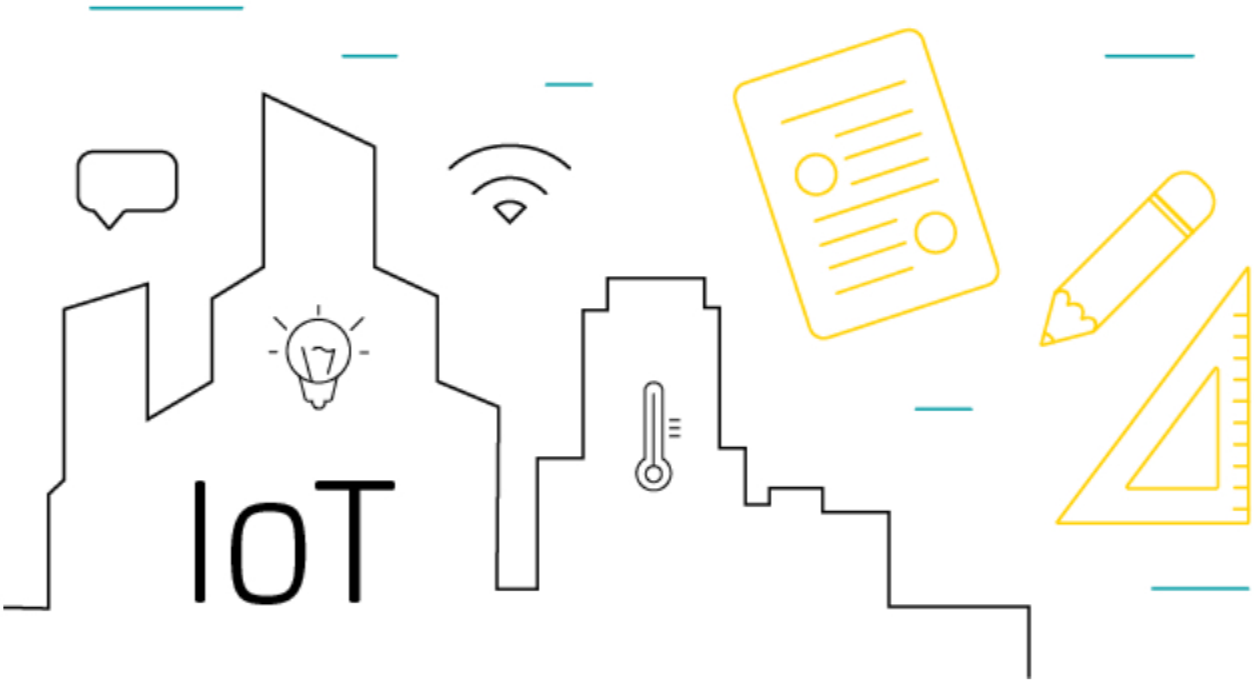
What is IoT architecture?



The concept behind the Internet of Things is as powerful as it is complex, and in order for the elements in the IoT puzzle to mesh together perfectly, they all have to be part of a well-thought-out structure. This is where IoT architecture enters the stage, especially in terms of IoT device management.

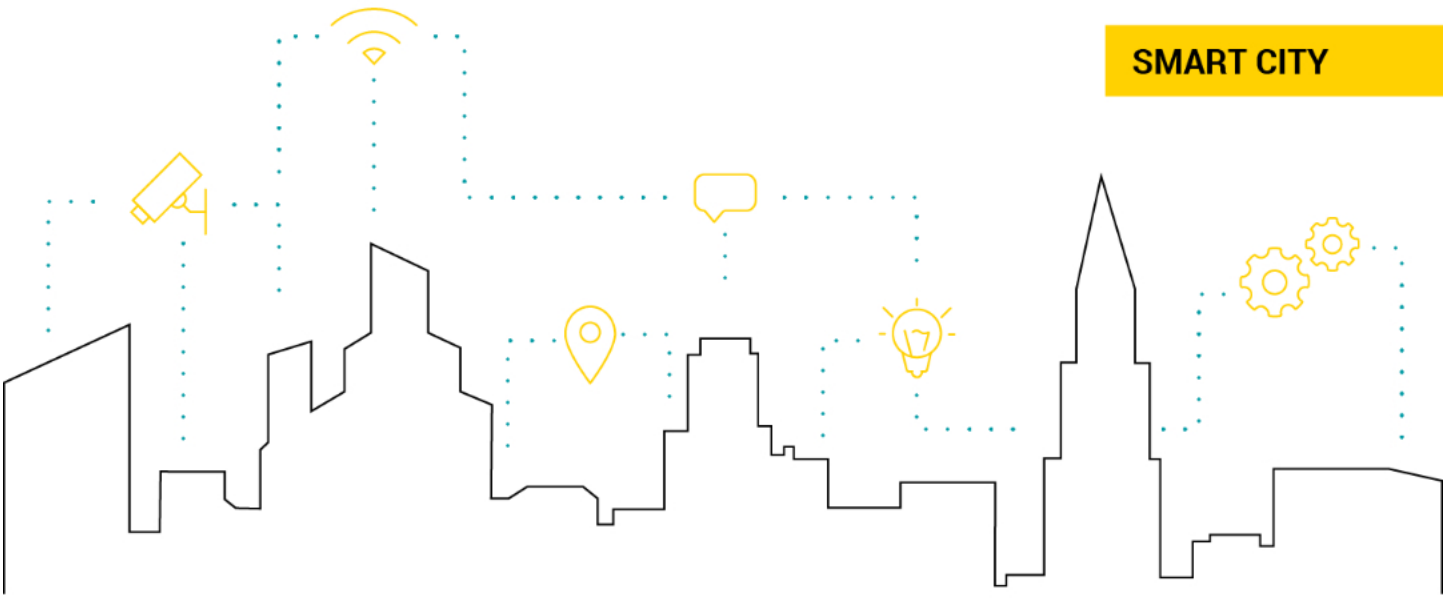
From IoT hype to IoT reality

The first thing that comes to the mind of an average John Doe when hearing the catchphrase ‘Internet of Things’ is probably a smart coffee maker that knows exactly what kind of coffee he will need in the morning before he even wakes up and realises it. Or, better still, a futuristic-looking autonomous car dashing through the IoT-empowered streets without the ‘driver’ even touching the steering wheel once.

While these hopeful-but-naïve visions are not as far-fetched from reality as they sound, IoT is not only about home and urban automation. In fact, far from being a mere buzzword, it stands for many, many more. Indeed, just as the Internet of Things has the power to change and improve our daily lives along with the ways in which we function as a society, it can also transform the way business is run and, ultimately, the way we perceive practically every aspect of our world.

Why do you need a robust Internet of Things architecture?

Still, when talking about the Internet of Things, much attention is paid to its potential. News about what IoT *will* be able to do and how it *will* empower our lives keeps flooding in, but for many it may seem that these uplifting visions don't translate into reality as fast as we wish they could. Nevertheless, the big change does happen, yet it happens in dribs and drabs rather than in giant leaps. The reason for this is quite simple, but it tends to stay out of the public eye: it is the inherent diversity of IoT systems that stifles the progress and often stands in the way to make all things connected.



As one of two presumably biggest challenges standing before IoT (the other being security), fragmentation is at the core of the Internet of Things because of the diverse nature of the Things that it aims to connect. Putting any IoT system to work requires harnessing all the resources, hardware, software, and systems, however varied they all may be, into one single framework to form an integrated, reliable, and cost-effective solution. In simple terms, every IoT deployment needs a rock-solid IoT architecture to be able to serve its designed purpose; the resulting efficiency and applicability of the system largely depends on the quality of the infrastructure developed.

IoT architecture building blocks

While every IoT system is different, the foundation for each Internet of Things architecture as well as its general data process flow is roughly the same. First of all, it consists of the Things, which are objects connected to the Internet which by means of their embedded sensors and actuators are able to sense the environment around them and gather information that is then passed on to IoT gateways. The next stage consists of IoT data acquisition systems and gateways that collect the great mass of unprocessed data, convert it into digital streams, filter and pre-process it so that it is ready for analysis. The third layer is represented by edge devices responsible for further processing and enhanced analysis of data. This layer is also where visualisation and machine learning technologies may step in. After that, the data is transferred to data centres which can be either cloud-based or installed locally. This is where the data is stored, managed and analysed in depth for actionable insights.

These are the four layers of IoT architecture described in detail:

Things, sensors and controllers

As the basis for every IoT system, connected devices are responsible for providing the essence of the Internet of Things which is the data. To pick up physical parameters in the outside world or within the object itself, they need sensors. These can be either embedded in the devices themselves or implemented as standalone objects to measure and collect telemetry data. For an example, think of agricultural sensors whose task is to measure parameters such as air and soil temperature and humidity, soil pH levels or crop exposure to sunlight.

Another indispensable element of this layer are the actuators. Being in close collaboration with the sensors, they can transform the data generated by smart objects into physical action. Let's imagine a smart watering system with all the necessary sensors in place. Based on the input provided by the sensors, the system analyses the situation in real time and commands the actuators to open selected water valves located in places where soil humidity is below the set value. The valves are kept open until the sensors report that the values are restored to default. Obviously, all of this happens without a single human intervention.

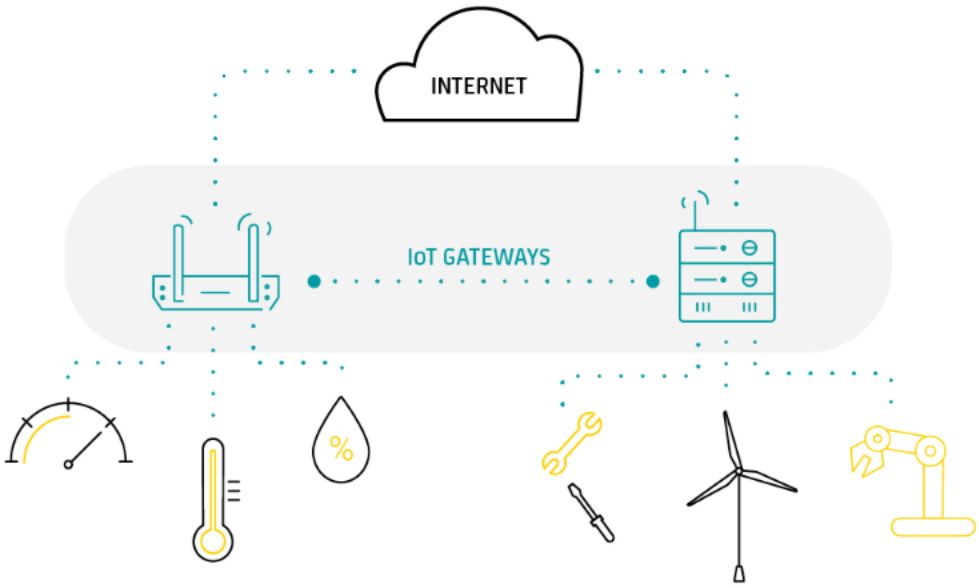
What is also important is that the connected objects should not only be capable of communicating bidirectionally with their corresponding gateways or data acquisition systems, but also being able to recognise and talk to each other to gather and share information and collaborate in real time to leverage the value of the whole deployment. In case of resource-constrained and battery-operated devices particularly, achieving this is not an easy task since such communication requires lots of computing power and consumes precious energy and bandwidth. Therefore, a robust architecture can only enable effective device management when it uses fit-for-purpose, secure and lightweight communication protocols, such as Lightweight M2M which has become a leading standard protocol for the management of low power lightweight devices which are typical for many IoT use cases

Gateways and data acquisition

Although this layer still functions in close proximity with sensors and actuators on given devices, it is essential to describe it as a separate IoT architecture stage as it is crucial for the processes of data collection, filtering and transfer to edge infrastructure and cloud-based platforms. Given the massive volume of input and output that million-device deployments may generate, capabilities for the aggregation, selection and transportation of data should be in the spotlight. As intermediaries between the connected things and the cloud and analytics, gateways and data acquisition systems provide the necessary connection point that ties the remaining layers together.

Sitting at the verge of the worlds of OT and IT, gateways facilitate communication between the sensors and the rest of the system by converting the sensor data into formats that are easily transferable and usable for other system components down the line. What's more, they are able to control, filter and select data to minimise the volume of information that needs to be forwarded to the cloud, which positively affects network transmission costs and response times. Thus, gateways provide a place for the local preprocessing of sensor data which is squeezed into useful bundles ready for further processing.

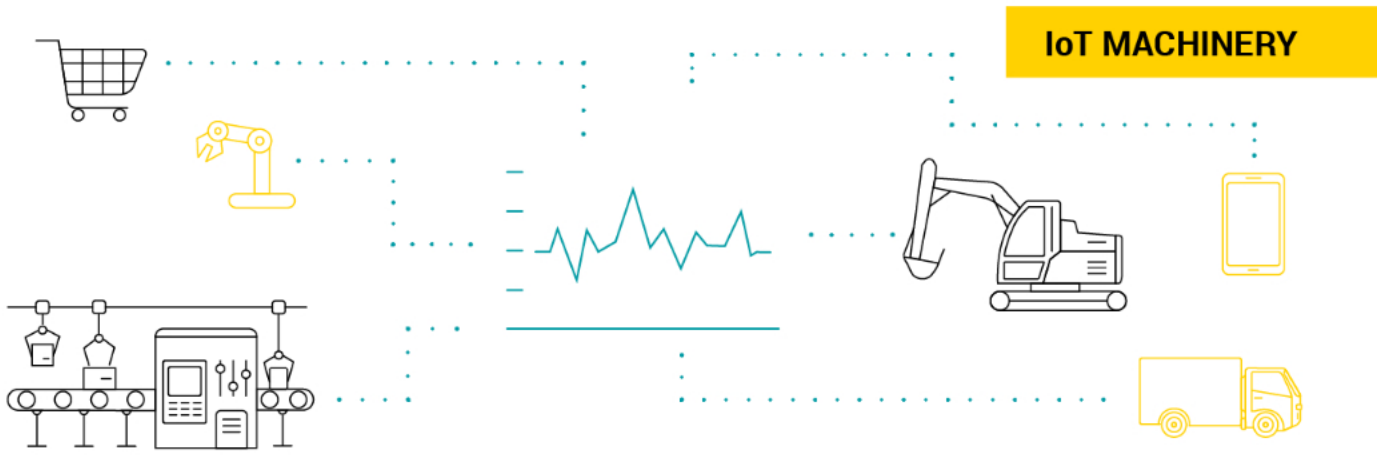
Another aspect that the gateways support is security. Because the gateways are responsible for managing the information flow in both directions, with the help of proper encryption and security tools they can prevent IoT cloud data leaks as well as reduce the risk of malicious outside attacks on IoT devices.



Edge analytics

While not being an inevitable component of every IoT architecture, edge devices can bring significant benefits especially to large-scale IoT projects. In the face of limited accessibility and data transfer speed of the IoT cloud platforms, edge systems can provide quicker response times and more flexibility in the processing and analysis of IoT data. As speed of data analysis is key in some Industrial Internet of Things applications, edge computing has recently seen a dramatic increase in popularity among Industrial Internet of Things ecosystems.

As edge infrastructure can be located closer to the data source in physical terms, it is easier and quicker for it to act on the IoT material in real time and provide output in the form of instant actionable intelligence. In this scenario, only the larger chunks of data which really need the power of the Cloud to be processed are forwarded there. By minimising network exposure, security can be significantly enhanced, while reduced power and bandwidth consumption contributes to more efficient leveraging of business resources.



Data centre / Cloud platform

If sensors are neurons and the gateway is the backbone of IoT, then the cloud is the brain in the Internet of Things body. Contrary to edge solutions, a data centre or a cloud-based system is designed to store, process and analyse massive volumes of data for deeper insights using powerful data analytics engines and machine learning mechanisms which edge systems would never be able to support.

Having seen increased adoption (especially in Industrial IoT architecture) over the past several years, cloud computing contributes to higher production rates, reduction of unplanned downtime and energy consumption and many other business benefits.

If furnished with proper user application solutions, the cloud can provide business intelligence and presentation options that help humans interact with the system, control and monitor it and make informed decisions on the basis of reports, dashboards and data viewed in real time.

Example Internet of Things architecture

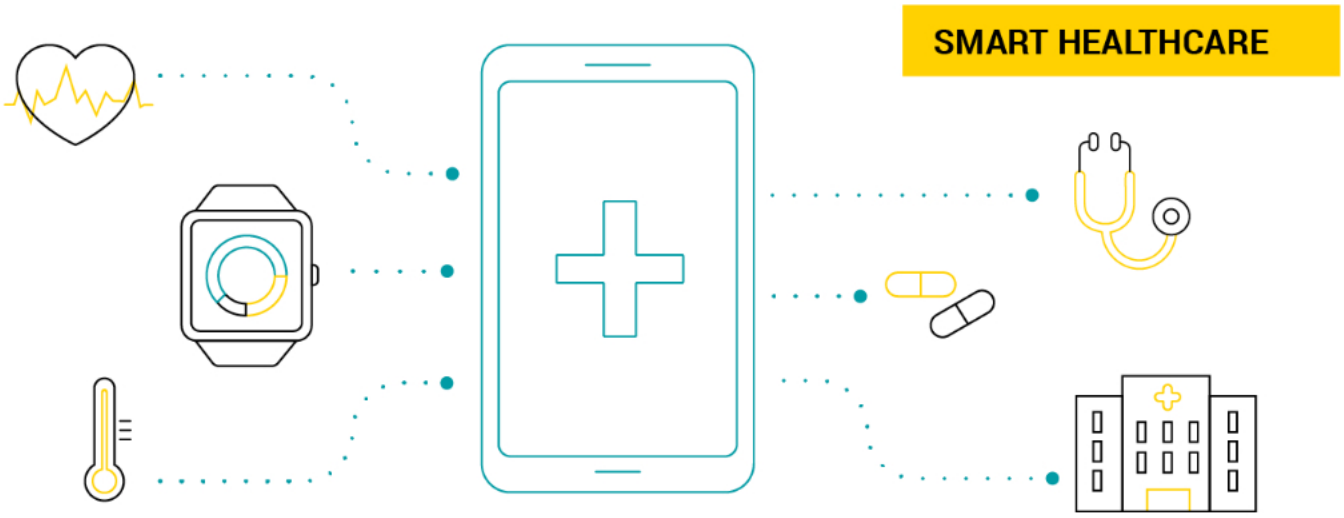
Healthcare is among the major industries that have been leaders and forerunners in the adoption of the Internet of Things technologies. The reason for this is that IoT systems help to leverage high quality care for patients and combine it with long-run but massive savings.

Within healthcare, the key IoT applications include, but are not limited to, enhancement of patient and personnel safety and security, reduction of unnecessary healthcare costs, and the provision of suitable support at the right time by employing IoT-empowered smart medical and emergency systems.

In view of the huge population challenges ahead, one of the greatest concerns in healthcare is elderly care and monitoring of illnesses like diabetes and heart-related diseases. Thus, prevention plays a key role in providing better health for elderly patients. Therefore, it is no wonder that the Internet of Things is gaining ground especially in health monitoring, where reliability, security and real-time precise control are a must.

The example automatic monitoring system for elderly patients requires data collection and real-time analysis, network connectivity for access to the infrastructure services, and an application to support user interface and display. Therefore, its architecture must include body sensors to collect patient data, gateways to filter and forward the data, microcontrollers or microprocessors to analyse and wirelessly send the data to the cloud as well as a communication tool to transfer the data to a remote location like emergency service or healthcare provider for monitoring and tracking purposes.

The IoT architecture for the system consists of three stages: physical, communication, and application. The first layer features a multiple-sensor network that evaluates the patient's vital readings such as nutrition, medical intakes, and physical activities. Also included in the physical layer is another monitoring network that consists of in-house sensors and actuators to maintain air quality, temperature, and to analyse and determine any hazardous conditions for the patient. The second layer includes OT devices that collect the information gathered by the sensors, translate it into meaningful data streams and transfer them to a back-end destination. The third layer is where data is received, stored, and processed using cloud-based data analysis engines and machine learning mechanisms. The resulting insights can be used to recommend the proper healthcare service for each specific situation or applied in further research or management purposes.



The healthcare monitoring system presented must provide accessibility to different users. For example, the healthcare provider, the patient themselves, and any family members or caregivers. In view of this, one of the challenges of using IoT within healthcare monitoring is providing data security and privacy. Security can be achieved by having an encryption when transferring the data. An example is the use of a microprocessor that ensures and provides a secure encryption communication method through a secure socket layer (SSL).

Conclusion

As stated previously, IoT architecture may vary from solution to solution, but its core consists of the four building blocks that are key in providing the fundamental features that make a sustainable IoT ecosystem: functionality, scalability, availability, maintainability and cost-effectiveness. What is important here is not to let oneself be overwhelmed by the perceived complexity of the Internet of Things architecture and not to lose sight of the possibilities for implementing attractive and future-proof IoT projects. It is worth noting that a growing focus on the development of a robust IoT architecture observed among many major business players from various industry sectors has led them to success in squeezing more business value from their data to give them a competitive edge and help to outperform their competitors.

While it is true that there are still tons of work to be done in terms of overcoming IoT technology fragmentation, upon looking back, it is quite evident that much effort has been done to date to integrate the vast range of technologies and standards embraced by IoT (examples: LwM2M, oneM2M) and there is hope for a more unified and standardised future. However, before this becomes reality, the key to making the promise of IoT happen doesn't necessarily lie in obtaining a single rule-them-all IoT technology, but rather putting all the technologies in line so that they are efficient in the collection, management, analysis, and exploitation of the data by building a strong, future-proof, scalable and secure IoT architecture.