## What is the Internet of Things?

The Internet of Things refers to millions of physical devices that are connected to the internet and share data. These devices are embedded with sensors, internet connectivity, and hardware to allow control and communication via the web. Connecting these different objects together and adding sensors to them turns them into intelligent devices and enables them to collect and send real-time data without depending upon human intervention. IoT has made devices smarter and more efficient, thus bridging the gap between physical and digital worlds.

To understand it better, let us look at an example of a lightbulb. Normally, a lightbulb is a simple device that turns on and off on the click of a button. With IoT integrated sensor, a lightbulb can be turned on or off from anywhere thorough a smartphone app. Similarly, you can set up an air conditioning device to turn on and off by itself on set times, thus making it an IoT enabled device. An IoT device can be a toy, a surveillance camera, or even a driverless truck controlled from a remote location.

The term IoT is generally used for devices that normally do not come with inbuilt internet connectivity, and can communicate on its own without human involvement. This is why a smartphone or a computer is not considered as an IoT device. However, a smartwatch or any other wearable device may be considered as an IoT device.

## How Does IoT Work?

In a nutshell, the way IoT works can be described as follows:

* Physical devices have sensors that can collect data
* This data is shared via cloud and then integrated with associated software
* The software interprets and transmits the data to its users over the internet via a website or a mobile application

To explain it better in detail, we will talk about four basic components of an IoT system, i.e., devices with sensors, connectivity to internet, data processing and user interface. Let us look at each of these briefly and see how each component works.

1. **Devices with Sensors**

The first step is the collection of data from the environment by devices or sensors that serve as [data provider](http://www.cardzgroup.com/SmartTokenBands.html). This can be a simple process like reading temperature, or a complex one such as a complete video feed. A device can have multiple sensors joined together to perform one task or a number of tasks.

1. **Connectivity**

Once the data is received by the sensors, it is sent to the cloud by connecting through satellite, WiFi, cellular data, Wide Area Network, Bluetooth, or directly to internet via ethernet. Every option has its own tradeoff between range, bandwidth, and power consumption. Choosing an option for connectivity depends on your specific IoT application. However, all of them serve the same purpose, i.e., sending data to the cloud.

1. **Data Processing**

When the data reaches the cloud, the associated software processes it. Depending upon the data, it can be simple checks such as temperature readings, or complex processing such as identifying objects in a video (for instance, face identification of intruders).

1. **User Interface**

Now what will happen if there are actual intruders in your house, or the temperature was too above or below the range? That’s where it needs to alert the user. This can be done either via text, push notification, or an email. For instance, sending a text alert if temperature is very high in the cold storage of a factory.

A user can also check the information proactively without waiting for alerts, such as videos recorded through surveillance camera. This can be done via a web browser or a phone app.

What makes it more exciting is that this process is not necessarily one-way. Depending upon the app, a user can also perform an action in response to the alert. For instance, they can adjust the temperature in cold storage remotely, or start a buzzer at their home to scare away the intruders.

The same actions can also be carried out without the user automatically. Instead of waiting for a user to adjust the temperature or start a buzzer alarm, the system can do this itself if it is fed with the predefined set of actions. It can also notify the relevant authorities in addition to alerting the user.

## Wrapping it Up

IoT technology has changed the way we interact with things. It has added to convenience of everyday lives as well as many industries including supply chain, healthcare, mining, etc. However, currently it poses threats to security and privacy. IoT products that are badly installed or not regularly updated can easily open doors for hackers to attack corporate networks and even breach individual privacy at homes. However, as connected devices continue to increase in number, our working and living environments will increasingly consist of smart devices. If security and privacy of users is wisely taken care of, IoT has a lot of potential in numerous markets in the coming decade.