computing.

Offline or intermittent mode operation

Does your application need to operate with intermittent of offline connectivity? IoT Edge devices automatically synchronize the latest state of your devices once they've reconnected to the cloud to ensure seamless operations.

Do you need to run machine learning algorithms on IoT Edge devices? IoT Edge enables you to deploy models built and trained in the cloud and run them on IoT Edge devices.

AI and analytics workloads to the IoT Edge

Optimize data costs

Management of costs in the deployment of Cloud resources is essential. You can design your system in such a way that data sent to the cloud is reduced by pre-processing on the IoT Edge devices.

Privacy for IoT Edge deployments

Do you need to ensure compliance for Privacy regulations? IoT Edge can protect personally identifiable data and keep data on-premises in that way improving compliance.

Azure IoT Hub

Azure IoT Hub enables secure and reliable communication between your IoT solution and the devices it manages. IoT Hub provides a cloud-hosted solution backend to connect devices with per-device authentication, device management, and scaled provisioning.

How IoT Hub works

Azure IoT Hub is the main Azure PaaS (Platform as a Service) which enables bidirectional communications between IoT devices and a cloud solution. IoT Hub is the starting point for any IoT solution, and it implements some essential functions that are common to IoT deployments. These include networking, compute, storage capabilities and security.

References:
https://docs.microsoft.com/en-us/learn/modules/introduction-iot-edge/2-what-is-iot-edge
https://docs.microsoft.com/en-us/learn/modules/introduction-to-iot-hub/2-what-is-iot-hub

IoT Hub features

Protocols supported:	IoT Hub allows devices to use the following protocols for device-side communications: MQTT, MQTT over WebSockets, AMQP, AMQP over WebSockets and HTTPS
Device Identity Registry:	IoT Hub maintains an identity registry. The identity registry stores information about the devices and modules permitted to connect to the IoT Hub.A device or module must also authenticate with the IoT Hub based on credentials stored in the identity registry.
Authentication:	Azure IoT Hub grants access to endpoints by verifying a token against the shared access policies and identity registry security credentials.
Device twins:	Azure IoT Hub maintains a device twin for each device that you connect to IoT Hub. Device twins store device-related information that Device and back ends can use to synchronize device conditions and configuration.

IoT Hub features (cont)

Endpoints that IoT Hub exposes:	For each device in the identity registry, IoT Hub exposes a set of endpoints: Send device-to-cloud messages; Receive cloud-to-device messages; Initiate file uploads; Retrieve and update device twin properties; Receive direct method requests.
Provisioning devices with Azure IoT Hub Device Provisioning Service:	The device provisioning service enables zero-touch, just-in-time provisioning to the right IoT Hub without requiring human intervention, allowing the customers to provision millions of devices in a secure and scalable manner.

Additional Features

The **telemetry function** is the essential component of the IoT Hub. The telemetry function involves recording and transmitting values received by an IoT device. However, IoT Hub is much more than the basic telemetry function.	The **scaling feature** of the IoT Hub allows you to ramp up (or down) the scope of the solution. The ability to scale a solution depends on two considerations: the features you plan to use and the amount of data you plan to move daily. Once you plan to deploy devices at scale, you need to manage these devices.

IoT Hub features (cont)

The **provisioning function** of IoT hub enables you to manage devices across the lifecycle of a device. Provisioning also establishes the security protocols for the device, its access rights, and privileges.

The security requirements can be seen as part of a **security function**, which manages the per-device authentication and access requirements with multiple authentication types. Based on the security functions, the **routing function** determines the message flow and the recipients of the message. Finally, you can connect to external devices natively using the **SDK functionality** and integrate with other services using the **service integration functionality.**

IoT Hub Decision criteria

Application complexity	**Azure IoT Hub offers two tiers**. If your IoT solution is based around collecting data from devices and analyzing it centrally, then choose the **basic tier**. The **basic tier** enables a subset of the features and is intended for IoT solutions that only need uni-directional communication from devices to the cloud. For more advanced configurations or to use distributed processing, use the **standard tier**. The **standard tier** of IoT Hub enables all features and is required for any IoT solutions that want to make use of the bi-directional communication capabilities. Both tiers offer the same security and authentication features.

IoT Hub Decision criteria (cont)

Data throughput	It depends on how much data you plan to move daily. Each IoT Hub tier is available in three sizes - numerically identified as 1, 2, and 3. Each unit of a level 1 IoT hub can handle 400 thousand messages a day, and a level 3 unit can handle 300 million.
Securing solution end to end allowing for per-device authentication	IoT Hub uses permissions to grant access to each IoT hub endpoint. Permissions limit the access to an IoT Hub based on functionality.
Bi-directional communication	Azure IoT Hub can be used to establish bidirectional communication with billions of IoT devices.In cloud-to--device messages, reliably send commands and notifications to your connected devices – and track message delivery with acknowledgement receipts. Automatically resend device messages as needed to accommodate intermittent connectivity.

More comprehensive list of considerations includes:

Telemetry

Does your solution need only basic telemetry services?

Geographic coverage

Does your solution need comprehensive geographic coverage?

Support for devices

Do you need to support a range of devices for your solution?

Manage a range of devices

Does your solution need only basic telemetry services?

Communication protocols

Does your solution need to connect over different kinds of communication protocols?

Message routing

How do you ensure that only the right devices talk to each other?

IoT Hub Decision criteria (cont)

Security	How do you secure the solution?

References:
https://docs.microsoft.com/en-us/learn/modules/introduction-iot-edge/2-what-is-iot-edge
https://docs.microsoft.com/en-us/learn/modules/introduction-to-iot-hub/2-what-is-iot-hub

By **Meri D.**
cheatography.com/meri-d/

Published 10th November, 2020.
Last updated 10th November, 2020.