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

List of Acronyms

IoT	Internet of Things
IT	Information Technology
API	Application Programming Interface
FHIR	Fast Healthcare Interoperability Resources
EHR	Eletronic Health Record
ECG	Electrocardiogram
IMU	Inertial Measurement Unit
RFID	Radio-frequency Identification
BLE	Bluetooth Low Energy
HIS	Health Information Service

List of Figures

List of Tables

1 Introduction

This report describes the work developed under the project "Wireless IoT Architecture for Smart Nodes deployed in Hospital Beds", which took place in the Institute of Systems and Robotics (ISR) in Coimbra in the past year.

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
"Based on our previous experiences in bringing digital heath solutions to the European hospitals (see for instance the swithome project), hospitals are more likely to accept a solution, if it is already connected to their hospital information system." The system should be non-invasive, reliable and satisfy the stringent security and privacy requirements of health information systems

1.3 Requirement Analysis

To-do: Brief overview of system requirements, but these will be later described in the next section.

1.4 Thesis Structure

To-do: Apresentar e explicar a estrutura / organização da tese "dizer como vamos responder a "HOW?" na restante dissertação."

2 State of the Art

In this chapter a survey of pervasive healthcare applications is presented.

To-do: Add small chapter introduction.

2.1 Internet of Things

2.1.1 What is IoT?

To-do: Discuss if this section should move to introduction instead

Internet of Things (or IoT) is an emerging communication paradigm, often hailed as the driver of the Fourth Industrial Revolution [3].

The definition of this concept has evolved over time with the development of other technologies such as data analytics, embedded systems, etc. Nowadays 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). 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 algorithms [4].

To-do: Discuss the potential of IoT technologies and bridge to pervasive healthcare applications (such as in Clinics, Hospitals, Smart Home). Cite articles with references to investments in these areas.
- smart systems enable continous patient monitoring

More specifically in the healthcare domain,

2.2 An IoT Reference Model for Pervasive Healthcare Applications

In order to develop an IoT system, it is crucial to design it based on a reference model. A reference model provides a general structure (or a "template") for designing systems, thus enabling the comprehension of these complex systems by breaking them down into simple and distinct functional layers, as also defines 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, enabling both edge / fog computing solutions and more cloud oriented approaches. However, from a hardware perspective, in this work we will restrict our focus to the most common approach taken by investigators, using 3 different components:

- **Endpoint** or **edge** nodes (Layer 1), which interact with the physical world, capturing data.
- **Gateway** devices (Layers 2-3), which integrate multiple **edge** nodes, filtering and aggregating the data generated by these and relaying it to a 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), we will focus on pervasive healthcare applications and its enabling technologies.

To-do: Make images that summarize key points of each layer (by adapting original images from Cisco documentation?)

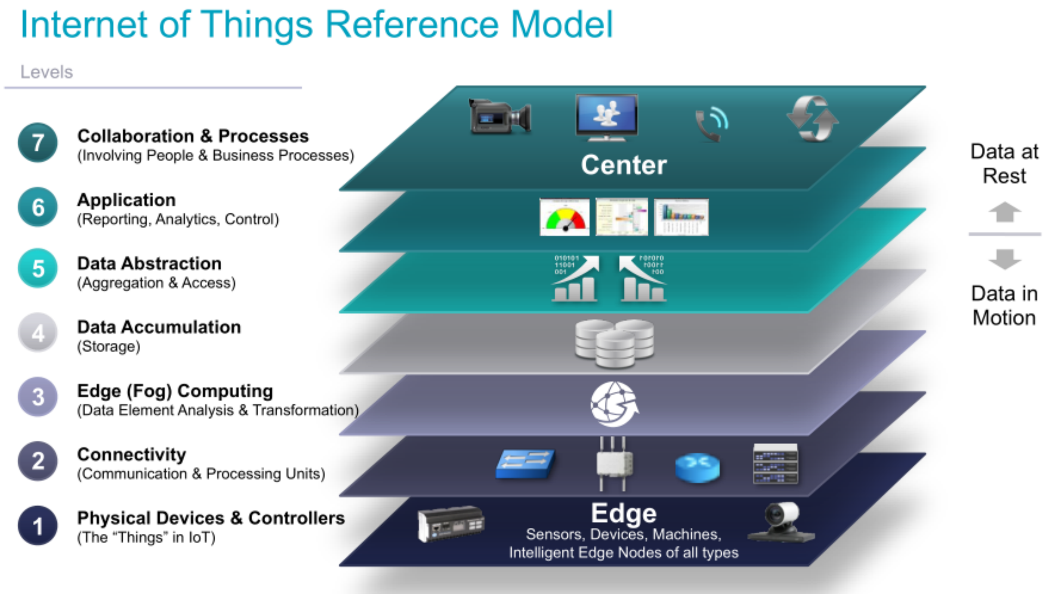

Figure 2.1: IoT reference model published by IoTWF. Source: [5].

2.2.1 Layer 1: Physical Devices and Controllers

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 processing and storage.

Currently, hospitalized patients need to be wired to various measurement instruments when continuous biomonitoring is required. This confines the patients to their beds, restricting their mobility, and may cause skin irritations and infections, contributing to their discomfort and deterioration of their health condition [6]. Moreover, the detachment of electrodes from the patient's body, provoked by patient's movements, is one of the main sources of false alarms. These require immediate attention from the hospital staff, contributing to their exhaustion and may ultimately result in the desensitization to the alarms, reducing their response time to real emergencies [7]. Wearable, wireless, and non-intrusive sensors may be able to minimize these issues to a large extent.

In recent years there has been remarkable progress on the development of smart wearable devices, driven by recent technological breakthroughs in the miniaturization of sensors and microfabrication processes [8]. From the literature, we can classify all these sensors into 3 distinct categories based on the information that can be retrieved from them, as shown in table 2.1:

- Monitorization of the patient's biosignals, used for evaluating the patient's health condition.
- Monitorization of 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.
- Monitorization of the patient's environment, mainly used for assessing environmental hazards, *e.g* gas leaks in a patient's home or an industrial workplace.

Type of monitoring	**Type of sensors used**
Vital Signs Monitoring	Body Temperature, Heartbeat, Respiratory Rate, Galvanic Skin Response, Blood Pressure, Pulse Oximetry, Electrocardiogram (ECG), Glucose Level Sensors
Activity Monitoring	Accelerometer, Gyroscope, Magnetometer, Ultrasound Sensors, Radio-frequency Identification (RFID) Tags
Environmental Monitoring	Air Temperature, Humidity, Hazardous Gas Sensors

Table 2.1: List of signals commonly used in pervasive healthcare applications, adapted from [9].

The first step when designing an IoT network should be to analyze the mobility and data requirements of the system [1]. **Mobility** describes the devices' ability to move and, if it is able to, how frequently it does so. Generally we find that the devices are attached to moving objects (*e.g.* a patient's body), and therefore can be classified as mobile. **Data** requirements describe how much data is generated and transmitted by each device per unit of time, and how critical is it to the operation. Simpler health monitoring applications can include a single temperature or heart rate sensor while more complex applications can include pulse oximetry, electrocardiogram (ECG), respiration rate, etc.

With these key requirements established, we can now discuss some other characteristics of the smart devices, like:

- **Power source**: This classification describes if the device has an internal energy supply powering the device or if it has continuous power delivery from an external source. If the device must be mobile, it is often requires using batteries to power it. Battery-powered devices are not bound to a single location, but the finite energy source constrains the device's energy consumption and lifetime, leading to limited memory, computation and connectivity capabilities.

- **Transmission range**: This classification describes how far away the devices can communicate. In healthcare, these have very short transmission ranges. For example, a fitness band that communicates with a smartphone will be at most located a few meters from it.

2.2.2 Layer 2: Connectivity

To-do: Remake this section!!!!

The second layer of the model focuses on connectivity.

The most important function of this model is ensuring reliable and timely data transmission. This includes all communications between each layer, but we will restrict our focus to communications between the edge devices, between edge devices and "gateway" devices and between "gateway" devices and the central servers.

This model proposes to make use of current networks to perform communications and processing, it does not imply the development of another network. However, some legacy devices may not be IP-enabled and others may need proprietary controllers to communicate properly. The network should be capable of integrating them by deploying specialized gateways that support those devices.

Communication Protocols

Each technology is designed with certain use cases in mind. They drive their development and thus it is natural that each one has their own advantages and disadvantages, depending on their use. For instance, short range wireless protocols like Wi-Fi or Bluetooth are limited by the transmission range, but long range protocols like NB-IoT usually have high energy consumption, which is unviable for constrained node networks. Each protocol also defines their own frame format and communicate within certain frequency bands, introducing additional differences. Due to the frequency bands used by UHF RFID, metal and water surfaces can introduce interference in its transmissions, thus reducing the effective transmission range [10]. The figure 2.2 shows some commonly used protocols in IoT systems grouped by range.

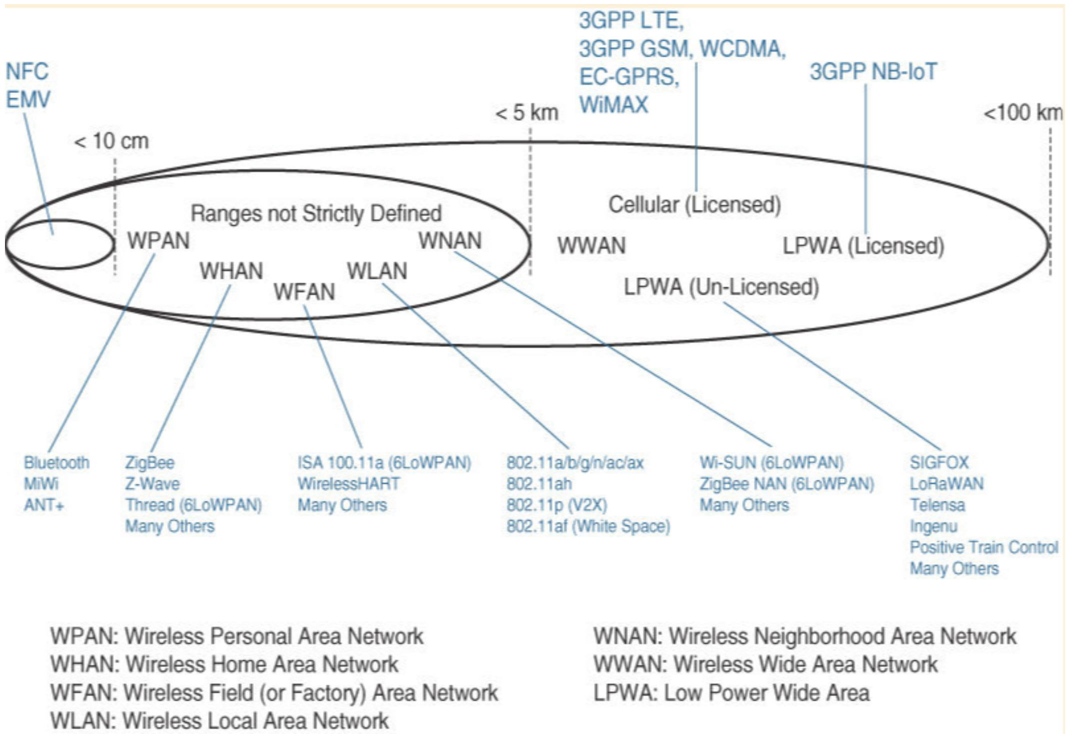

Figure 2.2: Classification and grouping of various network protocols by range. Source: [1]

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

The choice of the communication protocol is driven by the characteristics of the smart devices, as defined in the first layer. However, we can highlight other key points that affect this decision:

- **Cost**: The cost of implementing certain protocols may not be economically viable. RFID systems are a great example of this. The development of RFID tags is inexpensive, but this is offset by the immense cost of the RFID readers, which can quickly become unsustainable.

- **Throughput**: The communication protocol should ensure there is enough bandwidth to handle all communication within the designated transmission range. Even within similar technologies, this can vary wildly with the range as seen in figure 2.3.

- **Security**: Security is one of the most important requirements of any system. The communication protocol needs to implement security measures to ensure that the transmissions are not compromised in transit, thus denying malicious third parties the ability to snoop or tamper the transmissions.

- **Interoperability**: Not all communication protocols are globally adopted. To ensure the interoperability of the system it is imperative to choose protocols that are widely accepted and supported by the industry.

- **Scalability**: This determines how many devices are supported and how many more can be added to the system, thus giving us a measure of the system's flexibility for expanding beyond the initial development.

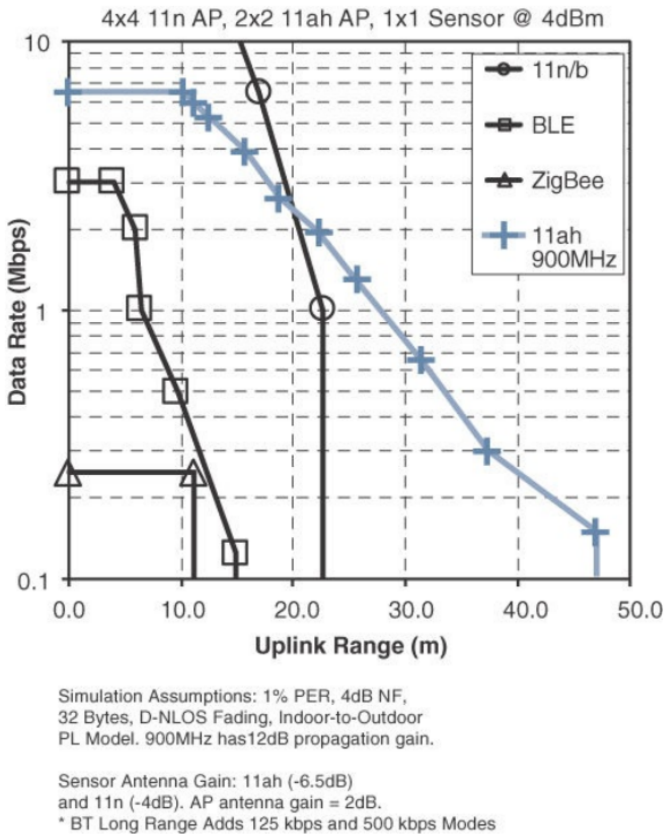

Figure 2.3: Throughput versus Transmission range for four WHAN to WLAN communications protocols. Source: [1]

2.2.3 Layer 3: Edge (Fog) Computing

To-do: Remake this section!!!!

The third layer of the model is driven by the need to convert the generated data into information suitable for storage and higher level processing at the fourth layer (Data Accumulation). 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 resources. Therefore, 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 data processing at this stage is generally limited to the incoming data, there's not concept of . More demanding and thorough analysis is left to layer 4-6 devices. Layer 3 processing generally provides these functions:

- **Filtering**: Assessing if the data should be processed at a higher level.
- **Formatting**: Reformatting data for consistent higher-level processing.
- **Decoding**: Handling cryptic data with additional context (such as the origin);
- **Cleaning**: Reducing data to minimize the impact of data on the network and higher-level processing systems.
- **Analysis**: Determining whether data represents a threshold or alert.

2.2.4 Layer 4: Data Accumulation

To-do: Remake this section!!!!

The data that is generated by the devices at the first layer is propagated through the network, moving through each layer as every. Up to this point the model is event driven. But applications often don't need or are unable to process data at the rate it is generated. The fourth layer, Data Accumulation, captures data and stores it so it becomes usable to applications when needed, thus converting event-based data to query-based processing.

In short, this layer focuses on converting event-based data to query-based processing.

This layer also evaluates if the data should be kept stored in non-volatile memory or if it should be kept for short-term use only, and defines how it should be stored (*e.g.* relational database, non-relational database, distributed file systems, etc.).

Cloud platforms are often seen as a solution to the data management and processing issues that arise from the massive data collection associated with ubiquitous systems [11]. This is made possible due to the elasticity in allocating, swiftly and inexpensively, shared resources on-demand, adjusting itself to the needs of the application. We can find 3 models regarding cloud services offerings:

- **Infrastructure as Service (IaaS)**: IaaS contains the basic building blocks for cloud IT, providing access to the networking features, computers (virtual or dedicated hardware) and data storage space. This gives the highest level of flexibility and control over the resources.

- **Platform as a Service (PaaS)**: PaaS remove the need for organizations to manage the underlying infrastructure (hardware and operative system) and focus on deployment their applications. The service provider manages all resource allocation, capacity planning, software maintenance and patching required.

- **Software as a Service (SaaS)**: This services provides a completed product that is fully managed by the service provider. When using SaaS platforms, we don't need to think about the infrastructure or how it is maintained. All this is handled seamlessly by the service provider, we only need to make use of the application, without regard to the underlying mechanisms. A common example of this is a web-based email service.

2.2.5 Layer 5: Data Abstraction

To-do: Complete section.

Fast Healthcare Interoperability Resources (FHIR)

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 users [12], which are called Eletronic Health Records (EHRs). EHRs is the digital equivalent of a patient's paper-chart, it contains the patients' full medical history: previous diagnoses, treatment plans, test results, known allergies, among other details. It is now an essential component of health IT.

Fast Healthcare Interoperability Resources (FHIR) is a standard data format for exchanging EHRs, developed by Health Level Seven International (HL7). HL7 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 widely adopted within the healthcare industry.

2.2.6 Layer 6: Application

To-do: Complete section.

The sixth layer is the application layer, where the interpretation of the captured data occurs.

2.2.7 Layer 7: Collaboration and Processes

To-do: The Cisco model defines a seventh layer: Collaboration and Processes, but how can one model for it (if it is even possible)? This section doesn't seem to add any value other than aligning with the original proposal.

The information that is created by the IoT yields little value unless it prompts action, which requires people and processes (seventh layer) — this is what differs IoT from Information Technology systems. 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 [5].

To-do: Add a section exposing most common security measures and attack vectors?

2.3 Similar approaches

To-do: Complete section.

In

Adame et al. [8] propose an IoT hybrid monitoring system - CUIDATS - for health care environments which integrates RFID and WSN technologies in a single platform providing real-time location, status, and tracking of patients and hospital assets. The patients are monitored via a small wristband which holds a small low power mobile sensor node, equipped with temperature, pulse and accelerometers.

Wu et al. [13] 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 or mobile, by using smartphones. The gateway exchanges data with the cloud through bridged MQTT brokers, allowing the development of local features (e.g. local UI to interact with the patients) and cloud processing features (e.g. Big Data Analytics, data storage, UI for medical professionals).

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.

Zhang et al. [14] propose a infusion monitoring device based on an infrared sensor and NB-IoT (Narrowband IoT protocol), in order to prevent drop rate anomalies or unnoticed drug replacements.

2.3.1 Comparative Analysis

To-do: Place table with a list of criteria to compare the different approaches.

2.3.2 Weaknesses of literature

Security and Privacy

To-do: Complete section.

Interoperability

Despite recent efforts, interoperability is still an issue of IoT systems. Since there are not any clear industry standards and regulations, many manufacturers push their own proprietary data formats and communication protocols, which hampers the integration of new resources since they are developed within closed ecosystems [15].

To-do: Complete section.

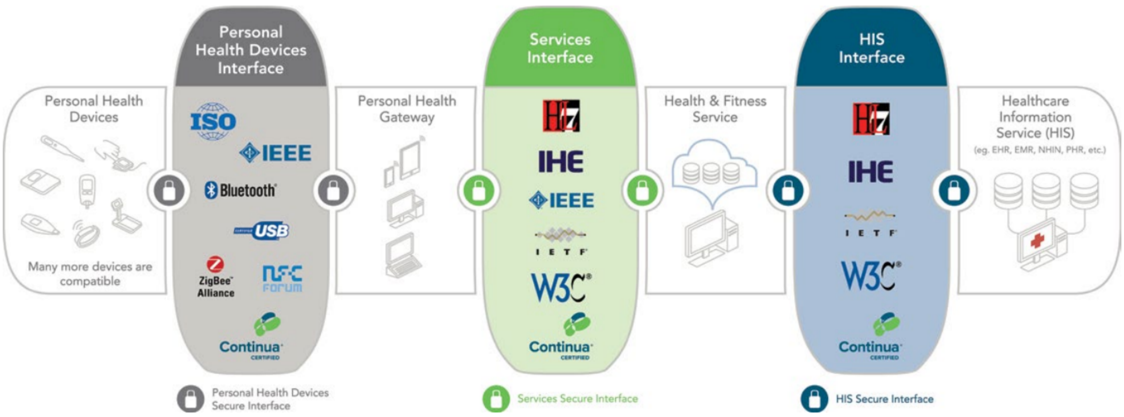

Figure 2.4: System architecture from the Personal Connected Health Alliance [2].

2.4 Statement of Contributions

To-do: Complete section.

- Hardware evaluation for edge nodes which integrate electronic wireless patches that gather patient's physiological signals;
- Integrating IoT system in an existing healthcare information system (Glintt GlobalCare software) through an FHIR API layer;
- Evaluation of the performance of the proposed system through a testbed and a real healthcare scenario;

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] Continua Health Alliance, "Continua Design Guidelines | Personal Connected Health Alliance."

[3] 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.

[4] A. Singh, A. Payal, and S. Bharti, "A walkthrough of the emerging IoT paradigm: Visualizing inside functionalities, key features, and open issues," *Journal of Network and Computer Applications*, vol. 143, no. February, pp. 111–151, 2019.

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

[6] A. Darwish and A. E. Hassanien, "Wearable and implantable wireless sensor network solutions for healthcare monitoring," *Sensors*, vol. 11, no. 6, pp. 5561–5595, 2011.

[7] 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.

[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] 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.

[10] J.-I. Cairo, J. Bonache, F. Paredes, and F. Martin, "Interference Sources in Congested Environments and its Effects in UHF-RFID Systems: A Review," *IEEE Journal of Radio Frequency Identification*, vol. 2, no. 1, pp. 1–8, 2018.

[11] 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.

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

[13] 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.

[14] H. Zhang, J. Li, B. Wen, Y. Xun, and J. Liu, "Connecting Intelligent Things in Smart Hospitals Using NB-IoT," *IEEE Internet of Things Journal*, vol. 5, pp. 1550–1560, jun 2018.

[15] 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.

Appendix A

My cool appendix!