# PLACEHOLDER COVER

Your Name Here

## Your Title Here

Bonn 1770

· U C ·

UNIVERSIDADE DE COIMBRA

FCTUC FACULDADE DE CIÊNCIAS
E TECNOLOGIA
UNIVERSIDADE DE COIMBRA

# Wireless IoT Architecture for Smart Nodes deployed in Hospital Beds

**José Nuno da Cruz Faria**

Coimbra, ? 2021


# Wireless IoT Architecture for Smart Nodes deployed in Hospital Beds

**Supervisor:**

Prof. Doutor David B. S. Portugal

**Co-Supervisor:**

Prof. Doutor Mahmoud Tavakoli

**Jury:**

Prof. Jury1

Prof. Jury2

Prof. Jury3

Dissertation submitted in partial fulfillment for the degree of Master of Science in Engineering Physics.

Coimbra, ? 2021

# Acknowledgments

# Resumo

# Abstract

*"Inspirational quotes are cool."*

— A renowned author, *A Great Book*

# Contents

**Acknowledgements** ii

**Resumo** iii

**Abstract** iv

**List of Acronyms** x

**List of Figures** xi

**List of Tables** xii

**1 Introduction** 1

1.1 Context . . . 1

1.2 Objectives . . . 1

1.3 Thesis Structure . . . 1

**2 State of the Art** 2

2.1 Internet of Things . . . 2

2.1.1 What is IoT? . . . 2

2.2 A Reference Model for Pervasive Healthcare Applications . . . 3

2.2.1 Layer 1: Physical Devices and Controllers . . . 4

2.2.2 Layer 2: Connectivity . . . 6

2.2.3 Layer 3: Edge (Fog) Computing . . . 11

2.2.4 Layer 4: Data Accumulation . . . 12

2.2.5 Layer 5: Data Abstraction . . . 14

2.2.6 Layer 6: Application . . . 15

2.2.7 Layer 7: Collaboration and Processes . . . 16

2.3 Similar approaches . . . 16

2.3.1 Comparative Analysis . . . . . 17
2.3.2 Weaknesses of literature . . . . . 19
2.4 Statement of Contributions . . . . . 19

**Bibliography** **21**

**A My cool appendix!** **24**

# List of Acronyms

| | |
|---|---|
| **IoT** | Internet of Things |
| **IT** | Information Technology |
| **WoW** | Wireless biOmonitoring stickers and smart bed architecture: toWards Untethered Patients |
| **ECG** | Electrocardiogram |
| **PPG** | Photoplethysmogram |
| **IMU** | Inertial Measurement Unit |
| **BLE** | Bluetooth Low Energy |
| **MQTT** | Message Queuing Telemetry Transport |
| **CoAP** | Constrained Application Protocol |
| **RFID** | Radio-frequency Identification |
| **IP** | Internet Protocol |
| **FHIR** | Fast Healthcare Interoperability Resources |
| **EHR** | Eletronic Health Record |
| **HIS** | Health Information Service |
| **API** | Application Programming Interface |

# List of Figures

2.1 IoT reference model published by IoTWF. . . . . 4
2.2 Throughput versus Transmission range for four communications protocols with similar ranges. Source: [1] . . . . . 8
2.3 Differences between the cloud offerings and on-premise solutions. . . . . 13

# List of Tables

2.1 List of sensors commonly used in pervasive healthcare applications. . . . . 5
2.2 Comparison between the more common communication protocols used within short range . . . . . 9
2.3 Comparison between CoAP and MQTT protocols. . . . . 10
2.4 Comparison between SQL and NoSQL technologies. . . . . 14
2.5 Comparison between different pervasive healthcare applications. . . . . 18

# 1 Introduction

## 1.1 Context

To-do: Steady increase of population lifespan introduces many challenges to healthcare systems (more elderly people, chronic diseases become more common, thus greater pressure on these systems, bigger healthcare costs, ...);
What has digital health done to help this? concepts: IoT, digital health...

## 1.2 Objectives

To-do: Discuss if this section should move to AFTER literature review

## 1.3 Thesis Structure

This document is organized into different sections. The first chapter provides an introduction to the theme of the dissertation, discussing the context and motivation behind the work developed. In the second chapter a brief overview into IoT infrastructures and its healthcare applications is shown.

# 2 State of the Art

In this chapter a survey of pervasive healthcare applications is presented. In order to gain a greater understanding of which are the building blocks of a typical Internet of Things (IoT) system, a reference model is also presented.

## 2.1 Internet of Things

### 2.1.1 What is IoT?

Internet of Things (or IoT) is an emerging communication paradigm, often hailed as the driver of the Fourth Industrial Revolution [2].

The definition of this concept has evolved over time with the development of other technologies such as data analytics, embedded systems, etc. Fundamentally, it describes a strategy supported on the development of networks of smart devices that exchange and process information through Machine-to-Machine (M2M) communications, usually based on the Internet Protocol (IP) [3]. This technology enables ubiquitous systems to gather remarkable amounts of information regarding the surrounding environment, which can later be turned into insight through the usage of data analytics tools, like Machine Learning.

More specifically in the healthcare domain, this technology can provide many benefits as it enables remote and continuous health monitoring [4, 5, 6]. It allows non-critical patients to be monitored from the comfort of their own houses rather than in hospitals or clinics, reducing the strain on scarce hospital resources such as doctors or beds. This is particularly beneficial to those who live in rural areas, with limited access to healthcare services. It allows elderly people and those with chronic diseases to have greater control over their own health, allowing them to live more independently. Moreover, with the automatization of medical procedures, these systems can make healthcare infrastructures more efficient and thus lower the costs of healthcare [7, 8]. Particularly, in the realm of clinical research, by analyzing

the data collected by these ubiquitous systems, it may be possible to find new relationships between certain pathologies and different physiological signals, such as variations in body temperature or heart rate [9]. These correlations, commonly referred to as biomarkers, can be used by these systems to assist clinical decisions, enabling novel predictive, prognostic, and diagnostic processes in healthcare.

To-do: Review paragraph — does it emphasizes too much remote health monitoring? should be more focus on demonstrating value for hospitals or is it fine as it is?

## 2.2 A Reference Model for Pervasive Healthcare Applications

To-do: Review this paragraph and section later.

A reference model provides an abstract framework for designing systems, a set of commonly recommended practices for the application domain. It serves as a starting point in the design process, enabling the comprehension of complex systems by breaking them down into simple and distinct functional layers, while also defining some common terminology used in its domain.

In 2014 the IoT World Forum (IoTWF) architectural committee published an IoT architectural reference model, composed by seven layers as shown in figure 2.1. This model provides a simple and clean functional view into the different components of an IoT system, without restricting the scope or locality of its components. However, from a hardware perspective, in this work we will restrict our focus to the most common approach taken by researchers, using 3 distinct components:

- **Endpoint** or **edge** nodes (corresponding to Layer 1), which interact with the physical world, capturing data.
- **Gateway** devices (Layer 3), which connect to one or multiple **edge** nodes, filtering and aggregating the data generated by these and communicating it to the central server;
- **Central** server (Layers 4-6), which is responsible for collecting, storing and analyzing the captured data in order to provide users with valuable insight;

While this model can be used to develop IoT systems for any industry (from agriculture

to smart cities), in the context of the dissertation we will focus on pervasive healthcare applications.

To-do: Make new image based on this one.

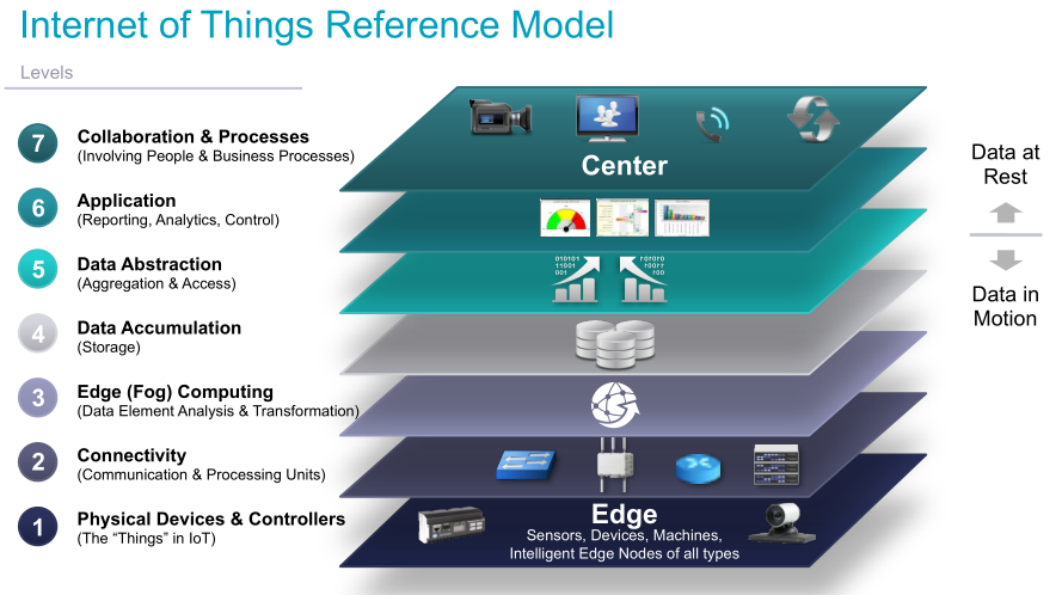


Figure 2.1: IoT reference model published by IoTWF. Source: [10].

### 2.2.1 Layer 1: Physical Devices and Controllers

To-do: Review this section later. Reminder to check if there are any statements that need citations.

The first layer of the model is the physical devices and controller layer. This layer houses the "things" in the Internet of Things: the endpoint devices composed of sensors and actuators that perceive and interact with the physical world. Through those interactions, the devices generate data, which is then sent across the network for analysis and storage.

Wearable, wireless, and non-intrusive devices are viewed as one of the key components of IoT-based healthcare systems [3]. In recent years there has been remarkable progress on the development of wearable devices, driven by recent technological breakthroughs in the miniaturization of sensors and microfabrication processes [8, 7]. These devices allow patients to be monitored while retaining their mobility, thus increasing the comfort of these users. The drawback of this approach lies on the restrictions imposed on the devices.

Due to the nature of the technology, these units will require a portable energy source, a battery, which will implies reduced memory, computation, and connectivity capabilities

in order to minimize energy consumption and maximize their lifetime. Shorter lifetimes translate into higher maintenance costs, as these devices will need to be replaced more often.

Another point to consider is the data requirements of the system, what and how much data is generated and transmitted by the devices. Some applications can include a single temperature sensor or heart rate sensor, while more complex systems can include pulse oximetry, electrocardiogram (ECG), respiration rate sensors, etc [5]. From the literature, we can also classify the sensors used in these devices in 3 distinct categories based on information that can be extracted from them, as shown in table 2.1:

- Monitoring the patient's physiological signals, used for evaluating the patient's health condition.
- Monitoring the patient's activity or motion, used for detecting fall events, determining the patient's location and travelled distance, estimating the patient's body posture, etc.
- Monitoring the patient's environment conditions, mainly used for assessing environmental hazards, *e.g.* gas leaks in a patient's home or an industrial workplace.

Note: Is it technically correct to designate these as "sensors" or should they be designated physiological / environmental signals instead?

| **Type of monitoring** | **Type of sensors used** |
|---|---|
| Vital Signs Monitoring | Blood Pressure, ECG, PPG, Body Temperature, Respiratory Rate, Galvanic Skin Response, Pulse Oximetry, Glucose Level Sensors |
| Activity Monitoring | Accelerometer, Gyroscope, Magnetometer |
| Environmental Monitoring | Air Temperature, Barometer, Humidity, Gas Sensors |

Table 2.1: List of sensors commonly used in pervasive healthcare applications. Adapted from [11].

### 2.2.2 Layer 2: Connectivity

The second layer of the model focuses on connectivity, on linking the different components of our system, ensuring reliable and timely data transmissions. This includes all communications within the system, which can be divided into two categories: communications within the local network (*e.g.* between edge nodes and the gateway devices), and communications between the edge of the local network (*e.g.* gateway devices) and the central server.

#### Communication Protocols

Technologies are designed with particular use cases in mind. They catalyze their development and thus it is natural that each one has its own advantages and disadvantages, according to its use. For instance, short range wireless protocols are limited by transmission range, but long range protocols have a higher energy consumption, which may be unviable for networks with very constrained devices. Each protocol defines their own frame formats and communicates within certain frequency bands, some of which may require licenses. Using licensed frequency bands can provide a better performance as it ensures greater reliability since the network operator grants you exclusivity of frequency spectrum within a certain area.

From the literature, we can identify a set of key requirements that drive the decision of the communication protocols [3, 7, 8]:

- **Energy consumption**: For networks composed of energy constrained devices, the communication protocol should be lightweight and energy efficient in order to maximize the devices' lifetime.
- **Latency**: Certain applications deal with time critical events, for example the detection of health emergencies [7]. In these cases, any delays in the communications can cause great detriment to the patient's well-being, making it crucial to minimize them.
- **Reliability**: Depending on the critical nature of the data that is being communicated, the network stack may need to implement processes such as error-detection, retransmission or handshakes in the communications to ensure more robust transmissions (*e.g.* as implemented in TCP/IP based protocols. Generally, these features come at the cost of greater latency. Therefore, when choosing the communication protocol a balance must be found between reliability and latency.

- **Security**: Security is one of the most important requirements of any system, but this is especially true for healthcare applications. Due to the sensitive nature of the information, it is crucial to secure it from malicious actors. Communication protocols must implement security mechanisms, such as encryption or data integrity verifications, that ensure the transmissions are not compromised in transit, thus denying third parties the ability to snoop or tamper the transmissions. This issue is studied in depth in [12].

- **Interoperability**: To ensure the interoperability of the system it is imperative to choose protocols that are widely accepted and supported in the application domain. This also contributes to the longevity of the system, as these will most likely remain supported for longer time periods.

- **Range**: The communication protocol must ensure the devices can communicate within the designated transmission range.

- **Scalability**: These systems contain an enormous amount of devices, and each one must be uniquely identified. The communication protocol must ensure that every device in the network is addressable.

- **Throughput**: The communication protocol should ensure there is enough bandwidth to handle all communications within the designated transmission range. Even within similar technologies, this can vary wildly with the range as seen in figure 2.2.

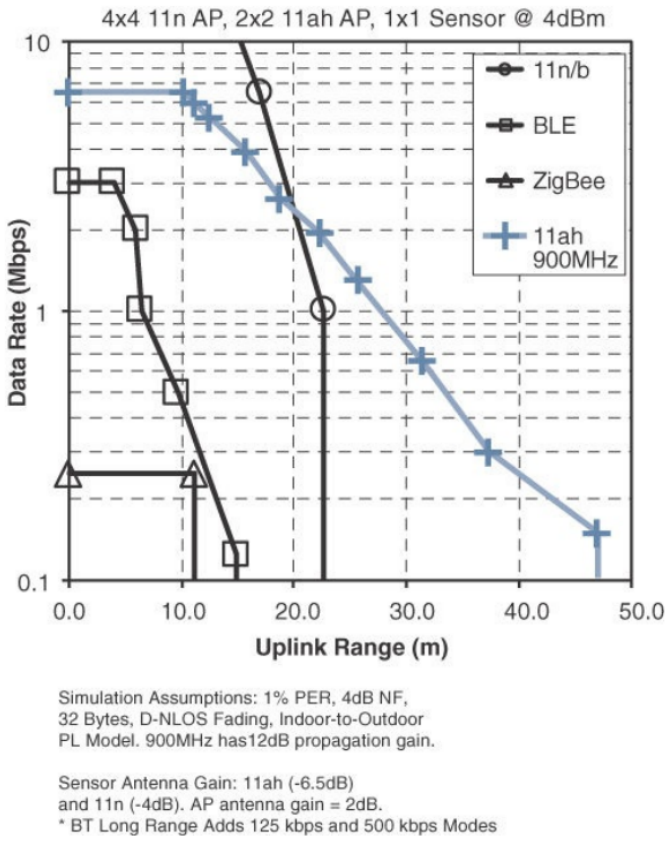


Figure 2.2: Throughput versus Transmission range for four communications protocols with similar ranges. Source: [1]

Regarding the communications within the local network, these generally have short transmission ranges [3]. Wearable devices can be often arranged in networks, aptly designated "Wireless Body Area Network". The most widely adopted protocol is Bluetooth Low Energy (BLE), a low-energy version of the classic Bluetooth protocol [4, 13, 5]. ZigBee and Radio-frequency Identification (RFID) are also used in many systems in this domain, particularly in more asset tracking oriented applications [14, 7, 8]. Although there isn't a universal specification for RFID, the most widely used standard is the EPCglobal Gen2 RFID [15], which will be the standard discussed in this work. For the sake of simplicity, we will only consider this standard, and EPC/RFID will be used to designate it.

Out of these three technologies, BLE offers greater throughput, better security, and nearly the lowest energy consumption [16]. Table 2.2 shows a comparison between the different protocols.

| | Bluetooth Low Energy | EPC/RFID | ZigBee |
|---|---|---|---|
| **Band of operation** | 2.4 GHz | LF, HF, UHF, EHF | 2.4 GHz |
| **Communication** | Bidirectional | Unidirectional (Bidirectional for Active tags) | Bidirectional |
| **Topology** | Point-to-Point, Piconet, Broadcast, Mesh | Point-to-Point | Mesh |
| **Range** | <100m | <10m, (100m for Active tags) | 20m |
| **Data rate** | 1Mb/s (up to 2Mb/s) | 40kb/s | 250kb/s |
| **IP Stack** | ✗ | ✗ | ✓ |
| **Security Features** | AES-128, Secure pairing prior to key exchange | ✗ | AES-128 (Optional), Network key shared across network, Optional link key to secure application layer communications |

Table 2.2: Comparison between the more common communication protocols used within short range. Adapted from [3].

Regarding the communications between the gateway devices and the central server, most researchers try to make use of existing infrastructure in order to facilitate the deployment of new systems. This means, that the communications between the gateway devices and the central server are often done through generic IP-based protocols such as Wi-Fi and Ethernet [8, 14, 5, 7].

To-do: Should a short comparison between long range protocols be discussed (e.g. NB-IoT)?

### Application Protocols

To-do: Review this section later.

So far we've discussed the underlying networking technologies that link the devices in our system. But according to the OSI Model, we can note that many of these technologies don't define the application layer: how the devices communicate with each other, how the data is formatted, if there's hierarchy within the network, etc. When considering networks composed of constrained devices, generic web-based protocols such as Hypertext Transfer Protocol (HTTP) may not be adequate for IoT applications, which prompts the development of novel lightweight messaging protocols suited for these systems. The most used application layer protocols in IoT systems are Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP). Table 2.3 shows a short comparison between these two.

| | **MQTT** | **CoAP** |
|---|---|---|
| **Transport protocol** | TCP/IP | UDP/IP |
| **Messaging pattern** | Publish-Subscribe | Request-Response |
| **Communication model** | Many-to-many | One-to-one |
| **Security** | SSL/TLS (Optional) | DTLS |
| **Strengths** | TCP and Quality of Service (QoS) options provide robust communications, easier to implement | Better for lossy networks, lower latency |
| **Weaknesses** | Higher overhead and energy consumption than CoAP | Not as reliable and is less supported than MQTT |

Table 2.3: Comparison between CoAP and MQTT protocols. Adapted from [1].

In [17] the authors compare these two protocols in greater length, along with the more commonly used web-based protocol Hypertext Transfer Protocol (HTTP). They analyze the latency in the communications (from the edge devices to remote servers) and the RAM usage in the devices for each protocol and for different data sources (respiration rate, oxygen saturation and heart rate signals) and found that CoAP presented the best overall performance. Nonetheless, all protocols had very low latencies (less than 1.5s) and low memory usage. The authors indicate that MQTT might be more suitable if considering a certain messaging pattern, designated "Publish/Subscribe" model.

In this model, the devices that want to send messages, also called "publishers", communicate them to intermediary message broker, along with a "message topic" (also called logical channels). The devices that wish to receive messages, also called "subscribers", can subscribe to these topics by requesting it the message broker. Whenever a publisher sends a message to the message broker, the broker broadcasts it to all devices that have subscribed to the selected topic. CoAP uses a different messaging pattern, called "Request-Response". In this paradigm, a device sends a request to receive certain data and the second responds to this request. We can observe that former model is event-driven while the latter is query-based.

### 2.2.3 Layer 3: Edge (Fog) Computing

IoT systems can often have hundreds or even thousands of sensors generating data multiple times per second, 24 hours per day, which can demand an unsustainable amount of network and computing resources. Moreover, certain applications may be time critical, where delays in communication can be very detrimental. To minimize these effects, it is crucial to initiate data processing as close to the edge of the network as possible. This paradigm is usually referred to as "edge computing" (when the data processing occurs at the endpoint devices) or "fog computing" (when it happens at the edge of local network, *e.g.* in "gateway" devices). The third layer of the model defines how the system prepares the data for storage and higher level processing for the next layers. However, the devices at this stage often have limited computing capabilities, so the data processing is generally very limited, mostly focused on "preprocessing" the data in real-time and handling more time critical events. More demanding and thorough analysis is left to the central server.

The different processes applied at this stage can be summarized into four distinct categories:

- **Filtering**: Assessing if the data should be processed at a higher level.
- **Formatting**: Reformatting data to ensure consistent formats for higher-level processing.
- **Cleaning**: Reducing data to minimize the impact of data on the network and higher level processing systems.
- **Evaluation**: Determining whether data represents a threshold or alert. This is especially relevant for applications that deal with time critical events as seen in the previous section.

### 2.2.4 Layer 4: Data Accumulation

To-do: Review this section later.

Also, maybe mention that in the context of the project, we'll be using a local server so distributed solutions like hadoop based systems are out of scope for this work?

The data that is generated by the edge devices is propagated through the system, moving through with each sensor reading. Up to this point, we can state that the system's architecture is event driven. However, most applications cannot make use of the data at the rate it is generated [1]. In this layer, Data Accumulation, we need to define how the system captures the data and stores it, so it becomes usable for applications when needed, thus transiting from event to query-based processing.

As the devices continuously generate data, the system will require more and more resources in order to process and store all of this information, raising some concerns regarding how the data can be managed. In [4] the authors propose the usage of cloud platforms as a solution to these problems. This is made possible due to the elasticity in allocating, swiftly and inexpensively, computing and storage resources on-demand, adjusting itself to the needs of each application. We can find 3 distinct types of cloud services:

- **Infrastructure as Service (IaaS)**: Provides control over the remote machine (composed of virtual or dedicated hardware), operative system and middleware. This approach gives system designers the highest level of flexibility over the infrastructure, but requires more maintenance.
- **Platform as a Service (PaaS)**: Provides a simple framework for developing applications, where the service provider manages the underlying infrastructure issues such as software updates and hardware maintenance.
- **Software as a Service (SaaS)**: Provides the finished applications to be used by the end users, in this case health workers, that enable them to work. A simple example is a web-based email service, such as Gmail or Microsoft Outlook.

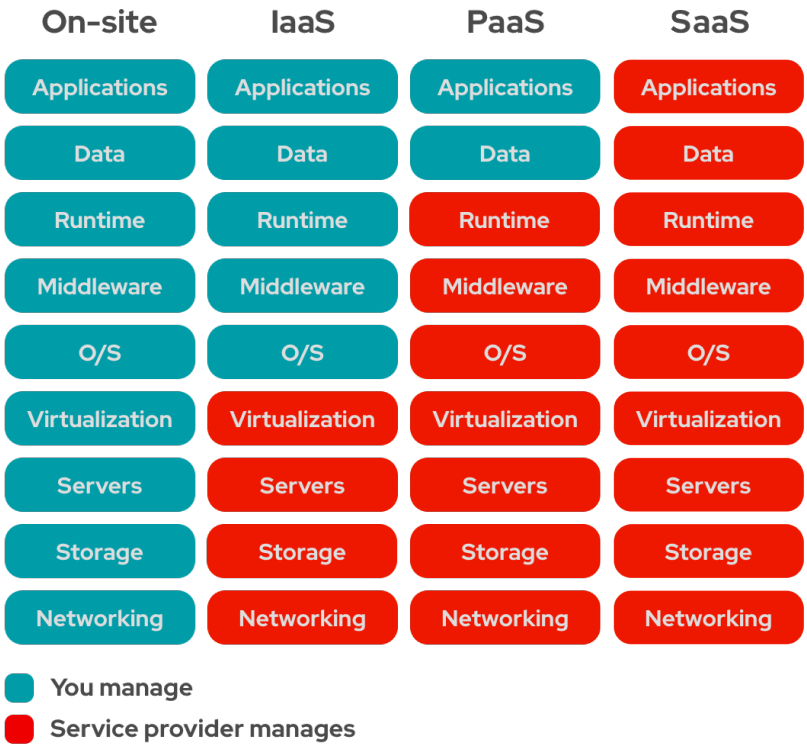


Figure 2.3: Differences between the cloud offerings and on-premise solutions. Source: [18]

To-do: Should homomorphic encryption methods be discussed? Discuss what is Hadoop? What are the 5 V's of Big Data?

Nonetheless, security and privacy remain as key concerns for the implementation of cloud-based solutions. The information must remain accessible to authorized parties such as health-care providers, but the patient's health data has to kept private. To solve this, there are two commonly adopted features in the literature: access control policies and data encryption [3]. Access control policies define who can access the data, by authenticating them (validating the identity of the user) and by authorizing them (ensuring that the user has permissions to perform a given operation). Data encryption ensures that, even if the data is leaked, it is still unreadable to third parties, and therefore sensitive information remains secure and private.

Regarding the storage solutions, most investigators opt to use traditional relational databases (SQL) as the means of storing data [14, 5, 7, 8]. However, as the data is very heterogenous and unstructured, the authors of [19] propose using non-relational databases (NoSQL) which can offer much greater flexibility as the schema in these databases is dynamic. Moreover, NoSQL type data stores outperform SQL databases as the databases get larger. Table 2.4 illustrates the differences between these two technologies.

| | SQL | NoSQL |
|---|---|---|
| **Type of database** | Relational | Non-relational |
| **Database model** | Table-based database | Document-based databases, Key-value stores, graph stores, wide column stores |
| **Data type** | Good for structured data | Good for unstructured or semi-structured data |
| **Schema** | Strict schema | Dynamic schema |
| **Query** | Uses Standard Query Language (SQL), good for complex query operations | Uses Unstructured Query Languages (*e.g.* UnQL), doesn't support complex query operations |
| **Scalability** | Vertical | Horizontal |
| **Performance** | Not as good as NoSQL | Optimized for large datasets |

Table 2.4: Comparison between SQL and NoSQL technologies.

### 2.2.5 Layer 5: Data Abstraction

To-do: To @David Portugal: What can I add in this section? I'm quite unsure of how I should develop the remainder of this section. FHIR functionality will be developed in a later chapter

In the previous layer, Data Accumulation, we've defined how the system captures the information. In some cases, the collection of data may require the development of multiple concurrent storage solutions, each using different technologies, resulting in a very complex environment. The purpose of this layer is to develop services that simplify how the applications access the data, to reconcile the different data stores and ensure the information is complete and consistent. Applications can then interact with these databases through interfaces exposed by these services designated Application Programming Interfaces (API).

An API is a computing interface that defines a set of rules that "explain how computers

and applications communicate with one another", acting as an intermediary between these different components [20]. It defines what operations can be performed, how to request them, which are the accepted data types, etc. In this case, it decouples applications from the storage solutions, by encapsulating their functionality behind the interface. This ensures the modularity of the system as the applications become independent of whichever technologies are used in the data stores.

To-do: Discuss what is a RESTful API? Or leave it for the FHIR chapter? Also, review later this bridge between APIs and EHRs

Now, we need to understand what and how information is shared within the healthcare domain. As patients continuously move around the healthcare ecosystem, their health information must be available, discoverable and understandable to different entities (hospitals, laboratories, pharmacies, etc.). This prompts the digitization of medical files and the development of standards for exchanging these records instantly and securely to authorized parties [21], which are called Eletronic Health Records (EHRs). EHRs are the digital equivalent of a patient's paper-chart, they contain the patients' full medical history: previous diagnoses, treatment plans, test results, known allergies, among other details.

One of the most prominent standards for exchanging EHRs is Fast Healthcare Interoperability Resources (FHIR). FHIR is a standard developed by Health Level Seven International (HL7), which is a non-profit organization involved in the development of international healthcare informatics for over 20 years. FHIR builds upon previous data format standards like HL7 v2 and HL7 v3, and is becoming more and more widely adopted within the healthcare industry [22].

### 2.2.6 Layer 6: Application

To-do: Complete section!

The sixth layer is the application layer, where the system ingests the captured data and proceeds to analyze it. Users can then interact with the system through Graphical User Interfaces (UI), which provide different functionalities depending on the application. Some may show simple reports regarding the collected data [4, 5], other may allow users to monitor and control the different components of the system. Thus, in this layer, the system delivers the value for the end users.

As previously mentioned, one of the greatest benefits IoT systems can provide is big data

analytics.

Recently, and motivated by the recent pandemic crisis, investigators from ISR-Lisboa developed a system called e-CoVig, a low-cost solution for monitoring patients during the COVID-19 quarantine [].

### 2.2.7 Layer 7: Collaboration and Processes

To-do: The Cisco model defines a seventh layer as a component of the system: Collaboration and Processes, but how can one model for it (if it is even possible, is it relevant)? Should this section be removed entirely, or what should be added to make it more complete?

The information that is created by the IoT yields little value unless it prompts action, which requires people and processes (seventh layer). The objective is not the application — it is to empower people to work better and more efficiently. The sixth layer (Applications) provides business people the right insight, at the right time, so they can make the right decision. To do this people must be able to communicate and collaborate, which often requires multiple steps and transcends multiple applications [10].

## 2.3 Similar approaches

To-do: Right now this section only contains 3 articles, I've removed some outdated references here so it might be .

To-do: Complete section.

In [14] one of the first IoT applications for healthcare is described. The authors propose a real-time locating system (RTLS) using RFID tags. These tags are placed in hospital equipment, staff, patients and medical files and using RFID readers placed in strategic locations around the hospital (*e.g.* entrance of rooms, handheld readers), it is possible to track the location of each object. When a RFID reader detects a RFID tag it communicates this information, using Wi-Fi, to a central server which stores it in a MySQL database. Healthcare workers can then view this information through a web application, which contains a location history of the tagged object. The authors show how RTLS systems can mitigate the risks of patient misidentification, loss or theft of assets and even drug counterfeiting. However, in this article, security and privacy issues are not discussed. Although not stated explicitly, communications between the RFID tags and the RFID readers are assumed to be

unencrypted, which means "unethical individuals could snoop on people and surreptitiously collect data (...) without their knowledge", even after leaving the hospital if the tags are not removed. This raises serious privacy concerns, as the tags could contain private information that can be detrimental to the patients if revealed.

In [8] the authors build upon this concept, introducing monitoring of the patient's vital signs, using a small wristband which holds a low power device equipped with temperature, PPG (used to obtain the heart rate) and accelerometer sensors. The system can also detect with 70% accuracy if the patient has fallen, sending an immediate message to the gateway, which will later alert the clinical staff of the emergency. The authors ran a pilot test within hospital premises which was well-received by the clinical staff who praised the system for its intuitiveness and non-intrusiveness, stating that it could be easily integrated with their current HIS. However, the authors pointed out some issues with the usage of RFID tags with sensors for patient monitoring. The RFID reader needs to provide power to the RFID tags, and when using these tags with sensors, the readers need to be configured to allow these tags to be powered up. Regarding e-health standards, the authors did not discuss any protocols for exchanging data such as FHIR, which can undermine the integration of the system with existing HISs.

Wu et al. [5] developed a system which uses wearable sensor networks to monitoring the patients' status. The wearable sensors transmit the different physiological signals (ECG, PPG and body temperature) using BLE to gateways, which can either by fixed (using a Raspberry Pi module) or mobile (using a smartphone). The gateway exchanges data with the cloud through bridged MQTT brokers, after which it is stored in a MySQL database. The local users can interact with the system through a web based user interface (UI) using the smartphone or other web browsers in the local area network.

### 2.3.1 Comparative Analysis

| References | Measured Signals | Networking Protocols | Data Storage | e-Health Standards | Features | Security Features |
|---|---|---|---|---|---|---|
| [14] | ✗ | EPC/RFID, Wi-Fi | MySQL | None | RTLS | Unspecified Storage Encryption |
| [8] | Temperature, Heart Rate, Accelerometer | EPC/RFID, Wi-Fi | MySQL | None | RTLS, Fall Detection, Vital signs monitoring | Unspecified Storage Encryption |
| [5] | Temperature, Heart Rate, Accelerometer | BLE, Wi-Fi, MQTT | MySQL | None | RTLS, Fall Detection, Vital signs monitoring | AES-128 |

Table 2.5: Comparison between different pervasive healthcare applications.

### 2.3.2 Weaknesses of literature

To-do: Review section later!

Despite recent efforts, interoperability is still an issue of IoT systems. Due to the lack of clear and concise industry standards and regulations, many manufacturers develop their own proprietary data formats and communication protocols, which hampers the integration of new resources since the systems are designed within closed ecosystems [17]. Moreover, the adoption of new systems can be often met with much objection from the clinical staff due to their mistrust of technology [23]. To facilitate the deployment of new healthcare systems in hospitals, these need to be integrated easily in existing HIS.

Fortunately, there are several international initiatives to promote the use of IoT in health in a standardized way, such as HIMSS (Healthcare Information and Management Systems Society) and the Personal Connected Health Alliance (PCHAlliance). PCHAlliance for example promotes the adoption of the Continua Design Guidelines (CDG), which facilitates the integration of personal health devices into health systems. These guidelines have been recognized by ITU (International Telecommunication Union) and the European Commission and are adopted by countries such as Denmark, Norway and the USA, among others [24]. These guidelines describe a series of e-health standards like FHIR which facilitate the transfer

Within this project we aim to continue to expand the capabilities of the Continua Design Principles to further extend the software to collect the data that is being exchanged between sensors, gateways, and end services to make implementations truly interoperable.

The PCHAlliance publishes and promotes the global adoption of standards and the implementation guidelines that unleash the massive amounts of medical-grade data that enables a more holistic perspective. Commercial ready software enables the rapid integration of these standards into your product. A conformity assessment program verifies that the standards have been properly and uniformly implemented.

## 2.4 Statement of Contributions

To-do: Complete section!

After studying the different approaches taken by investigators, and in context of the WoW project, we propose a novel IoT infrastructure that uses the FHIR standard in order to fully

integrate the data in the existing HIS, Glintt GlobalCare. Other researchers in the **ISR!** have already developed wearable devices, designated "biostickers", using two different networking stacks - BLE and EPC/RFID. The system must ensure reliable and secure communications with the devices, implementing the aformentioned security features in section 2.3.2. From an hardware perspective, the system will be composed of 3 different components: the biostickers, the "Smart Box", which acts as a central node of the WBAN, aggregating the data and then communicating it along the network, and the "Smart Gateway", which serves as a fog server in order to mitigate latency and other computing issues and acts as the gateway to the HIS. In the next chapter we will start the development of the system by first tackling the communication between the biostickers and the "Smart Boxes".

# Bibliography


[1] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, and J. Henry, *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. Cisco Press, 1st ed., 2017.

[2] G. Aceto, V. Persico, and A. Pescapé, "Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0," *Journal of Industrial Information Integration*, vol. 18, no. February, p. 100129, 2020.

[3] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," *IEEE Access*, vol. 5, pp. 26521–26544, 2017.

[4] C. Doukas and I. Maglogiannis, "Bringing IoT and Cloud Computing towards Pervasive Healthcare," in *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 922–926, IEEE, jul 2012.

[5] T. Wu, F. Wu, C. Qiu, J. M. Redoute, and M. R. Yuce, "A Rigid-Flex Wearable Health Monitoring Sensor Patch for IoT-Connected Healthcare Applications," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6932–6945, 2020.

[6] Yuan Jie Fan, Yue Hong Yin, Li Da Xu, Yan Zeng, and Fan Wu, "IoT-Based Smart Rehabilitation System," *IEEE Transactions on Industrial Informatics*, vol. 10, pp. 1568–1577, may 2014.

[7] L. Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and L. Tarricone, "An IoT-Aware Architecture for Smart Healthcare Systems," *IEEE Internet of Things Journal*, vol. 2, pp. 515–526, dec 2015.

[8] T. Adame, A. Bel, A. Carreras, J. Melià-Seguí, M. Oliver, and R. Pous, "CUIDATS: An RFID–WSN hybrid monitoring system for smart health care environments," *Future Generation Computer Systems*, vol. 78, pp. 602–615, jan 2018.

[9] E. Choi, M. T. Bahadori, A. Schuetz, W. F. Stewart, and J. Sun, "Doctor AI: Predicting Clinical Events via Recurrent Neural Networks.," *JMLR workshop and conference proceedings*, vol. 56, pp. 301–318, 2016.

[10] Cisco, "The Internet of Things Reference Model," 2014.

[11] L. Minh Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," *Electronics (Switzerland)*, vol. 8, no. 7, pp. 1–49, 2019.

[12] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, 2016.

[13] F. Wu, T. Wu, and M. R. Yuce, "Design and Implementation of a Wearable Sensor Network System for IoT-Connected Safety and Health Applications," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 87–90, IEEE, apr 2019.

[14] P. Fuhrer and D. Guinard, "Building a smart hospital using RFID technologies," *European Conference on eHealth 2006, Proceedings of the ECEH 2006*, pp. 131–142, 2006.

[15] EPCglobal, "Specification for RFID Air Interface EPC ™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz," *Intellectual Property*, no. October, 2006.

[16] A. Dementyev, S. Hodges, S. Taylor, and J. Smith, "Power Consumption Analysis of Bluetooth Low Energy, ZigBee, and ANT Sensor Nodes in a Cyclic Sleep Scenario," in *Proceedings of IEEE International Wireless Symposium (IWS)*, IEEE, 2013.

[17] J. N. S. Rubí and P. R. L. Gondim, "IoMT platform for pervasive healthcare data aggregation, processing, and sharing based on oneM2M and openEHR," *Sensors (Switzerland)*, vol. 19, no. 19, pp. 1–25, 2019.

[18] RedHat, "Cloud Computing - IaaS vs PaaS vs SaaS."

[19] A. F. Subahi, "Edge-Based IoT Medical Record System: Requirements, Recommendations and Conceptual Design," *IEEE Access*, vol. 7, pp. 94150–94159, 2019.

[20] IBM, "Application Programming Interface (API)."

[21] HL7, "FHIR v4.0.1," 2019.

[22] C. Peng and P. Goswami, "Meaningful integration of data from heterogeneous health services and home environment based on ontology," *Sensors (Switzerland)*, vol. 19, no. 8, 2019.

[23] F. Dursun Ergezen and E. Kol, "Nurses' responses to monitor alarms in an intensive care unit: An observational study," *Intensive and Critical Care Nursing*, vol. 59, no. xxxx, p. 102845, 2020.

[24] Personal Connected Health Alliance, "Continua Adoption Playbook Deploying Interoperable Connected Health in Your Health System," no. May, p. 20, 2017.

# Appendix A

# My cool appendix!