Chapter 3
The Things in IoT: Sensors and Actuators

3.1 Introduction

The Internet of Things (IoT) was defined in Chap. 1 as the intersection of the Internet, Things, and Data. Processes and standards were also added for a more comprehensive IoT definition. Things were defined as anything and everything stretching from appliances to buildings to cars to people to animals, to trees, to plants, etc.

Chapter 1 further categorized IoT into four main levels: IoT devices, IoT network, IoT services platform, and IoT applications. Each level has its own medium and protocols.

This chapter first defines the "Things" in IoT and then describes the key requirements for things to be able communicate over the Internet. The two main requirements for "Things" in IoT are sensing and addressing. Sensing is essential to identify and collect key parameters for analysis, and addressing is necessary to uniquely identify things over the Internet. While sensors are very crucial in collecting key information to monitor and diagnose the "Things," they typically lack the ability to control or repair such "Things" when overhaul is needed. This raise the question: why spend money to sense "Things" if they cannot be controlled? Actuators have been introduced to address this important question in IoT. With this in mind, the key requirements for "Things" in IoT now consist of sensing, actuating, and unique identification as shown in Figs. 3.1 and 3.2. It should be noted that sensing and actuating capabilities may be supported on the same device.

A. Rayes, S. Salam, *Internet of Things from Hype to Reality*,
https://doi.org/10.1007/978-3-030-90158-5_3

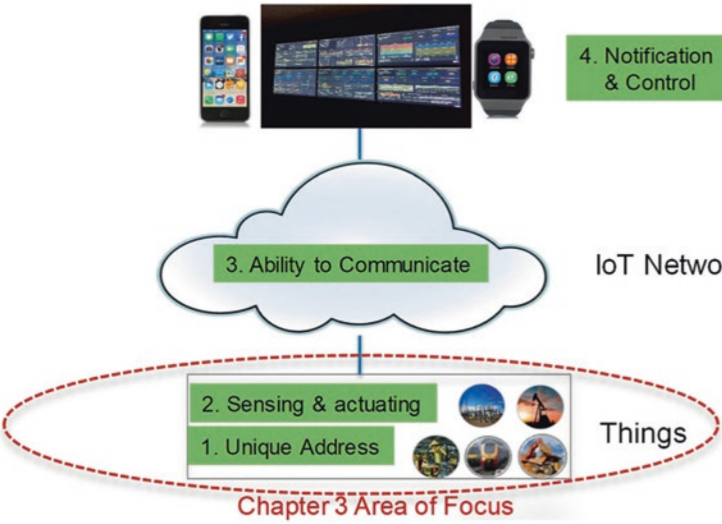

Fig. 3.1 "Thing" in IoT: definition view

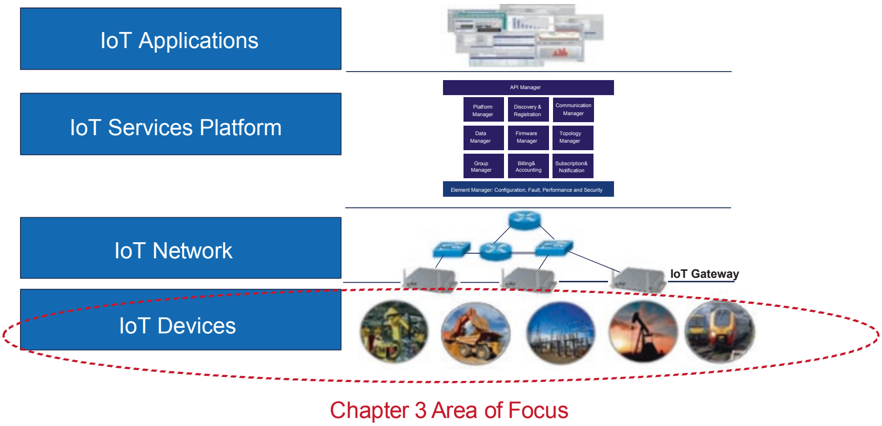

Fig. 3.2 "Things" in IoT: IoT level view

3.2 IoT Sensors

3.2.1 Definition

A sensor is a device (typically electronic) that detects events or changes in its physical environment (e.g., temperature, sound, heat, pressure, flow, magnetism, motion, chemical and biochemical parameters) and provides a corresponding output. Most sensors take analog inputs and deliver digital, often electrical, outputs. Because the

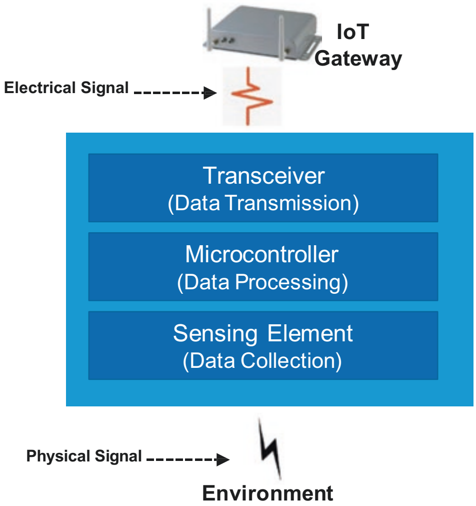

Fig. 3.3 Components of smart sensors

sensing element, on its own, typically produces analog output, an analog-to-digital converter is often required.

Sensors are comparable to the human five senses. They form the front end of the IoT devices, i.e., "Things." Sensors are very crucial in every IoT vertical (e.g., smart cities, smart grid, healthcare, agriculture, security and environment monitoring, and smart parking) as they bridge the world's physical objects with the Internet.

Sensors may be very simple with a core function to collect and transmit data or smart by providing additional functionality to filter duplicate data and only notify the IoT gateway when very specific conditions are met. This requires some programing logic to be present on the sensor itself. In this case, an IoT sensing device requires at least three elements—sensor(s), microcontrollers, and connectivity to send filtered data to IoT gateway or other systems. Figure 3.3 shows the components for smart sensor.

Sensors may collect large amounts of data at any time and from any location and transmit it over an IoT network in real time. The data is then analyzed and possibly correlated with other business intelligence databases to provide business insight or enhanced awareness of the environment, bringing onward opportunities and/or gains in efficiency and productivity.

3.2.2 Why Sensors

As we mentioned above, a sensor's main purpose is collecting data from its surrounding environment and providing output to its adjoining devices (e.g., gateways, actuators) or applications. Sensors typically collect data using physical interfaces (inputs) that sense the environment and then convert input signals into electrical signals (outputs) that are understood by the communication and computing devices. Output signals are then processed by the gateways and/or by applications of the IoT Platform. In some instances, sensors' outputs are processed directly by a lightweight application.

3.2.3 Sensor Types

There are many types of proprietary and nonproprietary sensors. The current IoT trend is to move away from proprietary and closed systems and embrace IP-based sensor networks. This allows native connectivity between wireless sensor networks and the Internet, enabling smart objects to participate in IoT. IP-based sensor networks require each device to be uniquely identifiable with a unique IP address so that it can be easily identifiable over a large network. Building an all-IP infrastructure from scratch, however, would be difficult because many different sensor and actuator technologies (both wired and wireless) have already been deployed over the years.

There are many different types of sensors across various technologies. The most common of which include:

1. *Temperature Sensors*: Temperature is perhaps the most commonly measured conservational quantity. This is anticipated since most physical, electronic, chemical, mechanical, and biological systems are affected by temperature. There are four types of temperature sensors:
   (a) Thermocouple Sensors: A thermocouple is a device consisting of two different and dissimilar conductors in contact. It produces a voltage as a result of the thermoelectric effect. Thermocouple sensor is made by joining two dissimilar metals at one end.
   (b) Resistance Temperature Detector (RTD) Sensors: RTDs are temperature sensing devices whose resistance changes with temperature. They have been used for many years to measure temperature in laboratory and industrial processes and have developed a reputation for accuracy, repeatability, and stability.
   (c) Thermistors: Similar to the RTD, the thermistor is a temperature sensing device whose resistance changes with temperature. Thermistors, however,

Fig. 3.4 Examples of temperature sensors and applications

are made from semiconductor materials. Resistance is determined in the same manner as the RTD, but thermistors exhibit a highly nonlinear resistance vs. temperature curve.

(d) Semiconductor Sensors: They are classified into different types like voltage output, current output, digital output, resistance output silicon, and diode temperature sensors. Modern semiconductor temperature sensors offer high accuracy and high linearity over an operating range of about 55 °C to +150 °C (−58 to 302 °F). They can also include signal processing circuitry within the same package as the sensor, thereby avoiding the need to add compensation circuits. Figure 3.4 shows examples of temperature sensor.

2. *Pressure Sensors*: Pressure sensors are used to measure the pressure of gases or liquids including water level, flow, speed, and altitude. Practical examples include sensors for pumps and compressors, hydraulic systems, and refrigerators. A pressure sensor typically acts as a transducer where it generates a signal as a function of the pressure imposed. Hence, pressure sensors are also called pressure transducers, pressure transmitters, and pressure senders, among other names.

   Touchscreen smartphones, tablets, and computers come with various pressure sensors. Whenever slight pressure is applied on the touch screen through a finger, tiny pressure sensors (typically multiple sensors located at the corners of the screen; see Fig. 3.5) determine where exactly pressure is applied and consequently generate an output signal that informs the processor. Pressure sensors have also been widely used in automotive applications to measure fluid level, airbag, and antilock braking system, in biomedical applications to sense blood pressure, in aviation to maintain a balance between the atmospheric pressure and the control systems of the airplanes, and in submarines to estimate depth and ensure proper operation of electronic systems and other components. Figure 3.5 shows examples of pressure sensors.
3. *Flow Sensors*: Flow sensors are used to detect and record the rate of fluid flow in a pipe or a system. They are also used to measure the flow/transfer of heat caused by the moving medium. Sensing and measuring the flow are critical for many applications ranging from bereave machine to more serious applications such as flow monitoring for high-purity acids.

Fig. 3.5 Examples of pressure sensors. (Source: Force Sensing & Fitbit)

Fig. 3.6 Examples of flow sensor

Fig. 3.7 Examples of level sensors with Wi-Fi propane remote monitoring. (Source: Tank Utility)

A good example about the importance of flow sensing and monitoring is the water crisis in Flint, Michigan, USA, which started in April 2014 and resulted in criminal charges filed against three people in regard to the crisis by Michigan Attorney General in April 2016.

Flint basically changed its water source from treated Detroit Water that was sourced from the great lakes and the Detroit River to the Flint River. Officials basically had failed to detect a very high lead contamination creating a serious public health danger. The acidic Flint River water caused lead from aging pipes to leak into the water supply, causing extremely elevated levels of the heavy metal. Thousands of children were exposed to drinking water with very high levels of lead, and many experienced health problems (Fig. 3.6).

4. *Level Sensors*: Level sensors are used to measure the level of fluids continuously or at point values. The element to be measured can be inside a container (Fig. 3.7) or can be in its natural form such as a well in an oil rig.

   There are many uses for level sensors. Ultrasonic level sensors, for instance, are used for non-contact level sensing of highly viscous liquids and even bulk solids. They are also widely used in water treatment applications for pump control and open-channel flow measurement. Another example is the capacitance level sensors to measure the presence of a variety of solids and liquids using radio-frequency signals in the capacitance circuit.

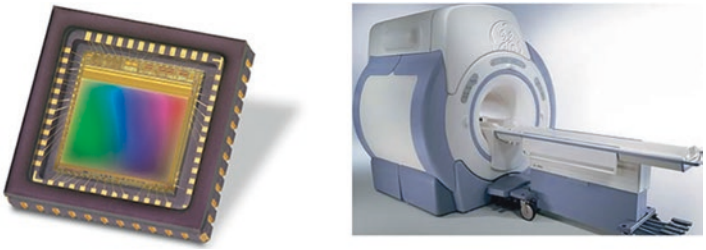

Fig. 3.8 Examples of imaging sensors. (Source: e2v & DGDL)

5. *Imaging Sensors*: Imaging sensors are sophisticated sensors used in digital cameras, medical imaging machines, and night vision equipment. They are utilized to measure image information by capturing and then converting variable attenuation of waves into signals (Fig. 3.8).
6. *Noise Sensors*: High noise can have damaging effects on humans (e.g., cardiovascular) as well as animals (e.g., hearing loss). Such noise is often caused by machines, airplanes, trains, construction, and loud music especially in closed spaces.

   Many government agencies have started installing noise sensors to measure noise pollutions or the so-called noise disturbance (excessive noise that may harm humans or animals).

   Ambient noise sensors continuously monitor noise levels in surrounding environments. When the noise level changes, they send electronic signal to an overall ambient noise system to take action. Such action may be an automatic action (e.g., adjust music level) or a simple notification to authorities.
7. *Air Pollution Sensors*: Many governments have established agencies to monitor and control the air quality in major cities. For instance, the USA has established the EPA (Environmental Protection Agency), in 1970, with a mission to protect Americans from significant health risks by providing accurate environmental information to its citizens.

   Air pollution sensors detect and monitor the presence of air pollution in the surrounding environment. They focus on five main components: ozone, particulate matter, carbon monoxide, sulfur dioxide, and nitrous oxide.
8. *Proximity and Displacement Sensors*: Proximity sensors detect the presence or absence of objects using electromagnetic fields, light, or sound. There are many types, each suited to specific applications and environments:

   (a) Inductive Sensors: Used for close-range detection of ferrous material.
   (b) Capacitive Sensors: Used for close-range detection of nonferrous material.
   (c) Photoelectric Sensors: Used for long-range target detection.
   (d) Ultrasonic Sensors: Used for long-range detection of targets with difficult surface (Table 3.1).

9. *Infrared Sensors*: Infrared sensors are used to track an object's movement. They produce and receive infrared waves in the form of heat.

Table 3.1 Examples of proximity sensor types

Sensor technology	Sensing range (mm)	Main use
Inductive	4–40	Ferrous metal (e.g., iron, aluminum, copper) close-range detection
Capacitive	3–60	Nonferrous material (e.g., wood, plastic liquid) close-range detection
Photoelectric	1–60	Material long-range target detection
Ultrasonic	3–30	Material long-range target detection with challenges (e.g., rough service, multiple colors)

10. *Moisture and Humidity Sensors*: Moisture and humidity sensors (sometimes referred to as hygrometer sensors) are used to measure and report the relative humidity in the air. They use capacitive measurement by relying on electrical capacitance.
11. *Speed Sensors*: Speed sensors are commonly used to detect the speed of transport vehicles. Examples include wheel speed sensors, speedometers, Doppler radar, and laser surface velocimeter.

There are so many other types of sensors. Examples include acceleration sensors, biosensors, gas and chemical sensors, mass sensor, tilt sensors, and force sensors.

3.2.4 Sensor Characteristics

Most IoT applications require smaller and smarter sensors with advanced functionality to collect more data, low-power processors, longer battery life, faster response time, and shorter time to market. Sensors are expected to be dynamic in their natural surroundings with embedded ability to collect real-time data.

In general, sensors can be either self-directed (autonomous) where they work on their own once they are installed or user-controlled where collection conditions are preprogrammed by the user depending on their needs. Finally, sensors should also have the capability to send the collected data (or a subset of it) to the appropriate system via the IoT gateway as we illustrated in Fig. 3.2.

IoT sensors are expected to have the following characteristics:

1. *Data Filtering*: A sensor's core function is the ability to collect and send data to the IoT gateway or other appropriate systems. Sensors are not expected to perform deep analytical functions. However, simple filtering techniques may be required. Onboard data (or signal) processing microcontroller (as shown in Fig. 3.3) makes a smart sensor smarter. The microcontroller filters the data/signals before transmission to the IoT gateway or control network. It basically removes duplicate or unwanted data or noise before transferring the data.

   As we mentioned in Sect. 3.2.3, non-autonomous sensors are custom-programmed to produce alerts automatically when certain conditions are met (e.g., temperature is above 70 °F in a data center). They often integrate VLSI technology and MEMS devices to reduce cost and optimize integration.

2. *Minimum Power Consumption*: Several factors are driving the requirements for low-power consumptions in IoT. Sensors for multiple IoT verticals (e.g., smart grid, railways, and roadsides) will be installed in locations that are difficult to reach to replace batteries.
3. *Compact*: Space will also be limited for most IoT verticals. As such, sensors need to fit in small spaces.
4. *Smart Detection*: An important sensing category for the IoT is remote sensing, which consists of acquiring information about an object without making physical contact with it; the object can be nearby or several hundred meters away. Multiple technology options are available for remote sensing, and they can be divided into three broad functions:

   (a) Presence or proximity detection—when just determining the absence or presence of an object is sufficient (e.g., security applications). This is the simplest form of remote sensing.
   (b) Speed measurement—when the exact position of an object is not required, but accurate speed is (e.g., traffic monitoring applications).
   (c) Detection and ranging—when the position of an object relative to the sensor must be determined precisely and accurately (e.g., vehicle collision avoidance).

5. *High Sensitivity*: Sensitivity is generally the ratio between a small change in electrical output signal and a small change in physical signal. It may be expressed as the derivative of the transfer function (the functional relationship between input signal and output signal) with respect to physical signal. Sensitivity indicates how much the output of the device changes with unit change in input (quantity to be measured). For example, if the voltage of a temperature sensor changes by 1 mV for every 1 °C change in temperature, then the sensitivity of the sensor is said to be 1 mV/°C.
6. *Linearity*: Linearity is the measure of the extent to which the output is linearly proportional to the output. Nonlinearity is the maximum deviation from a linear transfer function over the specified dynamic range.
7. *Dynamic Range*: The range of input signals which may be converted to electrical signals by the sensor. Outside of this range signals cause unsatisfactory accuracy.
8. *Accuracy*: The maximum expected error between measured (actual) and ideal output signals. Manufacturers often provide the accuracy in the datasheet, e.g., high-quality thermometers may list accuracy to within 0.01% of full-scale output.
9. *Hysteresis*: When a sensor does not return the same output value when the input stimulus is driven up or down. The width of the expected error in terms of the measured quantity is defined as the hysteresis.
10. *Limited Noise*: All sensors produce some level of noise traffic with their output signals. Sensor noise is only an issue if it impacts the performance of the IoT

system. Smart sensors must filter out unwanted noise and be programmed to produce alerts on their own when critical limits are reached. Noise is generally distributed across the frequency spectrum. Many common noise sources produce a white noise distribution, which is to say that the spectral noise density is the same at all frequencies.

11. *Wide Bandwidth*: Sensors have finite response times to instantaneous changes in physical signal. Also, many sensors have decay times, which represent the time after a step change in input signal for the sensor output to decay to its original value. The bandwidth of a sensor is the frequency range between these two frequencies. When a sensor is utilized to collect measurements, it is recommended to use sensors with the widest possible bandwidth. This ensures that the basic measurement system is capable of responding linearly over the full range of interest. The disadvantage, however, is that wider bandwidth may result in sensor response to unwanted frequency.
12. *High Resolution*: The resolution of a sensor is defined as the smallest detectable signal fluctuation. It is the smallest change in the input that the device can detect. The definition of resolution must include some information about the nature of the measurement being carried out.
13. *Minimum Interruption*: Sensors must operate normally at all time with zero or near-zero interruption and be programmed to produce instant alerts on their own when their normal operation is interrupted.
14. *Higher Reliability*: Higher reliability sensor provides the assurance to rely on the accuracy of the output measurements.
15. *Ease of Use*: Ease of use is considered the top requirement for any electronic system nowadays. Clear examples we have all experienced are Apple's iPhone vs. competitor devices with the same functionality. Users are willing to pay more for easy-to-use devices, and sensors are no exceptions. The best user interface is "no user interface" where sensors are expected to work by themselves once they are connected.

Other characteristics include some data storage and self-warning of anomalous symptoms.

3.3 RFID

Another way of capturing information from "Things" is through the use of RFID (radio-frequency identification). RFID is not a sensor but a mechanism to capture information pre-embedded into the so-called Tag of a thing or an object using radio waves.

RFID consists of two parts: a tag and a reader. Further, the tag has two parts: a microchip that stores and processes information and an antenna to receive and transmit a signal. The tag contains the specific serial number for one specific object. The reader reads the information encoded on a tag, using a two-way radio transmitter-receiver, by emitting a signal to the tag using an antenna. The tag responds with the information written in its memory. The reader will then transmit the read results to an RFID computer program.

An RFID-based solution has some advantages over older reader-tag-based solutions, such as barcode, including:

- RFID tag does not need to be within direct line of sight of the reader and can be read from a distance up to 12 m for passive ultrahigh frequency (UHF) system. Battery-powered tags typically have a reading range of 100 m.
- RFID data on the tag can be modified based on business needs. The barcode data is very difficult to change once deployed.
- RFID tags are durable. Barcodes, in comparison, are printed on a product for everyone to see. They can be damaged or changed. RFID tags are hidden and may be reused across multiple products. Also RFID tags are capable of storing much more data.
- RFID data may be encrypted on the tag, thereby preventing unauthorized users from changing the data or counterfeiting.
- RFID systems can read hundreds of tags simultaneously. This is significant in a retail store as it saves the staff valuable time that they can spend on higher-value tasks.

Figure 3.9 shows the RFID main components: a programmable RFID tag for storing data, a reader with an antenna to read the tags, and an application software hosted on a computer to analyze the data.

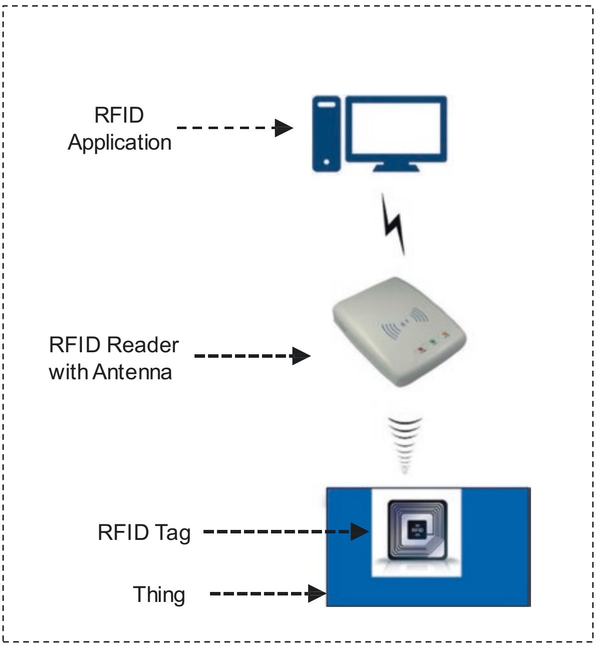

Fig. 3.9 RFID main components

Like any other technology, RFID has a number of disadvantages, but they are relatively minor. A top disadvantage is the susceptibility of the tags to jamming by blocking the RFID radio waves, for instance, by wrapping the tags with metallic material such as aluminum foil. Metallic ink on book covers can also affect the transmission of the radio waves.

Another potential disadvantage is the interference between multiple readers and tags if the overall system is not set up appropriately. Each RFID reader basically scans all the tags it picks up in its range. This may create a mix-up between tag information (e.g., charging a customer for items in someone else's shopping carts within the same range).

3.3.1 RFID Main Usage and Applications

RFID is already used by a large number of applications. Top examples include:

- *Access Control and Management*: Many companies and government agencies are using RFID tags in identification badges, replacing earlier magnetic stripe cards. With RFID, employees as well as authorized guest may be greeted by their name on a screen or by a voice message upon entering a building. Companies are currently using data collected from the information associated with each employee's badge to plan for workplace optimization.
- RFID tags are also widely used for electronic toll collections (e.g., California's E-ZPass) eliminating major delay on toll roads. Electronic toll collection system determines if the passing vehicle is enrolled in the program, automatically issues traffic citations for those that are not, and automatically withdraws the toll charges from the accounts of registered car owners.
- *Passport*: Many departments of state around the world (e.g., the USA, Canada, Norway, Malaysia, Japan, and many EU countries) are using RFID passports that can be read from a reader located up to 10 m away. In this case, passports are designed with an electronic tag that contains main information with a digital picture of the passport holder. Most solutions are also adding a thin metal lining to make it more difficult for unauthorized readers to scan information when the passport is closed. Standards for RFID passports have been established by the International Civil Aviation Organization, and are contained in ICAO Document 9303 (6th edition, 2006).
- *Healthcare*: With 2014 veteran complaints including allegations that 40 veterans may have died waiting for care at a Phoenix VA hospital, many hospitals or agencies, including the US Department of Veterans Affairs, have already started or announced plans to deploy RFID in hospitals across the USA to improve healthcare.
- RFID-based solutions in healthcare have started in private and public hospitals across the world, at least several years before the veteran's complaints, to track and manage expensive mobile medical equipment thereby allowing hospital staff

to track in real-time data relevant to healthcare equipment or personnel, monitor environment conditions, and more importantly protect healthcare workers from infections and other hazards.

- *Logistics and Supply Chain Tracking*: Major retailers in the world (e.g., Walmart), as well as the US Department of Defense, have published requirements that their vendors place RFID tags on all shipments to improve supply chain management. Such requirements allow retailers to manage their merchandise without manual data entry. RFID can also help with automatic electronic surveillance and self-checkout process for consumers. Finally, many factories are tracking their products throughout the manufacturing process using RFIDs to better estimate delivery dates for customers.
- *Athletic and Sport Event Timing*: Tracking the exact timing of runners in marathons or races is crucial, and often a portion of a second makes a difference. Athletic Timing is one of the most widespread use cases of RFID. Many runners are not even aware that they are being timed with RFID technology. Experts use such fact as an evidence of RFID's seamless ability to enhance consumer experience.
- *Animal Tracking*: Since the outbreak of mad cow disease, RFID has become critical in animal identification management, although RFID animal tagging started at least a decade before the disease. Some governments (i.e., Australia) are now requiring all cattle, sheep, and goats sold to be RFID tagged.
- *Other Applications*: RFID is also used for airport baggage tracking logistics, interactive marketing, laundry management for employers with huge number of uniforms (e.g., casinos), item level inventory tracking, conference attendee tracking, material management, IT asset management, library system, and real-time location system.

3.4 Video Tracking

Video tracking is the process of capturing and analyzing the video feeds, frame by frame, of a particular object or person over a short time interval. It is used to measure and analyze movements, visual attention, as well as behavior. Video tracking is used for customer identification, surveillance, augmented reality, traffic control, and medical imaging.

It is yet another mechanism to identify and monitor "things" when sensors or RFID tags are not available. Video tracking may also be used in conjunction with sensors and/or RFID to provide a more comprehensive solution.

Unlike preinstalled sensors and RFID tags in "things," video tracking can be turned on instantly. However, video tracking does have a major weakness, with today's technology. Video tracking is often time-consuming. It requires analyzing large amounts of video traffic and, in many cases, correlation with historical data, to arrive at accurate conclusions. Another challenge to video tracking is the complex object/image recognition techniques. This is a huge area of research in machine learning today.

3.4.1 Video Tracking Applications

- *Retailers*: Many retailers have started using video tracking solutions, often in conjunction with Wi-Fi access point data (how?; see problem 22), to increase sales and provide a better customer experience. Video traffic is analyzed using complex algorithms that track eye movements and identify fixation (e.g., desirability, obsession, and attraction to a product) and glissades (e.g., wobbling movements). The collected data is then filtered against well-established business rules to determine an internal action (e.g., change location of merchandize, add more checkout lines) or external action (e.g., offer the customer a certain discount).
- Determining the business rules is a very challenging problem. Many companies use advanced systems and techniques (e.g., machine learning, analysis of social media data, artificial intelligence) or hire a marketing firm to survey a large number of customers to arrive at such rules. Example of new rules is the fact that the faster a shopper finds the first item she/he needs, the more she/he purchases in such category. This dispels the pervious myth that the more time a shopper spends in a particular area, the more she/he buys.
- Video tracking is also used to improve the overall shopping experience in the store as a service differentiation especially if the store is a bit more expensive than similar stores in the area. The analysis of multiple grocery store traffic indicated that customers did not mind paying a bit more for faster checkout lines with friendly cashiers, bright lights, and clean belts. Analyzed data also indicated that the vast majority of customers do not pay attention to internal signs inside the store.
- *Banking*: Similar to retailers, banks have also started using video tracking solutions, often combined with Wi-Fi data. Access to Wi-Fi data in banks is easier given that most of the customers download the bank's mobile app on their smartphones. With the right setting, mobile apps often allow the bank to track the whereabouts of the customer.
- Banks use the data to quickly identify the customer (often before he lines in the queue). Depending on the priority of such customer (e.g., has large sums of money deposited at the bank), special greeting may be zero-wait private service if offered by the bank manager.
- *Other Uses*: The applications of video tracking with advanced backend analytics are unlimited, ranging from physical monitoring and security to traffic management and control and to augmented reality where an actual view is augmented by a computer-generated sensual input such as video.

3.4.2 Video Tracking Algorithms

To perform video tracking, an algorithm analyzes sequential video frames and outputs the movement of targets between the frames. There is a variety of algorithms, each having its own strengths and weaknesses. Considering the intended application is important when choosing which algorithm to use. There are two major components of a visual tracking system: target representation and localization and filtering and data association.

Target representation and localization are mostly a bottom-up process. These methods give a variety of tools for identifying the moving object. Locating and tracking the target object successfully are dependent on the algorithm. For example, using blob tracking is useful for identifying human movement because a person's profile changes dynamically [6]. Typically, the computational complexity for these algorithms is low. The following are some common target representation and localization algorithms:

Kernel-based tracking (mean-shift tracking [7]): an iterative localization procedure based on the maximization of a similarity measure (Bhattacharyya coefficient).

Contour tracking: detection of object boundary (e.g., active contours or Condensation algorithm). Contour tracking methods iteratively evolve an initial contour initialized from the previous frame to its new position in the current frame. This approach to contour tracking directly evolves the contour by minimizing the contour energy using gradient descent.

Filtering and data association is mostly a top-down process, which involves incorporating prior information about the scene or object, dealing with object dynamics, and evaluation of different hypotheses. These methods allow the tracking of complex objects along with more complex object interaction like tracking objects moving behind obstructions [8]. Additionally, the complexity is increased if the video tracker (also named TV tracker or target tracker) is not mounted on rigid foundation (onshore) but on a moving ship (offshore), where typically an inertial measurement system is used to pre-stabilize the video tracker to reduce the required dynamics and bandwidth of the camera system [9]. The computational complexity for these algorithms is usually much higher. The following are some common filtering algorithms:

Kalman filter: an optimal recursive Bayesian filter for linear functions subjected to Gaussian noise. It is an algorithm that uses a series of measurements observed over time, containing noise (random variations) and other inaccuracies, and produces estimates of unknown variables that tend to be more precise than those based on a single measurement alone [10].

Particle filter: useful for sampling the underlying state-space distribution of non-linear and non-Gaussian processes.

3.5 IoT Actuators

3.5.1 Definition

An actuator is a type of motor that is responsible for controlling or taking action in a system. It takes a source of data or energy (e.g., hydraulic fluid pressure, other sources of power) and converts the data/energy to motion to control a system.

3.5.2 Why Actuators?

As mentioned in Sect. 3.2, sensors are responsible to sense changes in their surroundings, collect relevant data, and make such data available to monitoring systems. Collecting and displaying data by a monitoring system are useless unless such data is translated into intelligence that can be used to control or govern an environment before a service is impacted. Actuators use sensor-collected and analyzed data as well as other types of data intelligence (see problem 11) to control IoT systems, for example, shutting down gas flow when the measured pressure is below a certain threshold.

3.5.3 Actuator Types

- *Electrical Actuators*: Electric actuators are devices driven by small motors that convert energy to mechanical torque. The created torque is used to control certain equipment that requires multi-turn valves or to control gates. Electric actuators are also used in engines to control different valves.
- *Mechanical Linear Actuators*: Mechanical actuators convert rotary motion to linear motion. Devices such as screws and chains are utilized in this conversion. The simplest example of mechanical liner actuators is referred to as the "screw" where leadscrew, screw jack, ball screw, and roller screw actuators all operate on the same principle by rotating the actuator's nut, the screw shaft moves in a line.
- *Hydraulic Actuators*: Hydraulic actuators are simple devices with mechanical parts that are used on linear or quarter-turn valves. They are designed based on Pascal's Law: when there is an increase in pressure at any point in a confined incompressible fluid, then there is an equal increase at every point in the container. Hydraulic actuators comprised of a cylinder or fluid motor that utilizes hydraulic power to enable a mechanical process. The mechanical motion gives an output in terms of linear, rotary, or oscillatory motion. Hydraulic actuators can be operated manually, such as a hydraulic car jack, or they can be operated through a hydraulic pump, which can be seen in construction equipment such as cranes or excavators.

- *Pneumatic Actuators*: Pneumatic actuators work on the same concept as hydraulic actuators except compressed gas is used instead of liquid.
- *Manual Actuators*: Manual actuator employs levers, gears, or wheels to enable movement, while an automatic actuator has an external power source to provide motion to operate a valve automatically. Power actuators are a necessity on valves in pipelines located in remote areas.

3.5.4 Controlling IoT Devices

There are two main philosophies to monitor and control IoT devices: local control and global control. The first approach requires an intelligent local controller (e.g., home's thermostat to control furnace and air conditioning system). The second approach is to move the control onto the cloud and simply embed inexpensive sensors everywhere (e.g., in this case, thermostat is eliminated altogether), and instead put temperature sensors around the house. An extension of this would be to pull the controller boards out of the furnace and air conditioner—connect their inputs and outputs to the Internet as well, so a cloud application can directly read their states and control their subsystems.

Clearly this approach requires many more, much finer-grained connected devices. And it offers the possibility of control strategies that would not be possible for an isolated thermostat. You could use ambient weather conditions, forecasts, and the current locations of the residents as inputs, for example, to determine an optimum strategy for making life comfortable while saving energy.

We believe the right approach is a combination of the two approaches depending on the specific IoT vertical and environment. This area will be covered in more details in Chap. 9.

3.6 How Things Are Identified in IoT?

As we mentioned in Chap. 2, the most convenient way to identify every IoT devices is to assign unique IP address to each sensor and actuator. However, IPv4 addresses are expensive and limited. IPv6 addresses are not widely deployed yet. In addition, many sensors and actuators are not IP enabled. IoT gateways, however, do have unique IP addresses. Hence, non-IP-enabled sensors and actuators may be identified by their associated gateways.

Chapter 5 will provide compressive details of various sensing protocols and illustrate how IoT sensors and actuator will be tracked and identified.

3.7 Summary

This chapter defined the "Things" in IoT. Three main techniques to identify things were discussed in details: embedded hardware sensors that sense the thing or surrounding environment and notify a client application, RFIDs with a tag to store information on a thing and a reader to read such information and pass them to an application to analyze, and finally video tracking. The advantages and disadvantages of these solutions were discussed. Once the data is analyzed (from sensors or other sources), IoT actuators are responsible for controlling or taking action if required. Finally, we have discussed the procedure to identify various devices in IoT networks.

Problems and Exercises

1. List the top three requirements for "Things" in IoT? What is the purpose behind these requirements?
2. Why are actuators required in IoT networks?
3. What is the definition of a sensor in IoT? Why is there a need for A/D converters in most sensors?
4. Why are sensors required to convert physical signals into electrical signal?
5. In a table, list and compare the various types of actuators. Which actuator type is considered to be environmentally friendly and why?
6. What are the key differences between sensors and actuators?
7. Chapter 1 (Sect. 1.2) mentioned that connecting objects together is not an objective by itself. Sections 3.1 and 3.5.2 mentioned that collecting data from sensors is not an objective by itself either. What is the business objective for connecting things and collecting data? How to achieve such objective?
8. What are the two main uses of flow sensors?
9. In a table format, list the key functionality of all sensors (A through I) listed in Sect. 3.2.3. Which sensor type is considered to be the least sophisticated, and which type is considered to be the most sophisticated? Why?
10. What is an autonomous sensor? When does it notify neighboring system(s) or IoT gateway? What is the difference between "autonomous" and "user-controller" sensors?
11. In a table, list and compare the ten characteristics of good sensors. Which characteristic you believe is the most important and why?
12. It was mentioned in Sect. 3.3 that actuators use sensor-collected and analyzed data as well as other types of data intelligence to control IoT systems. What is data intelligence? Provide two examples of data intelligence.
13. What is the definition of sensitivity and dynamic range? What are the typical units of sensitivity and dynamic range?
14. What is hysteresis? What is a typical unit of hysteresis?
15. How do touch screens operate with the presence of touch sensors?
16. In a table, list five examples of industries where pressure sensors are used. In each case, list at least one main application.

17. Some people have raised concerns about the potential invasion of privacy in RFID-enabled solutions (e.g., track the whereabouts of a person who checked out an RFID-enabled library book). Is this a major concern? How would you address it?
18. Athletic Timing: Athletic Timing is one of the most popular use cases of RFID, but often race participants never realize they are being timed using RFID technology. How does it work?
19. Describe how RFID works for laundry management. List three benefits.
20. Provide an example of how RFID works for interactive marketing.
21. How does RFID track the real-time location of assets or employees? What other technology can be used to track an employee location in real time?
22. How do retailers use Wi-Fi access point data in conjunction with video tracking to improve sales and customer experience?
23. This chapter discussed three different ways to obtain information from IoT "Things": sensors, RFID, and video tracking. In a table, compare the three technologies addressing:
    (a) Advantages
    (b) Disadvantages
    (c) Key requirements for the things
    (d) Two applications
24. What are transducers? How are they related to sensors and actuators?
25. Wind speed sensors typically involve a rotating element that is set in motion by wind. These sensor report the frequency of rotation of that moving element. An application receiving the frequency readings needs to apply a "transfer function" to translate the frequency to actual wind speed. In the weather monitoring station at Vancouver International Airport, two wind speed sensors are installed: an RM Young 05103 Wind Sensor and a Vaisala WM30 Wind Sensor. The first has the following transfer function: Wind Speed (m/s) = $0.0980 \times$ Frequency. The second has this transfer function: Wind speed (m/s) = $0.699 \times$ Frequency $- 0.24$.
    (a) If the RM Young sensor is reporting frequency of 20 Hz, and assuming both sensors are measuring the same wind speed value, then what would be the frequency reported by the Vasiala sensor?
    (b) What would be the actual wind speed measured?

References

1. A Framework for IoT Sensor Data Analytics and Visualisation in Cloud Computing Environments, University of Melbourne, Online: http://www.cloudbus.org/students/Krishnakumar-IoT-Project2011.pdf
2. Wikipedia, Online.: https://en.wikipedia.org/wiki/Sensor
3. Sensors: Online Electr. Eng. Online: http://www.electrical4u.com/sensor-types-of-sensor/

4. I. Gubbia, R. Buyyab, S. Marusica, M. Palaniswamia, Internet of things (IoT): A vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
5. L. Patrono, A. Vilei, Evolution of wireless sensor networks towards the Internet of Things: A survey, 19th IEEE SoftCom, p. 106, Sept. 2011
6. Sukanay, A Walk Through IoT, Online: https://opentechdiary.wordpress.com/2015/07/16/a-walk-through-internet-of-things-iot-basics-part-2/
7. T. A. Kinney, Proximity sensors compared: Inductive, capacitive, photoelectric and ultrasonic, Online: http://machinedesign.com/sensors/proximity-sensors-compared-inductive-capacitive-photoelectric-and-ultrasonic
8. Sensor Basics - Different Types of Sensors with Working Principles, https://www.youtube.com/watch?v=Xs1uicalZYA
9. Thermocouple, Wikipedia, Online: https://en.wikipedia.org/wiki/Thermocouple
10. T. Agarwal, Temperature sensors – Types, Working & Operation, white paper, Online: http://www.elprocus.com/temperature-sensors-types-working-operation/
11. Future Electronics, Online: http://www.futureelectronics.com/en/sensors/humidity-dew.aspx
12. Paul Garden, Electronic design, Online: http://electronicdesign.com/communications/iot-requires-new-type-low-power-processor
13. Common Actuator Types, Online: http://www.vma.org/?ActuatorTypes
14. Actuators, The Green Book, Online: http://www.thegreenbook.com/four-types-of-actuators.htm
15. Type of Robot Actuators, Robot Platform, Online: http://www.robotplatform.com/knowledge/actuators/types_of_actuators.html
16. S. Duquet, Smart sensors, enabling detection and ranging for IoT and beyond, ladder technology magazine Elektronik Praxis, April 2015, Online: http://leddartech.com/smart-sensors
17. 50 Sensors Applications for Smarter World, Libelium, Online: http://www.libelium.com/top_50_iot_sensor_applications_ranking/
18. P. Seneviratne, Internet Connected Smart Water Sensors, September 2015, Online: https://www.packtpub.com/books/content/internet-connected-smart-water-meter
19. P. Jain, Pressure sensors, prototype PCB from $10, Online: http://www.engineersgarage.com/articles/t
20. D. Merrill, J. Kalanithi, P. Maes, Siftables: Towards sensor network user interfaces, Online: http://alumni.media.mit.edu/~dmerrill/publications/dmerrill_siftables.pdf
21. A. Alcom, RFID Can Be Hacked: Here's How, & What You Can Do To Stay Safe, October 2012, Online: http://www.makeuseof.com/tag/rfid-hacked-stay-safe/
22. B. Hoffmann, S. Moebus, A. Stang, E. Beck, N. Dragano, S. Möhlenkamp, A. Schmermund, M. Memmesheimer, K. Mann, 2006, Residence close to high traffic and prevalence of coronary heart disease. Eur. Heart J. **27** Online: http://www.ncbi.nlm.nih.gov/pubmed/17003049
23. J. Thrasher, RFID vs. Barcodes: What are the advantages?, RFID Insider, April 2013, Online: http://blog.atlasrfidstore.com/rfid-vs-barcodes
24. S. Egloff, Advantages and disadvantages of using RFID Technology in Libraries, information Technology at the University of Maryland, Online: http://terpconnect.umd.edu/~segloff/RFIDTest3/AdvantagesandDisadvantages.html
25. P. Harrison, EU considers overhauling rules for lost air luggage. Reuters, September 2009, Online: http://www.reuters.com/article/eu-aviation-baggage-idUSLS63631320090728
26. P. Sweeney, Social Media Winner's Circle at Geneva Motor Show, Social Media Today, September 2013, Online: http://www.socialmediatoday.com/content/social-media-winners-circle-geneva-motor-show-video
27. J. Thrasher, "How is RFID Used in Real World Applications?", August 2013, Online: http://blog.atlasrfidstore.com/what-is-rfid-used-for-in-applications
28. M. Nystrom, K. Holmqvist, An adaptive algorithm for fixation, saccade and glissade detection in eye tracking data. Behav. Res. Methods **42**(1), 188–204 (2010)
29. Tank Monitoring on a New Level, Online: https://www.tankutility.com/