**Immagine che contiene testo, Carattere, Elementi grafici, logo

Descrizione generata automaticamente**

**Master’s Degree in Computer Science**

**Academic year 2024/2025**

**INTERNET OF THINGS**

**AND SMART CITIES**

**Prof. Marco Giordani**

Written by Michael Amista’

A course offered by the School of Engineering (DEI) –

Master’s Degree in ICT for Internet and Multimedia

**Index of contents**

[**Internet of Things and Smart Cities course introduction** 3](#_Toc178803944)

[**1. Internet of Things** 4](#_Toc178803945)

[**1.1 Introduction** 4](#_Toc178803946)

[**2. Smart Cities** 13](#_Toc178803947)

# **Internet of Things and Smart Cities course introduction**

Course prefix to use as email object: IOTSC

From a customer perspective the IoT is the ability to use sensors and other devices to connect things in a way they work together. IoT finds its main use in smart home, smart cities and industrial systems.

Obviously, the main issue when we talk about IoT is the **reliability** of the collected data and this is a big challenge in protecting our privacy, we will deal with that during the course. Another important problem is the **energy consumption**: many sensors and devices have a limited amount of battery. **Interoperability** is another problem: there are many manufacturers and many different devices, so it is important to have a common standard to make different devices work together. Furthermore, depending on the number of devices, larger networks are created, and it is crucial that these networks are well handled.

The course is more focused on IoT technology and, only at the end, on its application to build smart cities.

Course schedule:

* Frontal lectures.
* LAB experiences: it starts in November and there will be 3(+1) practical lab experiences. We will use Arduino as an emulated sensor to send data to IoT LoRa gateway and we will see how to process those data to return an output.
* Guest lectures (even those part of the written exam).

**Slides (and attendance) are enough to pass the exam**.

The exam consists of two parts:

* **PART 1 (up to 28/33 points): Written test (mandatory)** that consists of both multiple-choice questions and open questions (even the guests lectures can be part of the written exam) with a duration of 1 hour and half.
* **PART 2 (up to 5 extra points): LAB assessment (optional)** which is “only” a replication of what done during lab lectures so if you follow the lab you should not have to study anything else to work on the assessment. The assessment can be submitted in December, before the written exam session. To submit the assessment, you must follow all lab lectures.

# **1. Internet of Things**

## **1.1 Introduction**

IoT is characterized by two fundamental concepts: **internet** and **things**.

The precursors of the modern Internet (ARPANET, CSNET, NSFNET) were resource sharing networks: computers were bulky and expensive, and researchers used nationwide connections to access them from far away. As personal computers became ubiquitous, and packet-switched traffic was ported to the ubiquitous telephone network, the Internet became the means for people all over the world to communicate with each other. In 1990, Tim Berners-Lee defines HTTP and HTML, leading to the explosion of the World Wide Web.

From interconnecting computers and people now IoT interconnects personal devices. The goal is to create a network, an architecture able to sustain all the different interconnected devices that shape the network. The basic idea is that interconnection needs to be invisible to users who do not have to do anything, **everything is automatically**, data are processed, and the users have an automatic response having so an **autonomous network that works without human interaction**.

Immagine che contiene testo, schermata, diagramma, Carattere

Descrizione generata automaticamente

WPAN is a technology specifically developed for IoT sensors. IoT sensors can use many technologies to communicate each other, from the nonspecific ones (e.g., WLAN) to more specific ones (e.g., WPAN).

Immagine che contiene testo, schermata, Carattere, Diagramma

Descrizione generata automaticamente

We will see how IoT can decrease the costs and optimize operations, that’s why the IoT revenues are so high. Some statistics: the number of Italian enterprises using IoT technologies is around 32%.

But what is IoT? We need a definition. There are a lot of definitions of what IoT is, all of them are correct but we will use a more formal definition than the ones that appear in the textbooks.

***Internet of things means connecting every thing.***

The key part of the definition of Internet of Things is the **Internet**, where Internet means IP protocol: No IP 🡪 No IoT. So, the definition we will use during the course will be the following:

*“Internet of Things is a paradigm according to which every thing, real or*

*virtual, is assigned an IP(v6) address and can be reached (for example for*

*sensing or actuating purposes) via the standard Internet Protocol stack.”*

If you assign an IP address to a device, that device is actually part of an IoT network.

**An example of a “Smart” IoT system**

* One typical evening planning next working day...
* Tomorrow first office meeting at 8:30 am.
* Typical car trip in these days: 1 hour time.
* 45 minutes to wake up and get ready.
* I decide to set my alarm to wake up at 6:45 am.

What could (will) possibly go wrong?

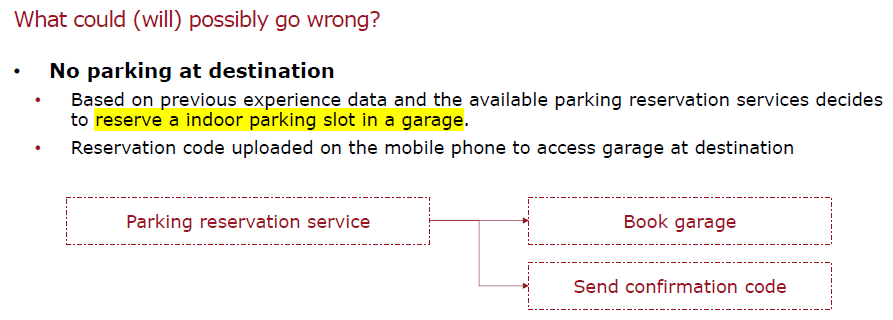
* At 4:30 am it starts snowing
* Truck obstruction along the usual path
* Traffic congestion on alternative paths
* No parking at destination
* Bathroom cold when having shower
* Coffee cold when having breakfast
* Left my car keys at home when in garage
* Elevator busy when leaving my flat

**Leaving 10 min. late + 30 min. additional travel time 🡪 missed the meeting!**

An IoT approach to improve this scenario…

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente



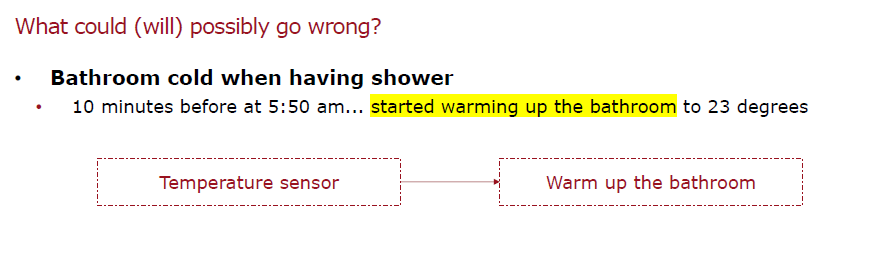


Immagine che contiene testo, schermata, Carattere, linea

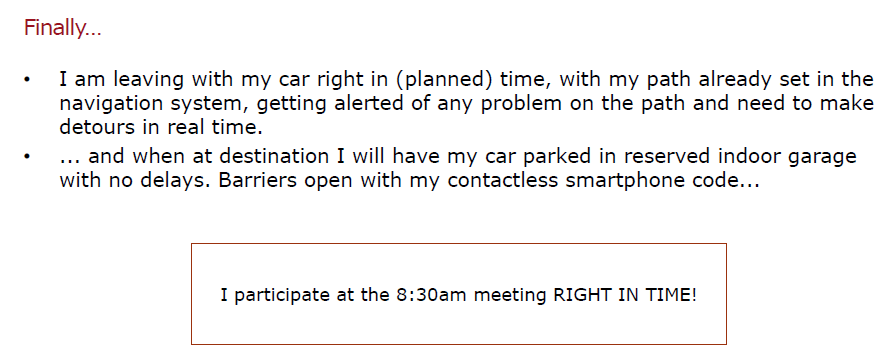
Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, diagramma

Descrizione generata automaticamente

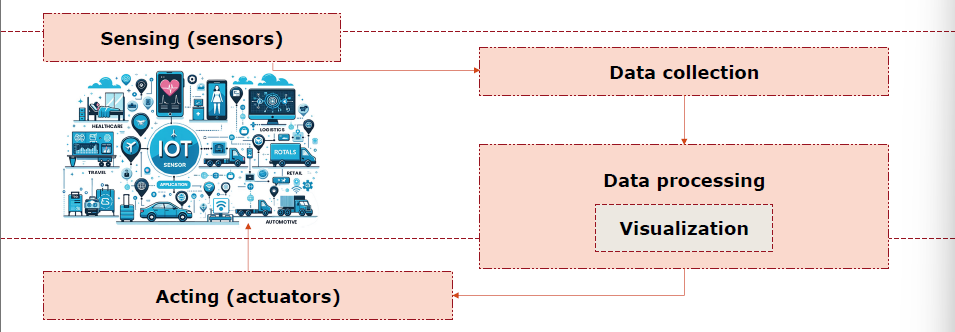
Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente



We want to have an integrated system made by smart things that make the life easier for the final consumer and so to take actions without human intervention.

**IoT high-level architecture**



The core parts of an IoT system are sensors that produce data to be consumed. Data are collected by a gateway and then they are processed (trigger actions) or only visualized (only to monitor the system making sure everything goes well). The actuator is another type of device that implements an action based on the result of data processing.

**Data collection**

* Sensors acting as a physical-cyber interface that monitors and reports states of some physical entity or device.
* Produce a digital representation suitable for use in the cyberspace.
* Relatively early in the process, metadata (a sort of appendix to real data, used to store other information such as the location) needs to be captured and used to annotate the data. In IoT systems, metadata generally describe the nature and context of data capture, such as the sensor type, its location, and in some cases structural relationships to other elements of the system.

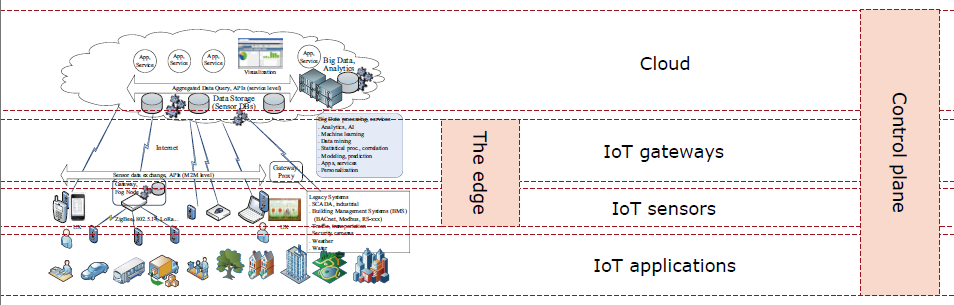
**Processing and visualization**:

* Types of IoT data processing:
  + (Simple) control loop algorithms performed on the incoming data as they arrive.
  + Sophisticated forms of analytics and machine-learning algorithms based on past behaviours and observations of the system.
  + Common data processing steps:
    - Sampling, aliasing, quantization, saturation, hysteresis and non-linearities, calibration, error propagation, optimization and predictions (we’ll see…).
* In industrial and complex control systems, it is customary to visualize the system state and points of interest to system operators à digital twin / dashboard.
  + System state, notifications, alarms when faults or anomalous behaviors are detected.

**Acting**:

* Acting upon insights and predictions is the output and the ultimate purpose of deploying IoT systems.
* Common types of actions:
  + From simple remote actuation initiated by operators in response to visualized conditions in a basic monitoring configuration to automated guidance of control points.
* Actions can be implemented as direct actuation or indirectly, in the form of advice to system operators or optimizations resulting in adjustments to the manufacturing process.
* Identification of cause of failures and anomalous conditions followed by direct or indirect execution of the appropriate remediation actions.

**A more technical IoT architecture**



Let’s explore the different elements that shape this more technical architecture.

**IoT applications**

These are the actual use cases and services that benefit from IoT technology. They span a wide range of industries, including smart cities, health monitoring, industrial automation, transportation, and more. These applications rely on IoT sensors and gateways to collect and process data to offer services like predictive maintenance, asset tracking, or smart energy management. Examples of IoT applications: look at slides.

**Sensors**

* Sensors can measure some quantity in the environment (e.g., a thermometer).
* Actuators can do something in the environment (e.g., turn on the heating system).
* Some sensors contain sufficient functionality to perform some local operations.
* Some sensors and things are designed to connect directly to the Internet and communicate with applications and services residing in the cloud.
  + It may require external computation platforms given energy constraints.
  + Security cameras, fire sensors, thermostats, appliances, and power meters, …

**Gateways**

Sensors connect to the Internet using intermediaries, such as gateways. Gateways (and fog nodes) are usually more powerful devices 🡪 connection via local network links, often wireless, such as: ZigBee, variants of 802.5.14 networks, Bluetooth, and low-power Wi-Fi, LoRa, NB-IoT.

Gateways usually provide **wide-area connectivity and edge processing** for the attached sensors that may come in the form of protocol conversion, data storage and filtering, event processing, and analytics.

**Communication layers**

Enables a vast array of edge devices and things to exchange messages with each other, the rest of the IoT system, and ultimately the Internet.

Communication layers may include a variety of wireless and wired links, spanning local areas and including long-haul connections. Represent a complex infrastructure of links, bridges, and routers that can transport payloads from local point-to-point segments all the way to any endpoint and application on the Internet.

**The cloud**

“Back-end” processing is depicted by a generic cloud.

* Data from a variety of diverse sources are aggregated and processed for optimization and discovery of global trends and relations.
* Depending on nature and real-time requirements, sensor data may be processed “inflight” as streams, stored for post-processing and archival purposes, or both.
* May also contain some common services such as large-scale storage, analytics processing engines, data visualization and graphing, as well as management functions such as security and provisioning.
* Machine learning (ML) and artificial intelligence (AI) algorithms are usually operated in the cloud where they can work with large aggregations of data.

**Control plane**

* Data plane / user plane: main IoT functionalities: collect, process, and act on data.
* Control plane: task of keeping the IoT infrastructure itself running and secure.
  + Service configuration and aggregation
  + Service problem management
  + Service quality management
  + Resource provisioning
  + Trouble and anomaly management
  + Performance management

**IoT: why today?** A confluence of technological and infrastructure developments centered around the Internet forms much of the basis and impetus for the construction of IoT systems.

* **Industry 4.0** and digitalization.
* **Sensors** – installed base, variety, lower cost, and easier integration.
* Multi-sensors **miniaturization and mass production**.
* **Smart phones** – sensors, gateways, and UI devices.
* **Cloud computing** – global and capacity on demand.
* **AI and ML technologies** – actionable insights with IoT data.
* **Internet** – technology, global infrastructure, and users.
* **Pervasive communications**: mobile devices always connected to the Internet.

The main problems in the IoT:

1) **The energy problem**

* Sensors might be placed in hard-to-reach locations: they need to be batterypowered and work for months or years.
* Sometimes they have solar panels or other energy harvesting methods, but we need to be careful: size and cost matter!
* Energy has a significant impact on every IoT operation: communication, computation, sensing, actuators...
* Due to the energy problem, sensors are often optimized to consume little power:
* We cannot operate on an always-on basis.
* We need to consider every aspect: any calculation or long transmission is expensive.
* For this reason, sensors often transmit very few bytes at relatively long intervals (no transmissions for hours or days in some applications).
* Limited processing capabilities (and so latency concerns).

2) **The security problem**

* The simplicity of IoT devices also makes them hard to secure.
* Impossible to run strong cryptography.
* Difficult to patch and update to solve vulnerabilities.
* Connected by design to the open Internet.
* There are possible security solutions against hackers, but there is also a privacy issue: what do sensors say about our lives? Who gets to see the data?
* Sensor data can tell a lot about our lives:
* Location data can identify movements and activities.
* Domotic systems tell stories about our habits.
* Data are often used by IoT companies and law enforcement agencies.

3) **The scalability problem**

* Cellular networks and wireless technologies were designed for few devices with high requirements (e.g., humans streaming videos).
* In the IoT, we have thousands or millions of devices with very little data to send.
  + New access mechanisms.
  + Sensor identification problems.
  + How do we get the data with the minimum amount of transmissions?

4) **The reliability problem**

* The “converse” problem (what do we need to ensure that we get the relevant information) can be crucial in industrial and safety systems:
  + How do we identify anomalous (and potentially hazardous) situations?
  + Anomalies can be single-sensor or multi-sensor.
  + How do we trust that there is an anomaly when sensors are unreliable?

# **2. Smart Cities**

…