IoT Infrastructure Guide

The Internet of Things (IoT) covers a broad range of industrites and applications. There many [IoT use cases](https://www.macrometa.com/solutions/use-cases/iot%22%20%5Ct%20%22_blank) which require:

* Cloud connectivity (asset tracking, home automation, industrial automation, etc.) using technologies like WiFi or cellular networks like NB-IoT, LTE-M, GSM, etc.
* Long-range local networks (smart city, smart agriculture, etc.) using technologies like LoRa, Zigbee, Sigfox, etc.
* Short-range local networks (tracking vital health parameters using wearables, smart door locks, etc.) using technologies like BLE, NFC, ZWave, etc.

While implementation specifics vary across these applications, the fundamentals of IoT infrastructure is the same.

As a result, a solid understanding of IoT infrastructure is an important aspect of building reliable IoT systems across industries. In this article, to help you improve your IoT skillset, we’ll take a deep dive on the topic of IoT infrastructure.

Infrastructure Requirements for IoT

At a basic level, Internet of Things refers to any system of interconnected devices that have sensors and embedded processing abilities. Note that devices don’t have to use the Internet. Even locally connected devices interacting and exchanging data are an IoT system.

With that in mind, we can break down the IoT infrastructure required to make an IoT system into these elements.

| **IoT Infrastructure Elements** |
| --- |
| **IoT Infrastructure Element** | **Description** |
| Sensor | Used for measuring physical quantities that the IoT device shares over the network |
| Controller | The brain of the device; acts as a bridge between the sensor and the network and also performs onboard computations and storage |
| Network | The technology used for exchanging data with either other devices in the system, or the Cloud |
| Cloud | Computing, storage and gateway resources accessible over the internet |
| User-facing applications | Mobile and web applications that allow the user to interact with the IoT system and visualize the data |
| Data Analytics | The tools and resources (often on the Cloud) that enable users to derive insights from the data sent by the IoT system |

In addition to these basic IoT infrastructure elements, optional hubs can connect a cluster of [IoT devices](https://www.macrometa.com/topics/iot-edge-computing-devices) to the internet. And finally, an attribute spanning all these infrastructure elements is security. In the following sections, we’ll take a closer look at each of these infrastructure elements.

### ****IoT Sensors****

IoT sensors are vital component of enabling IoT use cases. These sensors can monitor conditions like the temperature of a room using a temperature sensor or track a vehicle via GPS. IoT sensors are usually powered by a battery or external DC power source.

While most IoT systems have sensors, there can be some that don’t need them. For example, if you need to control a smart light using an app, you only need an IoT controller.

### ****IoT Controller****

An IoT controller is the brain of an IoT application. It acts as a bridge between the sensor and the network and often performs local computations. Today, IoT controllers are becoming more powerful in terms of storage and compute resources. This evolution is driving the popularity of [edge computing](https://www.macrometa.com/topics/edge-computing-vs-cloud-computing), which moves storage and compute closer to data sources (e.g., IoT sensors).

Like IoT sensors, controllers' use a battery or external power source.

### ****IoT Network****

Next comes the ‘interconnectivity’ part. Without network connectivity, a device is not an IoT device but just a standalone computing device. To create an IoT system, devices must connect to other devices or the cloud.

The types of connectivity vary depending on the application, ranging from cloud connectivity to short-range local connectivity (e.g., BLE). Likewise, different network communication mediums will require different IoT hardware (e.g., Bluetooth, WiFi, or LTE chips).

### ****IoT Cloud****

If IoT devices communicate with the cloud, you’ll need an IoT cloud platform.  You can either take up the monumental tasks of provisioning your own cloud infrastructure (in which case you will need to set up a dedicated server room with UPS, fire safety, redundancy, and backups) or use a cloud service provider like AWS, Azure, GCP, or [Macrometa](https://www.macrometa.com/solutions/use-cases/iot).

Cloud infrastructure for IoT applications involves not only the traditional data processing (app services, virtual machines, serverless functions, etc.) and storage (databases, cache, etc.) services, but also gateway services to gather incoming data and interact with the devices (HTTP/MQTT server, WebSocket server).

Scale is an essential consideration for cloud infrastructure built for IoT applications. If you plan to grow from a handful of devices to millions of devices, your cloud infrastructure should also scale in tandem. This is one of the reasons in-house server infrastructure isn’t ideal for IoT applications. IoT cloud platforms are more straightforward to scale than in-house physical server infrastructure.



Elements of Infrastructure for an IoT [System](http://ddd/)

### ****User Facing IoT Applications****

Depending on the application, the cloud infrastructure may also need to interface with **user-facing applications** (mobile or web apps), to enable the end-users to visualize the data and send commands to the devices. Thus, user management (sign up, sign in, forgot password, data APIs, etc.) becomes another consideration for your cloud infrastructure.

In some cases (especially BLE applications), the device may directly communicate with the end-user application without the cloud intermediary.

### ****IoT Analytics****

As the number of IoT devices increases, you may also start deriving insights from the data that these devices are dumping on your cloud. Thus, **data science and analytics** evolve into a subsystem and start taking up infrastructure on the cloud. Over here, infrastructure can be in the form of ETL tools, data warehouses, machine learning resources, etc.

### ****IoT Security****

Finally, let’s discuss the all-pervasive infrastructure attribute: **security**. Security is an attribute that influences the choice and design of every infrastructure element. Depending on the sensitivity of the data, you may need to secure it in transit and at rest. Thus, you may use HTTPS and not HTTP.

This security requirement may compel you to use a controller with hardware accelerators to perform the otherwise heavy encryption operation. Similarly, you may need to define access control rules for your cloud databases and define network inbound and outbound rules for your servers (so that not anyone can post or get data). When handling users’ personal data, you may need to adhere to the applicable regulations (like GDPR) and conduct regular security audits. You may even need dedicated resources to ensure compliance.

## ****Putting it All Together: The minimum IoT infrastructure for a real-world application****

Now that we understand the individual elements, let’s answer the question: **“What is the minimum amount of IoT infrastructure required for an IoT application?”**. We’ll use a cloud-connected temperature monitor system for a data center or computer room for this example.

First, you’ll need a thing. For this application, that thing is an IoT temperature sensor, a controller, and WiFi connectivity. We’ll use WiFi as our network medium because you can easily find controllers with built-in WiFi capabilities.

Next, you will build an MQTT or HTTP server on the cloud that will receive the data packets sent by your thing (sensors spread around your datacenter) and a database to store the packets. You can run a computation service to trigger notifications if the temperature crosses a threshold. You can optionally run a service to perform analytics on the historical data and report metrics like the mean temperature per day, typical variation in temperature, etc.

You will need a mobile or a desktop app to monitor the live data (and optionally historical data and analytics results).

If this data is for a secure facility, like a testing lab, you will need to encrypt the database and define its access control. You will need to ensure that all data transmissions are encrypted. You will also need to add user authentication to your app.

With all that, you’ve tied all the IoT infrastructure elements in this article come together to create an IoT system.