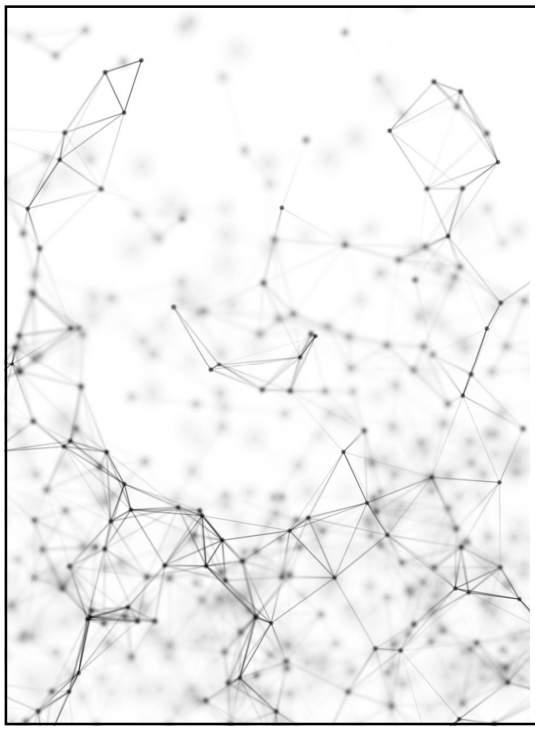


Data and System Security

Internet of Things

Stefano Chessa

1

Learning objectives

- Internet of Things
- IoT & machine learning
- IoT & the cloud
- Interoperability and standards
- Security in IoT

2

Definition based on what IoT means.

Change between IPv4 and IPv6 was because internet was full and was not possible to attach anything else. 2014 saw the switch, with IPv6 we can connect *

Internet of Things (IoT)

a large, major change in internet completed in the last years

The transition from IPV4 to IPV6

Enables up to

655.571 billion of billions

of devices per square meter on Earth (included oceans!)

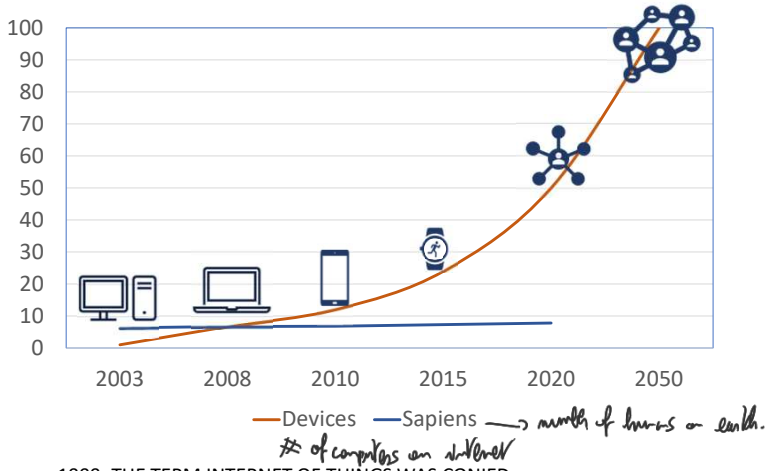
Is there any purpose/need?

Who needs all this?

3

1. Switching from IPv4 to IPv6 was a nightmare. So we want to do it once and for all.

IoT devices VS humans:



→ number of humans on earth.

* of computers on internet

1999: THE TERM INTERNET OF THINGS WAS CONIED

IN 2008 MORE DEVICES IN INTERNET THAN PEOPLE

IN 2014 THE NUMBER OF **MOBILE** DEVICES ON INTERNET SURPASSED THE NUMBER OF HUMANS ON EARTH

BY 2020 THE NUMBER OF DEVICES ON INTERNET WILL EXCEED 50 BILLIONS

4

A computer was designed to remain where it is, respond to a user and full stop. But when computers are larger than the # of human beings, this concept doesn't work anymore. IoT is internet populated of computers being environments and taking stimuli from somewhere else (surrounding environment, so we have embedded sensors) In IoT we are talking about sensors.

Internet of Things (IoT)

- Most of the devices are not directly in use by human beings
- Independent physical objects with their own businness logic
  - Embedded with electronics, software, sensors and network connectivity
  - Mostly sensors and actuators
  - not human-operated!

KEY POINT

Created to make them work for a long period of time. We don't want to fix them.

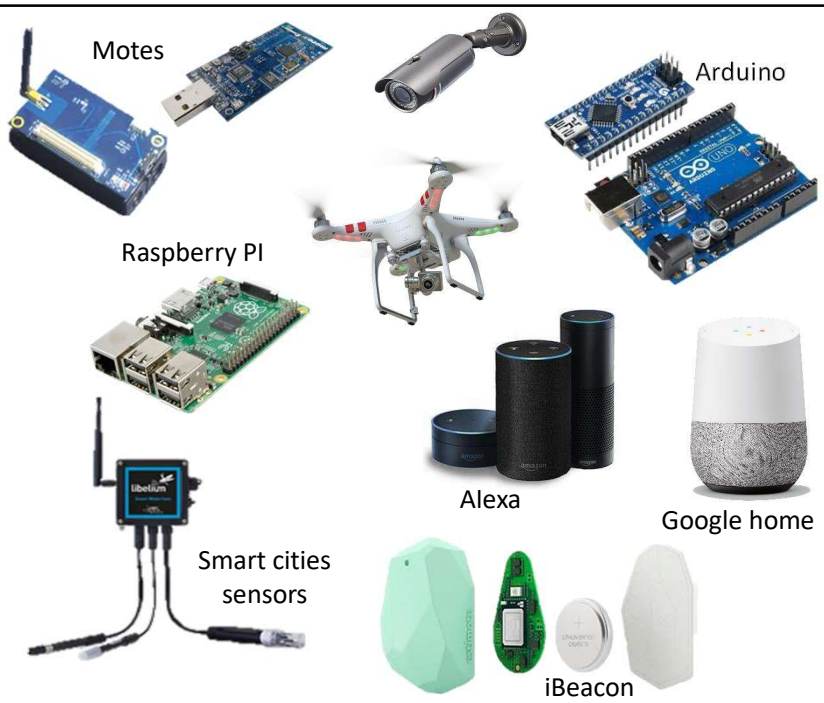
5

What's the environment for IoT devices?. You can be the environment too. Smartphone with sensors.

Wearable devices

6

Environmental devices



7

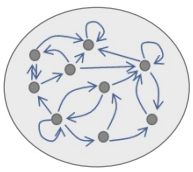
Each IoT device...

Sensors/actuators

Microprocessor specialised for I/O management

Microcontroller

Wireless interface



Software (business logic)

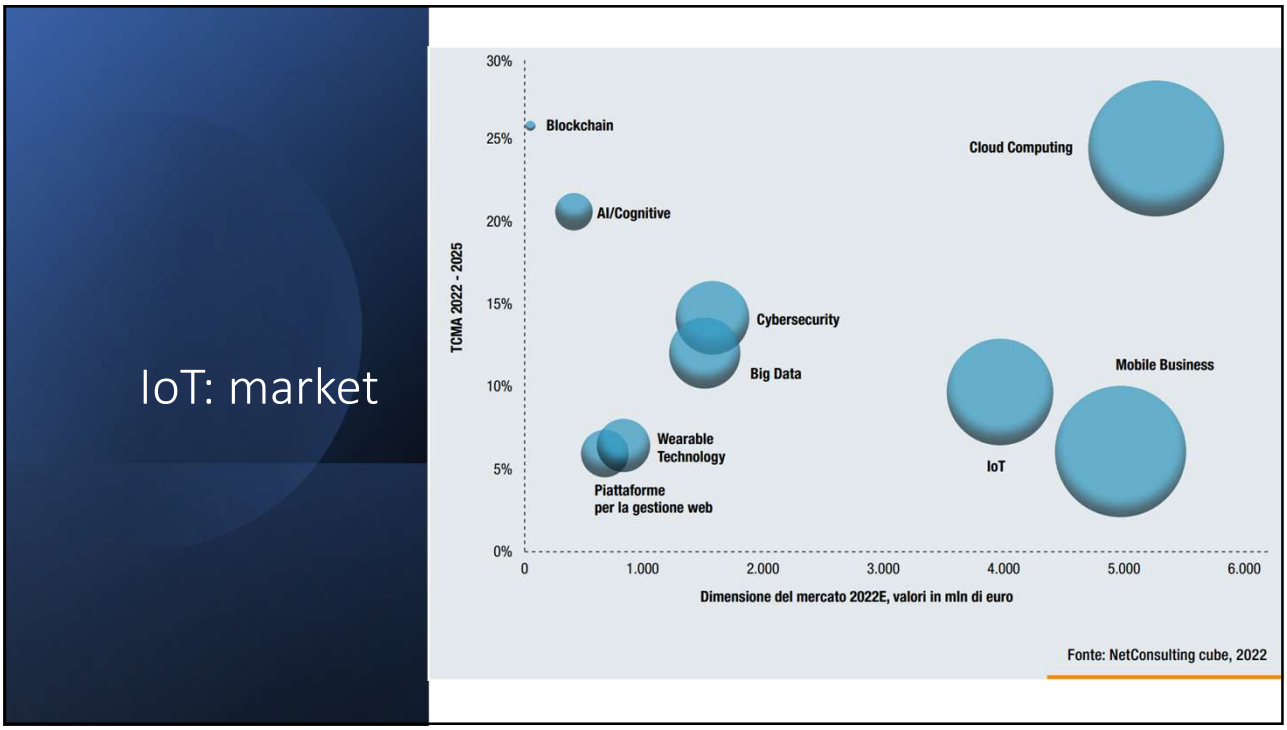
8

My is extremely simple :

DESPITE BEING SO SIMPLE, APPS ARE LIMITLESS


Few elements, many apps…

9


IoT: market
30%
25%
20%
15%
10%
5%
0%
TCMA 2022 - 2025
Blockchain
AI/Cognitive
Cybersecurity
Big Data
Wearable Technology
Piattaforme per la gestione web
Cloud Computing
Mobile Business
IoT
0
1.000
2.000
3.000
4.000
5.000
6.000
Dimensione del mercato 2022E, valori in mln di euro
Fonte: NetConsulting cube, 2022

10

IoT is the last development of the internet.

Another type of devices: very very low power and energy. Low size because we want to embed them everywhere. Then we have powerful devices (ex. high resolution camera with high computational power).

… in summary

- IoT: expanding interconnection of smart devices, from appliances to tiny sensors
  - embedding of short-range mobile transceivers into everyday items
  - enables new forms of communication between people and things, and between things themselves
  - the Internet supports the interconnectivity usually through cloud systems
- The objects deliver sensor information, act on their environment, and in some cases modify themselves, to create overall management of a larger system
- The IoT is primarily driven by deeply embedded devices
  - Low-power, low-bandwidth, low-energy that communicate with each other and provide data to the cloud
  - … but also embedded appliances, such as high-resolution video security cameras, video VoIP phones, etc., that require high-bandwidth streaming capabilities

11

We can divide evolution of net in 4 stages: 1st phase as ①. Refers to the first stage, internet populated by servers, personal computers, routers etc. Just to provide info to experts. Mostly wired connection. ② Computers become progressively embedded in machines for efficiency. Early 2000s, still using wired connectivity.

… in summary

Wrt end systems supported, four generations of deployments of Internet (culminating in the IoT):

Information technology (IT) ①	PCs, servers, routers, firewalls, and so on, bought as IT devices by enterprise IT people, primarily using wired connectivity
Operational technology (OT) ②	Machines/appliances with embedded IT built by non-IT companies, such as medical machinery, SCADA, process control, and kiosks, bought as appliances by enterprise OT people, primarily using wired connectivity
Personal technology ③	Smartphones, tablets, and eBook readers bought as IT devices by consumers (employees) exclusively using wireless connectivity and often multiple forms of wireless connectivity
Sensor/actuator technology ④	Single-purpose devices bought by consumers, IT and OT people exclusively using wireless connectivity, generally of a single form, as part of larger systems

It is the fourth generation that is usually thought of as the IoT, and which is marked by the use of billions of embedded devices

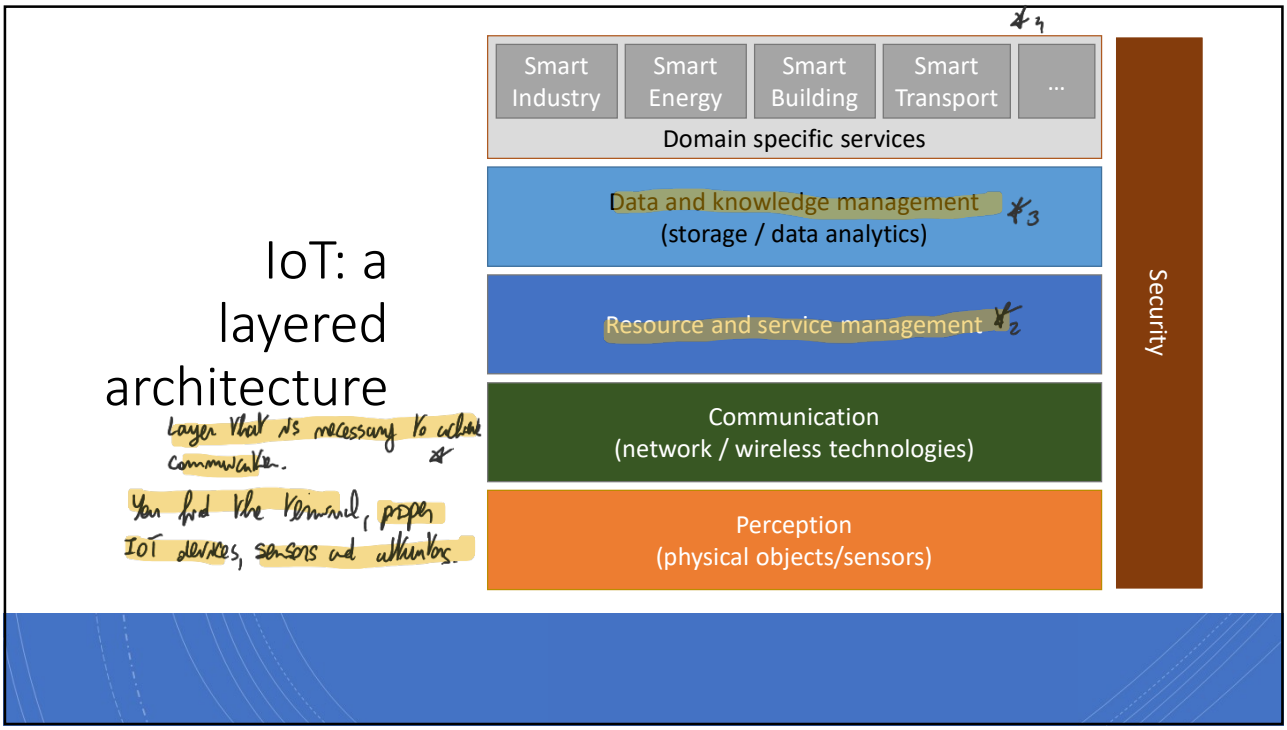
12

③ corresponds with introduction of smartphones. Extra set of components, characterised by mobility and development of wireless technology.

④ Age enabled by IPv6, internet populated mostly by devices, sensors, actuators.

On one hand, IoT is a reality. At the same time strongly under development. Note: to make IoT devices work, we need powerful infrastructure. This is to be taken into account when talking about IoT.

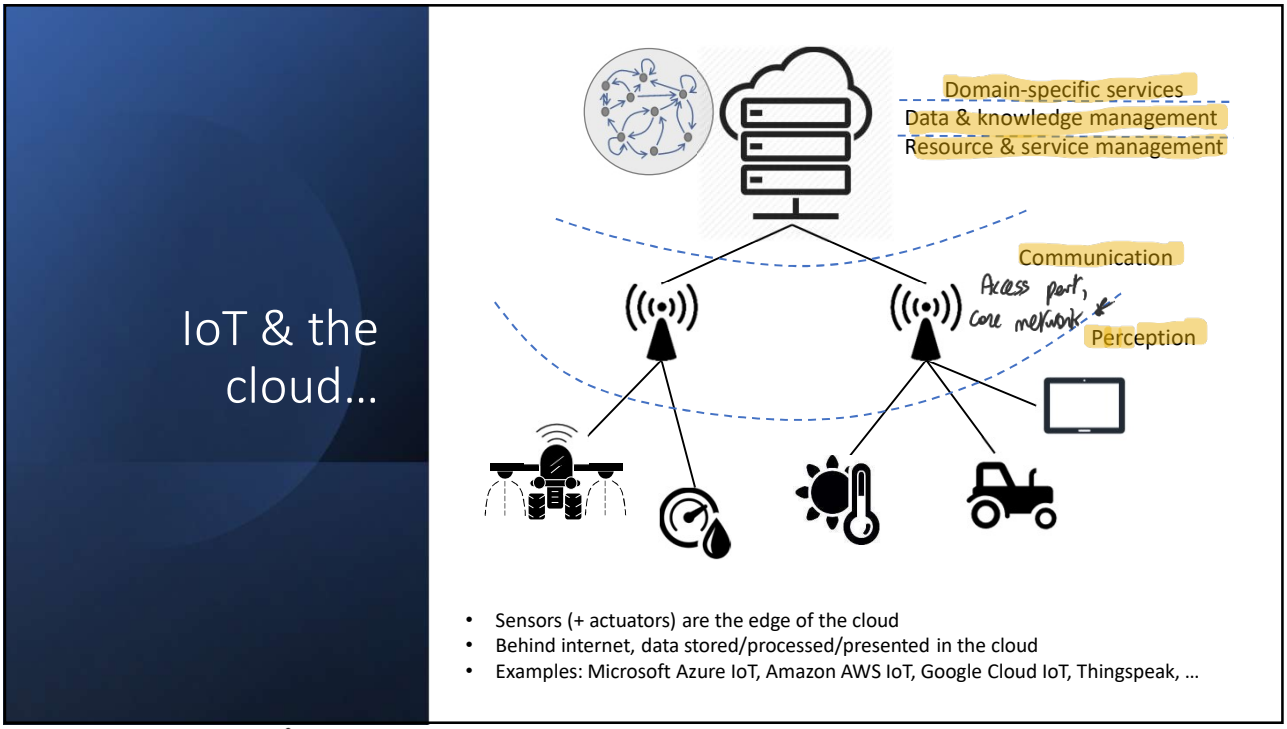
In this architecture, we have different layer.



13 Both wired and wireless. Wires are a limit, in the last mile we use mostly wireless. And for this reason you need autonomous power.

Beyond, we find layers virtually (but not necessary) embedded in cloud.

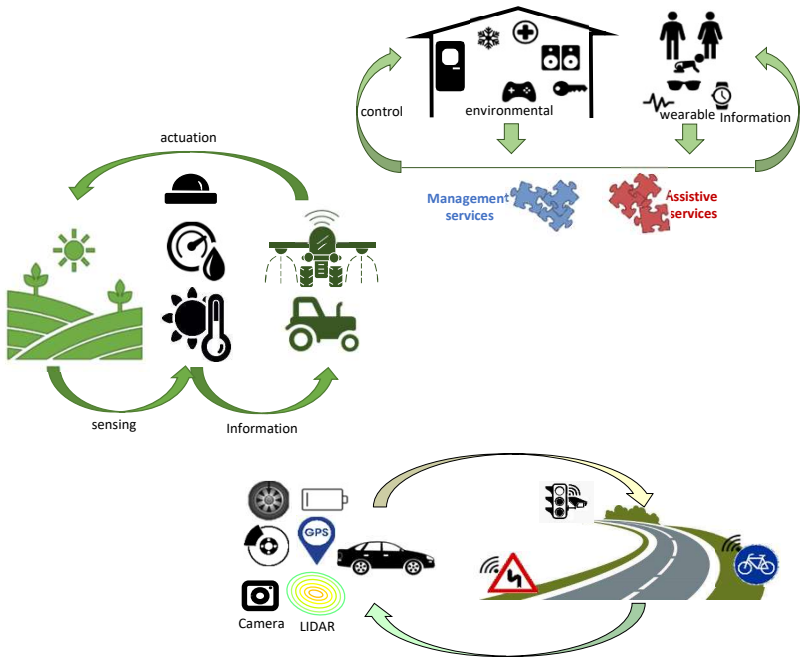
2 Organizes devices 3 Manages the huge amount of data produced. 4 Varies depending on the service you need to implement. Security has to cover this all.



14 Layers correspond to physical representation of network. Provide communication between end and cloud.

What are these sensors? Varying on the application! Even within application field we might have different applications with different sensors.

Sensors at the perception layer



15

Example: sensors for asset tracking

May be

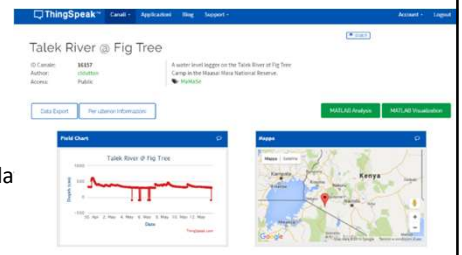
Tracking (products, objects, workers,…):	• GNSS geo-localization • Proximity (NFC) • Time of flight (UWB)/Angle of arrival (BT) localization • Orientation (gyroscope) / Presence (PIR,…)
Warehouse logistics:	How to automate warehouse to know where to find stuff • Proximity (NFC) • Time of flight localization (UWB) • Angle of arrival localization (Bluetooth) • Height/floor detection: pressure Different sensors!
Outdoor monitoring (containers, fleet, livestock,…):	• GNSS geo-localization • 3D-accelerometers • Inclinometer • Pressure Radio collar, data for physiological conditions exc.
Goods guarantee (food, …) :	• Temperature, • Humidity, • Accelerometer, • Inclinometer

16

Platforms: big SW specialized to support IoT that implement these layers and support you

Platforms for IoT

- Sensors (+ actuators) are the edge of the cloud
- Behind internet, data stored/processed/presented in the cloud
- Several platforms available: Microsoft Azure IoT, Amazon AWS IoT, Google Cloud IoT, ThingSpeak, …
- Example: ThingSpeak
  - https://thingspeak.com
  - a web-based DB
  - can be configured to store data from sensors
  - use input channels to receive and store sensor da
  - some channels are public

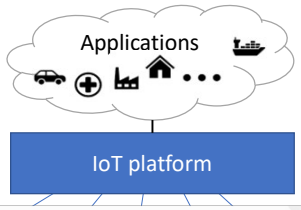


17

Platforms for IoT

Configure, monitor and keep secure a solution. Many services provided.

- IoT Platforms:
  - software layer(s) between the IoT devices and the applications
  - their functionalities may be distributed between devices themselves, gateways and servers in the cloud (or at the edge)
- Not just for data collection from sensors or commands for actuators… they provide several complex functionalities



An IoT (Internet of Things) platform is a type of software or cloud-based service that helps manage, connect, and analyze data from various IoT devices and sensors. Think of it as a bridge that connects the physical world of devices (such as smart home gadgets, industrial sensors, or connected vehicles) to the digital world, allowing them to communicate, gather data, and perform automated actions.

IoT platforms often include tools for device management, data collection and analysis, connectivity support, and application development. They enable developers to build applications that can process and respond to data from connected devices, making everything from smart thermostats to complex industrial systems run more efficiently and smartly.

18

Platforms for IoT

Several functionalities:

- Identification for a device (at application level)
- Discovery where are devices, what they are doing. Tries to discover devices connected and services provided.
- Device management
  - also includes support for deployment, maintenance and decommissioning
- Abstraction/virtualization *
- Service composition: devices provide simple services *2
- Semantics: you want to give semantics to data and sensors themselves. Associate a semantic to what it does.
- … and then, management of the data flow
  - from sensors to applications
  - from applications to actuators
  - support for aggregation, processing, analytics

19

* Devices or appliances are mapped to virtual objects. Used to control devices digitally [DIGITAL TWIN]

*2 In a complex environment you want to compose services for a larger application.

Relevant issues in IoT

- Performance/reliability: IoT devices are spread on the wild. They may be damaged, stolen, moved exc.
- Energy efficiency: battery powered. Not last forever. More efficiency = less maintenance.
- Security
- Data analysis/processing
- Communication/brokerage/binding/…
  - How to bring together data producers (sensors) with consumers (users/actuators/applications)
- Data representation
  - Data formats, standardization
- Interoperability in IoT there are many standards being produced *3

Deployment and maintenance of devices.

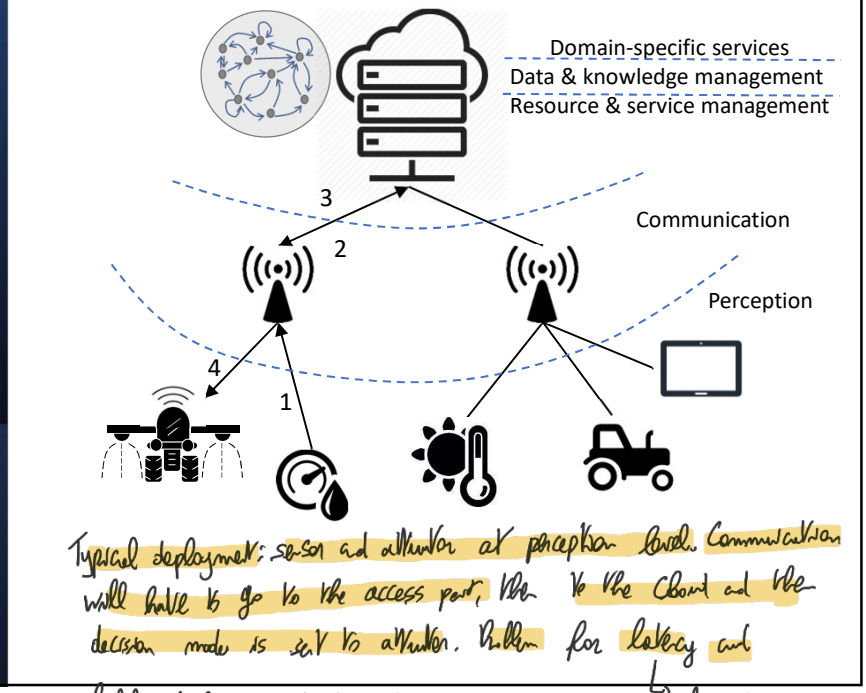
Many standards already available
- At MAC level: Bluetooth, IEEE 802.15.4,…
- At network level: ZigBee, Bluetooth, 6LowPan,…
- At application level: MQTT, CoAP, oneM2M, …

20

* Batteryless devices are becoming popular: work only when energy harvesting system are working. They are built with a supercapacitor that stores a small charge. When no energy production, SW sends interrupt to device to prepare for turn off. If this device is dealing security measures we have to deal with them

*3 In IoT interexchange is important. You don't want a device for another brand is not work.

IoT issues: latency, reliability

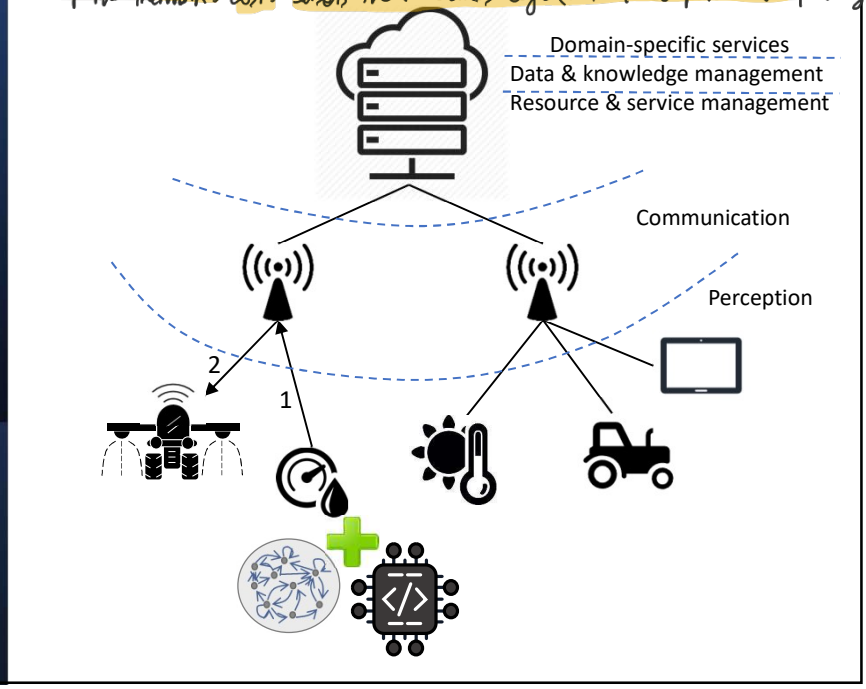


Typical deployment: sensor and actuator at perception level. Communication will have to go to the access part, where to the cloud and the decision made is sent to actuator. Problem for latency and availability (if one node doesn't work no operation) ↳ alarms!

21

For those weaknesses alternative: move computational capability to the edge of the network: cost: sensors need business logic (SW) and computational capability.

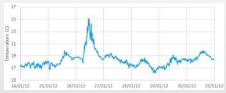
IoT issues: latency, reliability



22 But the previous model is there also for business reasons: binding you to a company and obstaculing interoperability.

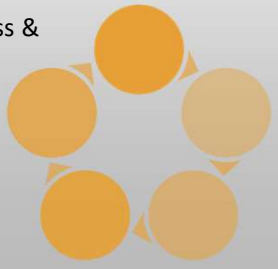
What happens when you put all of these together? Huge amount of devices, data; huge flow of data which is also unreliable (new sensors deployed, sensors breaking down exc.), it is inconsistent because sensors might have different pov. But at the same time you want to manage this with devices with ①
and you want to deal with all of this with efficient processing of data with AI.

IoT issues: latency – analysis – efficiency – …

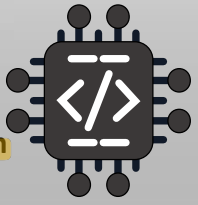


Producing fast-streaming heterogeneous sensed data (… Edge and Fog Computing)

Context awareness & continuous adaptation (…AI)



① **Power** and **communication** constraints



23

IoT & Artificial intelligence

- AI aims at getting computers to behave in a smarter manner
- either through…
- … curated knowledge… ⓐ
- … or through machine learning

- Capabilities of AI include:
- understanding human language (Watson, Siri, Cortana, Translators …)
- Conversation in human language (chatGPT)
- Strategic game systems (Deep Blue for chess, AlphaGo for GO,…)

Bard AI

24 ① If we want to reproduce intelligence, we can attempt to recreate the way in which human beings learn or how they reason. CK ML
Create a base of knowledge 1, and create ability to reason about that (inference) 2

AI through Curated knowledge

Big database of knowledge is extremely difficult.

Many ways of representing knowledge, Often based on (a large number of) cause/effect rules

Examples:

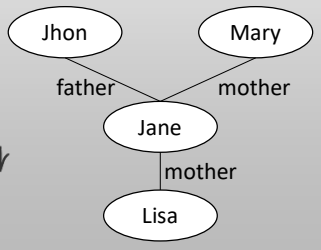
- Propositional logic:

$$It\ is\ hot \rightarrow I\ wear\ shorts\ \wedge\ I\ drink\ ice\ tea$$

- Predicate logic:

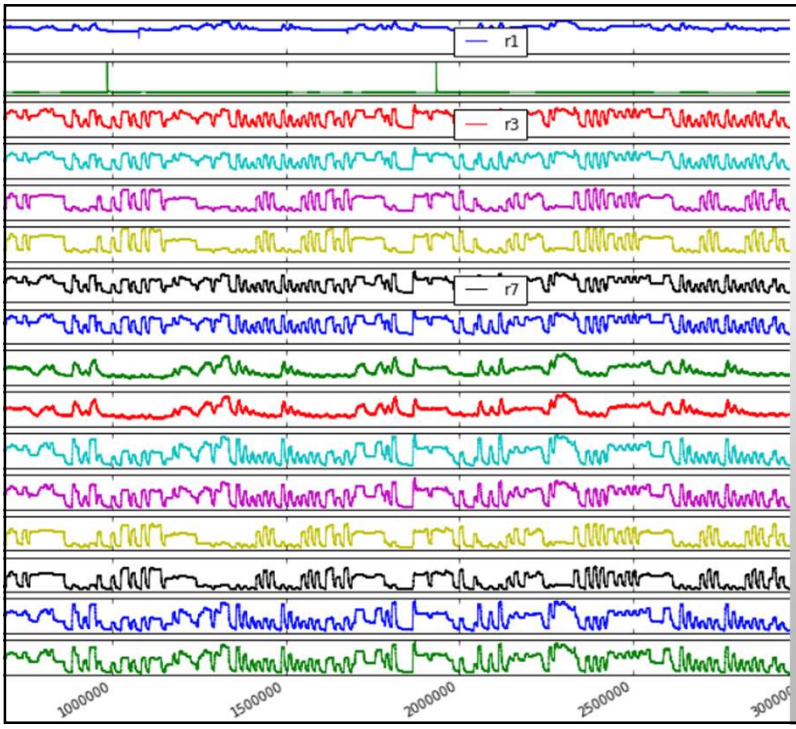
$$\forall x: day\_of\_week(x, wednesday) \vee day\_of\_week(x, friday) \\ go(me, football\_court) \wedge play(me, football)$$

- Production rules:
  $if\ having\ a\ sandwitch\ then\ hungry$
- Semantic networks:



Many approaches. For years AI was this. Creating machines that could learn were very difficult.

25



In the picture of IoT we have this: you cannot have a description of this and create a database of knowledge from this.

Heterogeneous Time-Series of Sensed data

- Fast flowing
- Noisy
- Redundant
- Missing
- …

26

Machine learning

- It is a subfield of AI that deals with:

  «automatic systems that can learn from data»

- Replaces «human writing code» with «human supplying data»
  - The system is fed by examples to learn how to associate input with output
  - Some examples are used to train (training set)
  - Some examples are used to test (test set)
- When given in input a data never seen in the training phase the system produces anyway an output
  - If well trained the output will be (most likely/hopefully) correct…
  - Due to the generalization capability of ML

27

SEVERAL PARADIGMS OF ML:

- **UNSUPERVISED LEARNING**
  - ANALYSE DATA
  - FINDS STRUCTURES/RELATIONSHIPS/SIMILARITIES AMONG DATA POINTS
  - AIMS AT UNDERSTANDING THE PAST
- SUPERVISED LEARNING
  - LEARN FROM PAST EXAMPLES
  - FOR EACH EXAMPLE REQUIRES INPUT + DESIRED OUTPUT
  - AIMS AT PREDICTING THE FUTURE OR INTERPRETING THE PRESENT
- REINFORCEMENT LEARNING
  - LEARNS FROM EXAMPLES
  - FOR EACH EXAMPLE REQUIRES ONLY INPUT AND A REWARD
  - E.G. TO LEARN A GAME THE REWARD CAN BE +1 FOR WINNING, -1 FOR LOSING, 0 OTHERWISE

Machine learning

28

ML and IoT…

- Flexibility, robustness
  - The training phase infers the ML classifier from data
    - a ML classifier is a universal approximation of any function
    - Robustness: performance degrades proportionally to the degradation of the input
- Customizability
  - Maximize the accuracy;
  - Reduce the memory footprint of the classifier (for embedding in low-power devices)

AND …

29

IoT & Edge, Fog, Cloud

	Cloud network/data centers: • Wired • Transactional response time	Hundreds of devices
①	Core network: • IP • QoS/QoE response time	Thousands of devices
②	Fog network: • Real-time response time • Distributed intelligence • 3G/4G/5G/WiFi	Tens of thousands of devices
	Edge network of IoT devices: • ZigBee, Bluetooth, WiFi • Millisecond response time	Billions of devices

30

15

Devices here. They may have simple computational capabilities. They can be connected to network directly or through a gateway (ex. Bluetooth)

Edge

At the edge of a typical enterprise network is a network of IoT-enabled devices consisting of sensors and perhaps actuators

- These devices may communicate with one another
- A cluster of sensors may all transmit their data to one device that aggregates the data to be collected by a higher-level entity

A *gateway* interconnects the IoT-enabled devices with the higher-level communication networks

- It performs the necessary translation between the protocols used in the communication networks and those used by devices

31

Intermediate layer of servers. Faster response time than cloud, and remove load from cloud. They can do a lot, usually functionalities related to ①

Fog

In many IoT deployments, massive amounts of data may be generated by a distributed network of sensors

Rather than store all of that data permanently (or at least for a long period) in central storage accessible to IoT applications, it is often desirable to do as much data processing close to the sensors as possible

The purpose of what is sometimes referred to as the edge computing level is to convert network data flows into information that is suitable for storage and higher-level processing

Processing elements at these levels may deal with high volumes of data and perform data transformation operations, resulting in the storage of much lower volumes of data

The following are examples of fog computing operations:

① Evaluation | Formatting | Expanding / decoding | Distillation / reduction | Assessment

32

This layer exists to increase the performance of a system based on cloud.

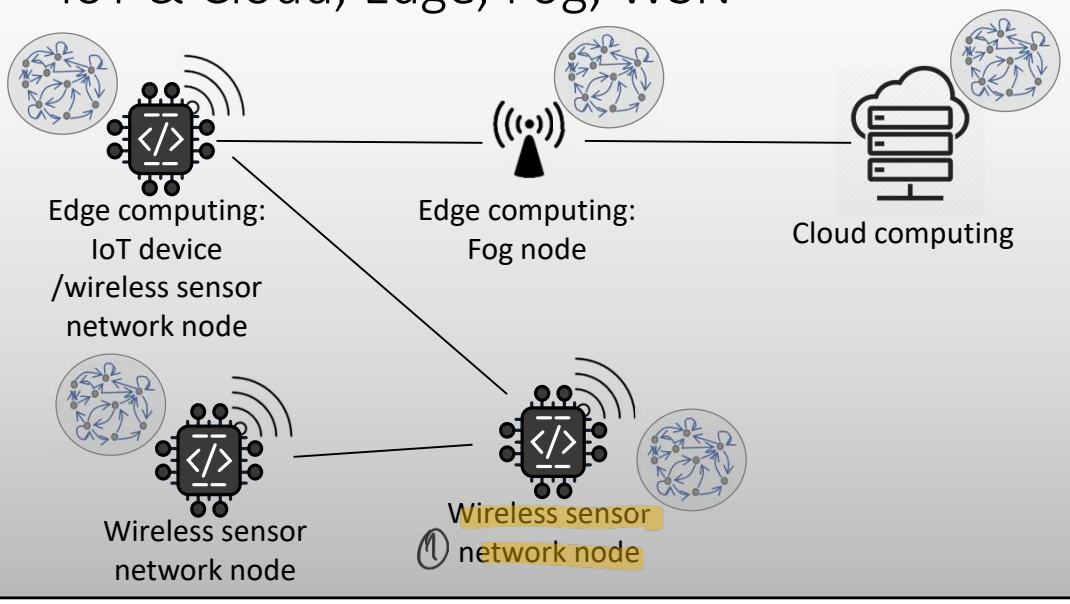
Fog

- Generally fog computing devices are deployed physically near the edge of the IoT network near the sensors and other data-generating devices
- Fog computing and fog services are expected to be a distinguishing characteristic of the IoT
- Fog computing represents an opposite trend in modern networking from cloud computing
  - Cloud: centralized storage and processing for a relatively small number of users
  - Fog: distributed processing and storage resources close to the massive number of IoT devices
- Fog computing addresses the challenges raised by the activity of thousands or millions of smart devices
  - including security, privacy, network capacity constraints, and latency requirements
- The term *fog computing* is inspired by the fact that fog tends to hover low to the ground, whereas clouds are high in the sky

33

From an architectural POV that's not all. IoT device itself may be a bridge for other devices that form a network called ①

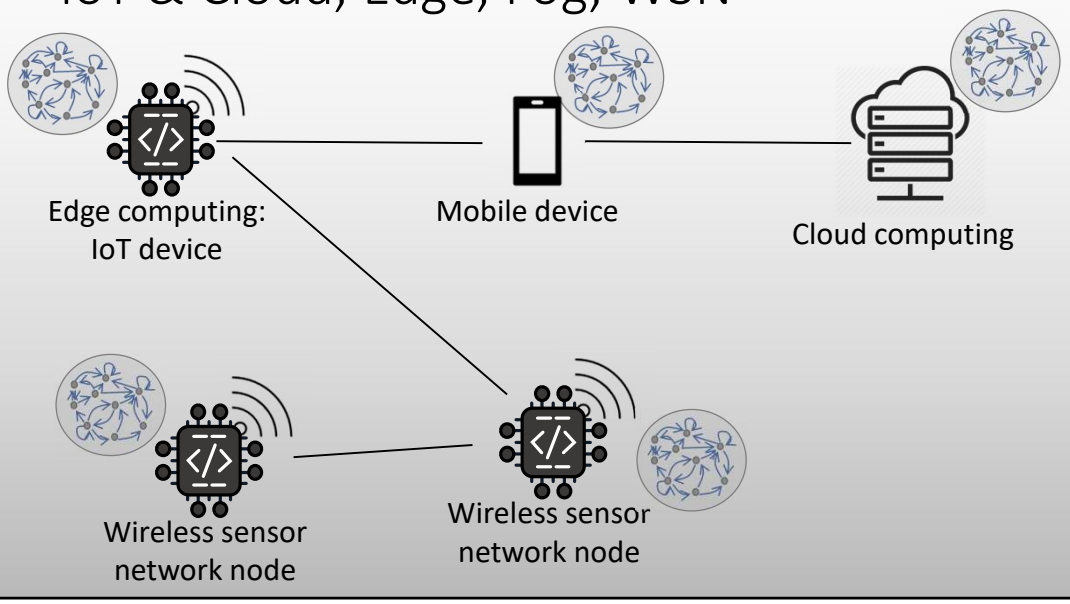
IoT & Cloud, Edge, Fog, WSN



35

Fog node may be implemented by smartphones.

IoT & Cloud, Edge, Fog, WSN



36

lot of effort to attempt to join IoT and blockchain applications.

IoT and emerging paradigms

- blockchain is a shared and trusted public ledger for making transactions
  - everybody can inspect it
  - nobody controls it
  - the transactions within cannot be altered

INTEGRITY and AUTHENTICITY OF DATA

- the blockchain thus provides a single point of truth: it is shared and tamper-evident

Think of ETH.

- participants involved in a business can use a blockchain to record the history of business transactions

37

Blockchain & IoT

On the BC you can implement transactions associated to passage of value. Something run by only machines, BC is a good opportunity.

- Blockchains imply a paradigm shift for IoT
  - From centralized storage to a decentralized one, in a distributed ledger
  - Supports the expanding of IoT ecosystem
- Blockchain approach:
  - Reduces maintenance costs (the distributed ledger is public…)
  - Provides trust in data produced
- Different potential scenarios…

decentralized storage you can trust.

also reduces the cost for things you have to coordinate.

38

Let's say I am manufacturing IoT devices. We might want updates. How do we manage this? Broadcast that a new update is present with the hash of the update. So they can download it from wherever you want because you have hash.

Deployment scenarios (1) – updates management of IoT devices

- All IoT devices of a manufacturer operate on the same blockchain
- The manufacturer deploys a smart contract to store the hash of the last firmware update
- Each device shipped with the smart contract address in their blockchain client
- IoT devices can query the contract and find out the new firmware update (and its hash)
- The binary of the firmware could be placed on a P2P storage
  - so that it can be retrieved by any device also when the manufacturer stops publishing it

39

Marketplace of IoT devices: your sensor might provide data for other devices. You can create a marketplace of data, and manage this with BC to record data transfer: every device has account with smart contract that shares data.

- blockchains with cryptocurrency to provide a *billing layer to* implement of a *marketplace of services between devices*:
  - devices that store a copy of binary codes or storage for sensed data may charge for serving it;
  - E.g. Filecoin which allows devices to ``rent their disk space'';
- every device can have its own *bank account* on the blockchain
  - it can then expose its resources to other devices (or users) and get compensated for their usage via microtransactions

Deployment scenarios (2) – marketplace of IoT services

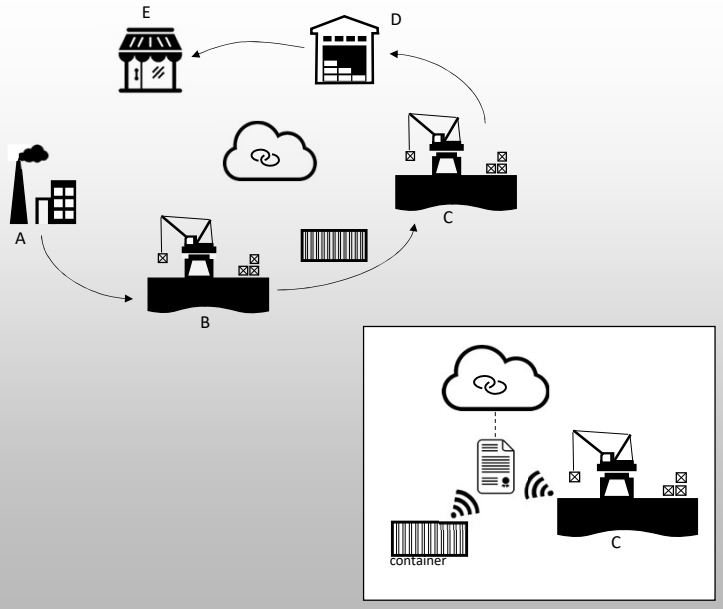
40

Monitor supply chain with BC. Different manufacturers, distributors; several actors, that might not trust each other. To keep track of who did what, trackability. So flow of data will flow for this. And since entities might not trust each other, so you use a BC.

- blockchain as a shared ledger between the companies in a supply chain
  - IoT devices monitor the quality of the goods along the chain…
  - … at each production stage and during shipping.
- Smart contracts to certify each intermediate delivery of goods
  - Each company in the supply chain can query the ledger to see the (certified) state of the goods

Deployment scenarios (3) – monitoring supply chain

41



Deployment scenarios (4) – asset tracking

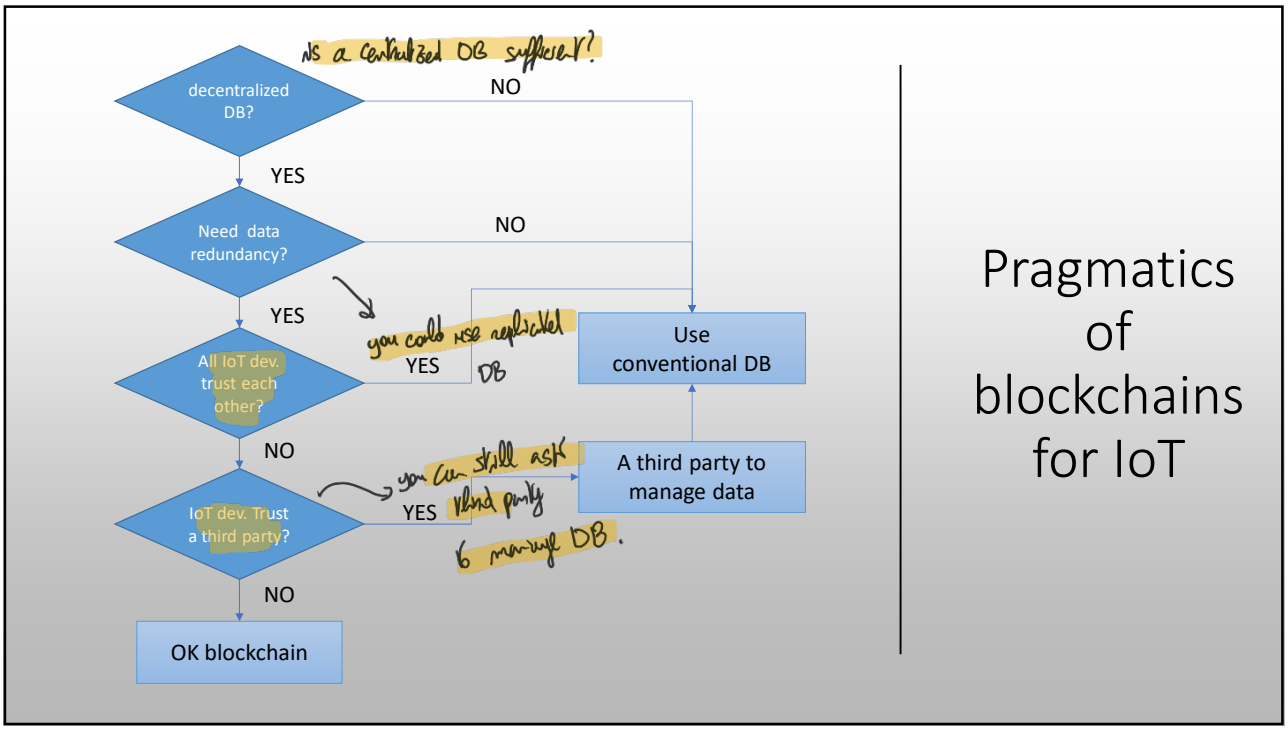
42

Devices producing energy with harvesting may sell energy and devices that might buy it.

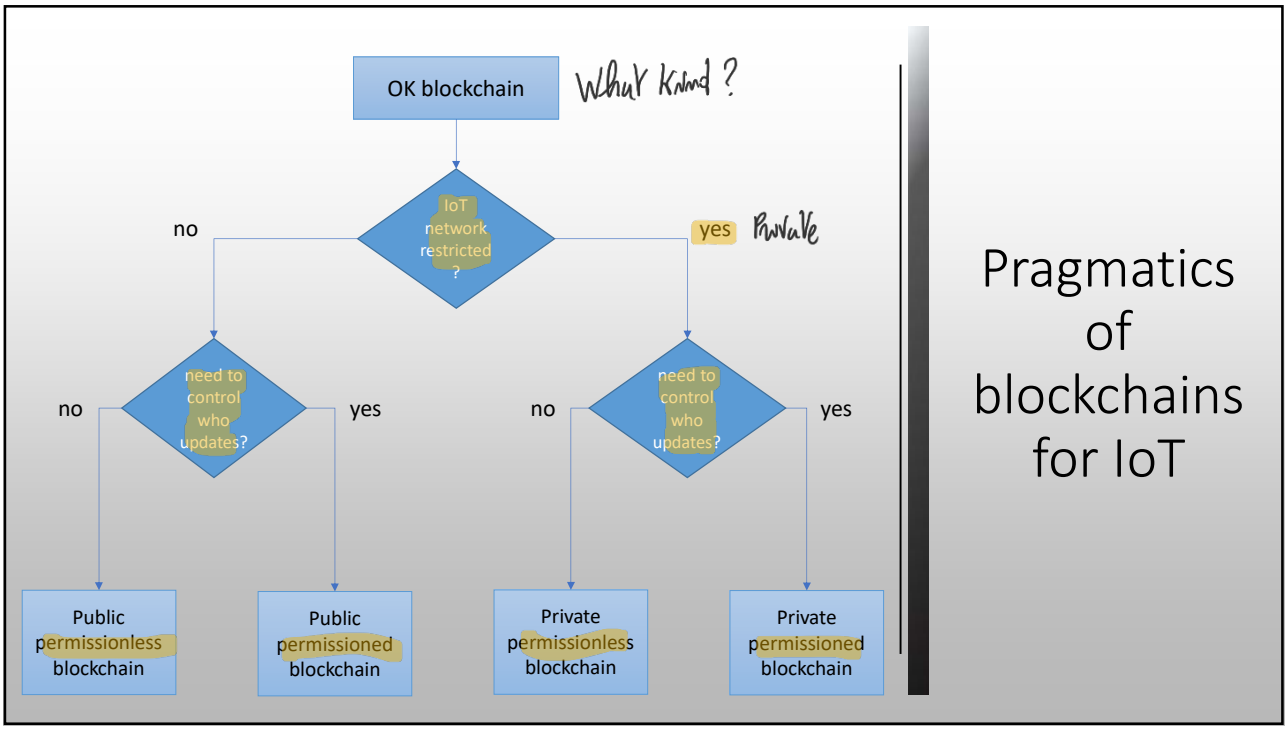
- In the energy sector
  - IoT devices can buy and sell energy automatically
  - IoT devices with surplus of energy (e.g. with solar panels) may share their energy with other devices
- In precision agriculture, with IoT sensors to monitor the state and good health of the crops
  - Agreed and visible by all companies in the supply chain
  - Can certify the quality of the production

Deployment scenarios (5) – energy marketplace, precision agriculture, …

43


decentralized DB?
NO
YES
Need data redundancy?
NO
YES
All IoT dev. trust each other?
YES
Use conventional DB
NO
IoT dev. Trust a third party?
YES
A third party to manage data
NO
OK blockchain
Pragmatics of blockchains for IoT

44


OK blockchain
IoT network restricted ?
no
yes
need to control who updates?
no
yes
need to control who updates?
no
yes
Public permissionless blockchain
Public permissioned blockchain
Private permissionless blockchain
Private permissioned blockchain
Pragmatics of blockchains for IoT

45

Interoperability & Reference Standards

46

Interoperability

- often, a straight implementation of an IoT solution is not a problem by itself
  - you can design the solution from the bottom (physical layer) up to the application layer
- this is what is informally called a "**vertical silos**" ①
- your solution will only work alone: ②
  - only your devices
  - any change/update requires your intervention
  - other vendors cannot interfere

Very feasible. You can find sensors, interfaces exa. Don't have problem with complex problems

Problem: if you do thing on your own, you build a ①, protected system, with keyed org., but: ②

47

Interoperability

Business model of "vertical silos" design strategies:

- Entrap your clients – this is often called "**vendor lock-in**"
- Prevent the use of components from another vendor
- Force high costs to migrate to another vendor
  - full redesign and deployment of a new solution
  - with the risk of entering another silos…
- Example: wristbands for fitness

48

Interoperability

solution: introduce standards (electricity plugs)

- In the past the problem was mostly at hardware level
  - Example: mains sockets
- Now also at software level
- The solution is to introduce standards…

49

Wireless technologies & standards

50

When you start developing a tech, you need big investment with low revenues for a while. When tech comes to the market it's costly. Usually you have competitive advantage. But over years other competitors will appear (with lower costs). At this point the market shifts. The price goes down, so manufacturer look for large numbers and small revenue per piece.

Why standards?

- Require common interests and agreements among different stakeholders
- Usually motivated by a reduction of the costs for development of a technology
- "coopetition" among different stakeholders ①
- Usually happens when technology becomes mature:
  - the big revenues are somewhere else
  - no interest in investing big money in developing the technology
  - without these conditions the standards will most likely fail

Once a new tech is mature, that's not anymore added value. When this happens your org. may fail because you are competing with low cost org. Usually org. switch on different markets

51

① Model for this: share cost of research for underlying tech and compete for what's above that. Lower layers maintained by cooperation.

In IoT this happened for wireless communications. For communication we have cooperation. So we are looking at higher layers.

Standards in IoT

- So far, this happened in wireless communications
  - That's explains the large number of wireless standards
- Now the problem of interoperability (and thus of standardization) is moving up at middleware/application layers
- Currently many application-level protocols available for IoT:
  - ZigBee, Bluetooth, MQTT, CoAP, ligtweightM2M

52

Interoperability is an advantage for the user to avoid vendor lock-in. In general " " is a requirement imposed by end users and politicians. However becomes an advantage for vendors too: when competitors copy innovation, prices become low, with low revenues.

Standards in IoT

At that point for manufacturers there's no point in still investing in the new technology, but they still have to maintain what has now become a common base. So creating standards becomes convenient: standardise base line and compete on higher layers.

- … but what happens when there are (too) many standards available?
- the interoperability is not only an issue between "vertical silos"…
- … but also between different standards
- to deal with several incompatible standards a solution is to introduce application-level gateways
  - do not translate only low-level protocols
  - also map one into the other different application-level behaviors

53

Idea is to cooperate on standards for common solutions, we do not want to spend energy in developing them.
But: sometimes groups of companies might form a consortium that work with multiple and incompatible standards.

How can this problem be solved? We should make different standards converge, but it's not easy. A practical approach is to find bridges that connect two standards. In IoT you can use bridges to do that.

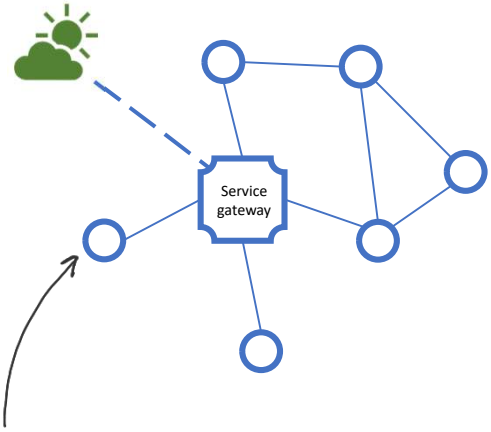
[NOTA: mantenere una base è costoso => diventano a pezzi]

Standard protocol lets different vendors interact with each other working together. In this case it is possible to build a service gateway to achieve connection with the rest of the world. Not obvious before: Zigbee is a case. Standard for wireless sensor networks. Meant to work alone without connection to the internet.

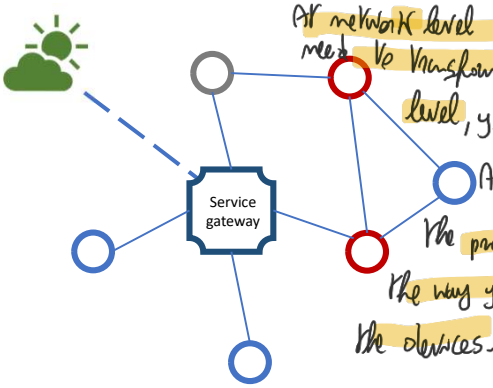
Different configurations…

In both cases, service gw just has to map some behaviour from one protocol to another (network, transport or even application level service gw)

Type A configuration:
- same vendor and same protocol



Type B configuration:
- different vendors but same protocol



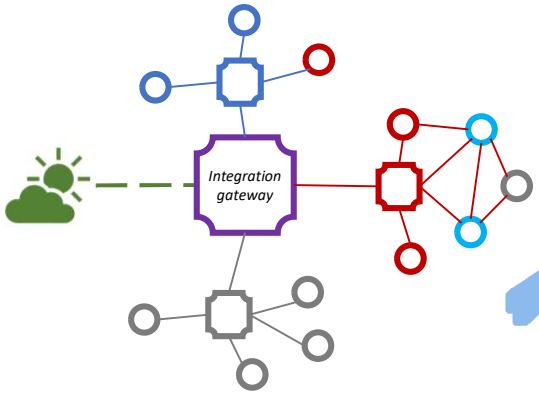
At network level you would just need to transform header of netw. level, you convert it.

At application level, the protocol may specify the way you interact with the devices.

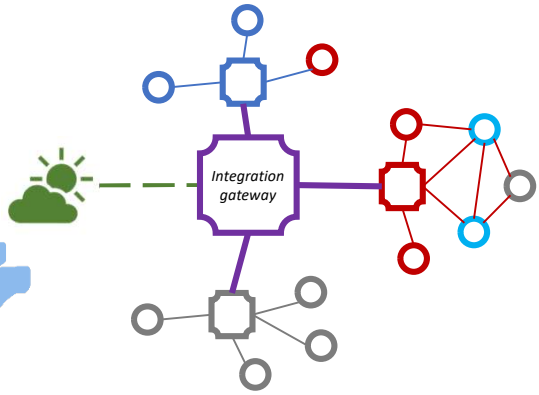
54 Manufacturer has its own devices and protocols. If an internet connection is realized, a service gateway connects its protocols to the ones on the net. Not necessarily exposing its protocols to the internet, possibly. We are making internet interoperable with own protocol

Different configurations…

Type C configuration:
- different vendors and different protocols



Type C/II configuration:
- e.g. google home, alexa, …



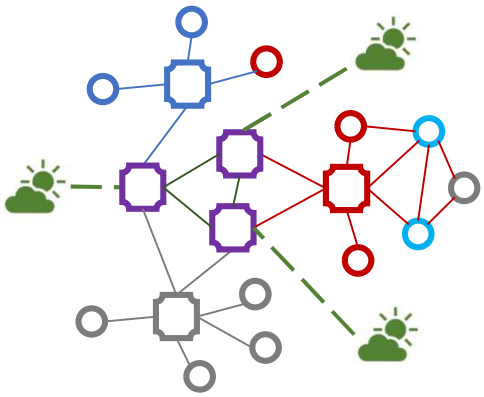
55 Integration gateway speaks different levels and connect different islands to make everyone be able to talk to each other. Ex: Alexa is acting as Integration gw: "I can provide to the market something only I can provide. To other vendors, if you want to use this service you have to conform to how I do it. So a standard is imposed to manufacturers. If you want to use a

service provided by them you have to use their language".

Different configurations…

Type D configuration:

- Different vendors, different protocols, distributed integration gateways



56

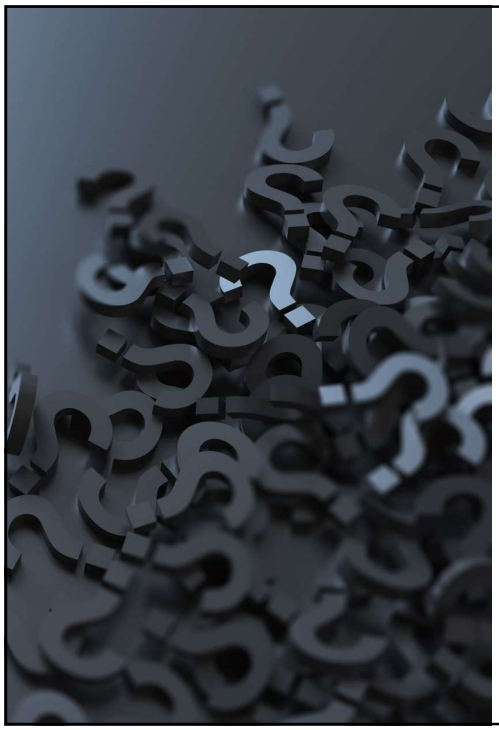
Integration GW distributed. Can be adopted for redundance, reliability, performance. Solution is to develop an internal GW for the whole GW, GW to make them communicate.

Review question

May blockchains in IoT have a relationship with interoperability?

If IoT devices are using a blockchain as a mean to interact with themselves, you can have different devices that may interoperate by means of blockchain. To some extent. Still, so many blockchains, so you have interoperability problems.

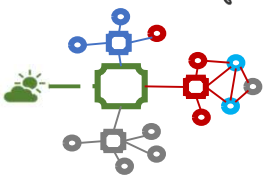
57



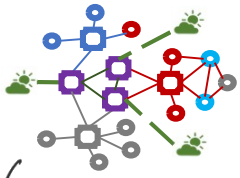
Question

- In type C configuration, how many mappings from one protocol to another (at the same level) the integration gateway should be able to manage?
- What about in type D configuration?

$O(m^2)$ → can become very complex



type C configuration



type D configuration

every IG transforms every protocol into 1 protocol

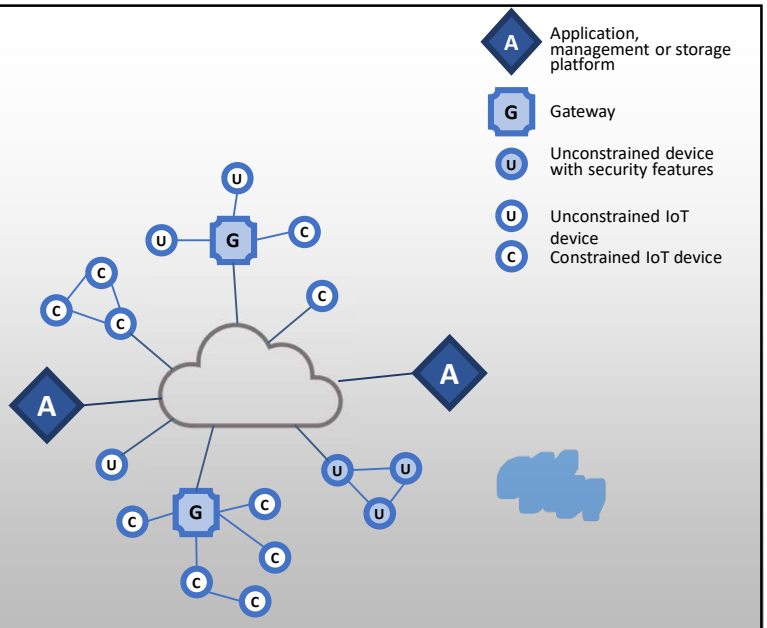
58

Security in IoT

59

With IoT you have heterogeneous devices, with constraint or power, computational capabilities etc, and unconstrained devices. At the same time you might have devices connected to the net directly or through gw. Some devices (especially U) might have security features, others not. Nightmare for security. No definite border/surface to protect.

IoT security: elements of interest



60

There is a magazine paper that explains that we are close to a crisis pt. In IoT there's a strong pressure to come in the market. So you sacrifice time spent for security. In the case of IoT, these devices are sold to users unaware of security aspects, not informed on even how to make secure. There isn't even patch for update.

Patching Vulnerability

There is a crisis point with regard to the security of embedded systems, including IoT devices
The embedded devices are riddled with vulnerabilities and there is no good way to patch them
Chip manufacturers have strong incentives to produce their product as quickly and cheaply as possible
The device manufacturers focus is the functionality of the device itself
The end user may have no means of patching the system or, if so, little information about when and how to patch
The result is that the hundreds of millions of Internet-connected devices in the IoT are vulnerable to attacks
This is certainly a problem with sensors, allowing attackers to insert false data into the network
It is potentially a graver threat with actuators, where the attacker can affect the operation of machinery and other devices

Patching those devices is very complex. You have to replace the firmware without destroying the devices and most solutions generally don't work.

So filling net with insecure, unpatchable devices with unaware users. Problem is with sensors: if one is useful, we can inject data to make things behave in the wrong way.

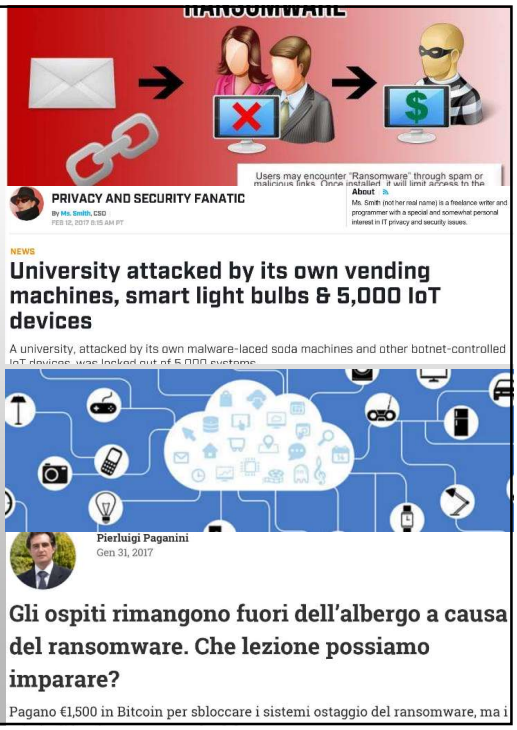
It is also a matter of confidentiality: wristband example

61 Even worse with actuators that act in the physical world.

Cybercrime with IoT

Kits for these attacks can be found on the Internet …

… for 15 €



62

So internet.org.ua working for defining standards for IoT.

IoT Security and Privacy Requirements

- The IUT-T standard Recommendation Y.2066 includes a list of security requirements for the IoT
- these are functional requirements during capturing, storing, transferring, aggregating, and processing the data of things, as well as to the provision of services which involve things
- The requirements are:
  - Communication security CIA
  - Data management security
  - Service provision security [Address unavailability, stealing,]
  - Integration of security policies and techniques
  - Mutual authentication and authorization
  - Security audit

  to all you might expect from a data system.

63

IoT Security and Privacy Requirements

- **Communication security** (secure, trusted, and privacy protected communication capabilities):
  - enforces confidentiality and integrity of data during data transmission or transfer
- **Data management security** (secure, trusted, and privacy protected data management capabilities):
  - enforces confidentiality and integrity of data when storing or processing data
- **Service provision security** (secure, trusted, and privacy protected service provision capabilities):
  - deny any unauthorized access to service and fraudulent service provision
  - protect privacy information related to IoT users

64

① Interesting case: in case of constrained devices ever executing security protocols become a problem. For low end devices you may be unable (ex. cryptography). In some case we either ignore it or work with simpler devices. In some cases, auth only on one side, so undirectional.

IoT Security and Privacy Requirements

- **Integration of security policies and techniques:**
  - ability to integrate different security policies and techniques
  - ensures a consistent security control over the variety of devices and user networks
- **Mutual authentication and authorization**:
  - mutual authentication and authorization between devices (or device/user) according to predefined security policies
  - before a device (or an IoT user) can access the IoT
- **Security audit:**
  - any data access or attempt to access IoT applications are required to be fully transparent, traceable and reproducible according to appropriate regulation and laws
  - support security audit for data transmission, storage, processing, and application access

① Common req. that has to do with tracking all security related events, but no strong, no bumper proof!

65

In the case there is a gw, you have unconstrained devices, IoT applications often rely on powerful GW. Two steps: make secure interaction between cloud and gw, and then auth. and secure data transfer for device.

IoT gateway security functions

setup defenses on the gateway regulations.
Enforce security and privacy on the gw.

66

Relevant features:

IoT gateway security functions

may be relaxed, one way, with simplistic approaches (precomputed keys exc.)

- Identification of each access to the connected devices
- Authentication with devices
  - based on application requirements and device capabilities
  - either mutual or one-way authentication...
  - one-way authentication is weaker: either the device authenticates itself to the gateway or the gateway authenticates itself to the device, but not both.
- Mutual authentication with applications.
- Security of the data based on security levels
  - data stored in devices and the gateway
  - data transferred between the gateway and devices
  - data transferred between the gateway and applications.

More standard

67

IoT gateway security functions

Ability to diagnose devices, detect failure and control and run update of devices.

- Protect privacy for devices and the gateway.
- Self-diagnosis, self-repair and remote maintenance.
- Firmware and software update.
- Auto configuration or configuration by applications.
  - support multiple configuration modes
  - e.g. remote and local configuration; automatic and manual configuration,
  - support dynamic configuration based on policies.

manage update of device if you have a gw as easier. You have to download it, verify it, using hash, complex ops.
Support soft. of

68

IoT gateway security functions

built with support of gw easier.

- These requirements may be difficult to achieve if they involve constrained devices
  - e.g. if the gateway should support security of data stored in devices. Without encryption capability at the constrained device, this may be impractical to achieve.
- These requirements make several references to privacy
  - with massive IoT, governments and private enterprises will collect massive amounts of data about individuals:
    - medical information
    - location and movement information
    - application usage..
  - privacy is an area of growing concern with the widespread IoT
  - especially in homes, retail outlets, and vehicles and humans

you deal with data, may concern privacy of individuals on of the OP.

69

Review question

Is it sufficient to focus on the gateway to address all IoT security issues?

Not all devices are connected by means of gw,

And the still keeping possibility

70

Summary

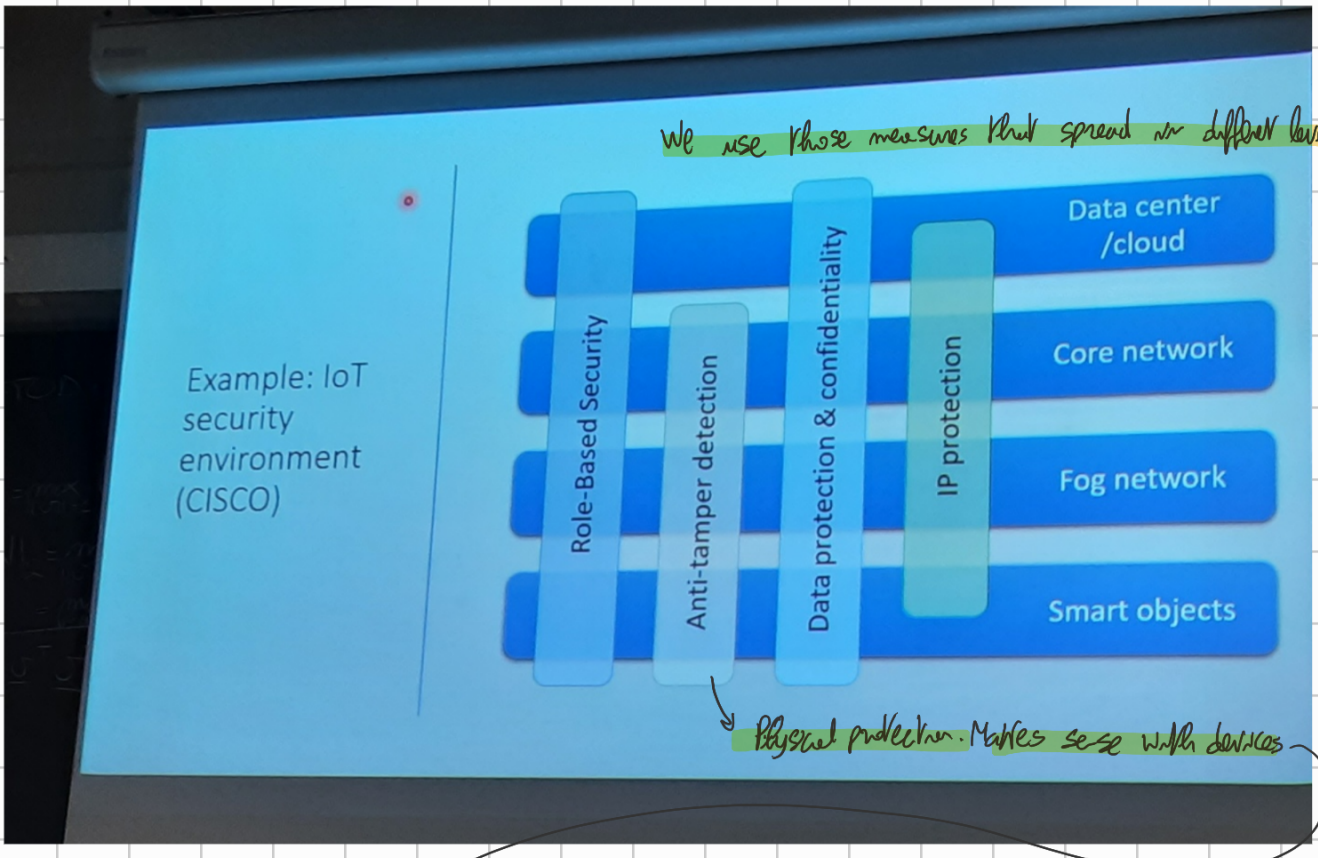
IOT & IOT PERSPECTIVES

IOT AND MACHINE LEARNING, CLOUD AND BLOCKCHAINS

INTEROPERABILITY AND STANDARDS

SECURITY IN IOT

71



We use those measures that spread in different levels

Physical protection. Makes sense with devices

We do not want for ex. Vo need key down.