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

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

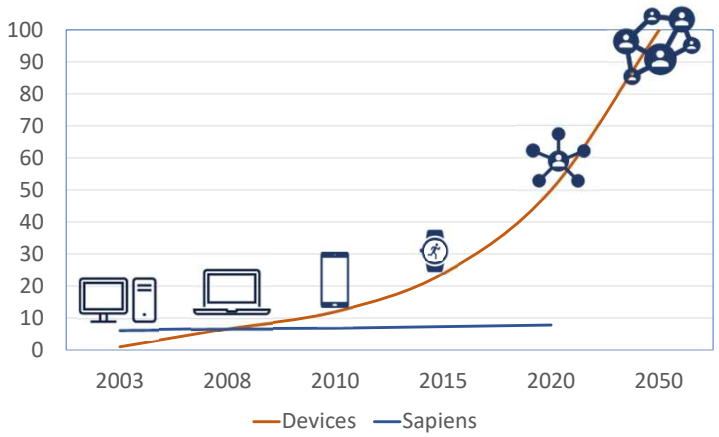
of devices per square meter on Earth (included oceans!)

Is there any purpose/need?

Who needs all this?

3

IoT devices VS humans:



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

Internet of Things (IoT)

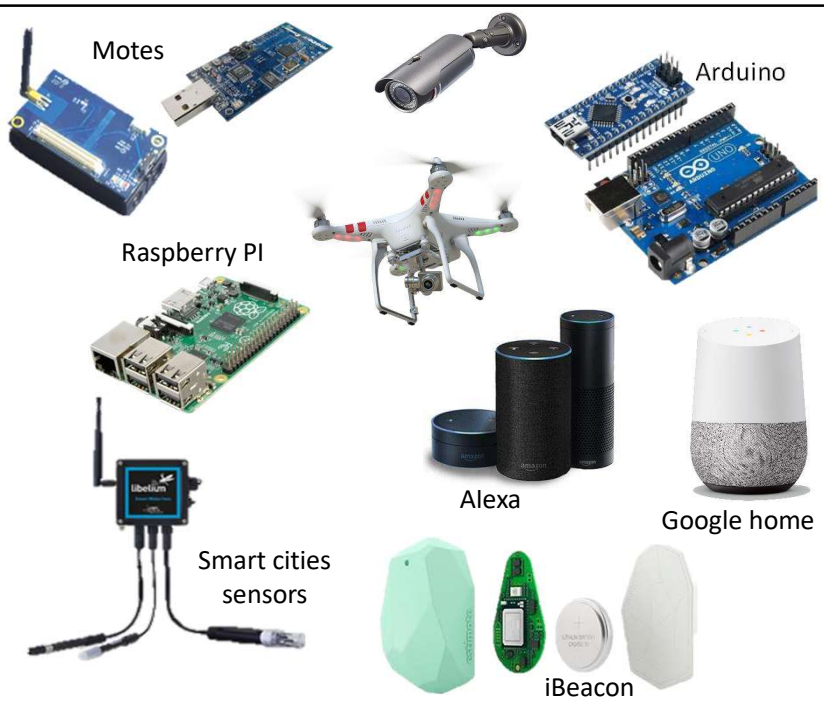
- Most of the devices are not directly in use by human beings
- Independent physical objects with their own businness logic
  - Embedded with electronics, software, sensors and network connectivity
  - Mostly sensors and actuators
  - not human-operated!

5

Wearable devices

6

Environmental devices



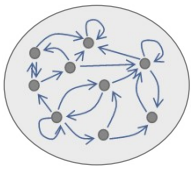
7

Each IoT device...


Sensors/actuators


Microcontroller

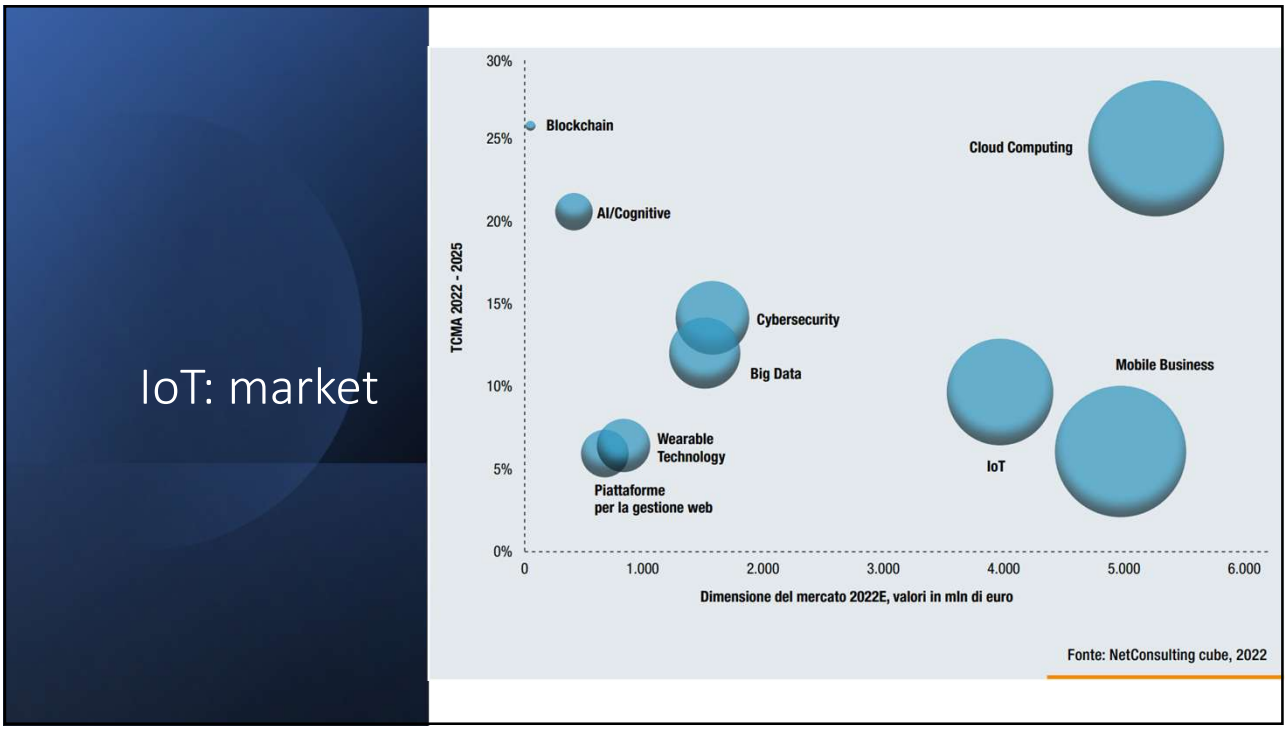

Wireless interface


Software (business logic)

8


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

… 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

… in summary

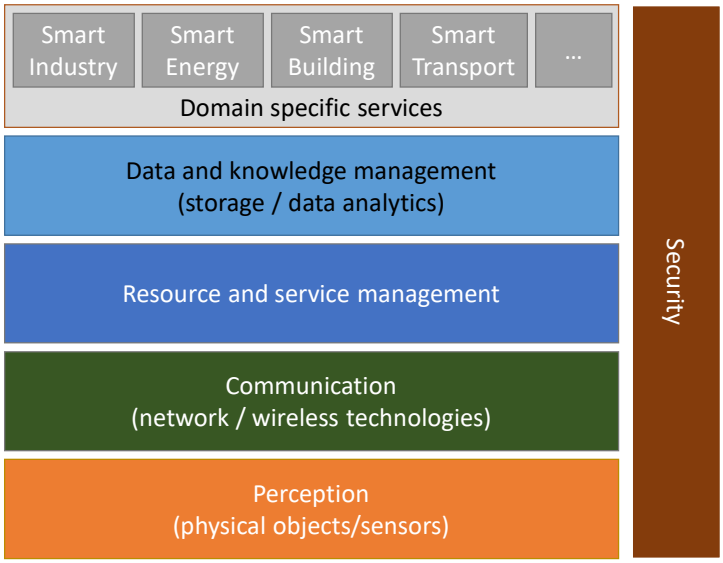
Wrt end systems supported, four generations of deployments of Internet (culminating in the IoT):

Information technology (IT)	PCs, servers, routers, firewalls, and so on, bought as IT devices by enterprise IT people, primarily using wired connectivity
Operational technology (OT)	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	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	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

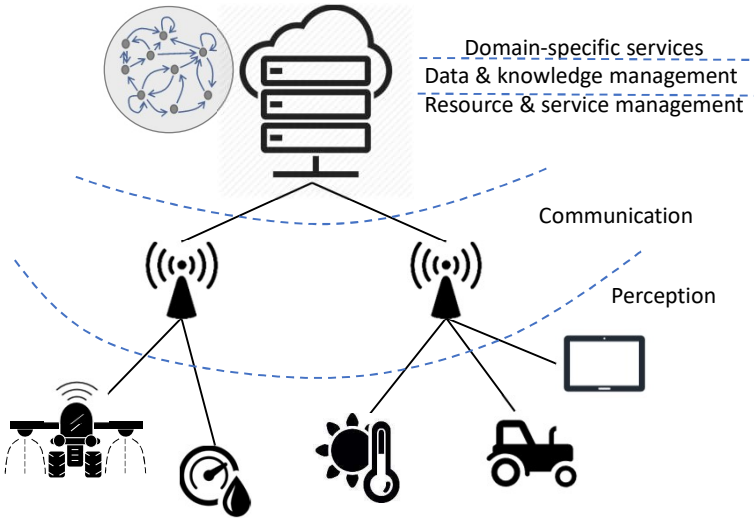
12

IoT: a layered architecture



13

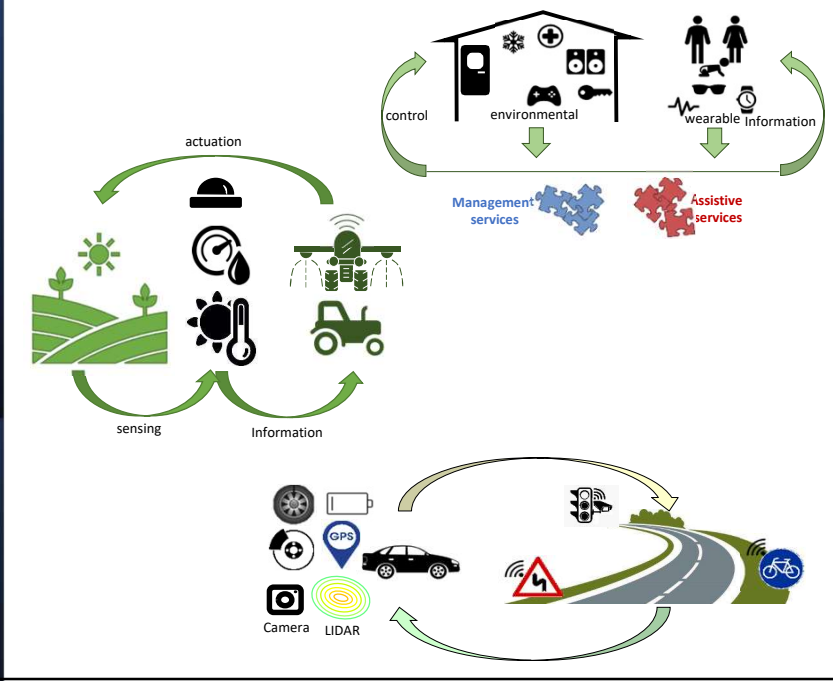
IoT & the cloud…



- Sensors (+ actuators) are the edge of the cloud
- Behind internet, data stored/processed/presented in the cloud
- Examples: Microsoft Azure IoT, Amazon AWS IoT, Google Cloud IoT, Thingspeak, …

14

Sensors at the perception layer



15

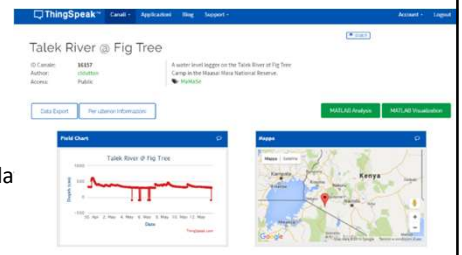
Example: sensors for asset tracking

Tracking (products, objects, workers,…):	• GNSS geo-localization • Proximity (NFC) • Time of flight (UWB)/Angle of arrival (BT) localization • Orientation (gyroscope) / Presence (PIR,…)
Warehouse logistics:	• Proximity (NFC) • Time of flight localization (UWB) • Angle of arrival localization (Bluetooth) • Height/floor detection: pressure
Outdoor monitoring (containers, fleet, livestock,…):	• GNSS geo-localization • 3D-accelerometers • Inclinometer • Pressure
Goods guarantee (food, …) :	• Temperature, • Humidity, • Accelerometer, • Inclinometer

16

Platforms for IoT

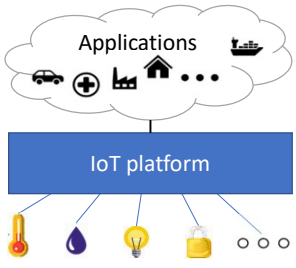
- Sensors (+ actuators) are the edge of the cloud
- Behind internet, data stored/processed/presented in the cloud
- Several platforms available: Microsoft Azure IoT, Amazon AWS IoT, Google Cloud IoT, ThingSpeak, …
- Example: ThingSpeak
  - https://thingspeak.com
  - a web-based DB
  - can be configured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



17

Platforms for IoT

- 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



18

Platforms for IoT

Several functionalities:

- Identification
- Discovery
- Device management
  - also includes support for deployment, maintenance and decommissioning
- Abstraction/virtualization
- Service composition
- Semantics
- … and then, management of the data flow
  - from sensors to applications
  - from applications to actuators
  - support for aggregation, processing, analytics

19

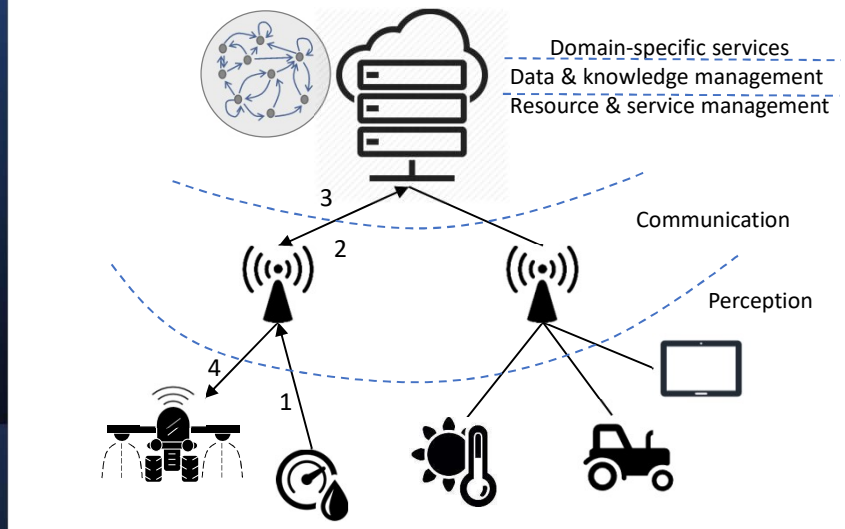
Relevant issues in IoT

- Performance/reliability
- Energy efficiency
- 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

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

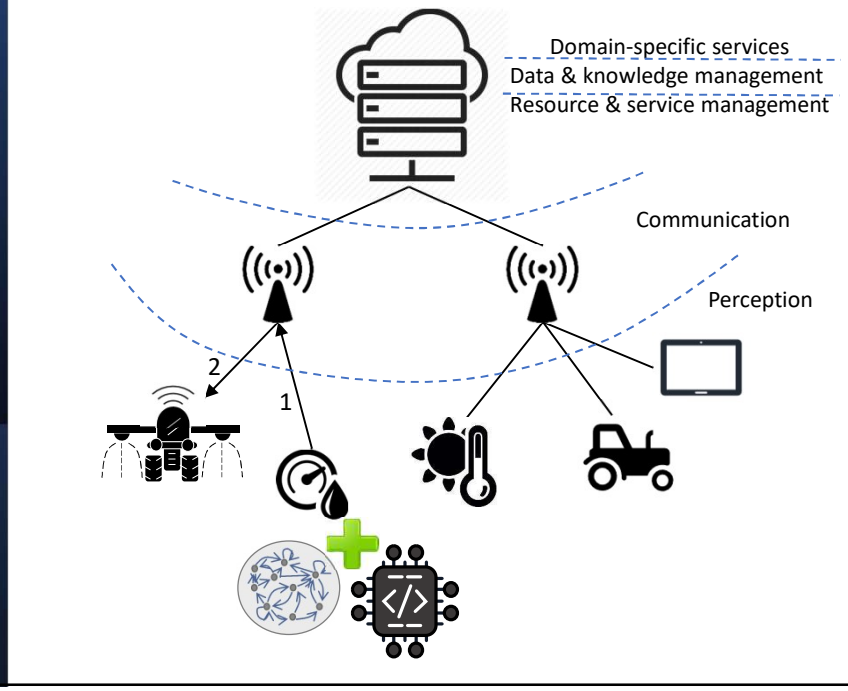
20

IoT issues: latency, reliability



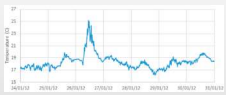
21

IoT issues: latency, reliability



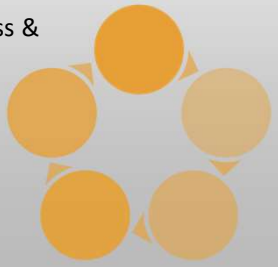
22

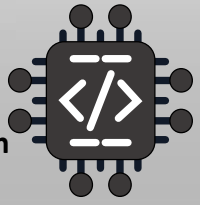
IoT issues: latency – analysis – efficiency – …



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

Context awareness & continuous adaptation (…AI)





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

AI through Curated knowledge

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

Examples:

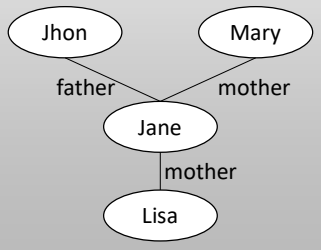
- Propositional logic:

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

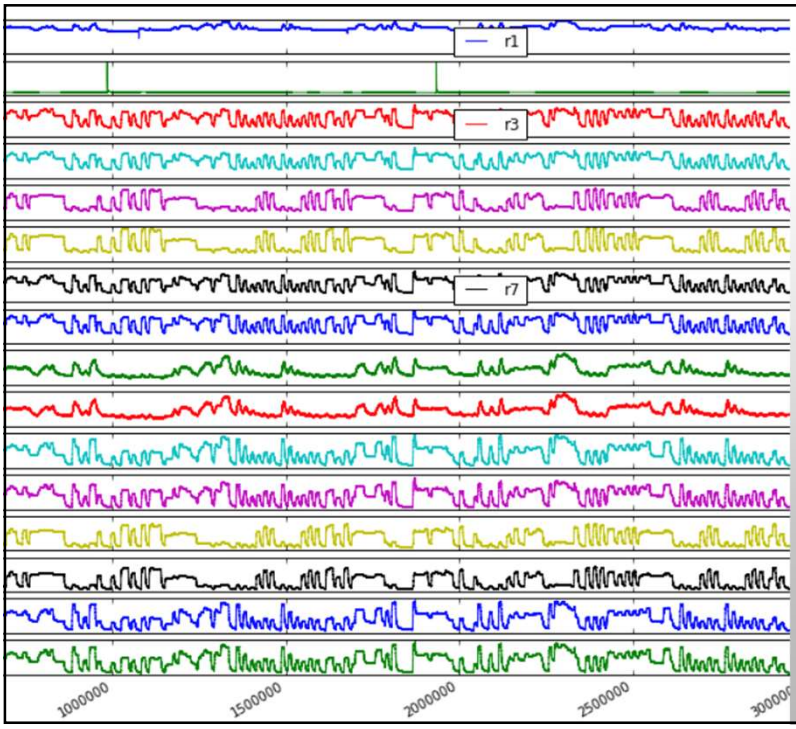
- Predicate logic:

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

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



25



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…

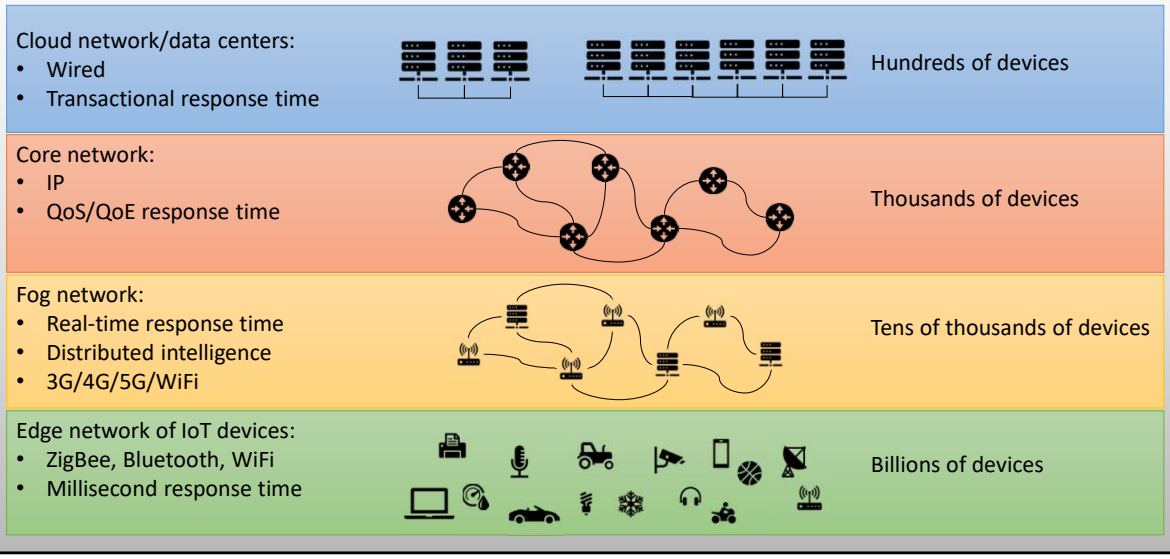
- Flexibility, robustness
- The training phase infers the ML classifier from data
  - a ML classifier is a universal approximation of any function
  - Robustness: performance degrades proportionally to the degradation of the input

- Customizability
- Maximize the accuracy;
- Reduce the memory footprint of the classifier (for embedding in low-power devices)

AND …

29

IoT & Edge, Fog, Cloud



30

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

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:

- Evaluation
- Formatting
- Expanding / decoding
- Distillation / reduction
- Assessment

32

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

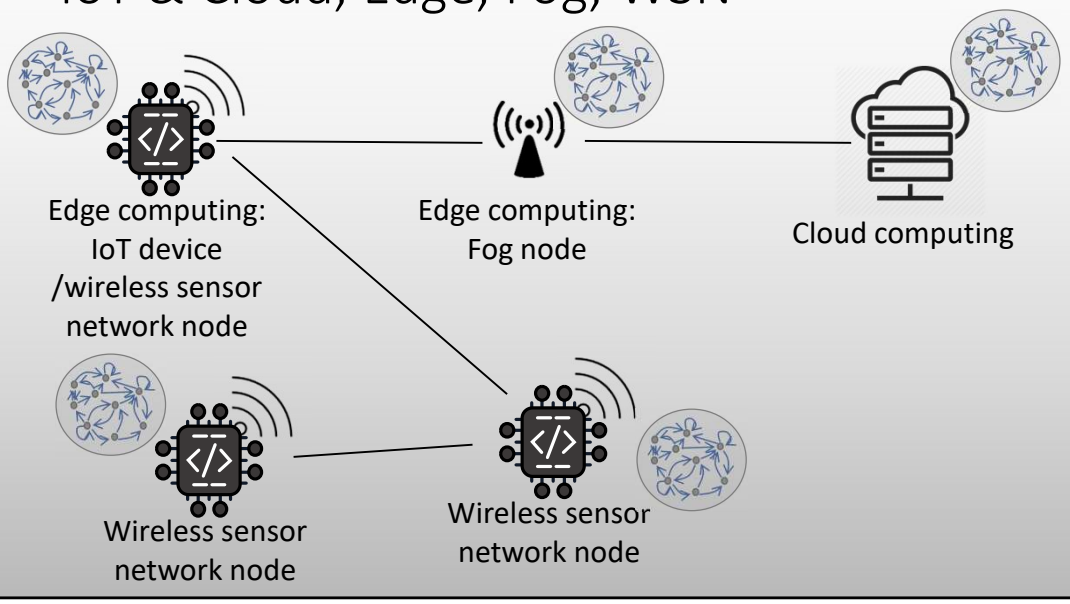
Fog computing addresses the challenges raised by the activity of thousands or millions of smart devices

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

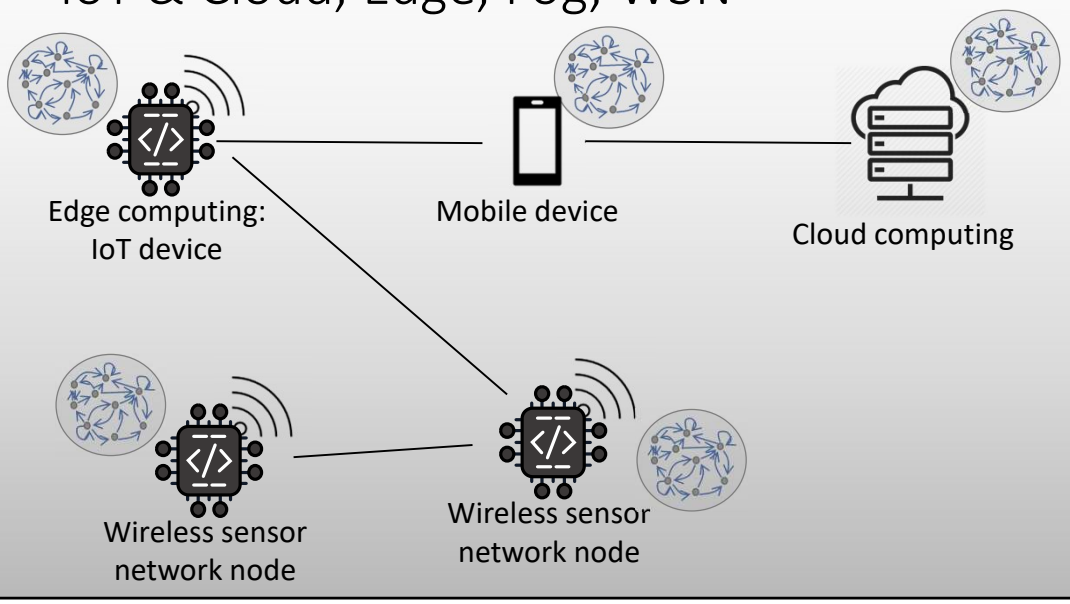
33

IoT & Cloud, Edge, Fog, WSN



35

IoT & Cloud, Edge, Fog, WSN



36

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
- the blockchain thus provides a single point of truth: it is shared and tamper-evident
- participants involved in a business can use a blockchain to record the history of business transactions

37

Blockchain & IoT

- 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…

38

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

Deployment scenarios (2) – marketplace of IoT services

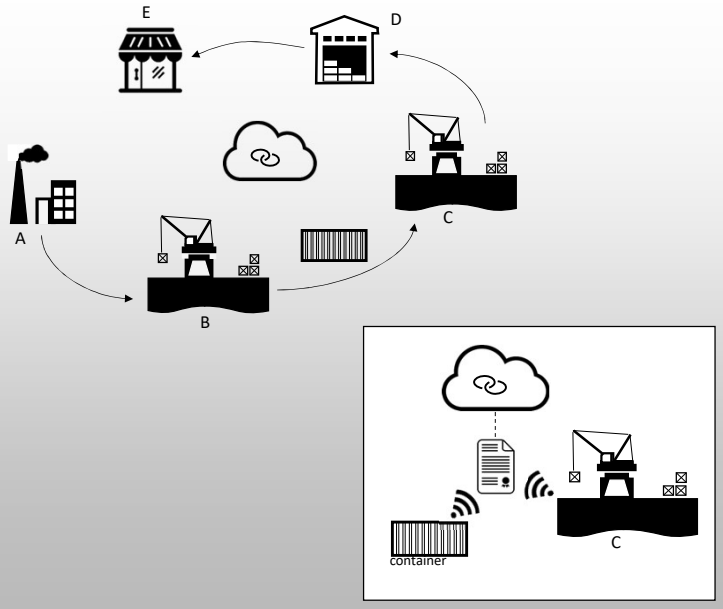
- blockchains with cryptocurrency to provide a *billing layer to* implement of a *marketplace of services between devices*:
  - devices that store a copy of binary codes or storage for sensed data may charge for serving it;
  - E.g. Filecoin which allows devices to ``rent their disk space'';
- every 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

40

Deployment scenarios (3) – monitoring supply chain

- 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

41



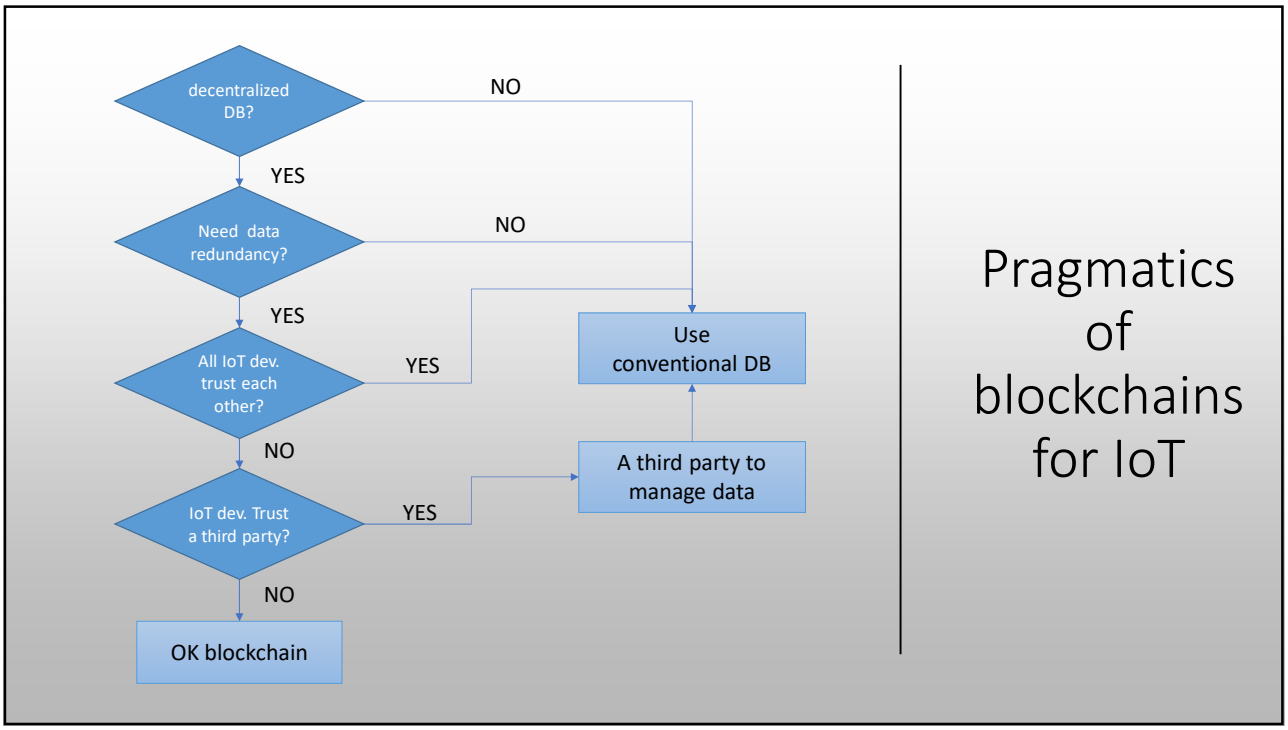
Deployment scenarios (4) – asset tracking

42

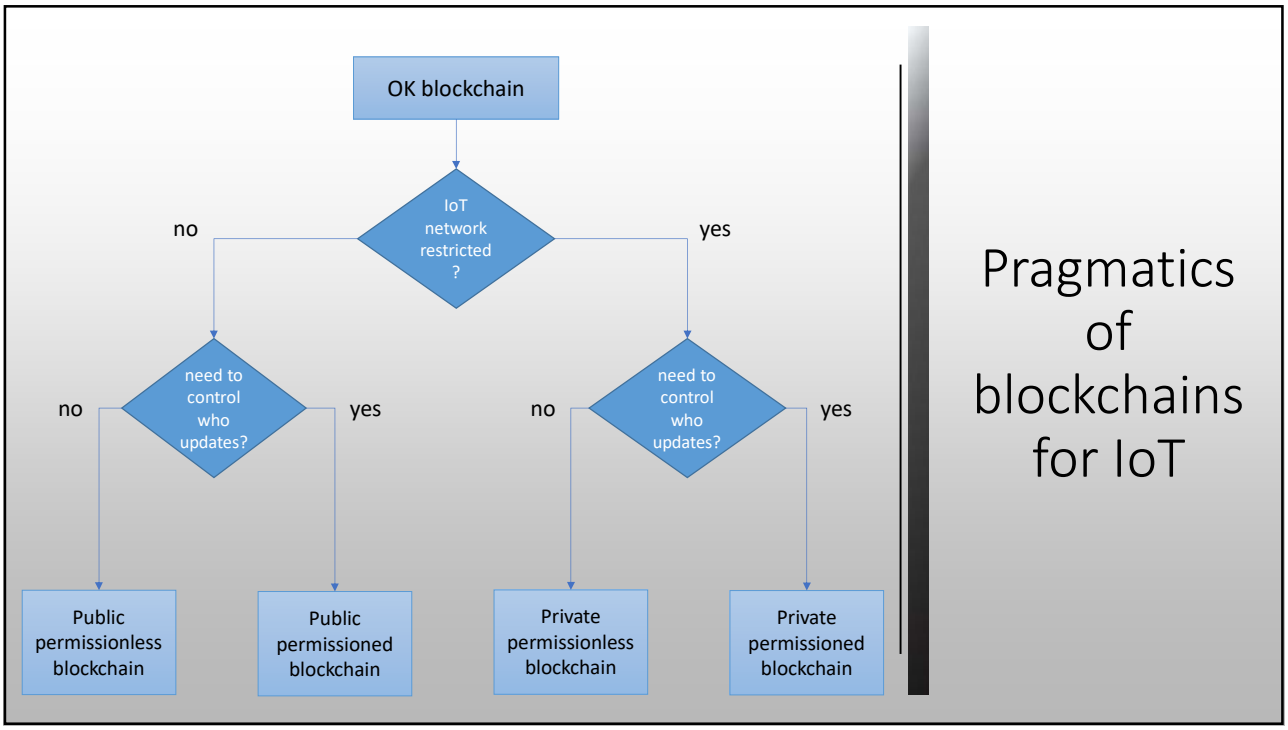
- In the energy sector
  - IoT devices can buy and sell energy automatically
  - IoT devices with surplus of energy (e.g. with solar panels) may share their energy with other devices
- In precision agriculture, with IoT sensors to monitor the state and good health of the crops
  - Agreed and visible 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
A third party to manage data
IoT dev. Trust a third party?
YES
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**"
- your solution will only work alone:
  - only your devices
  - any change/update requires your intervention
  - other vendors cannot interfere

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

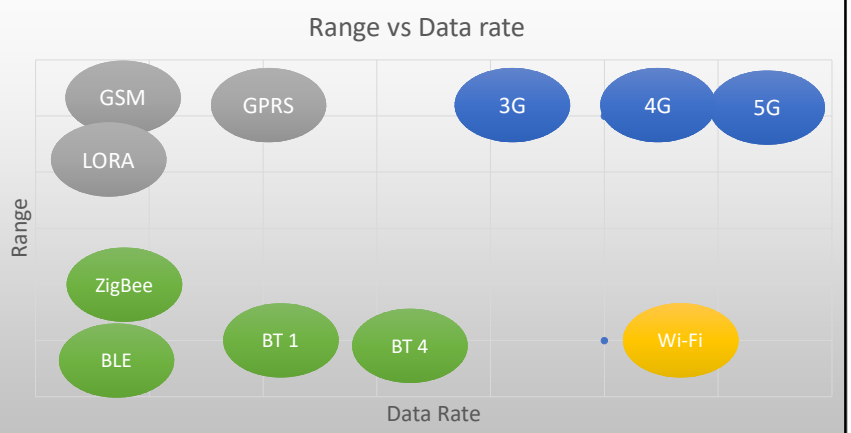
48

Interoperability

- 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

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
- 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

51

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

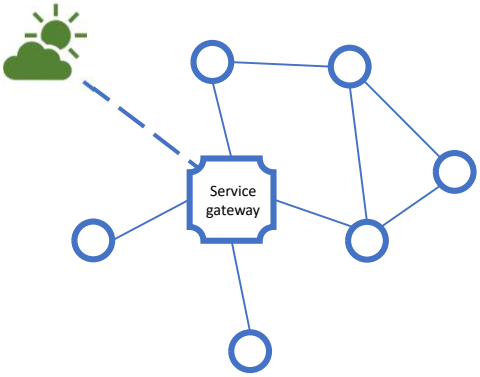
Standards in IoT

- … 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

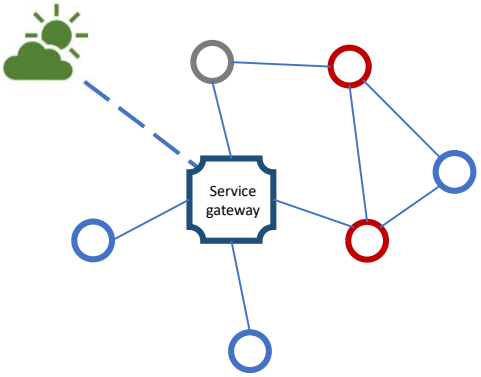
53

Different configurations…

Type A configuration:
- same vendor and same protocol



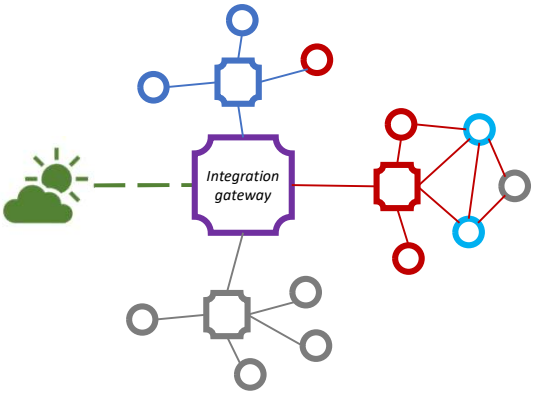
Type B configuration:
- different vendors but same protocol



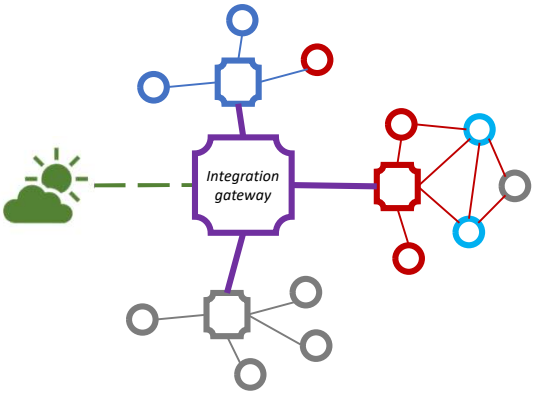
54

Different configurations…

Type C configuration:
- different vendors and different protocols



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

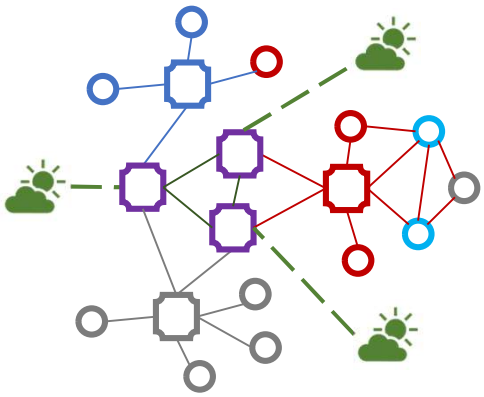


55

Different configurations…

Type D configuration:

- Different vendors, different protocols, distributed integration gateways

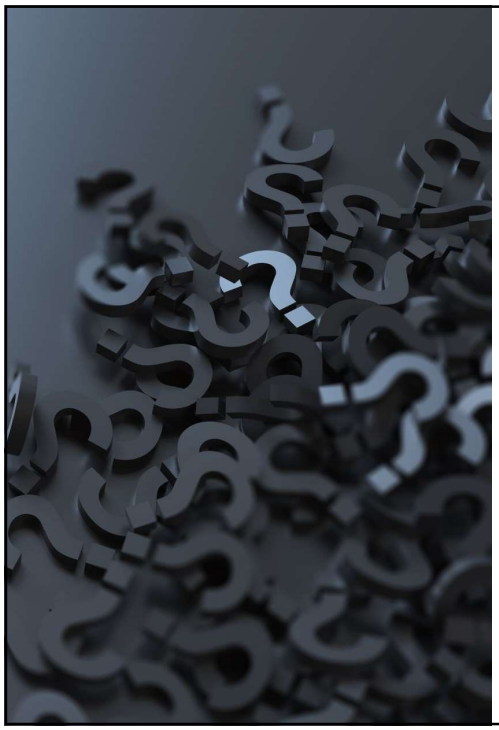


56

Review question

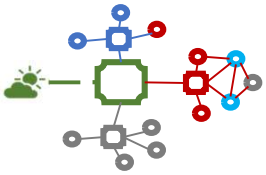
May blockchains in IoT have a relationship with interoperability?

57

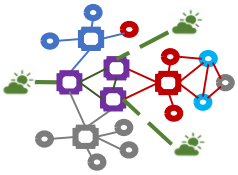


Question

- 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?



type C configuration



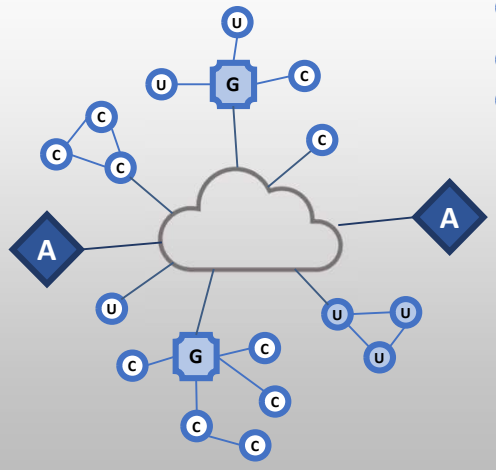
type D configuration

58

Security in IoT

59

IoT security: elements of interest



60

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

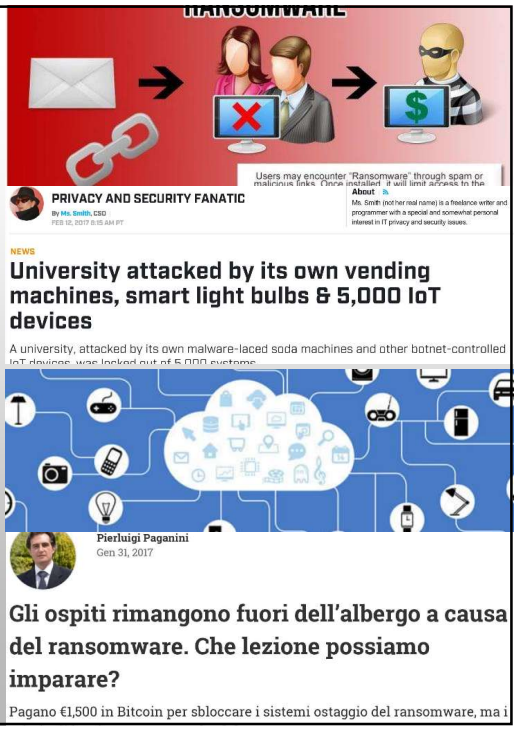
It is potentially a graver threat with actuators, where the attacker can affect the operation of machinery and other devices

61

Cybercrime with IoT

Kits for these attacks can be found on the Internet …

… for 15 €



62

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
  - Data management security
  - Service provision security
  - Integration of security policies and techniques
  - Mutual authentication and authorization
  - Security audit

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

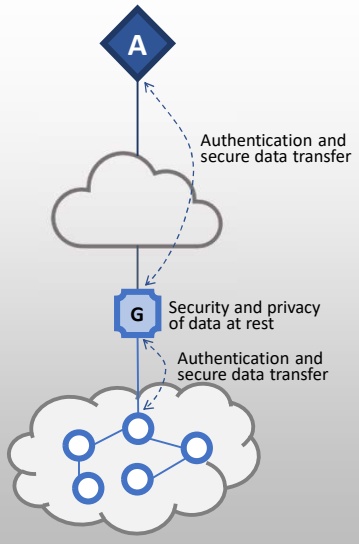
64

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

65

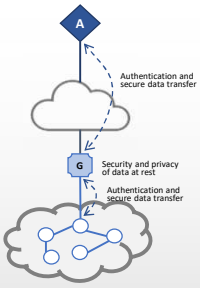
IoT gateway security functions



66

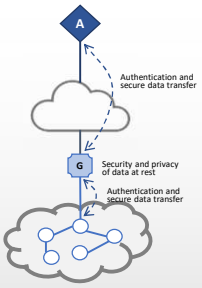
IoT gateway security functions

- 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.



67

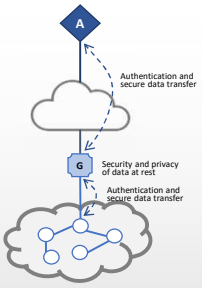
IoT gateway security functions



- 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.

68

IoT gateway security functions



- 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

69

Review question

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

70

Summary

IOT & IOT PERSPECTIVES

IOT AND MACHINE LEARNING, CLOUD AND BLOCKCHAINS

INTEROPERABILITY AND STANDARDS

SECURITY IN IOT

71