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
WoW	Wireless biOmonitoring stickers and smart bed architecture: toWards Untethered Patients
API	Application Programming Interface

List of Figures

List of Tables

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
"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."

Based on previous knowledge of digital health solutions, the main objective of this work is the development of a IoT architecture in the context of the WoW project. The system should be non-invasive, reliable and satisfy the stringent security and privacy requirements of health information systems.

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 systems and pervasive healthcare 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 an 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. 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.

More specifically in the healthcare domain,

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

2.2 A 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, 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 investigators, using 3 different components:

- **Endpoint** or **edge** nodes (corresponding to Layer 1), which interact with the physical world, capturing data.
- **Gateway** devices (Layers 2-3), which connect to multiple **edge** nodes, filtering and aggregating the data generated by these, while 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), in the context of the dissertation we will focus on pervasive healthcare applications and its enabling technologies.

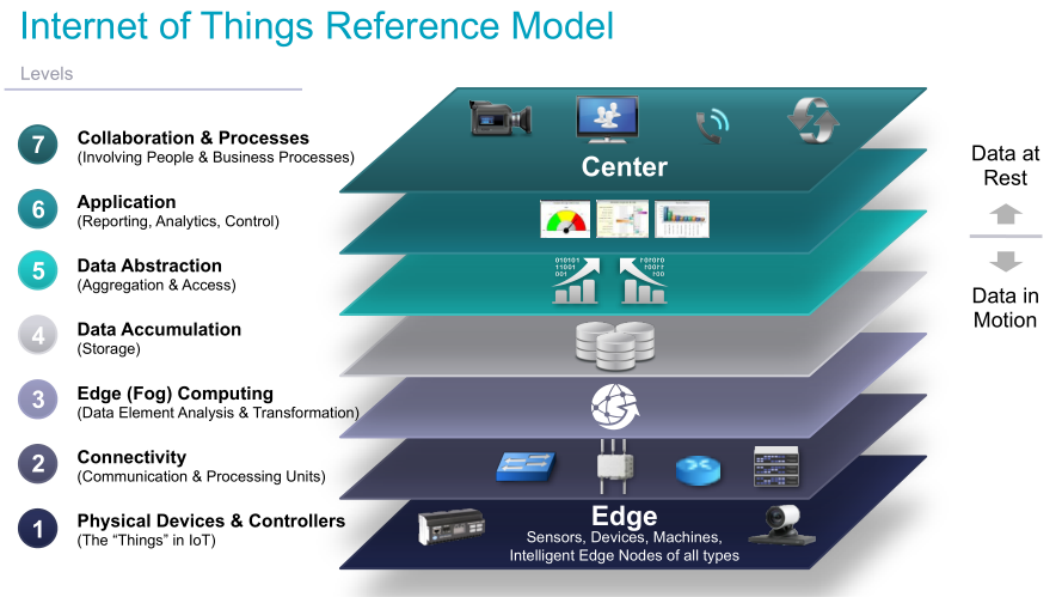

Figure 2.1: IoT reference model published by IoTWF. Source: [3].

2.2.1 Layer 1: Physical Devices and Controllers

To-do: Review this section later.

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.

When designing an IoT network, the first step 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. **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 sensors, 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 will require a portable power source, a battery. Battery-powered devices are not bound to a single location, but the finite energy source con-

strains 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 usually have short transmission ranges. For example, a fitness band that communicates with a smartphone will be at most located a few meters from it.

In order to properly design these devices, it is necessary to understand what problems currently reside within clinical environments. Today, 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 also cause skin irritations and infections, aggravating their discomfort and deterioration of their health condition [4]. 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 [5]. Wearable, wireless, and non-intrusive devices can to minimize these issues to a large extent, and are seen as one of the key components of IoT-based healthcare systems [6].

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 [7]. From the literature, we can 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 biosignals, 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, 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, Heart Rate, Heart Rate Variability, Respiratory Rate, Galvanic Skin Response, Blood Pressure, Pulse Oximetry, 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 sensors commonly used in pervasive healthcare applications, adapted from [8].

2.2.2 Layer 2: Connectivity

To-do: Review this section later!!

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 split 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 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 are limited by the transmission range, but long range protocols usually have a higher energy consumption, which may be unviable for networks with very constrained devices. Each protocol also defines their own frame format and communicate within certain frequency bands, which may require special licenses. Due to the frequency bands used by UHF RFID, metal and water surfaces near the devices introduce great interference in its transmissions due to signal reflections, thus reducing the effective transmission range [9]. The figure 2.2 shows some commonly used protocols in IoT systems grouped by range.

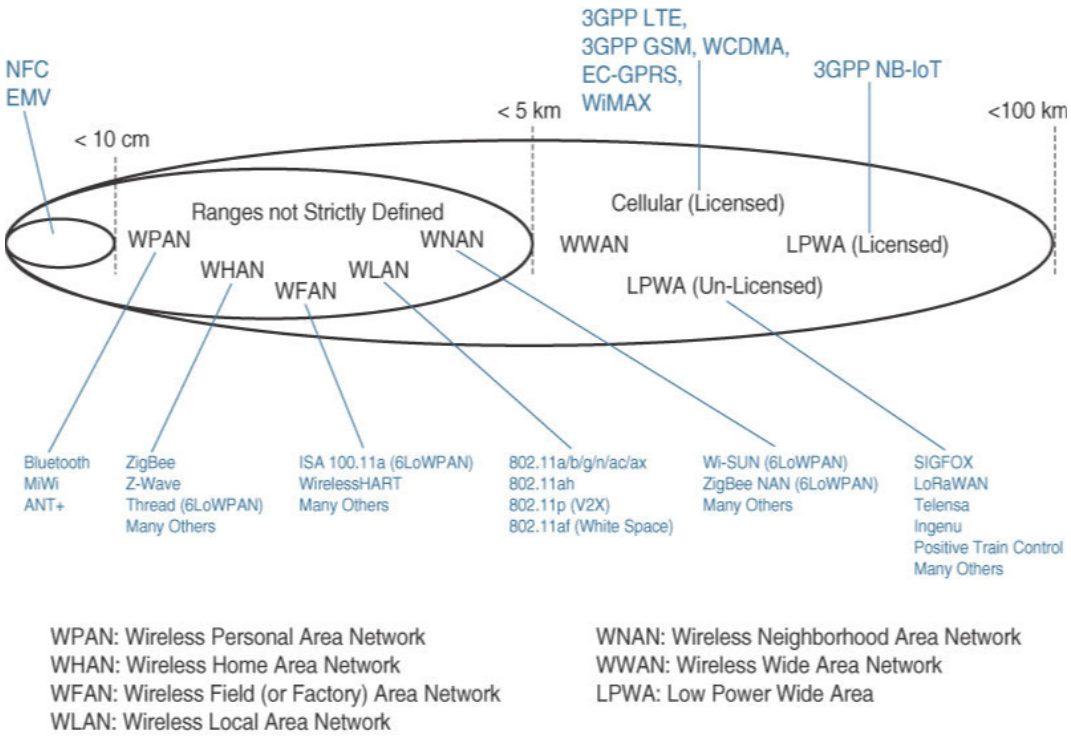

Figure 2.2: Classification and grouping of various network protocols by range. Source: [1]

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

Regarding

To-do: Add small comparison of most common protocols WSN used in healthcare? BLE, ZigBee?

Regarding

To-do: Complete section with short comparison between NB-IoT, LTE? Mention WiFi as the best solution tho

To-do: Complete section with short comparison between MQTT and CoAP

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:

- **Latency**: Certain applications deal with time critical events, for example the detection of health emergencies. In these cases, any delays in the communications can cause great detriment to the patient's well-being, making it crucial to minimize them.
- **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 2.3.

- **Security**: Security is one of the most important requirements of any system, but this is especially true for healthcare systems. Due to the sensitive nature of the information, it is crucial to secure the information 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 by [10].

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

- **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.

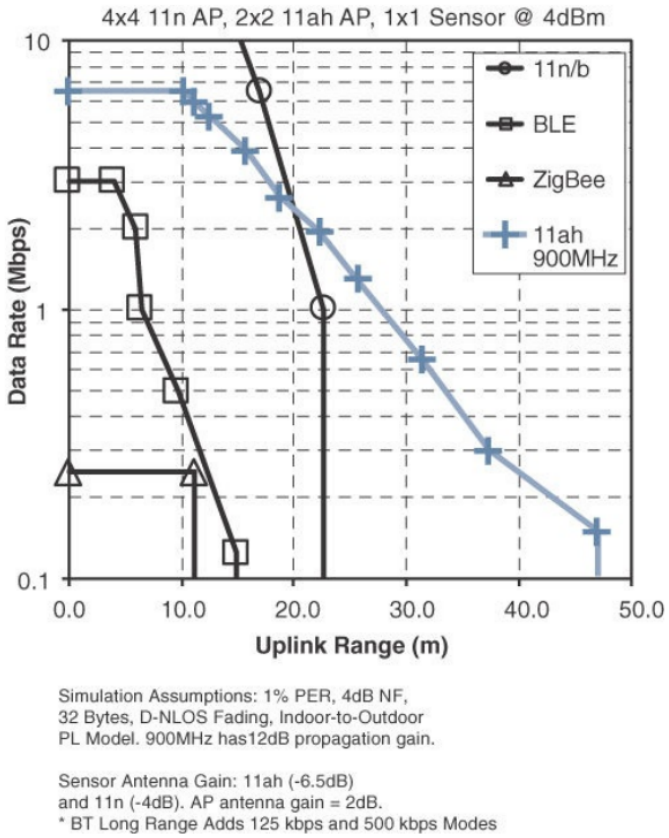

Figure 2.3: Throughput versus Transmission range for four WHAN to WLAN communications protocols. Source: [1]

2.2.3 Layer 3: Edge (Fog) Computing

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. The data processing at this stage is generally very limited, mostly focused on "preprocessing" the data and handling time critical events. More demanding and thorough analysis should be left to the central server, which holds much greater computing power. The different processes applied at this stage usually are:

- **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.
- **Analysis**: 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.

The data that is generated by the edge devices is propagated through the system, moving through each layer with each sensor reading. Up to this point, the model is event driven. However, most applications cannot make use of the data at the rate it is generated. In this layer, Data Accumulation, we define how the system captures the data and stores it, so it becomes usable for applications when needed, providing a transition from event to query-based processing. This includes any issues related with data storage: how the data should be stored (*e.g.* using a relational database, non-relational database, distributed file systems,

data compression, etc.), what data should be stored and which should be kept for short-term use, etc.

In healthcare, big data analytics is seen as one of the most promising features of IoT applications. However, the massive data collection that is associated with ubiquitous systems causes many issues concerning the processing and storage of data. Cloud platforms are often seen as a solution to this problem [6]. 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.

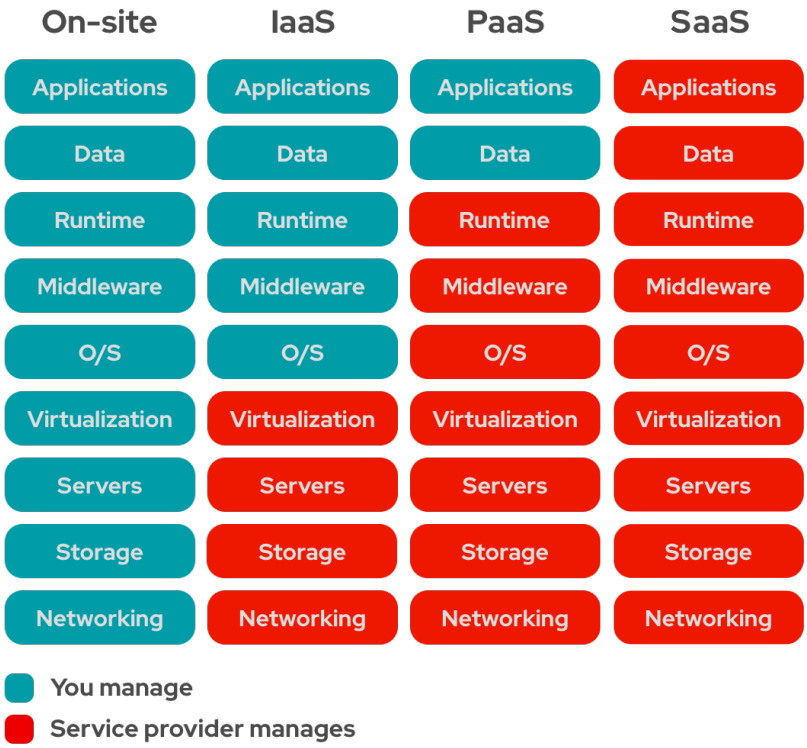

Figure 2.4: Differences between the cloud offerings and on-premise solutions. Source: [11]

Nonetheless, security and privacy remain as key issues in cloud systems. The information must remain accessible to authorized parties such as healthcare 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. 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 the sensitive information remains secure and private.

2.2.5 Layer 5: Data Abstraction

To-do: Review this section later.

In the previous layer, Data Accumulation, we've defined how the system captures the information. In large scale systems, 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 simplify how the applications access the data, to reconcile the different data stores and ensure the information is complete and consistent.

This is generally accomplished with the development of 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". [12], acting as an intermediary between different systems and software components. It defines what operations can be performed, how to request them, which are the accepted data types, etc.

Regarding healthcare services, 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 [13], 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. One of the most prominent 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 becoming more and more 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 system proceeds to analyze the data captured and

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)? 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) — this is what differs IoT from traditional 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 [3].

2.3 Similar approaches

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. Healthcare workers can then view this information with a web application, which contains a location history of the tagged object. The authors show how these RTLS systems can mitigate the risks of patient misidentification, loss or theft of assets and even drug counterfeiting, demonstrating the value that IoT applications can bring to hospitals. 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 [7] 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, 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 (although how the staff is alerted is not discussed). The authors ran a pilot test within hospital premises and found it 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.

Moreover, despite claiming the system can be easily integrated with the HIS,

[15]

In [16]

Wu et al. [16] 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.

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. Due to the lack of clear and concise 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 [17]. Moreover, the adoption of new systems can be often met with much objection from the clinical staff due to their mistrust of technology [5]. In order to facilitate the integration of new systems, these should be easily

2.4 Statement of Contributions

To-do: Complete section.

After studying the different approaches taken by investigators,

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

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

[13] HL7, "FHIR v4.0.1," 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] 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.

[16] 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.

[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.

Appendix A

My cool appendix!