



# IoT Architecture Explained

What is it and how does it work?



Launching a successful deployment starts with understanding how IoT is to work. We break it down and take a closer look at the framework or architecture that an IoT system is based on.

## What is IoT Architecture?

The Internet of Things (IoT) is a complex ecosystem of interacting elements, including sensors, gateways, servers, and platforms for accessing information. IoT's growth is often hindered by its fragmentation—it's a difficult task to get so many disparate components of hardware and software to communicate with one another and work together as a whole.

Launching a successful deployment starts with understanding how IoT is designed to work. To do that, we'll take a closer look at the framework or architecture that an IoT system is based on.



# Why IoT Architecture is Important for the Future

Imagine a future rife with IoT devices, from self-driving cars to self-watering crops. If the promise of IoT functionality is to be realized, millions of connected devices will need to link and function simultaneously, linked to secure networks and data management systems. Here are three ways building strong IoT architecture today is essential for tomorrow's success.

## Interoperability

Everyone has faced interoperability issues at some point—for example, when your Apple product won't connect with your PC because they use different operating systems. In the world of IoT, this problem is multiplied. Thousands of companies have created their own devices with distinctive software, data formats, and APIs, making it hard for companies to piece together IoT solutions that function well. Thankfully, many IoT companies are getting wise to the need for interoperability and offering solutions that are hardware agnostic or have open APIs to make designers' jobs easier. Ultimately, we have to create devices, gateways, and platforms that link up and play well together.

## Standards and Governance

Even as companies scramble to adopt IoT sensors and systems, the lack of standards and governance practices has led to chaos and insecure data. Enterprises and governments are taking notice and stepping up to create standards for IoT security and data governance solutions. That's good news—because establishing clear-cut standards for IoT now will provide a solid foundation for future innovation.

## Security

The wide range of devices and operating systems combined with a lack of oversight has created a perfect storm of IoT security vulnerabilities. Up to now, there haven't been any government-imposed standards on IoT, and few third-party organizations that could provide standards comprehensive enough to impact security. (GSMA has laid out a set of IoT security guidelines and assessments for device designers, but they only really cover cellular devices since GSMA represents mobile operators and technologies.) Taking the time now to learn best practices for IoT security throughout the stack will help you move forward with confidence.





## How Does IoT Architecture Work?

Now let's take a closer look at how the elements of IoT architecture work together in a cohesive whole.

### 3 Layers of IoT Architecture

IoT architecture can be explained as three distinct stages or layers that together form a comprehensive framework. There's the device layer, comprised of many sensors deployed in various use cases from smart farming to IoT manufacturing applications. Data from the edge devices flows through a gateway for aggregation and cleansing before moving on to the platform layer. Here's a detailed look at each stage of IoT architecture.

#### Device Layer

Data-gathering devices are the centerpiece of IoT. All IoT devices, from a connected automotive system to a tiny LPWA sensor in a parking garage, are part of this layer, which generates the data that analysts need to derive value. Sensors can also be embedded in or attached to machinery or vehicles that weren't designed with IoT in mind—for example, many manufacturing companies are adding IoT sensors to their PLC systems and factory floor robots.

Actuators are another important part of the device layer. They're tightly linked with IoT sensors and allow task automation based on the data the sensors gather. For example, soil moisture sensors in a cornfield might show a need for irrigation. Actuators respond to that data by opening the irrigation valves and watering the crops. When the moisture sensors indicate that enough water has reached the crops, the actuator closes the valves. The entire process happens automatically, without the need for human oversight. With the addition of artificial intelligence (AI) and machine learning technologies at the edge, actuators are becoming able to carry out tasks that are more and more complex.



## Gateway Layer

At the gateway layer, data from disparate IoT devices is gathered before it's sent onward to a platform. An IoT gateway can be either hardware or a software program and acts as a doorway for data headed in either direction. One of the main benefits of an IoT gateway is the ability to preprocess at the edge. Mass IoT deployments may involve hundreds or thousands of devices, generating a collective mountain of data. The gateway can sort and process that incoming data, take initial cleansing action to reduce redundancy and errors, and only send out necessary (or “clean”) data to the server. This preprocessing reduces costs associated with cellular connectivity and can give operators a better real-time picture of the data. Gateways also add data security with features like encryption and tamper detection, helping to safeguard information that's being sent on to the cloud.

## Platform Layer

The platform layer provides a window for IoT leaders to view and analyze the data their devices are gathering. Broadly, an IoT platform is a software as a service (SaaS) product that can oversee a fleet of connected things. It performs multiple tasks—hence the word “platform”—and features vary from product to product. In the world of cellular, “IoT platform” refers to a connection-centric device management platform, needed for activating a line of service, changing a plan, managing billing, monitoring a service, or deactivating a device.

Some IoT platforms are hybrids, offering a combination of features, and most are cloud-based and flexible, with points of access that include mobile apps and web portals.



# Hardware Components of IoT Architecture

Now let's take a closer look at the hardware components involved in each layer of IoT architecture.

## Sensors and Actuators

IoT end devices can take many forms, from simple to complex. On the lower end of that are small battery-powered sensors that take a minimalist approach to data storage, processing, and communication. Often, these sensors connect using low power wide area network (LPWAN) technology. They don't constantly check in with the network; instead, they collect and send packets of data at regular intervals. They're used in situations where some latency—or delay in receiving data—isn't a problem. Some examples include a water level sensor on a tank or a smart electricity meter.

More complex IoT sensors might include tablets used in healthcare IoT, POS systems, smart glasses, smart video systems, AI robots, and other endpoints that need to process data in much greater quantities. These types of sensors require more bandwidth and typically use different cellular standards such as 3G and 4G, rather than LPWAN.

## Gateways and Data Acquisition Systems

Two types of hardware fall under the heading of data acquisition systems: direct-to-IP systems and gateway-based systems. Direct-to-IP systems do exactly what their title implies—connect the sensor node to an IP network directly. Gateways, on the other hand, use wireless connectivity as their link to sensors. For most use cases, gateway-based systems are the more practical hardware choice.

As we've already talked about, IoT gateways act as doorways for data traveling from edge devices to the IoT platform, typically in the cloud. They cleanse and filter the data, weeding out redundancies and other errors. Then, they convert it into a common protocol, encrypt it, and transmit it to the IoT platform. Modern gateways are also starting to enable another layer of computing at the edge.

As IoT deployments become larger and more data is routed through edge gateways, there's a growing interest in **edge computing**. Empowering analytics close to the source of data can speed up decision-making and save on data transmission costs—and keeping data on-premise adds a welcome layer of security.

## Data Centers and Cloud Infrastructure

While some companies still maintain on-premise data centers, many have shifted toward cloud-based solutions, in part because there's just so much digital data to store and process today. According to one recent survey, 96 percent of organizations have adopted cloud computing in one way or another. IoT deployments only add to that weight of data, making cloud storage even more appealing. But what is it, and how does it work?

Cloud infrastructure is remote hardware and software that's made available to users over the internet. When launching an IoT sensor deployment, you'd typically choose a cloud provider—who might also be your IoT platform provider, if you choose an end-to-end service—to receive and store your data. In a cloud management scenario, sensor data is encrypted and sent by secure connection to the remote cloud server. From there, authorized users can access it via an online web or mobile interface, and/or the data might be routed to a third-party platform or set of analytics tools.

# Real-life Examples of IoT Architecture

Let's take a look at a few use cases to see how their components fit into the big picture of IoT architecture.

## Fleet Management

IoT fleet management allows companies to track vehicle location, optimize routes, and keep track of maintenance and fuel consumption. At the device level, fleet management relies on sensors placed or embedded in vehicles to deliver the data. Typically, each vehicle has an in-vehicle computer that acts as a gateway, gathering and sending the data to the cloud via wireless cellular connection. At the platform layer, managers can access data from across the vehicle fleet through a web- or mobile app-based portal, send issue updates to drivers, and revise itineraries in real time.

## Retail POS Systems

IoT has many potential applications in retail, but point of sale (POS) systems are currently one of the most common. The POS device, often a tablet equipped with a card reader, acts as both device and gateway, delivering data directly to the cloud platform. (Larger companies might use an IoT gateway to connect POS terminals to the company's IT infrastructure.) Managers can then access the data through a cloud-based platform and use it to manage inventory, loyalty programs, purchase orders, and e-commerce efforts all in one place.



## Wearable Health Monitors

Healthcare is another wide-open field for IoT development. Connected health monitors promise to allow more and better telehealthcare and help patients manage chronic illnesses at home. At the sensor layer, a wearable health monitor might look like a wristband that monitors heart rate or a patch on the skin that monitors blood sugar levels. The sensor gathers health metrics and delivers that data (often wirelessly using Wi-Fi or Bluetooth connection) to a dock, which acts as the gateway layer. The dock aggregates and sends the data on to a platform, where the patient and their healthcare providers can access and analyze it.

## Conclusion

As IoT adoption continues to grow, leaders need to learn and apply the infrastructure patterns that can help it succeed. Ill-formed IoT deployments can collect lots of data without the ability to do anything useful with it. By starting with an understanding of the building blocks and taking a thoughtful approach, businesses can find ways to harvest their sensor data and make good use of it in real-time—and that is leveraging the power of IoT.

# Want to try Hologram? Contact us.

We're ready to help you deploy your cellular devices anywhere in the world.

[SALES@HOLOGRAM.IO](mailto:SALES@HOLOGRAM.IO)