420-N23-LA Introduction to IoT

Introduction to IoT and Embedded Systems

Introduction to the Class

420-N23-LA
Introduction to IoT and Embedded Systems

Course Introduction and Outline

- Outline Download Location
  - Link to Léa download location.
- Technologies Used for this Course
  - Léa
    - Communication of the course outline, grades.
    - Used for scheduling of tests & assignments and deadlines.
    - Slides and Internet Links.
    - Lab material, and lab submission areas.
    - Assignments.

What is IoT?

Introduction to IoT

What is IoT?

- The ***Internet of Things (IoT)*** is a computing concept that describes a scenario where **everyday physical objects are connected to the internet** and can identify themselves to other devices or processes, via an IP address.

- The objects embedded with sensors, software, and network connectivity that enable them to collect and share data over the internet.

- Billions of physical devices around the world that are now connected to the internet, **collecting data**.

What is IoT

- Thanks to cheap processors and wireless networks, it's possible to turn anything, from a pill to an airplane, into part of the IoT.

- This connectivity adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate - merging the digital and physical worlds.

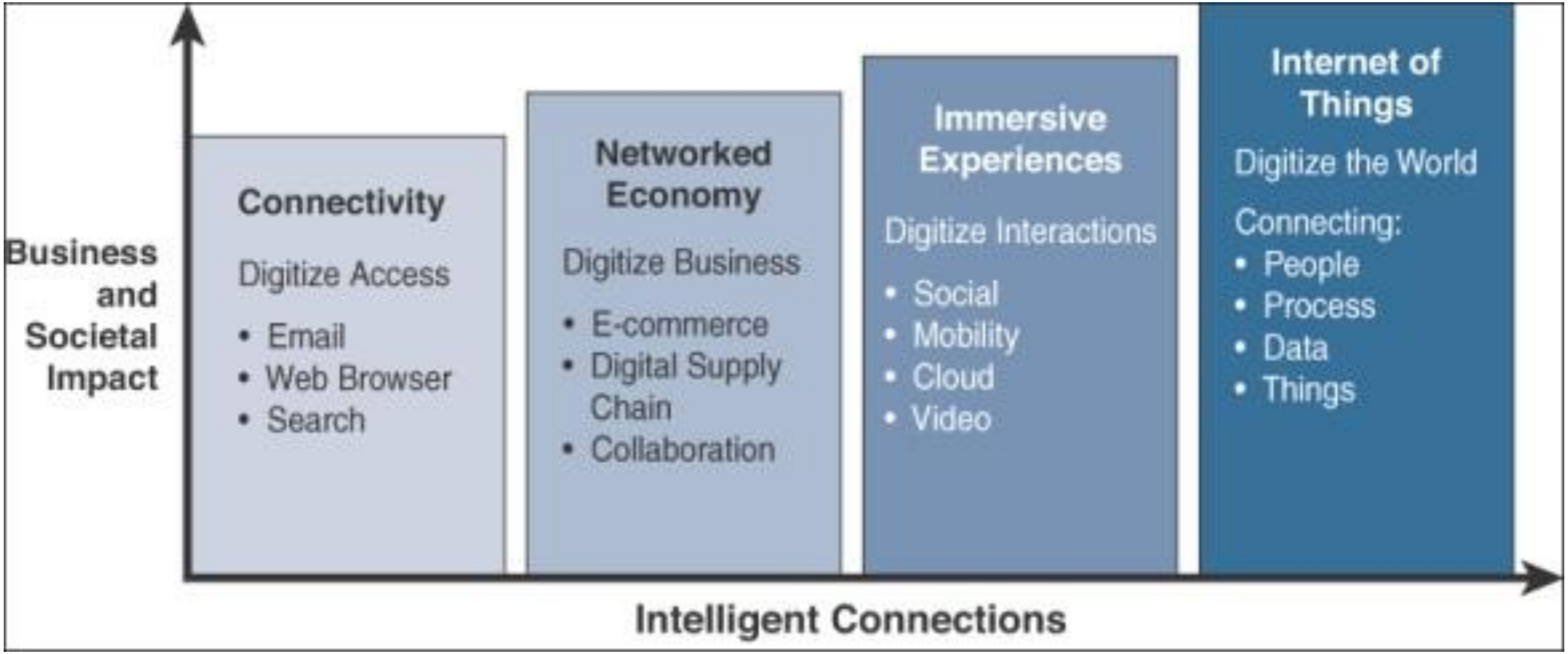
- IoT is considered M:M technology. **Machine to machine**.

What is IoT?

- The person credited with the creation of the term “Internet of Things” is Kevin Ashton.

- He was quoted as saying: “In the twentieth century, computers were brains without senses—they only knew what we told them.” Computers depended on humans to input data and knowledge through typing, bar codes, and so on. IoT is changing this paradigm; in the twenty-first century, computers are sensing things for themselves.

Evolutionary Phases of the Internet

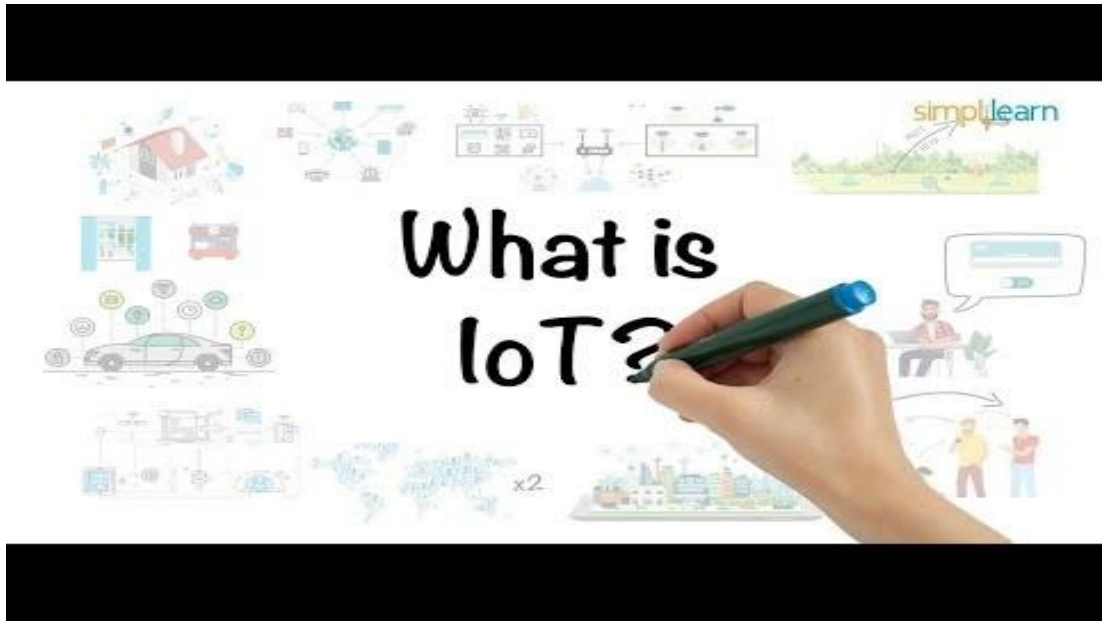


Internet Phase	Definition
Connectivity (Digitize access)	This phase connected people to email, web services, and search so that information is easily accessed.
Networked Economy (Digitize business)	This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business processes.
Immersive Experiences (Digitize interactions)	This phase extended the Internet experience to encompass widespread video and social media while always being connected through mobility. More and more applications are moved into the cloud.
Internet of Things (Digitize the world)	This phase is adding connectivity to objects and machines in the world around us to enable new services and experiences. It is connecting the unconnected.

Examples of IoT

- Pretty much any physical object can be transformed into an IoT device if it can be connected to the internet and controlled that way.
  - Lightbulbs (Hue system)
  - Thermostats (Nest system)
  - Jet airplane engines (thousands of sensors)
  - Smart cities

Examples of IoT



Benefits by Industry

- Consumers
  - Makes your home and your car smarter and more ergonomic.
  - Makes life easier (hey Google, hi Alexa).
  - Great help for disabled people, visually impaired people.
  - Personal example: My hallway light, and dining room light turn on when I approach my house (via my cell phone). Also, the Nest heating system turns up the heat by 2 degrees when I come back home.
- Businesses
  - Track location of orders, parts, packages.
  - Make sure temperature or conditions are OK.
  - Monitor performance (jet plane engines)
  - Manage problems proactively by analysing large scale data.

IoT Hardware Characteristics

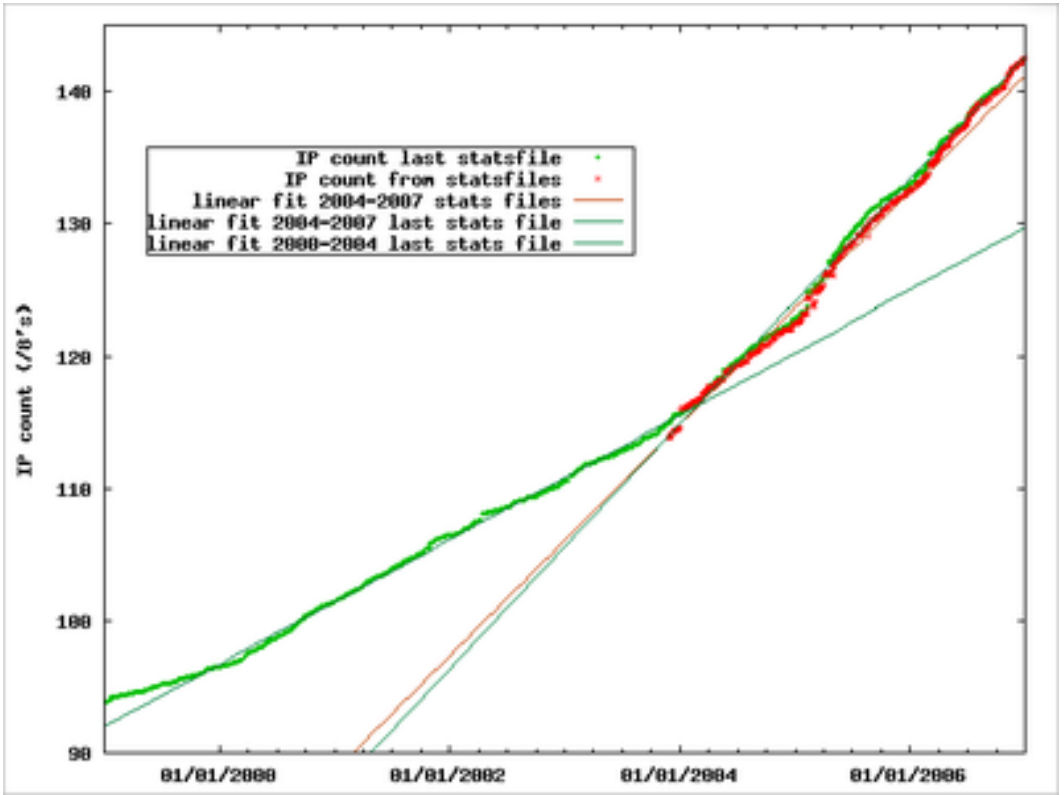
- CPU’s
  - Inexpensive.
  - Small.
  - No heat dissipation needed (usually).
- RFID Tags
  - Unique ID per tag.
  - Inexpensive.
- Wireless Capability
  - LTE / 4g / 5g
  - Low energy bluetooth

What's an IP (IPv4) Address?

- An IP address is a 32-bit number which defines all public facing Internet devices.
- Your home computer has a private IP address which connects to your router, which has a public IP address.
- An IP is in the form – 123.123.123.123, each number ranges from 0 to 255.
- It can be represented by bits (32): 10101010.10101010.10101010.10101010
- So, the total amount of numbers is approximately 2^{32}, so **4,294,967,296** combinations are possible.

IoT Software – NETWORKING (On the Public Internet)

- Networking
  - IPv6
    - An Internet protocol – 128 bits of address space.
    - Intended to eventually replace IPv4 – 32 bits address space.
      - https://en.wikipedia.org/wiki/IPv4_address_exhaustion
  - IPv4 does not contain enough IP addresses to handle all IoT devices.
    - Exercise: How many addresses are available in an IPv4 address?
      - Hint: *Calculate a power of 2.*
    - Exercise: How about IPv6?



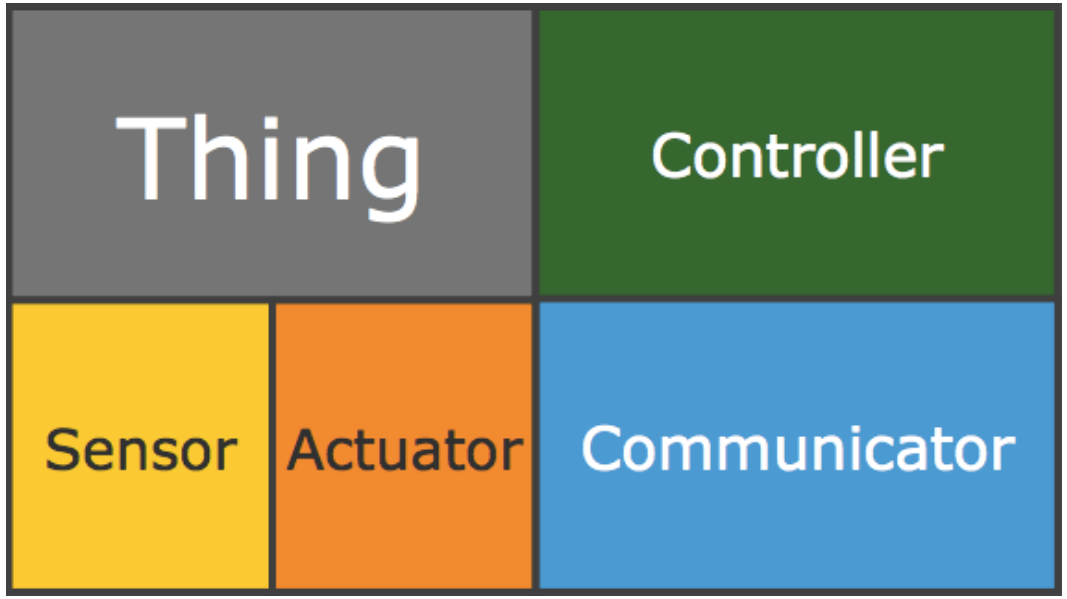
IoT Software

IoT Software – Data Related

- Unstructured databases
  - MongoDB https://www.youtube.com/watch?v=EE8ZTQxa0AM
  - NoSQL
  - Teradata
  - Oracle Big Data SQL
- Tools / Frameworks
  - Elastic Search
  - Hadoop
  - https://www.youtube.com/watch?v=9s-vSeWej1U
  - Apache Spark
- Platforms
  - Microsoft Azure
  - Cloudera
  - Oracle
  - SAP Hana
  - Amazon Web Services
  - IBM NIST

IoT General Device Composition

1. Physical object (“thing”)
2. Controller (“brain”)
3. Sensors
4. Actuators
5. Networks (Internet)



Risks, Privacy and Security

Privacy

- Secure private data collected
  - When I come home and leave. (People can know when you are away).
  - Voice is recorded and stored when I ask my Google home to do things.
- Very few devices encrypt data properly when in transit.
- All the data being collected, does not disappear.
- Data is sold legally on markets between businesses to know how to market to people.
- All data, if aggregated properly, can paint an accurate picture of who you are, what you like, what you eat, and more.
- You need to be careful about WHO OWNS the data. Them or you? In Canada you are supposed to control your own data.

IoT Hacking and Data Breaches

- Hacking
  - Many devices are very easy to reach and hack into.
  - IP cams for example, if accessed, can be used to record all video and audio from a home or office.

Some Major IoT Security Issues

- Lack of Compliance on the part of IoT Manufacturers
- Lack of User Knowledge & Awareness
- IoT Security Problems in Device Update Management
- Lack of Physical Hardening
- Botnet Attacks
- Industrial Espionage & Eavesdropping
- Crypto mining with IoT Bots

Unsecured Devices

- Perhaps the greatest challenge facing IoT devices and edge computing frameworks is that they greatly expand the surface area of a network, creating more potential attack vectors in the process.

- Many security experts have warned that even a single unsecured device connected to a network could serve as a point of entry for an active hacking attempt or an indirect attack using malware of some form.

Unsecured Devices

- Another IoT security concern for unsecured devices involves their ability to move from one network to another. Take, for instance, a smartphone or laptop that connects to a public WiFi network in a cafe and then later connects to the IT systems at the workplace.

- Exposure to other networks provides multiple opportunities for devices to be compromised in some way.

Too Much Trust

- Implementing a “zero trust” philosophy when it comes to IoT networks is an essential step to securing IT systems and internet infrastructure.
- Traditional networking architecture takes for granted that any device or user who gains access to a network is authorized to be there.
- This makes it possible for unauthorized users to move laterally through a system once they breach the outer firewalls.
- This is particularly dangerous where IoT devices are involved, because many of them are unsecured and easier to use as a gateway into IT systems.

Too Much Trust

- A zero-trust security philosophy implements much stronger authentication controls by starting with the assumption that anything in the network could potentially be compromised and then requiring stricter verification for any access request.

- This prevents lateral movement because even if an IoT device is compromised, the attacker will have a harder time moving to different parts of the network.

Poor Network Visibility

- The proliferation of IoT devices is taking place so quickly that many organizations aren't even able to keep up with all of the devices coming and going in their network.
- While traditional IT security systems focus on documenting every device and connection, the mobility and sheer number of IoT devices make it difficult to map out those relationships clearly.
- It's difficult to guard against IoT security issues, for instance, when that policy has to not only account for every device and sensor in the factory, but also every personal device and every device involved in the broader logistical network that may stretch around the world.

Software Vulnerabilities

- Any network involving IoT devices includes a variety of overlapping software systems and applications. Every one of those systems has its own features and vulnerabilities that could potentially be exploited. They could also create errors when they come into contact with each other, resulting in system downtime or compromising data.

- Keeping software up to date with patches and updates can be difficult, especially when every new device that joins the network could introduce a new set of vulnerabilities.

Software Vulnerabilities

- Many IoT devices use open source software that can be easily manipulated by hackers seeking to gain access to IT systems, so it’s important for those systems to account for as many known software threats as possible.

Knowledge Gap

- While all the technical vulnerabilities of IoT devices are important to note, it should also be remembered that all of them can be made worse when users are unaware of them. Since one of the great appeals of IoT devices is their convenience, people often don't stop to think about how something as simple as connecting their tablet to the office Wi-Fi could pose a security risk. Even if an organization doesn't make extensive use of IoT devices, its employees likely will be using them in their own homes. Making sure they understand why doing things like connecting a work computer to their home stereo over Bluetooth could potentially compromise data is a vital step in building a strong security policy that guards against data breaches.

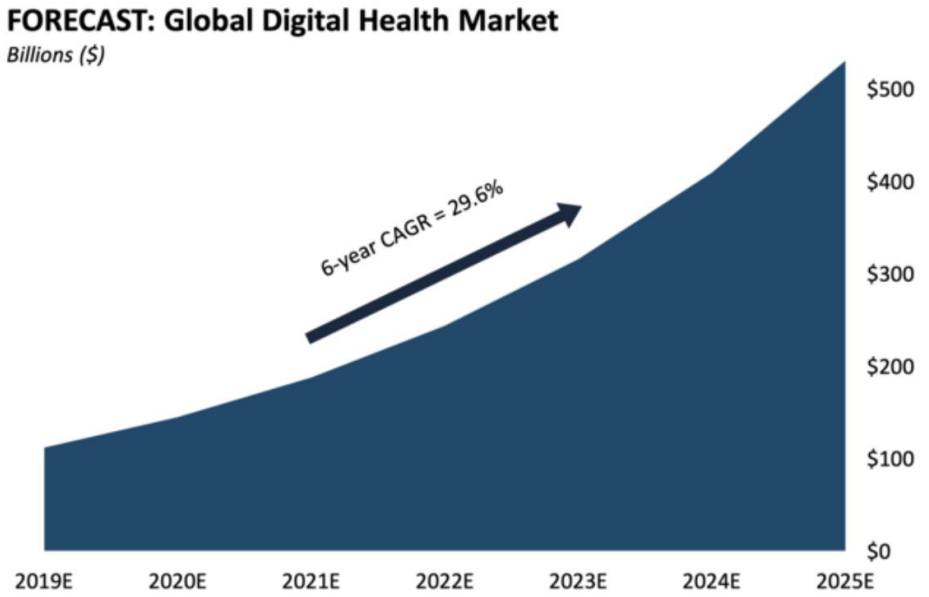
Other Areas IoT Extends into

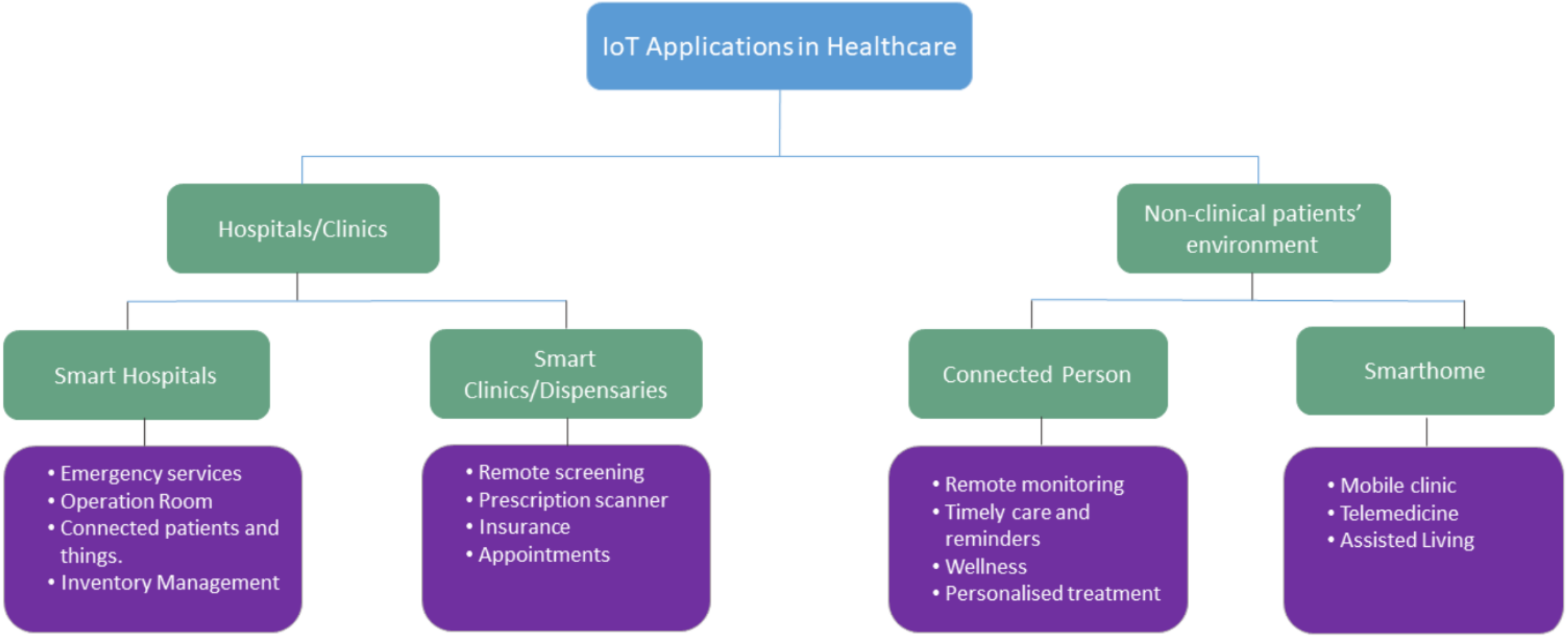
- Smart Cities
- Artificial Intelligence
- Marketing
- Medical
- Industrial
- Military

Medical IOT

The IoT is slowly starting to weave into healthcare on both the doctor and patient fronts. Ultrasounds, thermometers, glucose monitors, electrocardiograms, and more are all starting to become connected and letting patients track their health. This is crucial for those situations that require follow-up appointments with doctors.

- https://econsultancy.com/internet-of-things-healthcare/





https://smartsupplychains.ai/2020/03/04/iot-in-healthcare-an-introduction/

Industrial IOT (IIoT)

- The term IIoT refers to the Industrial Internet of Things. In broad strokes, it's the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transport, energy and industrial sectors.
  - IoT includes consumer-level devices such as fitness bands or smart appliances and other applications that don't typically create emergency situations if something goes wrong.
- There is more at stake with IIoT deployments where **system failures and downtime can result in life-threatening or high-risk situations**.
- Instrumentation for production lines can let companies track and **analyze their processes on an enormously granular level**, asset tracking can give a quick, accessible overview of a huge amounts of material, and predictive maintenance can save companies big money by addressing problems before they have a chance to become serious

IIoT Areas

- Smart factory warehousing applications
- Predictive and remote maintenance.
- Freight, goods and transportation monitoring.
- Connected logistics.
- Smart metering and smart grid.
- Smart city applications.
- Industrial security systems
- Energy consumption optimization
- Industrial heating, ventilation and air conditioning
- Manufacturing equipment monitoring.
- Asset tracking and smart logistics.
- Ozone, gas and temperature monitoring in industrial environments.
- Safety and health (conditions) monitoring of workers.
- Asset performance management
- Smart farming and livestock monitoring.

Challenges of Industrial IoT

- Lifespan
  - Should last long (build to last)
- Backends and systems are complex
  - Data transmission and storage
  - Endpoints, and data analysis
- Interoperability between environments
  - Different objects in the IIoT collection need to all be able to communicate in standard ways
- Costs
- Lack of standardization
- Security
  - Recall: Mirai Botnet
  - Lack of standardization
- People
  - There is a lack of skilled labour in the engineering sector related to IoT, machine learning, etc.

Features of an Embedded System

- Sometimes, must be **durable**
  - Additional problems can be caused for embedded computing by a need for protection from vibration, shock, lightning, power supply fluctuations, water, corrosion, fire, and general physical abuse. For example, in the Mission Critical example application the computer must function for a guaranteed, but brief, period of time even under non-survivable fire conditions.
- Must be **cheap** and easy to manufacture
  - Therefore they are sometimes considered disposable, and less effort is spent making them “perfect”.