

Chapter 1

Introduction to IoT

ADVANCED TOPICS IN DATA SCIENCE

A solid blue horizontal bar at the bottom of the slide.

Motivational example

Moisture **sensors** in the soil send information about moisture levels.



Information from online weather services is also provided.



The system decides if it needs to water and for how long.



Smart Sprinkler System



It then sends the command to the **actuators** (the valve and the solenoid) which start or stop the water flow.

Outline

- 1.Introduction
- 2.Key factors to IoT evolution (past) & its relevance for the future
- 3.IoT concepts & components
- 4.Fundamental characteristics
- 5.IoT high-level requirements
- 6.Machine to Machine (M2M)
- 7.Internet of Everything (IoE)
- 8.IoT challenges (connectivity, security,...)
- 9.IoT and individual privacy
- 10.Policies and regulations pertaining to the IoT

1.Introduction-IoT Definitions

- The Internet of things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of **connecting and exchanging data** with other devices and systems over the Internet.
- We could define IoT as the next stage in the Internet as some do, whereby things and objects with sensors and actuators are connected to the Internet so they can gather, send and get data, **leading to smarter solutions and in some cases also act upon data.**

1. Introduction-IoT Definitions

- The Internet of Things is a connection of multiple devices, and it consists **of things that we would not normally connect to the internet**. From fridges, ovens, ..., to more important environments, which we call the operational technologies.
- IoT is a network of connected devices with 1) **unique identifiers** in the form of an IP address which 2) have embedded technologies or are equipped with technologies that enable them to **sense, gather data and communicate about the environment** in which they reside and/or themselves.



1. Introduction-IoT Definitions

Definition by ITU

- A global infrastructure for the information **society, enabling advanced services by interconnecting** (physical and virtual) **things** based on existing and evolving interoperable information and communication technologies.
 - Physical things exist in the physical world and are capable of being sensed, actuated and connected. Examples of physical things include the surrounding environment, industrial robots, goods and electrical equipment.
 - Virtual things exist in the information world and are capable of being stored, processed and accessed. Examples of virtual things include multimedia content and application software.
- Explanation: The IoT clearly includes M2M (referring specifically to communication directly between devices, used in a vast array of applications and for a variety of purposes, but broader definitions of IoT technologies also include ambient intelligence and smart environments .

Note there is no universally agreed IoT definition although there is an ongoing project to build one and bodies such as the ITU (International Telecommunication Union) have done recommendations .

1. Introduction-What is IoT?

- Internet of Things is when we connect up everyday physical things to the internet. Yes, even things like shoes!
- These things can give us information that can be used to improve your life or your business or the environment. The Internet of Things means the internet doesn't just collect and distribute information. **It can also feel and intelligently respond.**
- Though, if you'd been working too hard, your shoe could send data to the internet cloud, where it would be analyzed, and then a message would be sent to your boss to say that it was time for you to have a holiday !

1. Introduction-IoT Example 1

- We can use the internet to connect things that we wouldn't normally think of putting onto the network, things like your fridge for a simple example.
- Find out when your milk's going off and when you need to order some more. But it's more than that, much more. In medical areas, in manufacturing, in agriculture, the internet of things is going to change the way we do things.



1. Introduction-IoT Example 2

Moisture sensors in the soil send information about moisture levels.



Information from online weather services is also provided.



The system decides if it needs to water and for how long.



Smart Sprinkler System



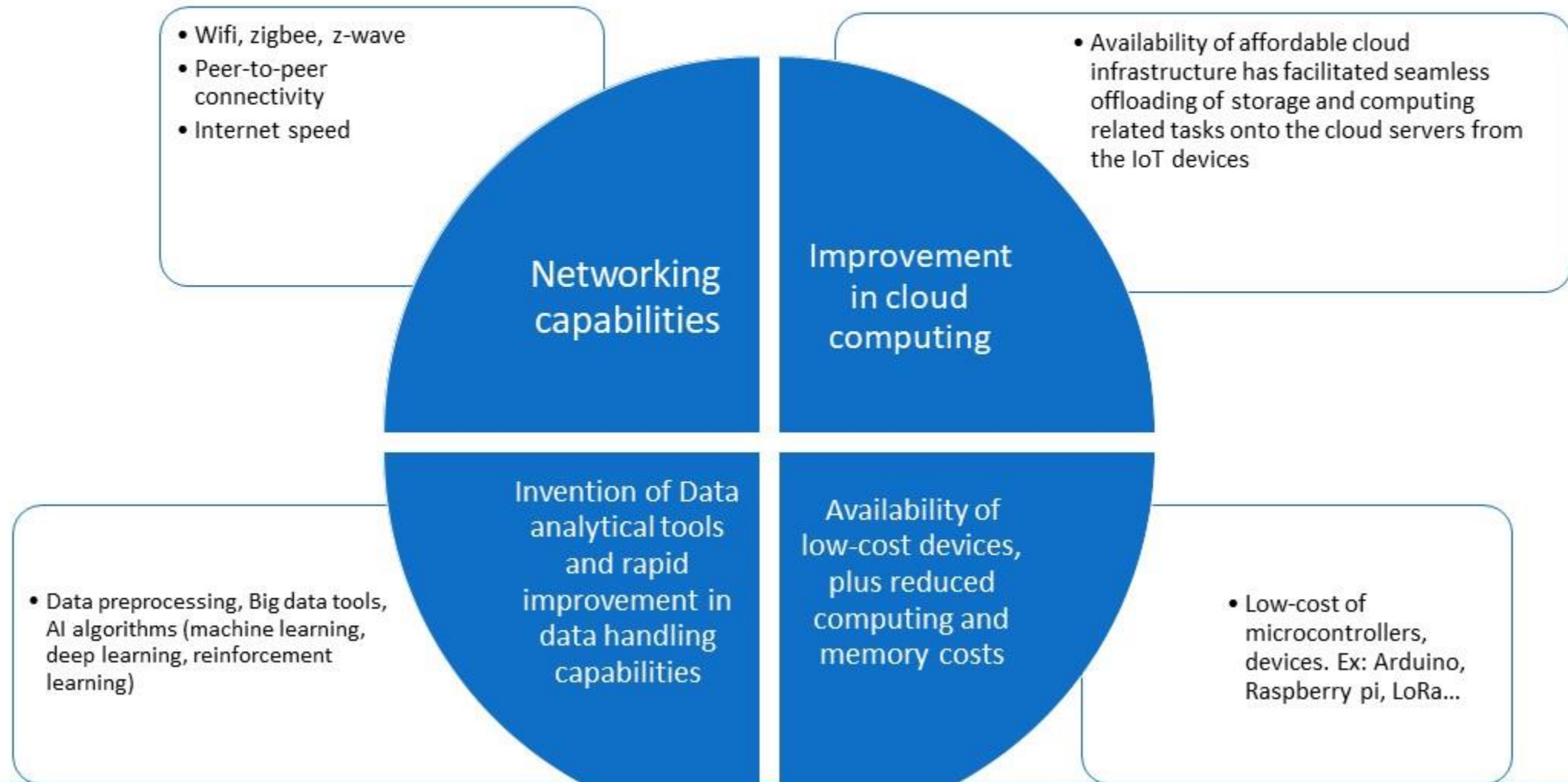
It then sends the command to the **actuators** (the valve and the solenoid) which start or stop the water flow.

1. Introduction-Why the society needs IoT

- We want to receive more data
- We want to control stuff
- We want to automate
- We want to reduce costs
- We want to make things faster
- We want to take better decisions
- We want to improve our life quality
- We want to feel more secured

2. Key factors to IoT evolution (past) & its relevance for the future

- Some of the key drivers of the IoT evolution:



2. Key factors to IoT evolution (past) & its relevance for the future

How far are we from IoT ?

- Already, IoT is delivering deep and precise insights to improve virtually every aspect of our lives. Here's a few examples:
 - IoT sensors in a factory can monitor and predict equipment failure before an accident.
 - Healthcare providers can provide remote monitoring of patient health—improving patient care.
 - Security cameras can better protect people with real-time notifications.

2. Key factors to IoT evolution (past) & its relevance for the future

Relevance of IOT for the future

- **By 2025, it is estimated that there will be more than 21 billion IoT devices**
 - A quick look back shows where IoT devices are going. Consider: In 2016, there were more than 4.7 billion things connected to the internet, according to IOT Analytics. Fast-forward to 2021? The market will increase to nearly 11.6 billion IoT devices.
- **94% of businesses will use IoT by the end of 2021**
 - According to a new report from Microsoft, almost all businesses will use some form of IoT by the end of next year. The core IoT industries such as manufacturing, retail, transportation, government and healthcare continue to introduce new IoT applications and solutions to their daily operations.
- **More cities will become “smart”**
- **Routers will continue to become more secure and smarter**
- **5G Networks will continue to fuel IoT growth**
- **5G's arrival will also open the door to new privacy and security concerns**

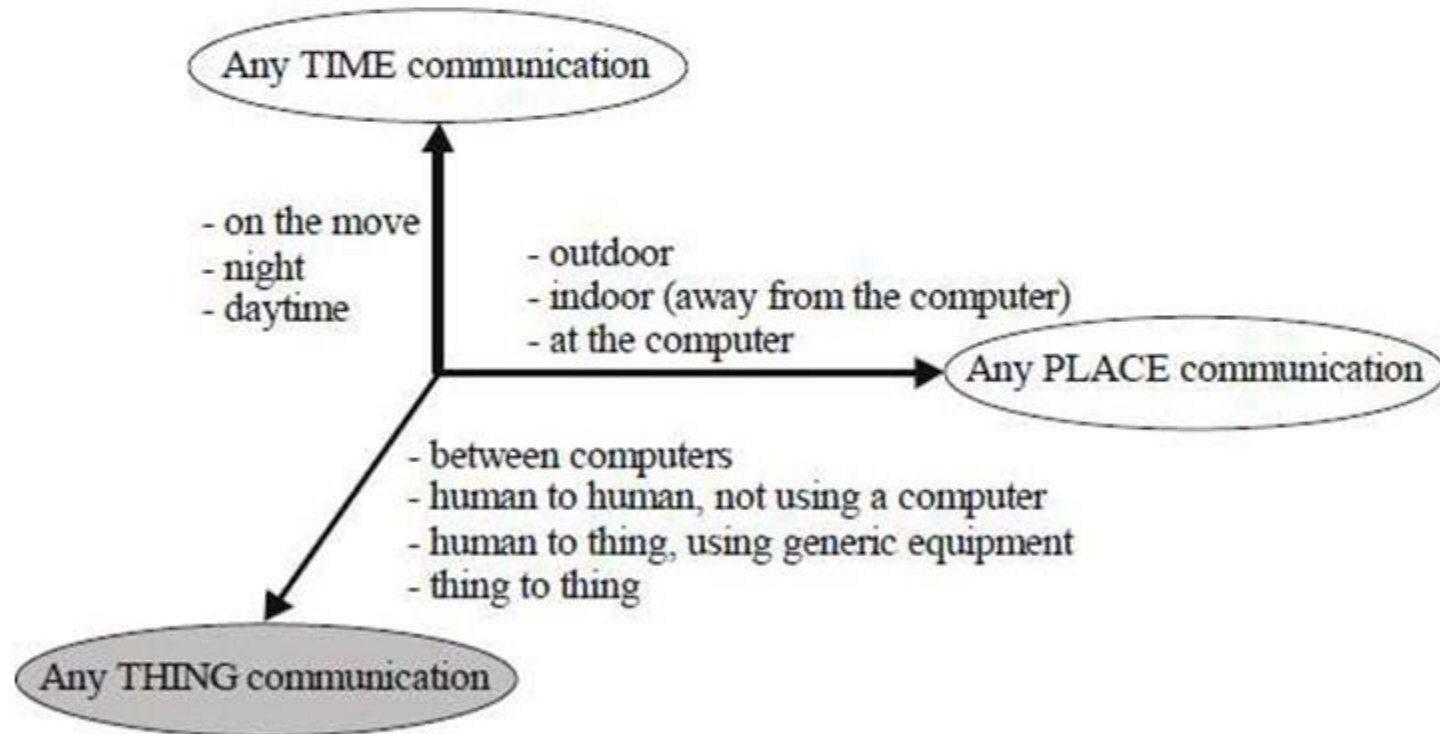
3. IoT Concepts

- From the perspective of technical standardization, the IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT).
- Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of "things" to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.



3. IoT Concepts

- the IoT adds the dimension "Any THING communication" to the information and communication technologies (ICTs) which already provide "any TIME" and "any PLACE" communication.



3.IoT components

Component 1: Sensing and embedding components

- This is the first tier of an IoT ecosystem and it forms the backbone of the entire Internet of Things network. This essential component consists of physical, micro appliances, embedded in an IoT device, which are responsible for collecting data or controlling a mechanism.
 - Sensors
 - Actuators

3.IoT components

- **Sensors** work to gather minute data from the surrounding environment. They are sometimes also known as 'detectors' as the primary function of sensors is to detect even the slightest changes in the surrounding environment. This allows an IoT device to capture relevant data for real-time or post-processing.



an IoT-enabled smart AC controller is used to make a conventional air conditioner smart. It consists of a sensor which detects room temperature conditions along with a transmitter to send signals and receive a response. The entire IOT ecosystem is in play to guide automated actions.

3.IoT components

Actuators work opposite to that of sensors. While sensors, sense; actuators act. They receive a signal or a command and on its basis they cause an action. They are as crucial as sensors as once the sensors have detected a change in the environment, an actuator is required to make something happen based on the trigger.



As an example, actuators may control the heating and cooling in a smart air conditioner or the valve in a smart tap. As soon as sensors detect that a person has exited an area, the actuator will be triggered to stop the flow of air conditioning or the flow of water in the case of a tap.

3.IoT components

Component 2: Internet Connectivity

- IoT is a network involving devices, sensors, cloud and actuators and all these needs to interconnect with one another to be able to decipher data and consequently perform an action.
 - Protocols
 - IoT Gateways

3.IoT components

- **Protocols:** Once the data has been collected by the sensors, it requires a medium for transport. In other words, a communication channel is necessary between sensors and the cloud. IoT protocols are responsible for transferring data in the online world and this transmission can only be possible if two devices are safely connected. IoT standards and protocols involve an invisible language allowing physical objects to communicate with one another.
- The choice of network depends on factors such as power consumption, speed of data transfer, bandwidth, ... Some of the most popular IoT wireless protocols and standards include Bluetooth, Wi-Fi, ZigBee, LoRaWAN, DDS, MQTT, cellular, etc. These and other channels make it easy as well as secure to transfer and exchange data to the next IoT layer for processing.

3.IoT components

- **IoT Gateways:** Incoming, raw data from the sensors must pass through gateways to reach the cloud. Gateways translate network protocols ensuring seamless communication of all devices within the network. Essentially this makes the gateways a crucial communication point and is responsible for easy management of data traffic.
- Moreover, gateways offer security by protecting the system from unauthorized access and malicious attacks. It can also be considered as a security layer as the data flowing through it protected by the latest encryption practices.
- Gateways can also preprocess data from the sensors before sending it to the cloud. In other words they minimize the large volumes of data 'sensed' in the previous stage. Not all, but some intelligent IoT gateways have the ability to also analyze and average data to transfer only the relevant data to the cloud.

3.IoT components

Component 3: IoT cloud

- Once the data has been collected and it has traveled to the cloud, it needs to be processed. It handles the data, stores it and makes decisions to make or break a deal. All of this is performed for colossal amounts of data in just under milliseconds – the time is critical for IoT, as especially in critical concerns such as health and safety, latency cannot be compromised.
- While the main purpose of IoT solutions is to provide and act on real-time information, there needs to be a component that is able to handle enormous amounts of data to cater to the time-sensitive nature of the IoT model. This is where cloud systems come into play. They form the brain of the IoT ecosystem as they are typically responsible for processing, commanding or taking analytics into account for the collected data. Devices, protocols, gateway and storage are combined for efficient real-time data analysis.
- While the cloud is not necessary for IoT, since local processing with Edge or Fog computing is an option too, the cloud may be preferred being a high-performance facility that offers massive scalability and decreased operational costs. Edge computing on the other hand is preferred when large amounts of data processing and storage are required on-premises.

3.IoT components

Component 4: IoT analytics and data management

- Data may be a small word but it holds immense power that can pose a huge effect on any business. IoT Analytics is used to make sense of the vast amounts of analog data. This for example can include the determination of key performance indicators in a certain application where one may be interested in viewing errors or irregularities in real-time.
- Once identified an immediate action would be required to prevent any undesirable scenarios. To put it differently, analytics involves converting raw data into useful insights that later are interpreted or analyzed to drive decision making.
- Smart analytics is useful in multiple scenarios. The basic role is to analyze a situation and formulate a decision based on this. This can be basic such as analyzing if a room's temperature falls in an acceptable range, or complex if for example a car is just about to crash. Data analytics helps determine vital business insights. Deep learning models can be used for predictive analysis. Various learnings can be derived from the data to predict trends, plan ahead and make useful business decisions.
- Analytics requires storage power and intelligent computation to be able to make sense of any data. Tasks such as this can be hosted on the cloud, depending on the IoT architecture.

3.IoT components

Component 5: End-user devices and user interface

- The user interface is the visible component that is easily accessible and in control of the IoT user. This is where a user can control the system and set their preferences. The more user-friendly this component of the IoT ecosystem is, the easier is a user's interaction.
- A user may interact with the system via the device itself, or this interaction can be conducted remotely via smartphones, tablets, and laptops. Smart home systems such as Amazon Alexa or Google Home etc. also allow users to communicate with their "things".
- Design is a major consideration in today's fast-paced world and one IoT device can set itself apart from a competitor on the basis of a strong design. Touch interfaces, use of colors, font, voice, and more are some of the factors that come to play here. While an attractive design is necessary, the interface should be user-friendly enough to avoid any difficulties for the user.

4. Fundamental characteristics

- **Connectivity.** With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.
- **Heterogeneity.** The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.
- **Things-related services.** The IoT is capable of providing thing-related services within the constraints of things, such as limited power supply.
- **Dynamic changes.** The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.
- **Enormous scale.** The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be the management of the data generated and their interpretation for application purposes
- **Intelligence.** The aspect of intelligence as in the sensing capabilities in IoT devices and the intelligence gathered from big data analytics (also artificial intelligence).

5.IoT high level requirements

- The following provide high-level requirements which are relevant for the IoT:
 - **Identification-based connectivity:** The IoT needs to support that the connectivity between a thing and the IoT is established based on the thing's identifier.
 - **Interoperability:** Interoperability needs to be ensured among heterogeneous and distributed systems for provision and consumption of a variety of information and services.
 - **Autonomic networking:** Autonomic networking (including self-management, self-configuring, self-healing, self-optimizing and self-protecting techniques and/or mechanisms) needs to be supported in the networking control functions of the IoT, in order to adapt to different communication environments and large numbers and types of devices.

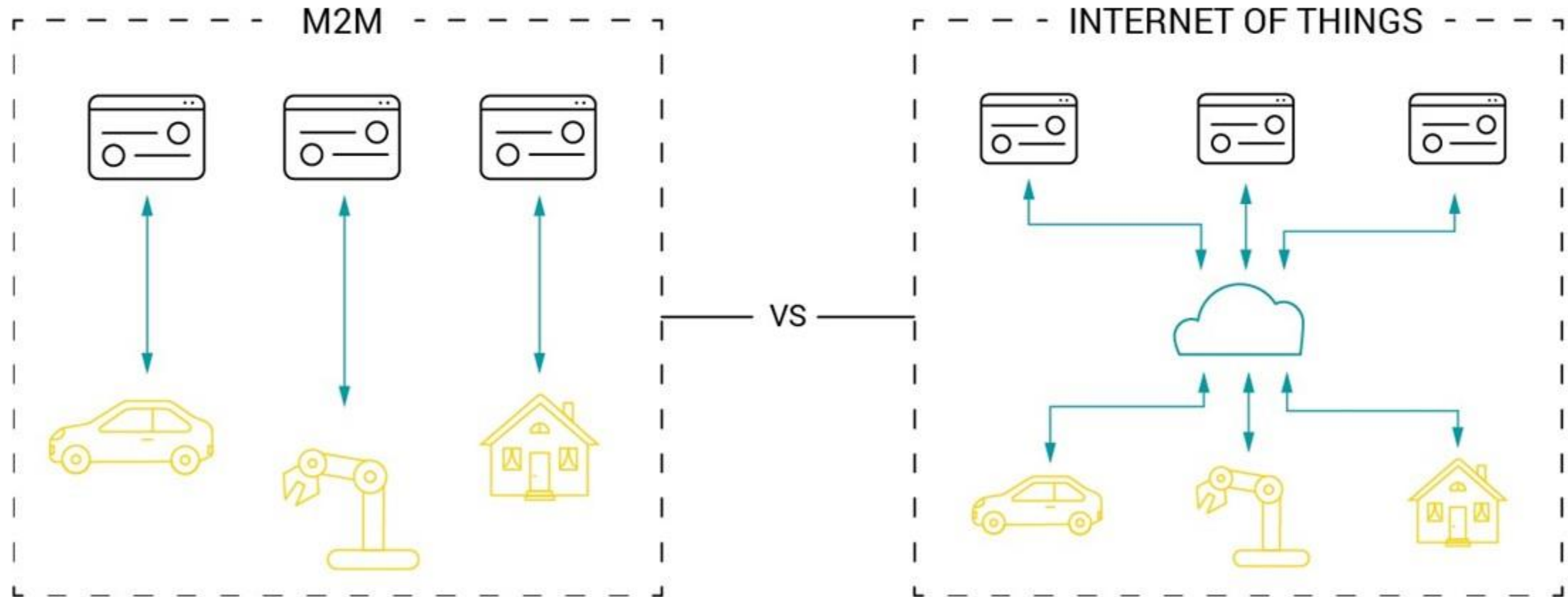
5.IoT high level requirements

- The following provide high-level requirements which are relevant for the IoT:
 - **Autonomic services provisioning:** The services need to be able to be provided by capturing, communicating and processing automatically the data of things based on the rules configured by operators or customized by subscribers. Autonomic services may depend on the techniques of automatic data fusion and datamining.
 - **Location-based capabilities:** Location-based capabilities need to be supported in the IoT. Something-related communications and services will depend on the location information of things and/or users. It is needed to sense and track the location information automatically. Location-based communications and services may be constrained by laws and regulations, and should comply with security requirements.
 - **Security:** In the IoT, every 'thing' is connected which results in significant security threats, such as threats towards confidentiality, authenticity and integrity of both data and services. A critical example of security requirements is the need to integrate different security policies and techniques related to the variety of devices and user networks in the IoT.

5.IoT high level requirements

- The following provide high-level requirements which are relevant for the IoT:
 - **Privacy protection:** Privacy protection needs to be supported in the IoT. Many things have their owners and users. Sensed data of things may contain private information concerning their owners or users. The IoT needs to support privacy protection during data transmission, aggregation, storage, mining and processing.
 - **High quality and highly secure human body related services:** High quality and highly secure human body related services needs to be supported in the IoT. Different countries have different laws and regulations on these services. NOTE – Human body related services refer to the services provided by capturing, communicating and processing the data related to human static features and dynamic behavior with or without human intervention.
 - **Plug and play:** Plug and play capability needs to be supported in the IoT in order to enable on-the-fly generation, composition or the acquiring of semantic-based configurations for seamless integration and cooperation of interconnected things with applications, and responsiveness to application requirements.
 - **Manageability:** Manageability needs to be supported in the IoT in order to ensure normal network operations. IoT applications usually work automatically without the participation of people, but their whole operation process should be manageable by the relevant parties.

6. Machine to machine vs IoT



6. Machine to machine vs IoT

M2M

It is a general concept involving an autonomous device communicating directly to another autonomous device. Autonomous refers to the ability of the node to instantiate and communicate information with another node **without human intervention**. The form of communication is left open to the application.

IoT

IoT systems may incorporate some M2M nodes (such as a Bluetooth mesh using non-IP communication), but aggregates data at an edge router or gateway. An edge appliance like a gateway or router serves as the entry point onto the internet. Alternatively, some sensors with more substantial computing power can push the internet networking layers onto the sensor itself.

6. Machine to machine vs IoT

Example

- A real life example of this dissimilarity could be found in telemedicine. Let us imagine a solution that connects a sensor monitoring the heart rate of a patient to an external application which lets the doctor know the patient needs attention. Such kinds of solutions could easily be provided by the M2M technology.
- On the other hand, if we take a sensor and integrate it with an interactive pillbox that would **advise the patient to take the medicine** and, moreover, would be able to send alerts to their family members' smartphones that the medicine has not been taken from the pillbox, it would definitely involve an IoT approach. To cut the story short, IoT could be viewed as M2M, but acting in a wider context.

7. Internet of Everything vs IoT

Machine to Machine M2M



A *device*...
that captures an *event*...
transmits it over a *network*...
to an *application*....
that translates it into
meaningful information.

Internet of Things IoT



A network of uniquely
identifiable "*things*"
that communicate
without human
interaction using
IP connectivity

Internet of Everything IoE



Bringing together the
people, process, data, and
things to make networked
connections more relevant by
turning information
into actions.

7. Internet of Everything - components

The four essential components that constitute the internet of everything:

- **Things:** Things are the building blocks of both IoT and IoE. By “things,” we mean connected objects that gather information about their status through sensors and share this information with one another over the internet. In IoT, connected things can be various devices—from consumer gadgets to water pipes. In IoE, almost every physical object can be a connected thing: from cows to monitor their health and track movements to milk cartons to manage their supply chain. Anything that is equipped with sensors and linked over public or private networks becomes part of IoE.
- **People:** People are integral to IoE since no intelligent connection is possible without them. All in all, IoE is made by people and for people: humans use connected devices every day, analyze data, and harness the potential of data insights. People not only play an essential role in P2M and P2P communication, but they may also become connected themselves. In healthcare, specialists can place sensors under patients’ skin or on the body to get information on a person’s vital signs for a better quality of patient care and treatment service. In this case, people act as nodes in the M2M communication process.
- **Data:** Data is yet another core component of IoE.
- **Process:** Last but not least, process is a major IoE component. It determines how each of the elements above works with the rest to provide greater value in the digital world. When a connected thing gathers the right data and transfers it to the right person at the right time, the process is successful. The process is a linchpin of IoE connectivity that allows for creating new opportunities across industries.

8. Challenges in IoT

- Because these IoT devices are powered by microprocessors or microcontrollers that have **limited processing power** and **memory**, they often rely heavily on AWS and the cloud for processing, analytics, storage, and machine learning. But as the number of IoT devices and use cases grow, people are finding that managing these connected devices presents new challenges. Sometimes an **internet connection** is weak or not available at all, as is often the case in remote locations. For some applications, a trip to the cloud and back isn't possible because of latency requirements (for example, an autonomous car interpreting its environment in real time). Also, as we will see in the future chapters, sensors have **low power**, which also will be a challenge in building IoT projects

9. IoT and individual privacy

- Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.
- Systematic literature review identified four key privacy themes that represent issues related to the collection of individuals' data through the IoT:
unauthorized surveillance, uncontrolled data generation and use, inadequate authentication and information security risks.
- Thereby, privacy protection needs to be supported in the IoT. The IoT needs to support privacy protection during data transmission, aggregation, storage, mining and processing.

10.Policies and regulations pertaining to the IoT

- Policy issues driving IoT
 - Who would create a policy for IoTs? ICT, another sector, all?
 - Policy aspects that have ICT regulatory impact
 - Policy aspects that require other sectoral regulatory intervention
 - Policy aspects that need industry, academia , R&D
 - Policies that needs international cooperation (Standards, spectrum, inter border movement, international taxation, international resources, data protection, security and privacy)

10.Policies and regulations pertaining to the IoT

- Form the ICT policy maker and regulator point of view some of the challenges faced would be:
 - Licensing (new IoT aggregators, scope of license etc..)
 - Spectrum (regulation will change based on the service and also technology, e.g.Long range (NB-IOT,) Vs short range (RFID, Bluetooth, WiFi); It will also change based on the band used (free vs licensed)
 - Numbering and addressing (IoT identifier)
 - International roaming
 - Interoperability and Standards
 - Data protection, privacy, consumer protection and Security.
 - Competition(platform competition, can the whole business or a smart city be treated as one customer reducing choice)
 - RoW: Use of Street furniture

10.Policies and regulations pertaining to the IoT

- There are many aspects of regulations that are national in nature Such as how to assign spectrum to telecommunication operators, decision to have national level licensing or region based licensing and many others
- Even national regulations have to be aligned to best practices to avoid issues such as cross border interference, technology neutrality, roaming, fee structure,etc

Questions