|NST|TUTO
UN|VERS|TÁR|O
DE L|SBOA

Centralized Management IoT Platform (IoT Central Hub)

António dos Santos Rodrigues

Master in Computer Science and Business Management

Supervisor:
PhD. Carlos Eduardo Dias Coutinho, Assistant Professor, ISCTE

October, 2021

Acknowledgments

I would like to thank my family who always support me and dedicated all the resources and time available to help me to achieve the goal. Especially my wife and my children who are my great passion today and I had to give up part of the time to prepare this work, that everyone was very patient and collaborative with me.

Also, to my supervisor, who had a lot of dedication and support to carry out this research project, guiding me to deliver the great result. I greatly appreciate your patience and dedication for this achievement.

ISCTE institution that believed in my potential to my scientific contribute to my studies carried out throughout the study period.

To my fellow students who stayed with me all time, supporting me and working together to deliver the best study material.

To my community computer's friends that friendly offered a lot of help to support me with technical issues at this research project, sometimes when I couldn't move forward, and they were very patient and willing to dedicate their time to my research work.

Finally, I want to dedicate a lot of gratitude to everyone who supported me to success, it's not only academically, but professionally throughout my life.

To all, my sincere thanks.

Resumo

Na área da tecnologia da informação, a cada dia a palavra inovação encontra-se cada vez mais presente. No âmbito da tecnologia de Internet das Coisas (Internet of Things – IoT) não é diferente. Todos os anos são criado e apresentados novos produtos e serviços de IoT que permitem facilitar e descomplicar a vida dos usuários, conectando pessoas aos dispositivos de forma remota e automatizada, gerando mobilidade e operabilidade de serviços de tecnologia através da heterogenerabilidade de aparelhos conectados na internet.

Com base nesse obstáculo encontrado no cotidiano dos usuários de tecnologia domésticos, esse trabalho de tese desenvolve o estudo de desenvolvimento de uma plataforma única e fácil utilização. Nessa plataforma é possível ter os dispositivos de IoT centralizado de uma mesma unidade de rede local de forma que possam ser gerenciados e manipulados através de uma interface gráfica simples e intuitiva. Assim, a gestão fica unificada e prática para qualquer tipo de usuário que tenha interesse em usar essa tecnologia.

Nessa tese foram estudadas as boas práticas e as melhores soluções pesquisadas dentro da prática de gestão de IoT em diversos cenários. Abrangendo tipos de tecnologias, propostas de arquiteturas, processos de configuração e analise de compatibilidade de recursos e funcionalidades de diferentes dispositivos existente atualmente no mercado. Assim, esse trabalho tem o propósito de apresentar em detalhes o estudo do protótipo de uma plataforma unificada que permite configurar, monitorar e gerenciar a integração entre dispositivos heterogéneos existentes no mercado atualmente para usuários residenciais.

Palavras-Chave: IoT, gestão de dispositivos, arquitetura de sistemas, Cloud Computing, Smartphone, infraestrutura de sistemas e redes de computadores.

Abstract

On information technology topics, the word innovation is increasingly present every day. Regarding Internet of Things (IoT) technology subject, it's not different. Every year new IoT products and services are created and presented that allow users to make their lives easier and simpler, connecting people to devices remotely and automatically, generating mobility and operability of technology services through the heterogeneity of devices connected to the internet.

Based on this obstacle found in daily home technology users, this thesis works to develop the study of the development of a unique and easy use platform. On this platform, it is possible to have IoT devices centralized on the same local network unit so that they can be managed and manipulated through a simple and intuitive graphical interface. Thus, management is unified and practical for any type of user who is interested in using this technology.

In this thesis, good practices and the best solutions researched within the practice of IoT management were studied in different scenarios. Covering types of technologies, proposed architectures, configuration processes and compatibility analysis of features and functionality of different devices currently on the market. Thus, this work aims to present in detail the study of the prototype of a unified platform that allows configuring, monitoring and managing the integration between heterogeneous devices currently on the market for residential users.

Keywords: IoT, device management, systems architecture, Cloud Computing, Smartphone, systems infrastructure and computer networks.

Contents

List of Figures

List of Tables

List of Acronyms

API – Application Programming Interface

CoAP – Constrained Application Protocol

GUI – Graphical User Interface

HD – Hard Disk

HTTP – Hypertext Transfer Protocol

IaaS – Infrastructure as a Service

IDE – integrated Development Environment

IEEE – Institute of Electrotechnical and Electronic Engineers

IoT – Internet of Things

IP – Internet Protocol

LPWAN - Low Power Wide Area Networks

NFC – Near Field Communication

PaaS – Plataform as Service

REST – REpresentational State Transfer

RFID – Radio-Frequency Identification

SaaS – Software as a Service

TB – Terabyte

TCP – Transmission Control Protocol

WiFi - Wireless Fidelity

WLAN – Wireless Local Area Network

WMAN - Wireless Metropolitan Area Network

XML - Extensible Markup Language

YAML – Yet Another Markup Language

1 Introduction

In this chapter the work is presented as follows: initially the contextualization of the studied content mentioned, then the motivation with approaching explored theme. Afterwards, the objectives are described to identify the purpose of the research. After, there are the research methodologies adopted and, finally, the structure of the dissertation.

1.1. Contextualization

It's ease of purchasing a device with Internet connection functionality has grown exponentially in society. Technological advances and the low cost of consuming these services have helped the popularization and diversification of these devices (Vasseur & Dunkels, 2010). The set of these objects, with the ability to iterate with users, through sensors, allows generating responses and information according to the needs of each individual. These types of devices have been termed as IoT (Internet of Things) (Gubbi et al., 2013)

The basic concept of IoT devices' functionality is the presence of RFID (Radio-Frequency IDentification) sensors, tags and readers in telephones, home robots, smart lamps, home appliances connected to the internet, etc. (Atzori et al., 2010). All this infrastructure generates a database of information that allows the user to interact intelligently and in a personalized way with the device. Thus, it is possible for the home user to have tasks of automated routines, better precision in decision making and interactions between the devices and the servers which they are connected (Ibsg & Dave Evans, 2011).

The use of this emerging technology has provided many challenges in the scope of management and integration of smart device services, as mentioned by Atzori et al (Atzori et al., 2010). According to him, this technology has as main challenge the interconnection of a group of totally heterogeneous devices. Therefore, each one has its specific protocol and technological infrastructure for each manufacturer. Another relevant factor in the complexity of using IoT is the accuracy of the information. The set of data generated by the sensors of the devices, can generate an inaccuracy of information between 60% to 70%, causing insufficient or unnecessary responses for the user (Ma et al., 2013).

In view of universe of complexity and difficulty of integration between objects connected in a network, this dissertation's work is aimed at researching the creation of a unique connection platform, which allows home users to make installations and configurations to create a unique environment where everyone can collaboratively exchange information in a synchronized manner to generate better results, such as synchronize smart devices easily, heterogeneity, usability and etc. However, the development complexity and time limitation are main factors that is restrictive to provide more functionality to the prototype.

1.2. Motivation

The applications' development for IoT devices is an increases study area. Currently, there are several researches carried out in the scope of smart device management. However, there is still a great difficulty in the usability and practicality of the operation of these devices. Therefore, the main purpose of developing this dissertation is to expand knowledge to reduce the complexity of handling this tool for home users developing a brand new application (Lee & Lee, 2015) (Chen et al., 2014). Thus, the focus of this study is based on analyzing and solving the following listed problems:

- **Administration interface centralized:** for each device added smartly to the home network, it presents a different application to perform the devices' configuration. When there are few devices, management is possible, but the environment where the user has countless devices on the same home network is becoming a complex factor to manage. (Talavera et al., 2015)

- **Simplicity in installation and configuration**: the applications of IoT devices, present a series of configuration and installation steps, in a way that requires the user to have technological knowledge to be able to install and configure. Thus, create a limitation in the use of technology. (Chaqfeh & Mohamed, 2012)

- **Interconnection between devices in heterogeneous environment:** each device has its own application with access to its own data. Thus, there is a limit of information and complexity in the computing environment because

> there are several technologies that are not connected. Thus, it is possible to reduce processing and increase excessive data traffic on the network, as there is no communication between the devices. (Chaqfeh & Mohamed, 2012)

On these challenges highlighted, this dissertation works aims to expand IoT studies' areas and create an alternative to reduce technological complexity for home users in a way that does not limit them to the use of this type of technological devices.

1.3. Research Objectives

The main purpose of this work is creation of a single, centralized platform where all IoT devices on the same home network are connected. This platform was called the IoT Central Hub. Being a prototype designed and developed for research and study purposes in order to contribute to the improvement of this technology in the future. In addition to the scope of the research, the work focuses on making it easier for home users, so that it can reduce the complexity of installing, configuring and managing various IoT devices from different brands, in the same computing environment.

The IoT Central Hub platform allows the unification of all recognized and configured IoT devices that are within the same local network. On Figure 1, it details how the IoT Central Hub works.

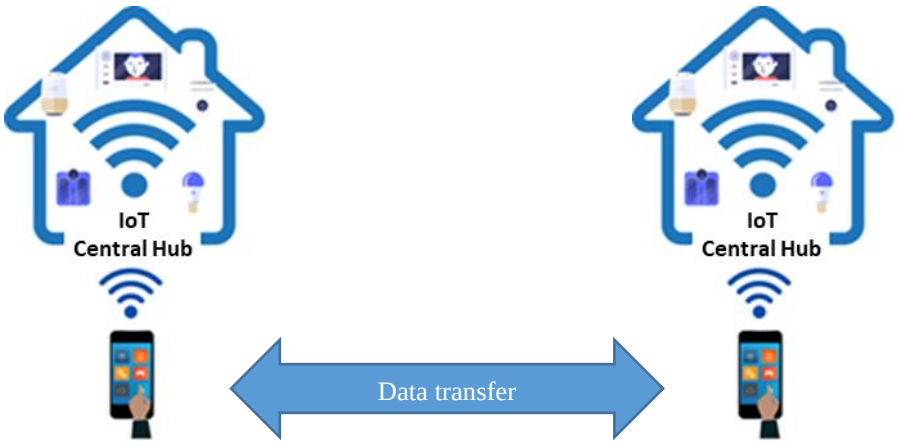

Figure 1 - IoT Central Hub environment

The IoT Central Hub platform integrates the functionalities of the devices identified within the local network, connection via wireless [1]network, in order to allow the management of all devices already registered in the application.

The prototype of the IoT Central Hub, in addition to managing it, also creates an environment that allows to quickly and simply identify all IoT devices that are within the range of the configured local network. Thus, the system facilitates the identification of device records automatically and simply, without complexity for the home user.

Finally, the IoT platform developed, it has a simple and intuitive interface so that users can operate it quickly and no complications and without any specific technical training.

The work of this project is developed in stages and gradually, with requirements and functional specifications being defined, detailing the project. Then, the technical development of the IoT Central Hub platform and tests to identify possible development and functionality errors are carried out. After the prototype is built, the results are evaluated through functional analysis and we conclude with usability research with users.

1.4. Methodological Approach

Initially, the research was carried out by basic bibliographies and published through articles, books, academic works, seminars, etc., based on documents made available by online searches that were identified as the state of the art and the trends in works carried out within the scope of researched technology (Carlos et al., 2002). Then, an exploratory work was carried out on the relevance of the theme, given the real purpose of solving the issue. A selection of criteria was carried out to refine the search and generate better results regarding the researched works.

According to Severino (Severino, 2014), technological advances have significantly contributed to research on academic works, raising the level of published works and making studies widely available to the entire scientific community with access to computational resources, strengthening scientific, cultural and academic commitment.

[1] Wireless: it’s kind of communication infrastructure that allows data and information to be transmitted without the need for cables

In order to facilitate research carried out based on scientific authors (Carlos et al., 2002) (Severino, 2014), the Table 1 was built to direct the readings relevant to the scientific work carried out on the topic addressed.

Table 1 - Research Table - Search Engine

DATABASES	KEYWORDS	ALL DOCUMENTS
ACM	"IoT"	11,008
	"IoT devices"	3,426
	"IoT Management"	47
	"Edge Computing"	1,476
IEEE	"IoT"	38,377
	"IoT devices"	5,893
	"IoT Management"	65
	"Edge Computing"	7,798
Springer	"IoT"	49,810
	"IoT devices"	7,682
	"IoT Management"	138
	"Edge Computing"	3,767
Web of Science	"IoT"	41,988
	"IoT devices"	6,507
	"IoT Management"	65
	"Edge Computing"	5,820
Scopus	"IoT"	67,408
	"IoT devices"	10,576
	"IoT Management"	90
	"Edge Computing"	8,738
TOTALS		1,745,773

Table 2 - Research Table – Refinement

KEYWORDS	ALL DOCUMENTS	TITLE OR ABSTRACT	YEAR > 2010	COMPUTER SCIENCE
"IoT"	1,488,818	99,248	45,824	9,373
"IoT devices"	147,137	14,804	17,990	1,549
"IoT Management"	26,461	182	24,418	300
"Edge Computing"	83,357	17,604	19,059	6,482
TOTALS:	1,745,773	131,838	107,291	17,704

According to Table 2, four keywords were used to search for publications relevant to the topic. However, many works were returned in which it was not significant for the

study in question. Then, a selection filter was approached to further refine the research work and allow for better assertiveness.

Table 3 - Research Table - Words Filter

KEYWORDS	BUSINESS MANAGEMENT	INNOVATION/TECH MANAGEMENT	KNOWLEDGE MANAGEMENT
"IoT"	3,127	260	16
"IoT devices"	1,569	151	9
"IoT Management"	2,269	191	14
"Edge Computing"	2,248	289	11
TOTALS:	9,213	891	50

According to Table 3, more assertive refinement was carried out with a focus on the relevant research topic. As the scope of study is related to the management of IoT applications and devices, the key word “management” was considered as the main one for the refinement of bibliographies. At that time, researches that were more aligned with the theme of application management and IoT devices found recently were selected, thus allowing a more consistent and assertive scientific basis for the IoT Central Hub project.

1.5. Structure and Organization

The present dissertation work is structured in five chapters that intend to reflect the different phases until its conclusion.

The first chapter introduces the subject of the investigation and its objectives, as well as a brief description of the structure of the work.

The second chapter reflects the theoretical framework and the fundamental theoretical concepts for IoT knowledge, cloud internet and network management technologies, called literature review.

The third chapter is dedicated to works related to the management of IoT devices already developed. The most relevant works on IoT management platform themes are addressed in a way that can contribute to the improvement of the project's development compared to what has already been built.

The fourth chapter presents the development in detail of the design of IoT Central Hub built, as well as the applied technologies and the architectures of the systems as they were structured, providing wide view of the work created for scientific contribution and future studies. In addition, the analysis of the test results obtained are carried out to identify the positive and negative points found in the scope of the study.

In the fifth and last chapter is the conclusions of the study are presented as well as the recommendations, limitations and future work.

2 Theoretical Foundation

This chapter presents the theoretical foundation for the IoT theme addressed in the introduction of this dissertation, with focus on IoT devices management. Initially, the meaning of IoT technology is presented, detailing the hardware, software and the main cloud computing systems. Then it is discussed how the integration and functioning of these types of technologies work and interact with each other.

2.1. Internet of Things (IoT)

The term internet of things (IoT) was known in late nineties by technological researcher Kevin Ashton in one of his conferences (Kevin Asthon, 2010). The concept of this emerging technology is basically the interaction between electronic devices connected to the internet, thus the internet of "things" denomimated today by smart lamps, appliances with computer systems, security systems with sensors and etc., thus, these objects became known as smart devices (Atzori et al., 2010).

All IoT objects' interaction is basically through the internet, collecting information and data for more accurate and appropriate decision for the user, as shown in Figure 2 (Marotta et al., 2013). Some characteristics of these interactions, to exemplify such behavior, are the detection of physical phenomena such as temperatures, light and humidity through sensors, computational capacity to analyze data and send response regarding a certain behavior, identification of physical objects, through format , size or movement, among others (Miorandi et al., 2012).

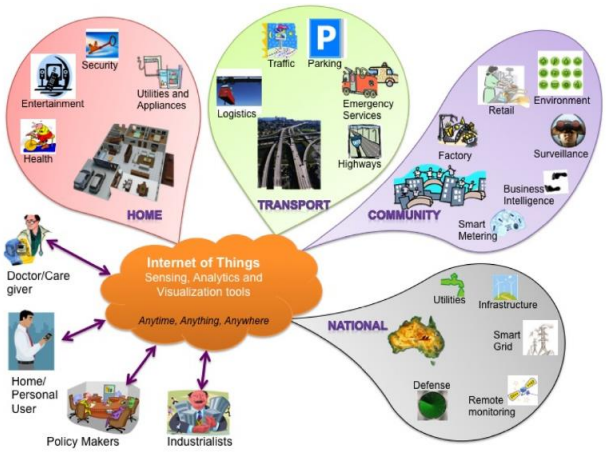

Figure 2 - Internet of Things Schematic. (Gubbi et al., 2013)

Smart devices connected, propelled the internet to higher technological level, where intelligent objects manage to bring facilities to business and people's private lives. But on the other hand, there are some concerns regarding this type of technology that are related to information privacy, technical complexity, difficulty of operability etc. (Miorandi et al., 2012).

Smart devices are composed of an embedded system containing electronic components, basically by microprocessors, a communication interface, usually wireless, power source and sensors. These sensors are electronic components that allow smart devices to collect information from the external environment and can also receive this information through other devices with the same functionality, creating a network of interconnected smart sensors (Vasseur & Dunkels, 2010)

Intelligent objects' behavior are still a "black box" in the world of science, as the behavior can vary according to the circumstances of the external environment and the interaction that may occur with other devices. However, this communication process can process a large amount of data in which the algorithms need to know how to interpret this information in a way that can make sense for the correct functioning of the device. For that, can be used algorithms of machine learning methods, genetic algorithms, neural networks and any other algorithms among on artificial intelligence to achieve the best possible results and with less processing (Gubbi et al., 2013).

2.2. Network Interfaces

There are several ways of intercommunication between IoT devices. But normally these communications are made through wireless networks of different technologies that vary in types, ranges, energy efficiency, frequency and even topology (Akpakwu et al., 2017).

WMAN (Wireless Metropolitan Area Network) and LPWAN (Low Power Wide Area Networks) are technologies that allow communication between wireless devices over long distances, such as: mobile device network, Sigfox, LoRaWAN and Narrowband IoT.

- **Mobile device network:** it's basically telecommunication technology network. The second generation (2G) was designed to transfer voice data

through wireless network, while the third generation (3G) technology was designed to traffic information data to access internet and the fourth generation (4G), also designated for data traffic trough internet, however, at a speed even bigger rather than 3G technology. But 4G has energy inefficiency which it does present a high energy consumption of the devices. With the technology of the fifth generation (5G), it aims to optimize the energy consumption of the devices and enhance the data traffic at high speed, being considered ten times faster than the previous technology. Given these characteristics, the 5G technology presents a synergy with the IoT technology, as it was designed for mobile devices with low energy consumption and high speed of data traffic (Talavera et al., 2015).

- **Sigfox:** it's an LPWAN technology that allows communication between IoT devices over long distances and reliably. It uses Ultra NarrowBand technology to transmit data efficiently and with high quality, as it transmits the message to the device at different times and frequencies, ensuring greater resistance even with interference on the way. The characteristics of a Sigfox network are the range of thirty to fifty kilometers in rural areas and ten kilometers in urban areas. The transmission rate varies from ten bps to 1000 bps[2]. The use of this type of technology is recommended for devices that have sensors and gauges, such as temperature gauges. On one hand this technology has great quality of transition as mentioned, on other hand the use cost of the technology is very high compare with others detailed on this research. (Peña Queralta et al., 2019).

- **LoRaWAN:** different of Sigfox's technology, LoRaWAN provides two-way communication technology, allowing devices to be controlled and send data at the same time when needed. Data rates vary from 0.3 kbps to 50 kbps, based on star topology and they are also based on LPWAN technology. Basically, LoRaWAN technology has the advantage of long-distance transmission and the disadvantage of small packet transmission. (Miles et al., 2020).

[2] BPS (Bits per second) is a standard way to measure data transfer rates, such as network connection and Internet download speeds.

- **Narrowband IoT (NB-IoT):** is based on LPWAN technology related with new standard of 3GPP [3]wireless cellular technology. Developed to allow several types of IoT devices and services, it has good energy efficiency, low cost and an optimized network architecture. This technology has been widely used in smart parking, utilities and industrial solutions (Abbas et al., 2020).

Unlike long-distance network technologies, such as short-distance technology networks, it also plays an important role in the operation of IoT devices, which we can highlight, RFID (radio frequency identification), NFC, Bluetooth, ZigBee and WiFi.

- **RFID:** basically, it is a technology that uses the radio frequency to transmit data. This technology automatically identifies objects according to which data is captured and is popularly known as radio frequency tags. The operation is basically through the transmission of data via an antenna, which emit radio wave signals to the reader where it identifies the object and is processed by the computer. Through this technology, RFID tag technology was developed, where today it is widely used in the patchwork store and in several other sectors. This system is basically composed of two components, the tags that are fixed on the objects to be identified and a reader to receive the object's information and be processed by the computer (Gubbi et al., 2013).

- **NFC:** it means, near field communication, this technology makes it possible to exchange information through two nearby devices without the need for wires. It works at a frequency of 13.56 MHz[4] and in a completely safe and automatic way without the need for configurations on both devices. Normally, this type of technology is present in mobile devices, cards and electronic tickets, bracelets etc. (Liébana-Cabanillas et al., 2019).

[3] 3rd Generation Partnership Project (3GPP) is a generic term for various mobile protocol development standards organizations.
[4] Hz is a unit of frequency measurement in terms of cycle per second.

- **Bluetooth:** it is a worldwide standard for wireless data communication. This technology allows communication between several devices with the same technology with approximately ten meters at most. The transmission is carried out by a radio frequency network that allows the identification of another device automatically. Bluetooth technology has undergone several changes in order to increasingly enhance its performance in energy consumption of devices and in the speed of data transmission. This type of technology is very present in mobile devices, computer accessories, electronics etc. (Mercader & Haddad, 2020).

- **ZigBee:** it is a low power network with low energy consumption. Developed by ZigBee Alliance in partnership with IEEE. This technology is more used with devices on few data transfer, being inferior to Bluetooth in 4 times, reaching up to 12 times less data transmission. But compared to Bluetooth it has the possibility to connect a large number of devices on the same network, as well as high battery life of the devices (Ramya et al., 2011).

- **WiFi:** it is a wireless local area network technology, called WLAN (Wireless Local Area Network), standardized by the 802.11 code by the IEEE [5]company. The use of this technology allows communication between devices that are connected to each other through the same technology. The data is also transmitted by radio frequency, creating an area limited in scope to the connected devices and secure by numerous forms of data encryption. This technology is very popular in several domestic or even business environments (Gubbi et al., 2013).

2.3. Edge Computing

Edge Computing is a technology that brings a mixture of data storage and computing processing, avoiding excessive data throughput, bringing computational benefit to the

[5] IEEE (Institute of Electrotechnical and Electronic Engineers) is an institution founded in US dedicated to advancement of technology.

users. The origin of this technology emerged in nineties with the work of connecting clients to servers through the internet. This technology has evolved and gained its space in IoT area where it was very well adapted in a way that it can assist the processing of intelligent devices on effective way (Kramp et al., 2013).

The costs of that type of technology have constantly reduced according to the advancement of technology, facilitating more the employability of those resources. Today, these devices are easily found in people's daily activities, such as in supermarkets, shopping malls, schools, etc (Kramp et al., 2013).

2.4. Cloud Computing

Cloud computing is an increase technology with several computing resources available over the internet. The consumption is based on resources need to use the specific service. The resources available for this type of technology are; data storage, systems applications, software development applications and others (Mell & Grance, 2011).

The cost of this type of technology is associated with the amount of resources and capacity required for each contracted service. In this case, the user can hire only one or all of the service features that are available for each cloud computing server, for example, the user can hire a 1TB[6] hard drive or simply all the features of computer, it with processor, memory, data storage and etc. (Mell & Grance, 2011).

Cloud computing can usually be classified in three ways, public cloud, private cloud and hybrid cloud.

- **Public Cloud:** they are cloud service providers that are available for public use, then, anyone can easily hire this type of service. These services can be free, but with limited use or they can be paid resources, as it can pay as you use model. Computational resources are shared between users and infrastructure security is the responsibility of the provider (Jadeja & Modi, 2012).

[6] TB (Terabyte): it’s a multiple of the byte unit for digital information.

- **Private Cloud:** it has the same characteristics as public clouds; however, the difference is that the data center is exclusively dedicated to a single company and there are no resources sharing. Thus, the cost of this type of technology is higher and normally, it's dedicated to a single company (Jadeja & Modi, 2012).

- **Hybrid Cloud:** on hybrid services, there are characteristics of public and private clouds. This structure is basically an architecture of private cloud with associated public cloud resources. This structure has the advantage of maintaining the services used in the dedicated datacenter for internal services of the organization and allows to associate with external services through the architecture of public cloud (Jadeja & Modi, 2012).

With large variety of existing computing services available, cloud service providers have classified into three main types of services available for users and companies to contract according each business needs. According Figure 3, it can be noted the three types of services, such as Iaas, Paas and Saas (Zhang et al., 2010).

Figure 3 - Types of Services. (INAP, 2009)

The three categories types mainly known are IaaS, Paas and SaaS and on figura 4 it can identified all services in each category (Zhang et al., 2010).

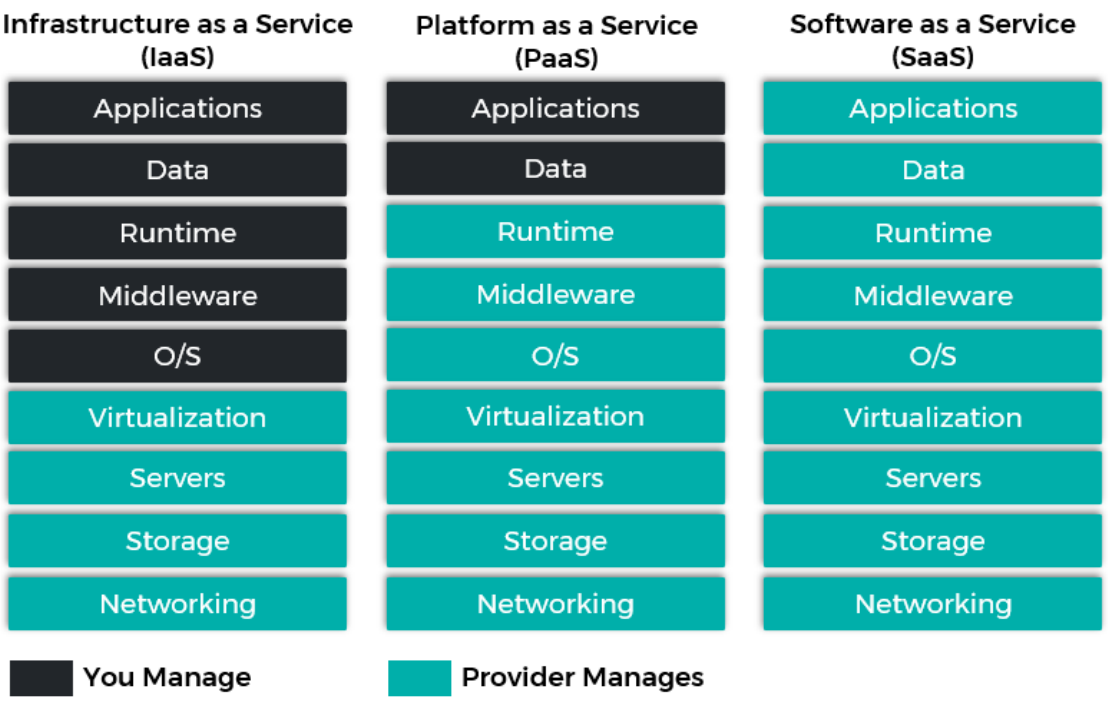

Figure 4 - Types of Services. (Heimdal, 2020)

- **IaaS (Infrastructure as a service):** this type of service providers can offer virtual servers, with physical computing resources with network connectivity and IP addresses, without the need to purchase a physical computer to have the service available. In addition, you can upgrade quickly and conveniently through the provider's virtual environment (Jadeja & Modi, 2012).
- **PaaS (Platform as a service):** it was developed in order to provide users with access to essential components to operate and develop applications, without the concern of setting the environment. Thus, companies and users are free to use applications without having to buy licenses and permissions to access servers, firewalls, databases and etc. (Jadeja & Modi, 2012).
- **SaaS (Software as a Service):** it allows users to use software applications directly from the cloud, without worrying about installation and configuration features (Jadeja & Modi, 2012).

2.5. IoT Management

Each year the number of IoT devices has grown more and more. According to Cisco technology and infrastructure development company, believes that smart device

technology is on rise in the market and estimates that by the end of 2020, 50 billion smart devices can be reached in the world (Ibsg & Dave Evans, 2011). However, this great demand for interconnected smart devices, demands a high need to have a more complete and detailed management of these devices, in order to reduce their complexity (Yin et al., 2020).

IoT management systems must consider security factor as a very important pillar to be researched to prevent access by unknown devices, data leak, security changes and so on. According to Delicato (Delicato et al., 2013), IoT management systems need to have a dynamic feature in the identification of objects in order to avoid the pre-definition of device configurations, thus making potentiation the safety factor that is essential in this type of technology.

Besides the security issue in IoT management applications, other points are very important to be considered and implemented, according to Chaqfeh (Chaqfeh & Mohamed, 2012). Scalability brings the possibility of expanding the technology and the functioning of the application's functionalities. Within the scope of automatic portioning, it helps in the dynamic and easy functioning of device activations. At the point of data science, the important thing is in the treatment of information, in order to make the devices work properly and allow them to have the most assertive response possible to users. And finally, interoperability in heterogeneous environments where devices of different characteristics, brands and functionalities are present so that they can communicate without much complexity.

The lack of standardization and definition of this type of technology, greatly increases the complexity and interoperability of smart devices. Because each IoT application presents a unique data structure in order to adopt different programming models that are not compatible with each other. Thus, it is necessary to create a set of data structures for the environment of smart devices that are called reference architectures. These architectures have a characteristic of facilitating and guiding the standardization of systems development for this technology (Nakagawa et al., 2011).

2.5.1. IoT system architecture

The reference architecture, by definition, is the composition of one or more reference models, in order to allow standardization, avoiding the ambiguity of information unifying

business rules, structuring systems architectures, creating good software development practices and alignment of hardware operation. Thus, the main objectives of the reference architecture can be achieved (Nakagawa et al., 2011).

The main objectives of the reference architecture according to Nakagawa (Nakagawa et al., 2011) are to facilitate software development, enabling time optimization and construction reduction and testing. Architecture systems standardization, in order to establish a reference architecture in terms of essential elements to define guidelines, integrations and compatibility between totally different systems. And finally, manage the evolution of existing systems, allowing to create a natural process for the evolution of new features without impacting those that are currently running.

The IoT reference architecture model (IoT-A), developed by researchers' group from Europe and Brazil (Kramp et al., 2013), it was a project created in the context of the development of a European IoT reference architecture. This architecture is based on the construction of set key characteristics, it defined at high level of abstraction, allowing a broadly dynamic view that can be used in any phase of the project, from functional development to production.

The functional vision defined in IoT-A architecture, it has nine groups of functionalities, namely: (i) application; (ii) management; (iii) service organization; (iv) IoT process management; (v) virtual entity; (vi) IoT service; (vii) security; (viii) communication, and (ix) device. These functional groups can present one or more components simultaneously, as detailed in Figure 5 (Kramp et al., 2013).

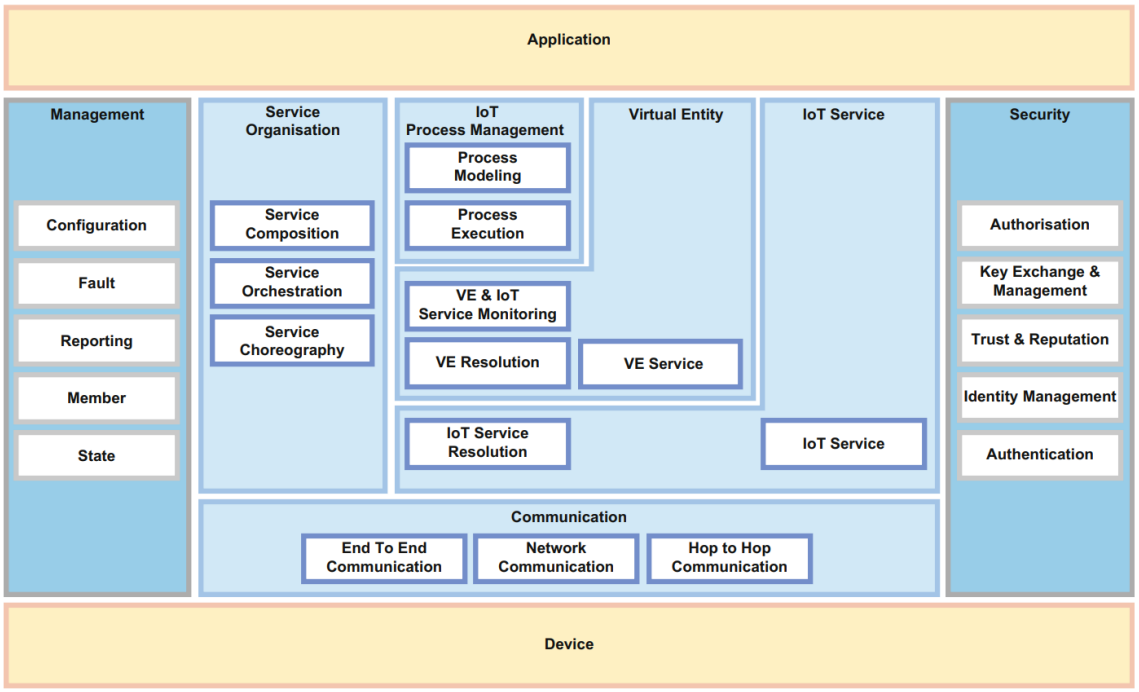

Figure 5 - IoT-A Functional decomposition, (Kramp et al., 2013), p.168

Security item functionality group is completely transversal in this reference model compared to the others, being classified as high important item (Kramp et al., 2013).

2.5.2. Security

In IoT communication data transfer topics, information security is an important factor, as it deals not only with privacy, but also with the integrity of interconnected devices. Then, it to be able to guarantee security on the network, countless data protection techniques are used to block any interference noisy in data treatment, preventing malfunction of the device or generating inefficient information for users. Furthermore, locks on access doors, use of security protocols, multi-layer authentication etc. can be used (Jan et al., 2015).

Smart devices plurality and heterogeneity pose numerous challenges for protecting and preventing devices and data integrity. That is why each system creates its own security and authentication method to protect information. This concern for protection and security expands much more with connectivity to the internet, as the various technologies and forms of connectivity present an increasing challenge for authentication and

certification of information that can serve efficiently, transparently and respecting all user data privacy rules (Jan et al., 2015).

2.6. Chapter Summary

In this chapter, fundamental theoretical concepts were presented to support and direct the contents that are specific in this dissertation on IoT device management subject. It is possible to realize that information security is a critical and essential factor for proper functionality of this device type. In addition, to the complexity of integrating smart devices in a way that can relate in simple and reliable way, the information treatment flow is also identified as an attention point and generation of information organization and proper devices function. In summary, the data must be properly structured, adequate connectivity and information security, as well as usability are highlights in this session. In the next chapter, the main related works regarding IoT management platform topic are discussed.

3 Related works

IoT management platform Technology is very recent and growing subject in the literature, as its already mentioned in chapter 1, in the introduction of this work. These platforms act as an intermediate layer between hardware and software, creating an integrated communication of the system architecture. These layers simplify the complexities and heterogeneities of the devices, facilitating resources' management and improving the execution of developed applications (Razzaque et al., 2016).

In several related works researched, a complexity in the treatment of data was identified due to the high volume of information transferred between the application and the device. For this reason, this subject was a topic present in all researched and identified as a pillar to allow the correct functioning of applications and devices (Atzori et al., 2010).

Another critical point identified in the research of related works is security. Many works have identified a minimal security control, allowing greater systems' reliability. However, the security issue is not the isolation topic on the application layer, but it also involves the network layer as an essential point to allow greater information reliability (Pires et al., 2015).

Thus, this chapter will discuss the related work regarding IoT platforms developed within the scope of this study. All research was based on the application's functionality and operability so that it could present reliability in information, security and performance. Therefore, topics such as information management, systems architecture, data and device management, heterogeneity, security and privacy, scalability and reliability were analyzed.

All works researched for this dissertation were the ManIoT platform (Antunes, 2016), which it allows local and remote devices management, being expandable, allowing the addition of new devices. Another platform studied was the platform called AutoDev (Rodrigues, 2018). This work was developed a prototype of an application capable of managing IoT devices using Raspberry Pi technology under a Linux operating system. However, the prototype developed by Marotta, presents more friendly interface and easy usability. It was developed in Java and its web based. This platform is called "Management by Delegation Smart Object Aware System for IoT" (Marotta et al., 2013).

Another researched platform, also based on the web, is Jemadarius (Barros, 2015). Being considered self-configurable, easy usability and configuration performed through API's.

Finally, this chapter will detail the features, architectures, benefits and results found in each one IoT application. In addition, a comparative table will be presented with the identified characteristics of all the applications researched and presented in this session.

3.1. ManIoT Plataform

The ManIoT platform is similar to IoT Central Hub platform in order to allow centralized management and easy integration between devices. These integration features of the devices, it facilitates the creation of new services such as capturing the luminosity and controlling the rate of light emission of a smart lamp. In addition, it allows controlling the lamp through the user's geographic position to indicate whether it should not work (Antunes, 2016).

Like IoT Central Hub, the platform provides generic services for automatic device identification, data storage and user profile authentication. Also, the platform performs the total management of the device remotely or locally according to the positioning of the user, it is just having administration permissions to perform this function. The main ManIoT platform requirements are the same those presented basically in the existing IoT systems on the market (Gubbi et al., 2013), such as; allow the heterogeneity of devices with different types of communication processing. Allow user authentication and access control for platform management and control. Expansion facility for adding new devices. Use of protocols already known in the market. Make use of data model and a coherent information model in a way that allows the simplified data structure and that facilitates the programming of different brands. Therefore, the definitions of the main functionalities developed for ManIoT platform are similar to IoT Central Hub platform (Antunes, 2016).

ManIoT management platform features have a local and a global architecture. The management of the local environment is carried out within the network itself and objectively managed all the IoT devices present on the platform. However, the global architecture environment allows remote device management, connected via the internet, allowing management of more than one configured local environment. As shown in Figure 6, it is possible to verify how this integrated operation is structured, being local and global (Antunes, 2016).

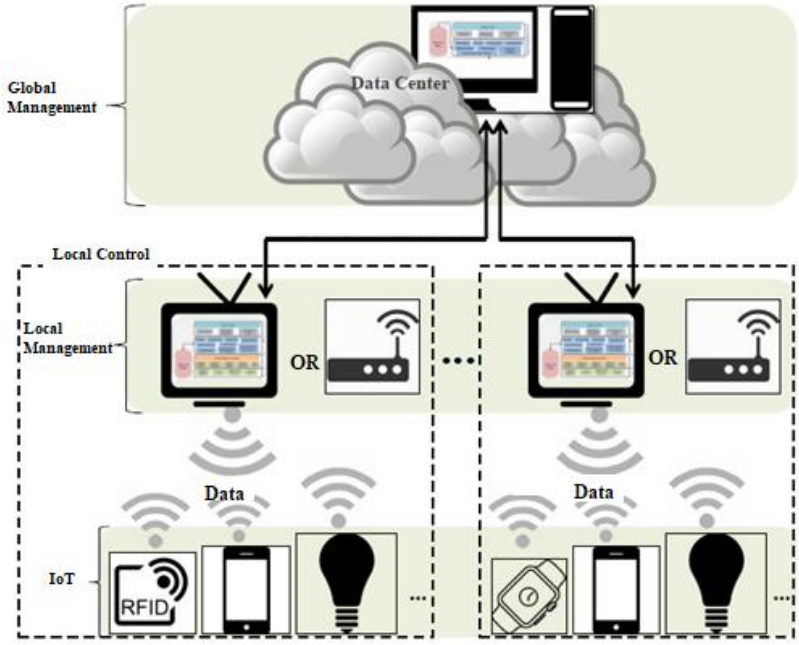

Figure 6 - ManIoT plataform topology, (Antunes, 2016)

The means of communication between the local and global architecture is entirely accomplished by connection using the TCP / IP protocol through a web interface where it is possible to access the application from anywhere in the world. The access control, it was built access by users, making it possible to have common access, where only restricted control of functionality is allowed or access as an administrator, in which you have broad permissions to control the application. In addition of globalized communication, the application has a standardized data model and information model structure that allows a simple and easy service communication, applications and devices. All of those are based on the requirement of heterogeneity which were mentioned at the beginning of this chapter (Antunes, 2016).

In information model, the devices status can be turned on or off and the smart devices' identification tag that were defined for each device identification. Thus, to maintain compliance and allow the platform to expand, a set of protocols are used in the data model such as XML and REST, facilitating data integration and communication between devices and systems (Antunes, 2016).

In ManIoT platform software layer has three layers in the local environment and two layers in the global environment. However, the first two layers of the two environments

are similar as we can see in Figure 7, which details the layers of the local environment and in Figure 8, which details the layers of the global environment.

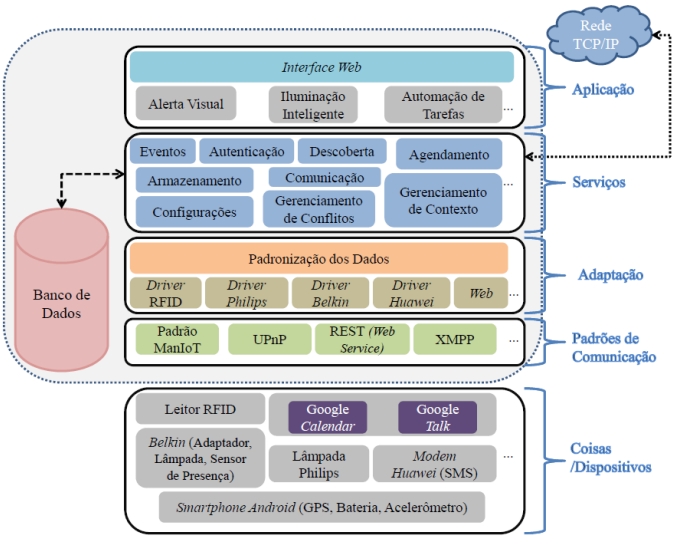

Figure 7 - ManIoT Local environment, (Antunes, 2016)

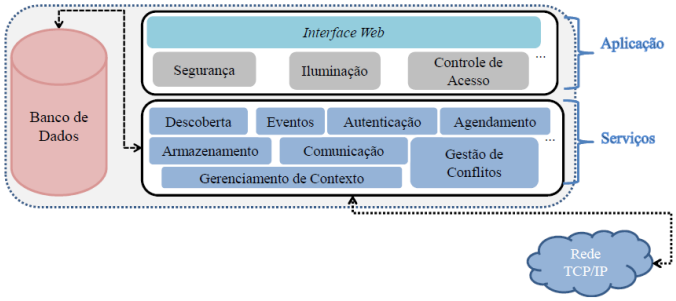

Figure 8 - ManIoT Global environment, (Antunes, 2016)

The first layer of both environments is the application front end layer. In that layer, the user initiates and terminates the communication channel with the platform through an intuitive and simple interface to manipulate. In the service layer, its where the platform translates and communicates all functionalities, using the abstractions implemented by the "drivers" that support the services. The third layer involves the adaptation and communication standards of the platform. This layer is composed of different types of access protocols to devices, composing the network by devices that can use different application protocols, facilitating communication between devices. And finally, the layer called “things or devices”, is the part that is composed of the IoT devices that are

connected to the platform through the communication protocols mentioned above (Antunes, 2016).

3.2. Automatic Device (AutoDev)

The prototype of the system called AutoDev was developed with the same essential as IoT Central Hub. The main purpose of the application is to reduce the complexity of using the IoT device identification system automatically. Thus, the home user has the facility to identify smart devices added to the same network in a fully automatic way and with an intuitive interface (Rodrigues, 2018).

The AutoDev application, similar to IoT Central Hub, aims to reach all users without age restriction, but for this, it was necessary to meet some basic functional requirements to be able to develop an architecture with the features of good performance, extensibility and flexibility, security, intuitive features and comfort for home users (Rodrigues, 2018). Since AutoDev application aims to reduce complexity and increase the ease of handling for the home user, the system was developed to adjust in a practical and objective way the functionalities of the devices generically. Thus, the application uses a common configuration profile in which all IoT devices have and accesses this information through USB, Bluetooth or any other connectivity available with each device. Information is transmitted via XML, JSON or YAML[7].

The structure of AutoDev application architecture consists of 3 layers; communication, service and configuration, as shown in Figure 9. In the communication layer, it is composed of a set of libraries that allows abstracting the communication protocols of the application. However, to configure devices via Ethernet or NFC, a specific configuration process is required. But if there is no device already configured, it will be necessary to configure it by NFC technology in contact with the smartphone that allows the configuration of the application automatically. But for this, the user needs to be aware of the configuration parameters of each device that will be configured. Finally, in this layer, the HTTPS protocol is responsible for protecting the application to carry out this configuration transaction via web service (Rodrigues, 2018).

[7] YAML (Yet Another Markup Language) is a human-readable data serialization language.

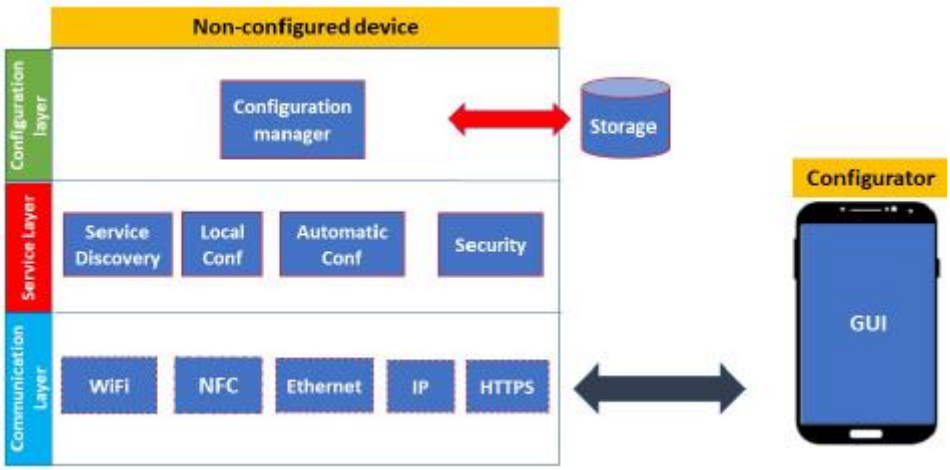

Figure 9 - AutoDev System Software Architecture (Rodrigues, 2018)

The the service layer is the next one, where the identification and translation of information is carried out to the configuration in the application. It is in this layer that the type of device that is being located on the network is identified, for the application, the Apple Bonjour protocol was used due to its configuration stability. To complete this layer, a security service was added to allow greater reliability and confidentiality of the data processed during the configuration process. The connection is made over a secure connection using TLS technology. Thus, all information exchanged between the application and the devices is encrypted and certified for data authenticity (Rodrigues, 2018).

Finally, there is the configuration layer, the purpose of this layer is to add and manage the settings received from the devices. In addition, there is a communication interface with the database to store the old information and user profiles for each type of configuration, thus allowing a simple and transparent translation for the home user (Rodrigues, 2018).

3.3. Management by Delegation Smart Object System for IoT (MbDSAS)

Like IoT Central Hub, the application of MbDSAS has the purpose of performing the management of IoT devices. However, the application was developed for more specific purpose, with the intention of managing the information that is received from the IoT devices, to exemplify such operation, the application can be used as an IoT device manager for airports, train stations, etc. In this case, the platform controls temperature

measurements, brightness and functionality adjustments as detailed in Figure 10, where it details the generic scenario that can be applied on this application (Marotta et al., 2013).

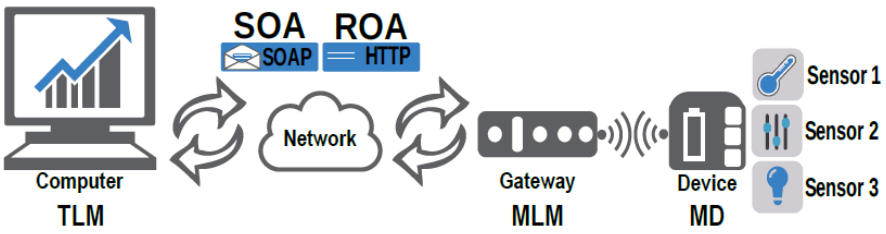

Figure 10 - MbDSAS generic scenario, (Marotta et al., 2013)

TLM is a management station where the IoT management application is installed, which can be a computer or a mobile device. This station was developed to allow consolidating the management of all the information that is captured from IoT devices. The communication of this system is made through the internet by webservice that communicates directly with the middleware layer called “Gateway MLM”. This layer is responsible for orchestrating all the data from the IoT devices and forwarding them to the TLM application through the SOA or ROA services. In the device layer, the device is responsible for capturing data collected in environment, for example, at the airport, at school, at the stadium, etc. and it sends the information to the gateway to process the information for IoT management application (Marotta et al., 2013).

The conceptual architecture of the MbDSAS application is composed of the components mentioned above and it can be seen in the architecture defined in Figure 11. Basically, the information management is defined in the TLM layer, where there is the application management, then MLM layer has the information processing function and both layers consult the database and store the information collected from the IoT devices. Finally, the MD layer is where the IoT device collects information from the environment to forward to TLM to analyze the data (Marotta et al., 2013).

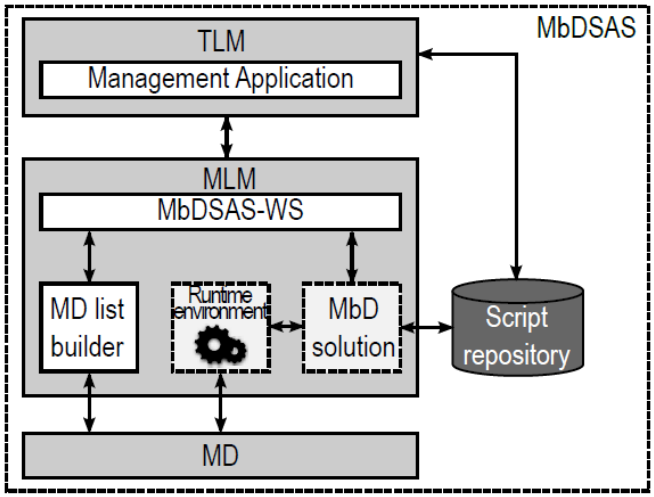

Figure 11 - MbDSAS conceptual architecture, (Marotta et al., 2013)

This architecture has a generic application characteristic, being possible to be applied in several business sectors, having the focus on performance and treatment of information in more efficient and effective way to generate a better result for the users.

3.4. Jemadarius (Web-API IoT Auto dectect)

The platform called Jemadarius is similar to IoT Central Hub platform in the scope of basic detection and configuration performed in an automated way with minimun human intervention. It is a web application developed to perform the self-configuration of IoT devices on the same local network through Contiki [8]and a low energy consumption technique, carried out through the CoAP [9] protocol (Barros, 2015).

The main purpose of this application is to optimize the work of configuring and adjusting IoT devices within the same network. This way, the user will not find any complexity in the configuration and will help to reduce the time wasted with basic configurations of these devices. However, to make this structure work, the user needs to run the Jemadarius application through the input of IoT devices available on the network, thus, CoAP methods will be made available to the server to receive the information and run the programs. The application will consult the configuration policies that will define

[8] Contiki is an operating system for memory-constrained networked systems, focusing on low-powered wireless Internet of Things devices.

[9] Constrained Application Protocol (CoAP) is a specialized Internet Application Protocol for constrained devices, as defined in RFC 7252.

the action and it sends the code to configure the device, as shown in Figure 12 (Barros, 2015).

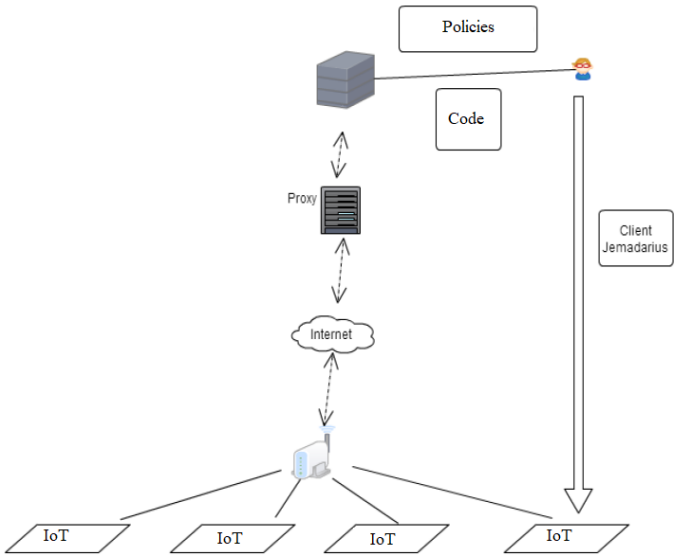

Figure 12 - Jemadarius Architecture, (Barros, 2015)

Jemadarius architecture has similar feature to IT Central Hub. Both are focused on reducing the complexity of configuring IoT devices within a local network. In this way, the architecture of Jemadarius, was developed to solve two main problems. The first is the configuration complexity that the IoT devices have when connecting with the configuration applications. The other is the reconfiguration of these devices, when they need to be reconfigured in the application. Thus, the user needs to remove it from the network and reconnect it to the application through "over-the-air" programming, which makes the new configuration codes available to devices that are within the transmission radius by "over- the-air" Deluge [10]at Contiki. (Dunkels et al., 2006).

The architecture structure developed for the Jemadarius project is formed by client and server through Web services with REST communication through a server in the cloud and the device that uses CoAP to communicate with the Web-API that performs all the self-configuration in the Contiki. On the client side, the service is performed by an application developed in C language, structured in a way that has low energy consumption and processing. Thus, on the client side, three methods are available on the server side; file

[10] Deluge is a free and open-source, cross-platform BitTorrent client written in Python.

transfer, file execution and data collection. Thus, the application receives a GET from the device to send the specific configuration characteristics, identifying the code that is returned to the application to start the autoconfiguration. Communication on the client side is carried out through the CoAP-13 protocol and on the server side the HTTP internet protocol is used, so it is necessary to use a Proxy to carry out the communication translation between these two protocols as shown in Figure 13 (Barros, 2015).

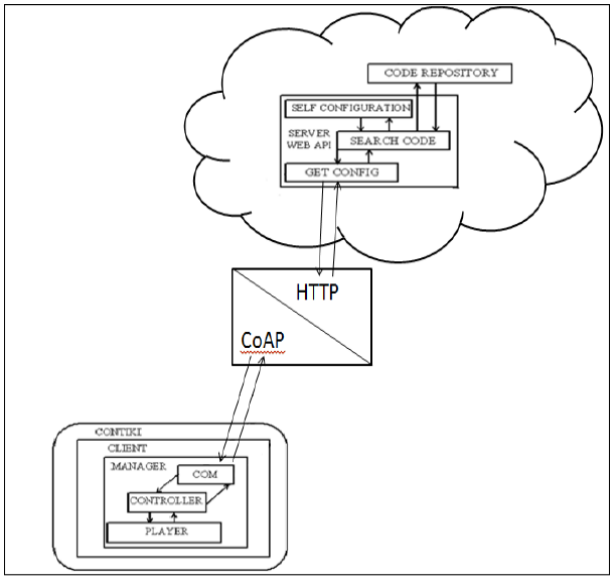

Figure 13 - Jemadarius Architecture, (Barros, 2015)

In the server structure, the Jemadarius Web-API was developed in PHP language and in the Symphony framework, using the HTTP protocol for communication, having one divided into four parts: User, Motes, Proxy and Files.

3.5. Comparison between applications

The applications' characteristics of the works developed were synthesized in this session so that the comparison between all the prototypes of related research works can be analyzed. In the Table 4 has the demonstrating purpose which features, and characteristics are present in the work developed and compared with the purpose of this thesis, with the development of IoT Central Hub platform. Because of that, the symbologies were determined for easy understanding of the features that are present, determined by the symbol (✓). However, when the feature in question is not present, it

is marked with the symbol (✕). And if it is not applied for the given item, the option is characterized as (N/A), also when it characterized as (●), it will be applied in future works. In this way, it can clearly perceive the characteristics that are or are not present in comparison with IoT Central Hub platform.

The main characteristic identified in the researched works was the heterogeneity functionality for IoT devices. Being considered one of the main items and was addressed in focus by several works, in the same way as it was treated by the prototype of this work. In addition, safety is like the other very relevant and present point in the works. Because the privacy of data and information that is transmitted over the network must be kept secure in order to prevail the integrity and security of information. Therefore, it is crucial that applications provide security strategies so that they can maintain the protection of the devices involved in manipulating data on the network. (Pires et al., 2015).

Connectivity technologies are also widely addressed in authors' works (Antunes, 2016), (Rodrigues, 2018), (Marotta et al., 2013) and (Barros, 2015), being cited as an auxiliary characteristic, due to the numerous connection possibilities that are available on the market today. Since for the work of IoT Central Hub it is not intended to focus on the scope of the connectivity of IoT devices, the proposed work was simply focused on wireless network connectivity, being sufficient to meet the need for connection between the device and the developed application platform.

Table 4 –Application comparation table

	MainIoT	AutoDev	MbDSAS	Jemadarius	IoT Central Hub
Heterogeneity	✓	✓	✓	✓	✓
Security	✓	✓	✓	✓	✓
Privacy	✓	✓	✓	✓	✓
Scalability	✓	✓	✓	✓	✓
Usability	✗	✓	✗	✗	✓
Autoconfiguration	✓	✓	✓	✓	✓
Cloud Access	✓	✓	✗	✗	●
Data management	✗	✗	✓	✓	✗
Device management	✓	✓	✗	✗	✓
Client / Server	✓	✓	✓	✓	✓
Remote management	✓	✓	✗	✗	●
RFID	✓	✗	**N/A**	**N/A**	**N/A**
Bluethoot	✗	✓	**N/A**	**N/A**	✓
Wi-Fi	✓	✓	✓	✓	●
NFC	✗	✓	**N/A**	**N/A**	**N/A**

The client and server structure are topics that is covered by all works and is based on the structure centered on information so that it can be accessed from anywhere. However, data management and remote device management are characteristics that are present only in two of the four applications researched, thus, a point of relevance regarding the work of IoT Central Hub where it is possible to perform data and data management devices in a simple and intuitive way (Marotta et al., 2013) (Barros, 2015).

Finally, usability was not addressed in a relevant way in the researched works, only one of the works was concerned with making usability easy and simple for the user (Rodrigues, 2018). Thus, it has already mentioned at the beginning of this work, usability is an essential topic because it aims to help the user to manipulate information in a simple and uncomplicated way.

3.6. Chapter Summary

In this chapter some applications were demonstrated where they present characteristics similar to IoT Central Hub platform. In general, the researched works present more intense concern with interaction and connectivity part of the devices, but in terms of usability, ease of handling the application and simplicity of information are subjects in which they are partially addressed in the research and raise little concern with that topic. However, the IoT Central Hub platform, in addition to allowing automatic connectivity, also allows having a concern with the way information is used by users, in order to provide an easy and intuitive interface to simplify users' lives.

In the next chapter, the features and characteristics of IoT Central Hub platform will be detailed, as well as the architecture and structure used to develop practical and easy prototype for the user.

4 IoT Central Hub Project

In previous chapters, it was detailed main contributions of IoT devices' functions, as well as the benefits they can bring to home users in their basic activities. In addition, prototypes were developed and elaborated by other researchers that could contribute highly relevant information to the evolution studies of the IoT Central Hub. An IoT service management platform with easy automatic device recognition system in the same local environment, which reduces installation and configuration complexity in devices when it is found by the platform with no obstables, thus enabling any user to use this prototype easily and quickly which is not required huge technology knowledge and it also needless specific market manufacturer brand use, so it allows being highly universal platform to reach any smart device brand in the market.

In this chapter, it's described the relevant information of IoT Central Hub prototype development, as well as its essential characteristics for the appropriate application functions, functional requirements, application design and technical information on the application structure. Also, the application architecture is widely detailed, such as, the layers and components that enable the IoT platform works properly.

4.1. IoT Central Hub Requirements

The impact of IoT technology in the market has been increased every day, it brings countless benefits to users of functionality types, such as ease of collecting information from the local environment (temperature, location data, etc.), handling devices remotely, agility in daily household activities, automation of tasks, monitoring behavior of features easily and so forth. Thus, IoT Central Hub brings this whole concept encapsulated in a simpler and easier way for the home users. Although there are already numerous applications that allow to have the same behavior as the IoT Central Hub, most device management platforms still have high installation and usability complexity, so the main objective of IoT Central Hub prototype is strongly reduce complexity and it allows more flexibility to the home user as on the market there is still few applications available.

The automatic management platform of IoT Central Hub already meets some main requirements of application type, such as heterogeneity, extensibility, privacy and usability. IoT Central Hub prototype must meet the following key system requirements:

- **known protocols in the market:** it is recommended to use protocols technologies and platforms already existing in the market and recognized in computer network area.

- **Environment identification devices:** it is expected that application automatically identify the devices that are available and visible to the IoT Central Hub automatic management application.

- **Installation and automatic configuration:** through the devices already identified by the application, it is recommended that an initial connection be made where data authentication is performed by the local connection (local network or Bluetooth) and the installation started if it is the first connection and the configuration of the new connected device.

- **Device management:** it is recommended that the platform is able to manage the devices found in the environment, being able to manipulate the data and control the devices.

- **Definition of data and information model:** the application must provide a data and information model for the supported devices, in this way, the data model will facilitate the programming devices use from different manufacturers.

Following the definition requirements presented, the automatic IoT device management platform, it should create simple and intuitive identification and installation processes, reducing as much as possible the complexity for the home user, allowing an optimized experience, totally comfortable and simple for the users.

4.2. IoT Central Hub Application

The smart device management platform, IoT Central Hub, is composed of an application installed on the user's mobile device, where it is possible to make the local tracking of IoT devices present in the same local environment through a wireless network connection or Bluetooth.

For devices that have available tracking visibility enabled, IoT Central Hub application initiates an attempt to establish a connection with the device and check for access or security restrictions to authenticate and authorize the connection. If the connection has been approved or there is no access restriction, the application starts the process of configuring and enabling the device to be used and configured through IoT Central Hub management platform.

Initially, the idea of using cloud connection was created to further expand the functionalities of IoT Central Hub application. However, during the concept of the prototype, a high complexity of code development was identified to synchronize information with the application locally and control the devices remotely, configuration of new devices identified, installation of technological infrastructure and availability of time to complete the study of the project. Due to all these restrictions of the prototype development, the configuration structure and cloud development was left to future work to be better exposed in future research.

At the beginning, to realize short distance connectivity it was considered using Bluetooth or Zigbee, in addition to Wi-Fi technology. However, it was decided to use Bluetooth technology instead of Zeebig technology, because Bluetooth has better connectivity with mobile devices, in addition, to have higher data transfer rate, as it was mentioned in the theoretical foundation chapter in this research.

The platform provides the devices' identification through wireless technology connectivity, such as cableless networking and bluetooth as already mentioned, so in this way, when device searching is started, it looks for available devices in the vicinity for an approximate time of 3 minutes. At the end of this time, the application ends the search and lists all devices found nearby and displays those available to initiate a connection, as shown in Figure 14.

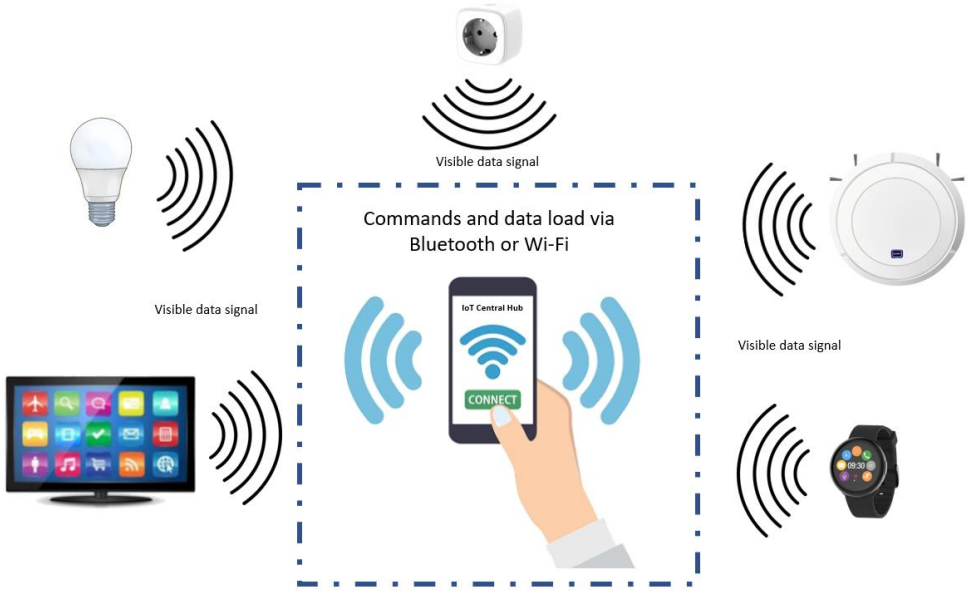

Figure 14 - IoT Central Hub Architecture

IoT Central Hub application considers the heterogeneity of devices, allowing connectivity from different manufacturers without having to be linked to a single brand in the market. As such, the platform does not require additional application installations from each manufacturer, as is often required when purchasing a brand-specific device.

The prototype developed for managing IoT devices is carried out through an application running on mobile devices, developed in Java programming language, using the integrated development environment (IDE) Android Studio to create the functionalities of IoT Central Hub, as well as the user interfaces created to optimized performance, comfortability, and usability to everyone, without any expertise on computer technology.

Regarding platform's data model and information structure, the application aims to create a standardization in data format and communication between the developed application and the connected devices. Thus, device identifier and connection status are examples of data structure characteristics used for device management. In order to allow wide integration and extensibility of the application with other systems, the prototype of IoT Central Hub uses the most common protocols and standards among developers for the structure of data models such as XML and REST.

The simplified communication and well-defined data structure are the main characteristics of IoT Central Hub application development, being these one of the biggest

enablers of the project in order to create a simple and easy-to-use environment for the home user.

4.3. IoT Central Hub Architecture

IoT Central Hub management platform architecture is composed of a smart device and a developed smart device management application. Differently from other researched works, as detailed in chapter 3, IoT Central Hub application does not need an intermediary hardware to perform a connection gateway with the devices, making it even easier to connect to the devices automatically. In addition of simplicity connection device, the other point that benefits this type of architecture is the additional cost to purchase a gateway device for every manufacturer in the market. Thus, avoiding an unwieldy accumulation of additional apparatus for the management of IoT devices.

IoT Central Hub application platform is composed of layers that allow data going through efficiently and structured within the application. As shown in Figure 15, IoT Central Hub application architecture is structured in three layers: Application, Services and Communication.

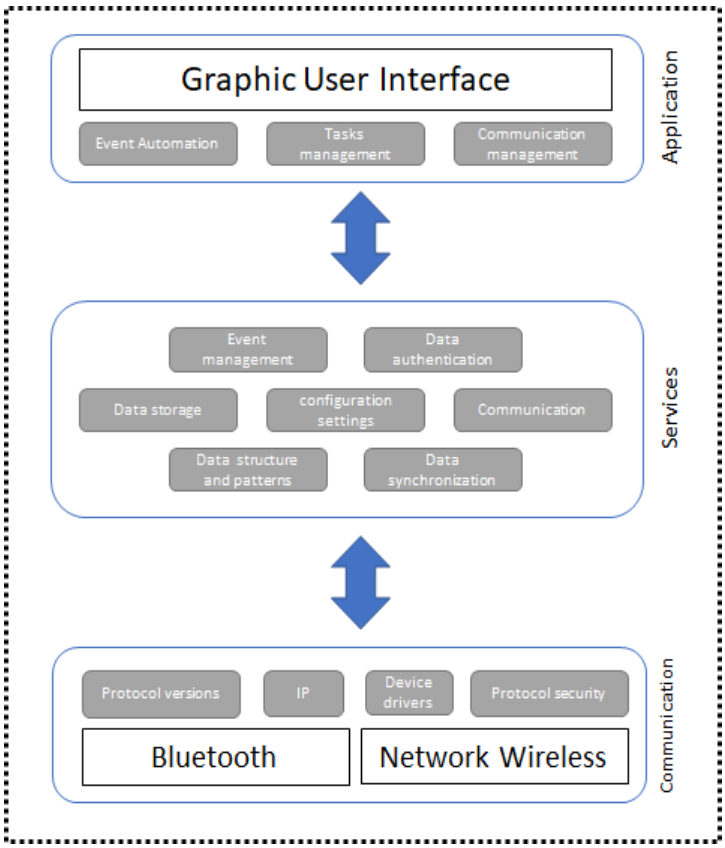

Figure 15 - IoT Central Hub Application Architecture

Application layer: it is the initial layer where the user has visibility of the operation and the autonomy to manage IoT Central Hub platform through the graphical interface, in a fast and intuitive way. It is in this layer where the management of device actions takes place, such as turning connections on and off, managing which devices will be connected to the platform and managing device data entries through the application.

Service Layer: application's intermediate layer is formed by the platform's services. The services interpret the data for correct functioning of events and provide support for device connectors to establish the connection efficiently for data processing. In the composition of this layer there are event management services that help in the orchestration of command actions sent and received by devices. In the data authentication service, it helps in the information security part, at this moment, there is a confirmation of data that are certified that only authorized devices are able to connect to the application. Even the “friendly visible” devices, this connection must take place in a safe and certified way through the connection protocols.

Data storage is part of service that allows saving relevant device information for future device connections and management, avoiding duplication of information and reworking of device reconnections and authentications. This is where data structure and patterns and data synchronization services run at the same time. Because the data is organized in such a way that it can be structurally indexed and located for other connections. The same is true with data synchronization. After the structured data, it is synchronized at each reconnection to update information and confirm device types.

Lastly, there is communication service with the next layer of protocols connection. In this layer, it happens the communication gateway service between the connection’s device and the application connectivity is performed. Communication protocols are received and identified so that they can interpret data for event activities to the application layer.

Communication Layer: it’s the layer where exist network communication protocols, Bluetooth and wireless networks are used at that moment. These protocols are used to encode and identify data transferred through the types of protocol versions that the application supports. In addition, the security protocols defined by each technology ensure information security through the correct authentication of data and in accordance with the type of devices a specific driver is activated for the correct functioning of

intelligent devices, for example, a lamp manages the brightness, the thermometer controls the temperature and simply a common feature of activating and deactivating the device.

4.3.1. Connection structure and data parameters sending

IoT Central Hub platform data structure was designed based on data flexibility, optimization and security, so that it is possible to add new functionalities with no huge changes need in the code structure. In addition, the application allows secure communication to prevent unwanted access to data that compromises the quality and stability of the system.

The platform communicates with the other device through the gateway on both sides to maintain system reliability. Thus, after pairing the devices, through the data structure configured in the application, the communication is carried out by parameters that are sent from one gateway to the other. On this way, the application has the possibility to work as a server and send the instructions to another device without having to configure or install any version from a specific manufacturer. Thus, the application allows the user to change or adjust any functionality of the applications already installed on the other device. The Figure 16 exemplifies the functionality of sending parameters between gateways in two different scenarios, where the one is composed by soundbar (model Ematic ESB210) and the application of the IoT Central Hub installed on the device, in scenario A. In scenario B, it is composed by security camera (model IMILAB C20) and also by an IoT Central Hub application installed on the device.

In the case of the prototype developed to IoT Central Hub application, the functionality designed was the verification of the battery status in remote device. In the future, other functionality parameters may be added to further complement and enhance the platform to bring greater benefits to domestic users. IoT Central Hub application was limited to battery status parameter, due to the complexity of the development and availability time to develop a prototype enhanced. Even so, the functionality developed, it allows the user to get an idea of great benefit of using the IoT device management platform.

The Following example shown in Figure 16 to check the battery status, there are basically four steps to the proper functioning of the application to send parameters. First, the device in scenario A sends the connection requests between the two gateways,

requesting to pair of two devices through Bluetooth connectivity, where the entire secure connection process between them is carried out. The device in scenario B then confirms and establishes the secure connection between two environments. In the next step, the device of scenario A requests the battery status of the other device through the parameter <BAT:>, as developed in the code shown in Figure 17.

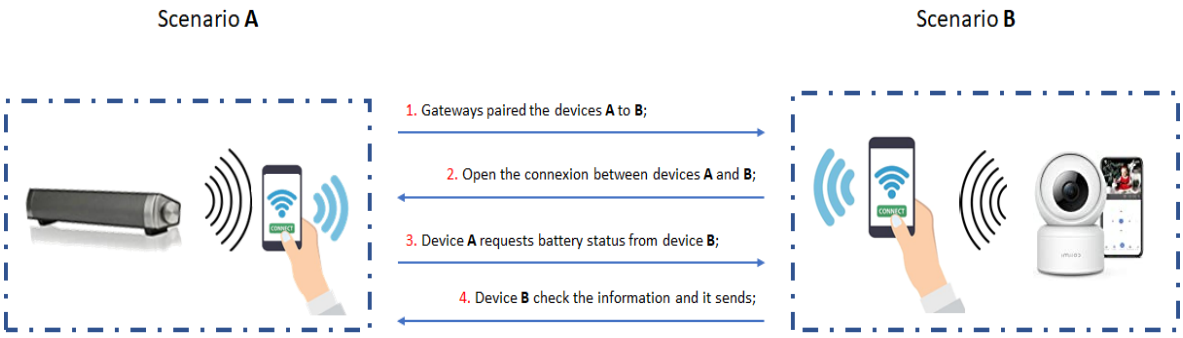

Figure 16 - IoT Central Hub Data structure communication

Finally, the device in scenario B provides the information requested by scenario A and in the application of scenario A, the battery status is displayed as requested.

```
sendInfo.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View view) {
        String infoString = "BAT:"+myBatteryStatus;
        sendReceive.write(infoString.getBytes());
    }
```

Figure 17 - Parameters communication code

Through the parameters within IoT Central Hub application, it is possible to request any information from any IoT device that is already installed in the mobile, so there is no require configure and new gateways added from each manufacturer to have the necessary information, such as sending a parameter to turn a device on and off, requesting sensor status or collecting temperature, even sending a command to perform an IoT device activity.

The prototype developed was carried out with some specific brands as informed in the following section on prototype deployment, so this study cannot fully guarantee compatibility with all existing devices available, due to constant innovations that frequently occur in the market.

4.4. Chapter Summary

In this chapter, the prototype developed to IoT device management platform called IoT Central Hub was presented. As presented throughout the section, the prototype intended to allow a heterogeneous and practical data management operation of IoT devices installed.

The application presented a simple system architecture based on three basic pillars, application, services and communication, which allows the user to have an excellent visibility of the proper functioning of the platform in a very intuitive way, there is no technical knowledge of the application required.

To summarize this chapter, the structural data functionality was exemplified, through functions transmitted by parameters between applications, allowing to future improvements without huge development complexity, as the prototype basic structure of IoT Central Hub has already been carried out.

In the next chapter, the platform implementation is going deep in detail, exemplifying the functionalities, usability and evaluation of the prototype implementation for different types of home users.

5 Prototype Implementation

In this chapter, it describes how the proposed solution was implemented based on the information already informed throughout the research work, identifying the most relevant points for development and demonstrating the proper functioning of the application.

The aim of developing the proposed prototype, as detailed at the beginning of the research work, it is to bring benefits of usability, flexibility and practicality of using an IoT device management platform with no needs to complex configurations and adding new hardware to complement the application operation. In this way, IoT Central Hub platform becomes an essential help to users for the heterogeneous functioning in IoT environment.

As an initial prototype, the application aims to exemplify the battery devices' consumption, so it is possible to send parameters and messages between the sending and receiving gateways of IoT Central Hub platform, determining the beginning of study that can be exploited for future application improvement.

5.1. Initial Considerations

When IoT Central Hub platform was started the implementation, a study of existing brands in the market was carried out to identify which would be the most efficient IoT devices testing. Due large numbers of the complexity particular features of each device, it was found that each manufacturer has a specific identification code, similar to MAC Address of the hardware device. So, the concern to create a prototype unfeasible, it was identified that creates a gateway, it would be useful to interpret the functionalities already configured in the smart device and it could provide greater flexibility and benefits for development.

IoT Central Hub platform prototype was developed in Java programming language in Android Studio, with libraries and classes reused that it already available and shared to be used for the developers to optimize the development, avoiding wasted development and time.

The application was developed only for Android operating systems, being IOS or any other system not compatible with the application, leaving this complementary version for future work.

The platform's connectivity was developed only for Bluetooth interface, as it was found immense variations and complexities of development, in which more study times were needed to allow greater security and stability for the application. Therefore, the focus is on Bluetooth communication to be able to present more stable and reliable product. The objective to encourage the scientific contribution, it was left open in the application to be added Wi-Fi feature in future studies.

To the application work properly, the user must allow access to the attributes of the Android operating system, by security reasons this restriction is applied to all applications that do not have access permissions. That permission is required to authorize IoT Central Hub platform to access Bluetooth functionalities, search for new devices, pair device IDs, send configuration parameters, among others.

IoT Central Hub platform is currently developed with the unique functionality of collecting and checking the battery status of the local device and the remote device. Due to high complexity development, that it was already mentioned, emphasis it was placed on a generic functionality that is useful to several IoT devices, the battery usage. Thus, efforts were concentrated on the development of functionality that could collect battery data in a generic way, regardless of IoT device manufactured. Additionally, a functionality to send parameters was developed that allows to add new functionalities in future works, allowing the prototype to become even more promising for future analysis and studies.

5.2. Prototype Functionalities

IoT Central Hub application is basically composed of five main features that were mentioned previously throughout this research work. The main functionalities of the developed work are turning the communication interfaces on and off, making the device searchable to be identified by another device, seeing the list of paired devices, searching which devices are visible and sending configuration parameters to the destination gateway.

Each functionality has a specific feature that allows the proper device management platform functioning. To the prototype elaboration, models of smartphones from the manufacturer Samsung were used, one it was a mobile Samsung Galaxy A41, and another is a Tablet Samsung Galaxy Tab S6. The application developed to manage the devices, it was installed in both devices, named IoT Central Hub through an executable ".APK" that runs automatically as soon as it is started, without any further configuration by the user.

Through the five basic application functionalities, it is possible to perform connection, pairing, search and it becomes searchable and sending parameters, as shown in Figure 18.

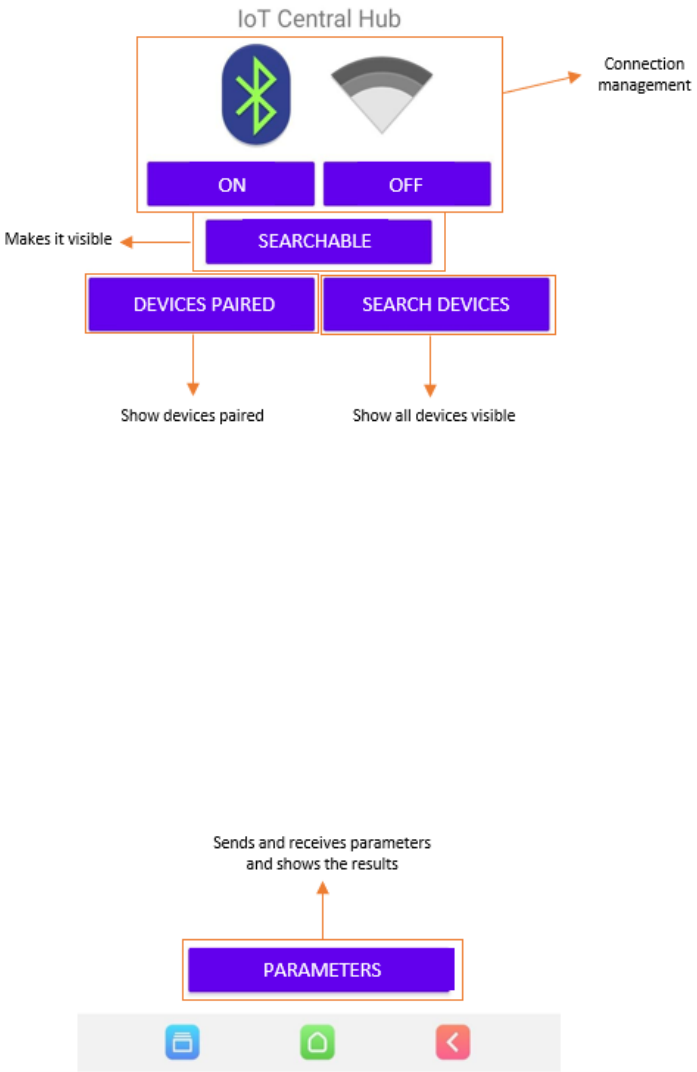

Figure 18 - IoT Central Hub functionalities

All five features developed in IoT Central Hub prototype were used functions and class methods in Java and compiled in Android Studio, this way, the code can access features that are already stored and installed on devices, differently of others proposed works studied, because other concepts required the installation of drivers, applications or even new hardware to the applications run properly.

IoT Central Hub differential is Java method calls straight to the device's functions where the data is stored, making it a benefit to the user, if there are other smartphones with different operating systems, as it does not require installation or configuration to perform the device management.

5.2.1. Connectivity management

The first functionality to be explored in the application is the connection availability environment. Connectivity between devices must always be active to allow access to data through the wireless communication interface. As previously mentioned, the prototype limited itself to use Bluetooth connectivity and left the other connection option, Wi-Fi connectivity, for future work. However, the prototype has already left a research path open to continue this type of connection in the future studies.

Bluetooth connectivity was used Bluetooth Low Energy (BLE) technology, which is a more appropriate technology to IoT devices, as they consume less energy and are more efficient in operation. Due to the use of this technology, it is recommended to use Bluetooth version 4.2 or higher to better data transmission rate.

The on and off functionalities of IoT Central Hub application is very simple. The user must only click on the button "on" indication and both connections are activatived and consequently click on the button "off" indication and the connections will be disconnected. This function is intended to enable and disable all the device's Bluetooth and Wi-Fi connections, as shown in Figure 19.

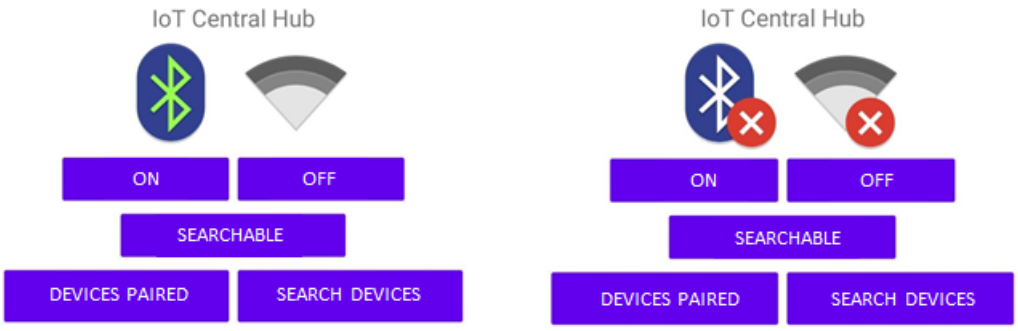

Figure 19 - IoT Central Hub functionalities – Bluetooth and Wi-Fi

In Figure 20, it can note which methods and classes were used to call the implemented connectivity functions.

```
if (mBlueAdapter.isEnabled()){
    mBlueIv.setImageResource(R.drawable.ic_action_on);
    mWifiIv.setImageResource(R.drawable.ic_wifi_on);
}
else {
    mBlueIv.setImageResource(R.drawable.ic_action_off);
    mWifiIv.setImageResource(R.drawable.ic_wifi_off);
}

//on btn click
mOnBtn.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View v) {
        if (!mBlueAdapter.isEnabled()){
            showToast( msg: "Bluetooth On");
            //intent to on bluetooth
            Intent intent = new Intent(BluetoothAdapter.ACTION_REQUEST_ENABLE);
            startActivityForResult(intent, REQUEST_ENABLE_BT);
        }
        else {
            showToast( msg: "Bluetooth is already on");
        }
    }
```

Figure 20 - IoT Central Hub functionalities – Bluetooth and Wi-Fi code

After the application's connectivity is active, it can be allowed to go ahead to search or make the application available for connection.

5.2.2. Searchable

The second function developed to IoT Central Hub platform was the option to make the device “searchable” to other devices. That means making the device “friendly visible” to other smart devices through the same connectivity. This functionality is important as it was identified during the research that some commercial products were not possible to be “showed” if they did not have the active option to be seen by other devices. That lock occurs because some devices have a security lock which it is not allowed to be accessed or even to be located.

During the study, it was not identified a unique identification pattern to all devices studied, therefore, to avoid any difficulty in locating the device, the “searchable” functionality was added.

According to Figure 21, as soon as the “searchable” functionality is activated in the device, a command is sent to the operating system to allow the device to become visible to other devices.

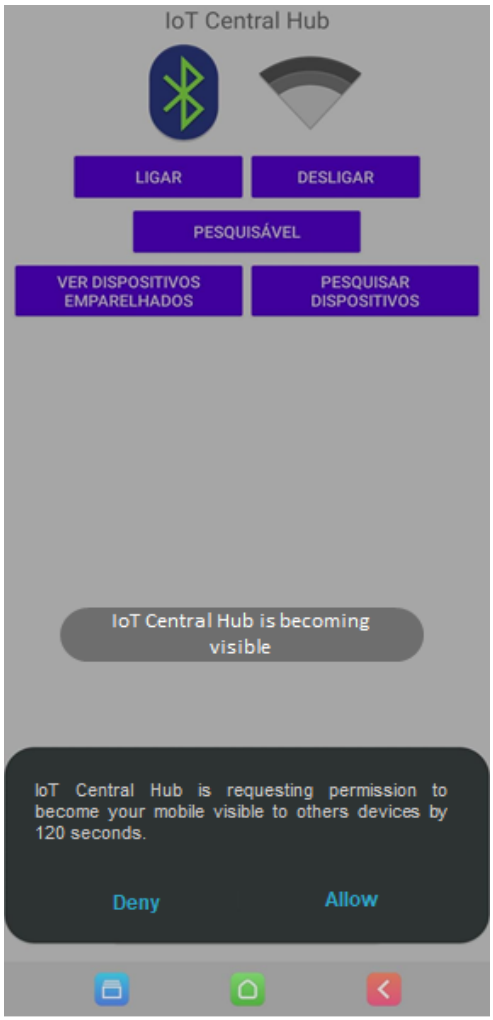

Figure 21 - IoT Central Hub functionalities – Searchable

This command triggers an action that prompts the user to authorize or not to make the device available to others in the same environment. This action is not part of IoT Central Hub application, but the user's Android operating system, allowing the device to be available within a 120-minute period. After that time, the device returns to its initial state.

The function called to operating system performed can be seen in the code developed in Figure 22.

```
mDiscoverBtn.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View v) {
        if (!mBlueAdapter.isDiscovering()){
            showToast( msg: "IoT Central Hub is becoming visible\n");
            Intent intent = new Intent(BluetoothAdapter.ACTION_REQUEST_DISCOVERABLE);
            startActivityForResult(intent, REQUEST_DISCOVER_BT);
        }
    }
});
```

Figure 22 - IoT Central Hub functionalities – Searchable code

After the device is available to be located by another device, it can be connected through the selected connectivity and the sending of requests to perform the management of smart devices can be started.

5.2.3. Paired Devices

Paired devices functionality allows to check all devices that have been connected to the IoT Central Hub platform. Thus, it is possible to identify the list of devices allowed to perform parameters requests for managing the other device.

When a command is triggered, a list of devices is showed, but for security reasons some devices omit that information, and it is not completely identified. Sometimes the name of the application is not identified, for privacy reasons, and only the MAC address of the devices is displayed, as shown in Figure 23.

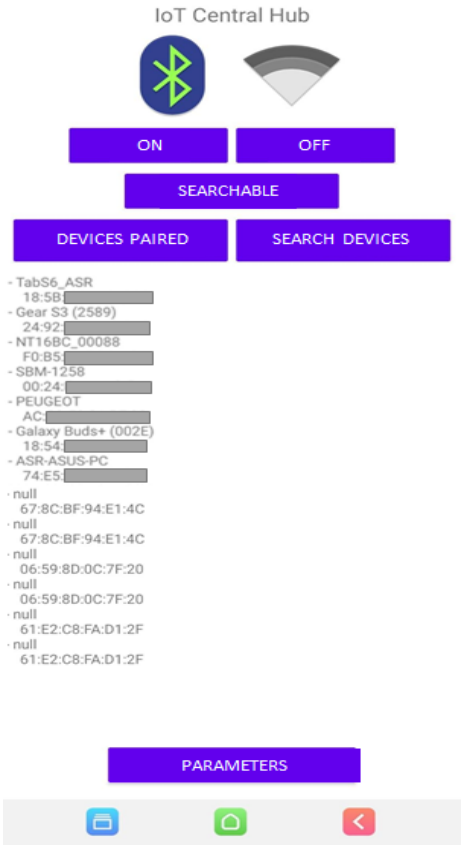

Figure 23 - IoT Central Hub functionalities – Devices paired

The code developed to identify the devices paired with the Central Hub IoT platform can be detailed in Figure 24.

```
mPairedBtn.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View v) {
        if (mBlueAdapter.isEnabled()){
            //mDiscoverBtn.setVisibility(View.GONE);
            mPairedTv.setText("Devices Paired");
            Set<BluetoothDevice> devices = mBlueAdapter.getBondedDevices();
            for (BluetoothDevice device: devices){
                mPairedTv.append("\n - " + device.getName()+ "\n      " + device);
            }
        }
```

Figure 24 - IoT Central Hub functionalities – Devices paired code

That functionality is essential that the user can perform requests by parameters for other devices. Only connected devices should be possible allow to execute the functions. In addition, the remote device must also have IoT Central Hub app installed and paired

with the source device. The connection structure is mandatory for the proper functioning of the application.

5.2.4. Devices searching

The search functionality to connect new devices, ideally performs the same way as smartphones do, however, this functionality makes it easier for the user to locate the device within the application without having to perform the search by the operating system and having to go back to the application again, as shown in Figure 25. Furthermore, at the end, when is searching is finished, the user can initiate the connection between the application and the device found.

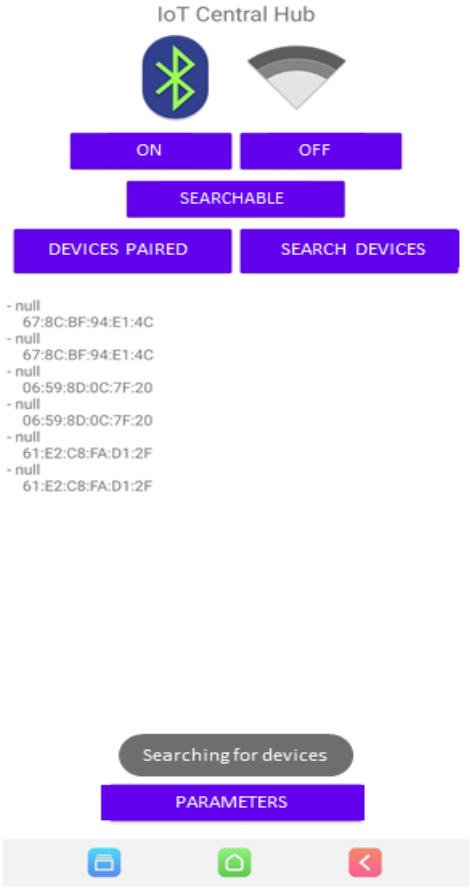

Figure 25 - IoT Central Hub functionalities – Search devices

To allow the searching for new device functionality works properly on IoT Central Hub platform, the code shown in Figure 26 was developed.

```
mSurveyBtn.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View v) {
        if (mBlueAdapter.isEnabled()){
            mPairedTv.setText("Searching for devices");
            IntentFilter filter = new IntentFilter(BluetoothDevice.ACTION_FOUND);
            registerReceiver(receiver, filter);

            requestPermissionLauncher.launch(Manifest.permission.ACCESS_FINE_LOCATION);
            requestPermissionLauncher.launch(Manifest.permission.BLUETOOTH_ADMIN);
            //ActivityCompat.requestPermissions(MainActivity.this,Manifest.permission.ACCESS_FINE_LOCATION),0);
            mBlueAdapter.startDiscovery();
        }
        else {
            showToast( msg: "Turn on Bluetooth connection to see all paired devices");
        }
    }
});
```

Figure 26 - IoT Central Hub functionalities – Search devices code

5.2.5. Parameters

The functionality of sending parameters is complexer functionality compared to others developements on IoT Central Hub platform. This function is intended to be the principal added value to future developments. This function opens a line of research to explore numerous possibilities to add new functionalities and enrich IoT Central Hub application even more.

For the development of the functionality of sending parameters, it was necessary to create an additional screen to allow better usability to the user and brings better benefits to the application. Thus, as shown in Figure 27, it is possible to identify the features developed for sending messages and new parameters to the connected device. In addition, you can automatically check the battery level function already added to the application that the local device is automatically identified. Then, when a new device is connected, it is updated with the battery level information of the new device.

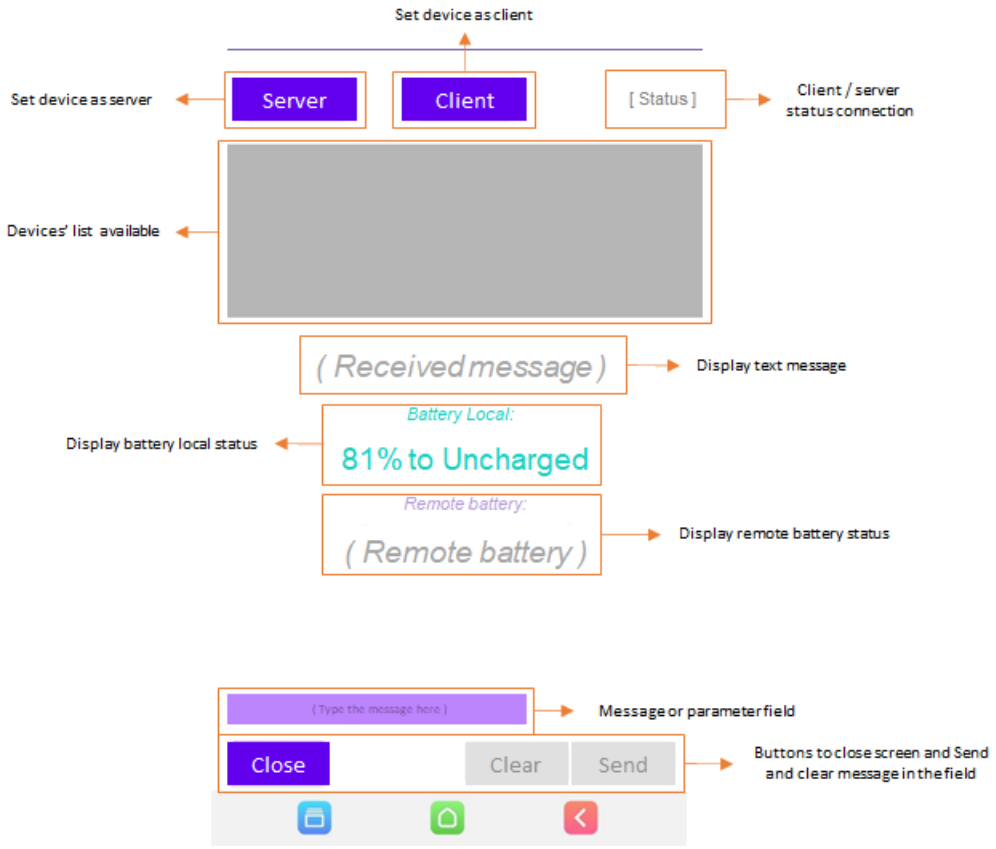

Figure 27 - IoT Central Hub functionalities – Parameter screen

On the second screen developed to IoT Central Hub platform is the main functionality of the application, sending a message to the remote device, checking the battery status of the local and remote device and sending parameters to the others. Therefore, the events of the second screen are detailed next.

Server button: the button is intended to configure the device as a server, which allows it to listen the remote device to initiate the connection. When the application is activated as a server, the client button is disabled to prevent the user to run the client event and server at the same time, which could cause the application a conflict and it generates a bug in the system.

The active listening of the server button is working for approximately 3 minutes, after this period the platform blocks and the functionality is inactive, and it needs to be restarted at the beginning of the process.

Client Button: The action to turn the device as a client is basically the reverse action of the server event, as seen previously. Client functionality allows the device to send a connection event to the remote device to establish connectivity and initiate data exchange.

In the same way of server event, as the server functionality works, the client button activity becomes active. The action inverse happens, it is turn server button disabled to avoid conflict with both active activities.

Status: The status option functionality presents the status of the current connectivity active between the client and server as the action is initiated. This functionality is essential to provide the user visibility into the workings of the connection between the client and the server. Because if that connection fails, nothing is supposed to be done.

To allow better visibility and usability of the application, the status event was created to the connection between the client and the server. Basically, those status are:

- **Listening:** enables server listening to wait for client connection.
- **Connecting:** starts action of connectivity between the client and the server, but at that time the connection between two devices is not confirmed yet.
- **Connected:** at this point the connection has been fully established and connectivity between client and server has been confirmed.
- **Failed:** This status identifies that the connection between two devices did not occur properly and an error was identified.

Device list box: When the device is triggered as a client, the device list box is automatically triggered to display the list of devices available to connect to the server. At that moment, a list of devices enabled to switch the connection between two points will be displayed.

After the connection is successfully established and the device list is displayed, the user must select which device will be used for the data exchange function. To complete the steps, the user should select the device name that is displayed in the list box and the connection it will start properly.

Text message: in text message option, the user can send message to recipient which will be displayed on remote device automatically.

Local battery: Local battery functionality is the function to display and control the battery status of devices that are installed locally. This functionality is the main point of IoT Central Hub platform development, because through it you can control and send device battery information.

This functionality is configured to automatically display the status of the local device via command function <BAT:>, that was mentioned in the previous chapter. In addition, this function also allows the user to know what action is taking place with the current battery status followed by the percentage of charge on the device.

The battery functions options are “Uncharged”, informing that the battery is being consumed and the charge will be reduced at each moment. “Charging” when the device's battery is currently being charged. “Full charge” which means that the device's full charge has already been reached and will no longer be charged as it is already full. “Not charging” means that the charging connector is plugged in, but it is not charging properly or there is some problem to be analyzed about charging the device's battery. And finally, “Unknown”, when no battery is identified in the device or the connected device cannot be identified.

Remote Battery: basically, the functionality of the remote battery is the same as that of the local battery, however, focus of this functionality is on bringing the battery information from the connected remote device. In this way, the status is exactly identical of the local battery.

Parameters field: it is in this field that the functions of sending parameters and messages to the remote device can be performed. Messages typed in this field will be displayed on the remote device in the field “text message” option, meaning everything typed and it will be sent and displayed exactly as written in the source device.

In addition, IoT Central Hub platform has developed the functionality of sending parameters through this field. It is by this field that the commands are sent to the target device that is displayed in the response in both. By default, the function <BAT:> has been developed and is running automatically. However, if this function is typed in plus and any other information following the parameter, this action is displayed in the status field. This functionality has the benefit of creating additional parameters to create extra management commands to the device, allowing to provide greater flexibility and customization to the user. At that moment, as it already informed during the research,

only battery functionality was developed, because due to the enormous complexity of development, research time development and devices compatibility and testing.

However, the functionality is a great door to the future works which they will be able to expand IoT Central Hub application functionality, being able in the future to become a potential commercial product in the market.

Close, Clear and Submit buttons: finally, to provide better usability to the user, three buttons with basic functions to the application were created. The first button created was the “Close” function, it simply closes the application on second screen, and it goes back to the first screen. This functionality is very useful, because when there is any inconsistency in the program, the user just should close it and open it again so that everything returns to ordinary. The second function is “Clear”, the purpose of clear button is to vanish all the information that is written in the parameters field.

This functionality is very useful because it facilitates the beginning of the new next action, bringing more agility to the user in a very effective way. And finally, there is the “Send” button function, by basic definition, it sends all the information written in the parameters field to the remote device.

5.3. Prototype Evaluation

After the development of the prototype, IoT Central Hub platform was moved to a controlled environment to user tests and evaluations. Numerous tests were carried out in order to certify the instability of the system and the ratification of results expected. In addition, some domestic users were chosen completely randomly based on technical profiles such as ages, education level and areas of activity.

Regarding age, the interviewees were grouped by intervals that could facilitate the results in the research. Thus, they were grouped as follows: group one, it has people aged between sixteen and twenty years. In group two, there were people aged between twenty-one and twenty-five. In group three, there were participants from twenty-six to thirty and, to finish, group four covers people between thirty-one and fifty-five years old.

The research aims to select people the most varied ways as possible to have wide understanding of satisfaction level, acceptability, usability, adaptability, and functionality. Within these home user groups there are two people from technology, four

from social humans' studies and communications, two from marketing, two from finance, and two non-graduates. The age range is between sixteen and fifty-five and everyone over twenty is active in the labor market at the moment of the survey.

Due to COVID-19 pandemic scenario experienced during the preparation study, the number of people was limited, as many of them were not comfortable to perform the tests, neither virtually, with no apparent justification, but rather a resistance of discomfort or no possibility to carry out the tests. Thus, the research was limited to the number of twelve people within the aforementioned profiles.

5.3.1. Parameters

The tests elaborated on the prototype of IoT Central Hub platform were carried out in the same way by the developer and the survey respondents. The test with the developer was prepared in person and with the results monitoring to be added into the survey, while the tests with the invited people were prepared virtually, with assistance at certain specific times according to their needs to the research.

In the environment assisted by the developer, two smart devices from Samsung brand were used, being a smartphone model Galaxy A41 (version: SM-A415F/DSN) and a tablet model Galaxy S6 (version: SM-P610), both using technology connectivity Bluetooth, with the smartphone configured as the client and the tablet as the server. Both devices were used to collect and send data to each other, sending data about the battery status of the connected devices. As shown in Figure 28, the regular behavior of the application's operation can be seen.

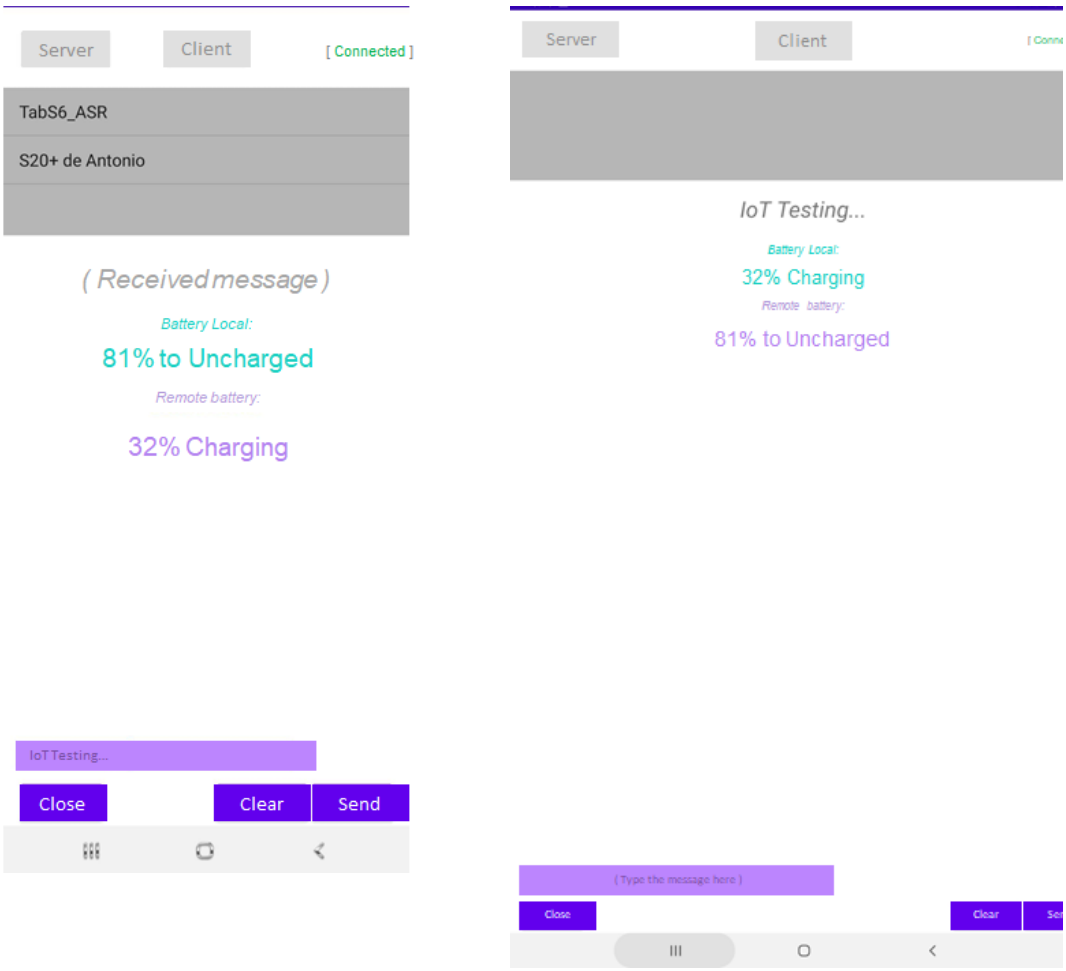

Figure 28 - IoT Central Hub functionalities – Tests results

In the given test performed, a message was sent to the remote device to certify the connectivity between them. The message was sent, and it was correctly received by the recipient. Likewise, tests were carried out to collect battery data from both smartphones and the devices connected to each of them. So, the activity work properly according of the functionality, the parameter <BAT:> should be used, which was described earlier in the research work, plus the technical model's name of the IoT device installed or the device identification code.

In the controlled testing environment developed by the programmer, the test was carried out with the charging status options of the batteries as already informed in the proposed work. All status were collected correctly and presented excellent results, confirming the real purpose data collection of the remote device accurate. In addition to the test, several other tests were designed by the developer to identify devices through search, pairing and connecting. However, during the connectivity tests between the server

and the client, some inconsistencies were found in a few moments that made the application terminate unexpectedly and abruptly, forcing to perform the entire process communication all over again.

Overall, IoT Central Hub platform behaves appropriately as expected and following the purpose of development. Even with some inconsistencies in the tests, apparently the operation is not impacted in a way that makes the prototype unfeasible.

5.3.2. Interviewee feedback evaluation

The evaluation and testing of the interviewed users occur freedomly, with no explanation, to check if the application is intuitive for all users, regardless of their area or expertise. After the first contact with the platform, if the user faced any obstacle that made the user blocked, the developer intervened in the test and explained the operation, giving them assistance to be able to continue with the tests.

After this first contact, a new attempt was made to see if users had no difficult to use the application after being provided some details of the proper functioning and environment for handling the application.

In addition, the time was controlled to realize how long it took the user to be able to use the application in an intuitive manner. After, the same time was timed to identify how long the user could perform the same activity on the same time slot, but now, as prior knowledge of the application. The time control supports to realize the usability and agility that IoT Central platform should have, demonstrating its efficiency and effectiveness in using a new technology to the users who have never had any contact before.

As shown in Figure 29, IoT Central Hub platform usability evolution could be analyzed, according to the instructions provided to users. The initial contact and without any further information about the platform how to use it, the application was available to respondents to be installed on their devices. The only information provided to the participants was that they need to have two devices to make the application work and superficial summary of the application's purpose, nothing else was informed to understand what the difficulty would be to install and usability of the application.

Regarding installation, one hundred percent of participants were able to install correctly and intuitively, confirming that application is easer to install through “.APK”

file (extension defined by Android as executable), thus, there is no obstacle or installation error.

Another relevant point to the research is the types of devices used by users. The only recommendation was that there were two devices running Android operating system to work application properly. Later on, the user did all the work without any intervention.

After installation, the user moved to the next stage of using the application, connecting and using the functionalities available in IoT Central Hub application. As can be noted in Figure 29, the amount of people who classified the application easier to use, they are between groups one and two when they did not get any explanation. However, after explaining the use and the interference during use, participants in groups three and four performed better.

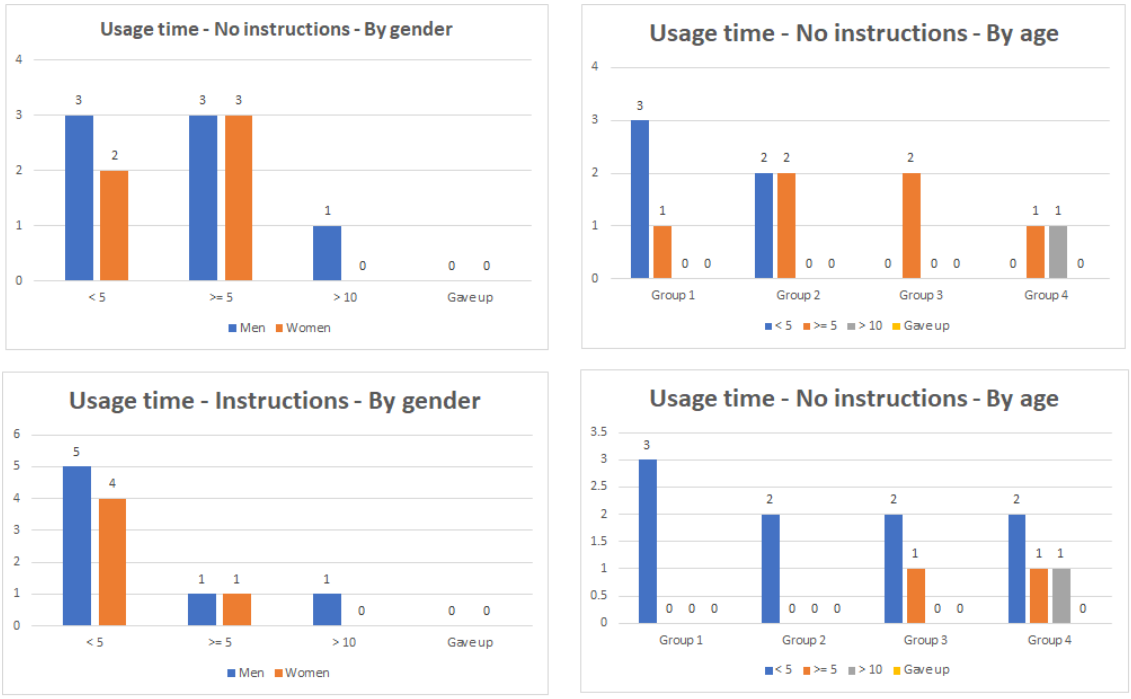

Figure 29 - Survey result – Application usage time

Although respondents belong different areas and some of them, non-graduation degree, the result was balanced. Also, regarding the gender of the participants, in general, men and women obtained the same level of response. The age of the participants was a critical factor issue identified, because it seems that youngest people are more familiar with current technologies and more up to date with current upgrades.

As additional information to support the evaluation of IoT Central Hub platform based on response of the participants, a satisfaction survey was resquested to be replied after the functionality test and to certify if the application is well acceptance by home users. Basically, they were asked about three simple questions:

- Did IoT Central Hub platform allow good usability?
- Would you install IoT Central Hub platform in your personal mobile?
- Would you recommend IoT Central Hub to a familiar or friend?

To measure respondents' answers, five categories were used. Strongly Disagree, Disagree, Neutral, Agree and Strongly Agree. This classification supports the research be more objective and clearer to the interviewee regarding the evaluation process.

At the first analysis of the survey results, it was mostly neutral, but at the second part there was a balance between group of people that disagree and agree. The categories classified to the extremes as strongly disagree and strongly disagree had a few votes in the results, as can be confirmed in Figure 30.

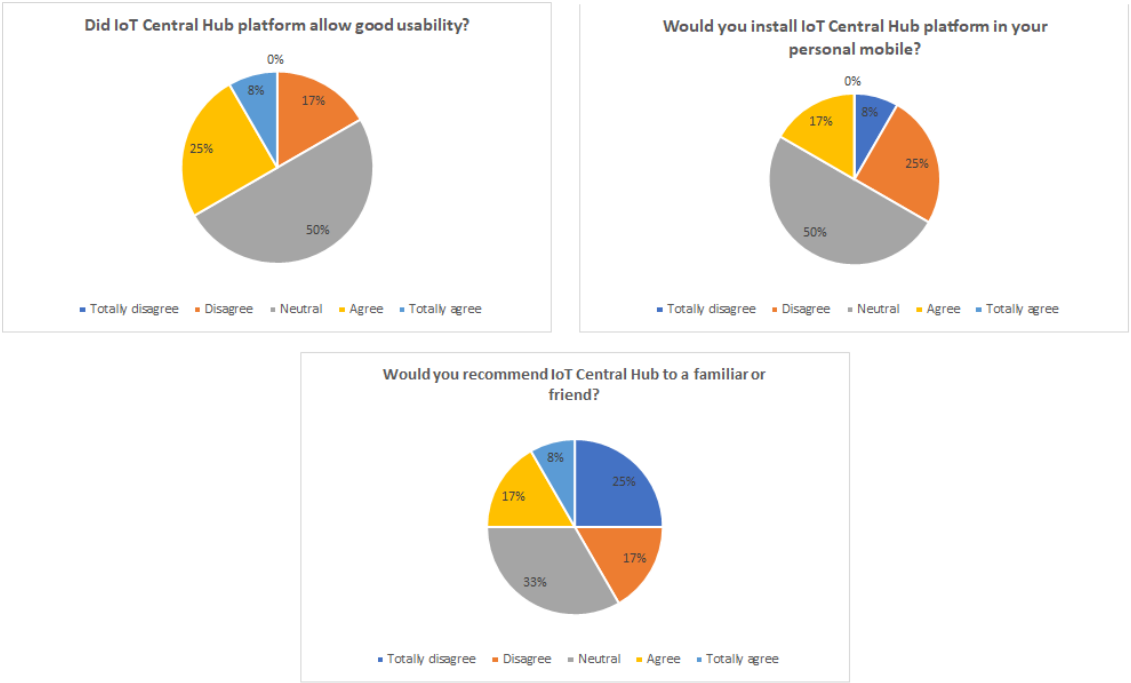

Figure 30 - Survey result – Questionnaire

Regarding the usability issue of IoT Central Hub platform that was not fully accepted by the interviewees. It believes that happen some instabilities in the system and some inconsistencies that impact in the result. But that could be adjusted in a later version, if the application were improved.

Regarding the possibility to have IoT Central Hub application installed on the personal smartphone of the participants, it has also not reached a percentage higher than fifty percent of acceptance. Probably, the additional features could be a raison that impact on better acceptance of the users. They have reported that the platform has potential, but extra features could enrich it and it could also make it more attractive.

The last question about recommending IoT Central Hub platform to a family member or friend have reached less than fifty percent, was identified referring to the arguments mentioned in the previous paragraphs. Some factors such as instability and addition features were the essential points that they rated the application at the lowest level. However, as already informed, IoT Central Hub platform was praised by respondents as a potential product of great value in the market that can positively contribute to future studies and improvements in future versions of IoT Central Hub application.

5.4. Chapter Summary

In this chapter, the proper functioning of IoT Central Hub platform was presented, as well as the essential attributes and functionalities of the application. All the functions that make up the developed system were presented in detail, as well as the configuration forms that must be carried out to the application to work correctly. In addition to the functional presentation of the application, key parts of the code development were presented to exemplify the purpose of the result of each function more clearly and objectively.

In order to identify the strengths and possible improvements of IoT Central Hub platform, entire focus on researching, a test was carried out in an environment controlled by developer before indicating it to domestic users. Then, after tests approval by developer, people with random profiles were selected to assess the application, thus, satisfaction surveys and usability testing were done with the users.

Finally, this chapter demonstrated the functionalities of IoT Central Hub application and the work developed in detail. In addition, the usability test was presented to the users to assess the development in general, presenting a result on base general view of the user.

6 Conclusions

Smart devices on the market have the ability to create an interaction and dynamism on the information that people receive from the devices. These devices bring many benefits and add value to the people life, as they facilitate the population all daily activity. Based on that, IoT devices have been pleased and popularized among all social groups, as it has been already mentioned throughout during research work.

However, IoT devices popularization, it has naturally increased the complexity and significantly numbers of opportunities in market. Therefore, the IoT Central Hub platform solution has brought a great benefit to domestic users who do not have any technical knowledge about this emerging technology.

Thus, as shown in the previous chapter, IoT Central Hub platform is partially achieving the goals, as the absence of additional features and a more attractive interface are some of the main points that limited in achieving the goals completely. But even so, IoT Central Hub platform presents a significant feature of controlling local and remote devices in a very intuitive way. Thus, the user has the advantage of using a single platform to manage their IoT devices installed on their smartphone.

This research work was able to present IoT Central Hub platform prototype fully usable and testable by user, creating a heterogeneous, scalable, and good usability solution. The platform also allows huge range of expandability of functionality and integration modules to new features to be added. Thus, the developed prototype gives rise to ample study possibilities to future system improvements.

Finally, IoT Central Hub platform presented the tests results performed by developer and by users such as good features performance and the usability that it was proposed at the beginning of the research. Thus, we can conclude that the smart device management platform can be installed and implemented to be used by domestic users with less complexity.

6.1. Achievements

IoT Central Hub platform has achieved as main objective the remote device data collection and the possibility to be widely exploited to future study to become it a

powerful IoT device management tool. Another great achievement of IoT Central Hub application is the complexless configurations, in addition, the system doesn't require to be the technology specialist to use it. Thus, it is possible to have an easy and intuitive tool.

In addition to usability, the installation of IoT Central Hub platform is very clear and straight to the point. There are no extra configuration steps and there is no need to configure the device to install, on this way, the user has the comfort of having an application installed without difficulties.

In the end, IoT Central Hub prototype was developed to become fully functional and testable. Even with recommendations to the system improvements, users praised the development and the concept of IoT Central Hub platform.

6.2. Future Research

IoT Central Hub project was an audacious challenge since the beginning it was intended to carry out the automation functionalities through several technologies and expand it to remote use through the Cloud technology. However, due to the time of research and development of the prototype, in addition to the complexity of the development, IoT Central Hub reaseaches allowed a wide range of possibilities to expand the project developed through the following features that were made available for future work. The following features are:

- Adds wireless network access functionality to search and connect devices found in the local network, as well as through developed Bluetooth technology.
- Extends IoT Central Hub prototype functionality through Cloud technology and add functionality for remote device management over the Internet.
- In addition to Cloud functionality, it should be created a service that allows the user to have centralized control through the server, where you can manage client applications by several users.
- Adds user profiles functionality that allows more flexibility to the user through customizable graphical environments and efficientest management of most used smart devices.

- Further improve the application's graphical interface so that it can have better usability and can be supported by other types of mobile devices, such as tablets and laptops.
- In addition to improving the graphical interface, it would be very useful for home users to have the reporting functionality regarding the collected data. Thus, it would be possible to create a customizable dashboard with a summary of the main functionalities that they are most relevant and essential for each user.
- Extends system compatibility for platform-appropriate functioning of devices running iOS operating systems in addition to Android on which the prototype was developed.
- Allows the application to have more heterogeneous data collection functionality from smart devices, so that it is possible to perform data processing efficiently.
- Add an artificial intelligence module to the platform, after the implementation of the data collection functionality, so that it can be possible to process the information in an intelligent and productive way for the user.

Finally, the the improvements implementations suggested in this chapter will allow the smart device management platform, IoT Central Hub, to become a potential commercial application, so that it would be possible to bring numerous benefits to home users, as already mentioned during this research.

Bibliographies References

Abbas, A. M., Youssef, K. Y., Mahmoud, I. I., & Zekry, A. (2020). NB-IoT optimization for smart meters networks of smart cities: Case study. *Alexandria Engineering Journal*. https://doi.org/10.1016/j.aej.2020.07.030

Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges. *IEEE Access*, *6*, 3619–3647. https://doi.org/10.1109/ACCESS.2017.2779844

Antunes, J. B. (2016). Uma plataforma para gerenciamento e aplicações em internet das coisas. *Belo Horizonte*, 87.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Barros, E. B. C. (2015). *Universidade Federal de Sergipe - Centro de Ciência Exatas e Tecnologia. Programa de Pós-Graduação em Ciência da Computação. São Cristóvão-Sergipe 2018*.

Carlos, A., Gil, C., Maria, A. A., Fernando, A., & Marcos, A. (2002). *Como Encaminhar uma Pesqllisa?*

Chaqfeh, M. A., & Mohamed, N. (2012). Challenges in middleware solutions for the internet of things. *Proceedings of the 2012 International Conference on Collaboration Technologies and Systems, CTS 2012*, 21–26. https://doi.org/10.1109/CTS.2012.6261022

Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with China Perspective. *IEEE Internet of Things Journal*, *1*(4), 349–359. https://doi.org/10.1109/JIOT.2014.2337336

Delicato, F. C., Pires, P. F., & Batista, T. (2013). Middleware Solutions for the Internet of Things. In *Automation Control - Theory and Practice*. http://link.springer.com/10.1007/978-1-4471-5481-5%0Ahttp://www.intechopen.com/books/automation-control-theory-and-practice/challenges-of-middleware-for-the-internet-of-things

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Heimdal. (2020). *Cloud Computing Threats: Beyond Vulnerabilities*.

Ibsg, C., & Dave Evans, A. (2011). *Cisco Internet Business Solutions Group (IBSG) A Internet das Coisas Como a próxima evolução da Internet está mudando tudo*.

INAP. (2009). *Cloud Solution*.

Jadeja, Y., & Modi, K. (2012). Cloud computing - Concepts, architecture and challenges. *2012 International Conference on Computing, Electronics and Electrical Technologies, ICCEET 2012*, 877–880. https://doi.org/10.1109/ICCEET.2012.6203873

Jan, M. A., Nanda, P., He, X., Tan, Z., & Liu, R. P. (2015). A robust authentication scheme for observing resources in the internet of things environment. *Proceedings - 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014*, 205–211. https://doi.org/10.1109/TrustCom.2014.31

Kevin Asthon. (2010). That ’ Internet of Things ’ Thing. *RFID Journal*, 4986. http://www.rfidjournal.com/article/print/4986

Kramp, T., van Kranenburg, R., & Lange, S. (2013). Introduction to the internet of things. In *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*. https://doi.org/10.1007/978-3-642-40403-0_1

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Liébana-Cabanillas, F., Molinillo, S., & Ruiz-Montañez, M. (2019). To use or not to use, that is the question: Analysis of the determining factors for using NFC mobile payment systems in public transportation. *Technological Forecasting and Social Change*, *139*(August 2018), 266–276. https://doi.org/10.1016/j.techfore.2018.11.012

Ma, M., Wang, P., & Chu, C. H. (2013). Data management for internet of things: Challenges, approaches and opportunities. *Proceedings - 2013 IEEE International*

Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, GreenCom-IThings-CPSCom 2013, 1144–1151. https://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.199

Marotta, M. A., Carbone, F. J., De Santanna, J. J. C., & Tarouco, L. M. R. (2013). Through the internet of things - A management by delegation smart object aware system (MbDSAS). *Proceedings - International Computer Software and Applications Conference, June*, 732–741. https://doi.org/10.1109/COMPSAC.2013.122

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *Cloud Computing and Government: Background, Benefits, Risks*, 171–173. https://doi.org/10.1016/b978-0-12-804018-8.15003-x

Mercader, P., & Haddad, J. (2020). Automatic incident detection on freeways based on Bluetooth traffic monitoring. *Accident Analysis and Prevention*, *146*(April), 105703. https://doi.org/10.1016/j.aap.2020.105703

Miles, B., Bourennane, E. B., Boucherkha, S., & Chikhi, S. (2020). A study of LoRaWAN protocol performance for IoT applications in smart agriculture. *Computer Communications*, *164*(September), 148–157. https://doi.org/10.1016/j.comcom.2020.10.009

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016

Nakagawa, E. Y., Oliveira Antonino, P., & Becker, M. (2011). Reference architecture and product line architecture: A subtle but critical difference. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6903 LNCS*, 207–211. https://doi.org/10.1007/978-3-642-23798-0_22

Peña Queralta, J., Gia, T. N., Zou, Z., Tenhunen, H., & Westerlund, T. (2019). Comparative study of LPWAN technologies on unlicensed bands for M2M communication in the IoT: Beyond Lora and Lorawan. *Procedia Computer Science*, *155*(2018), 343–350. https://doi.org/10.1016/j.procs.2019.08.049

Pires, P. F., Delicato, F. C., Batista, T., Barros, T., Cavalcante, E., & Pitanga, M. (2015). Plataformas para a Internet das Coisas. *Anais Do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, 110–169.

Ramya, C. M., Shanmugaraj, M., & Prabakaran, R. (2011). Study on ZigBee technology. *ICECT 2011 - 2011 3rd International Conference on Electronics Computer Technology*, *6*(February 2019), 297–301. https://doi.org/10.1109/ICECTECH.2011.5942102

Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Cla, S. (2016). Middleware for internet of things: A survey. *IEEE Internet of Things Journal*, *3*(1), 70–95. https://doi.org/10.1109/JIOT.2015.2498900

Rodrigues, B. (2018). *AutoDev- A system to simplify configuration processes of IoT devices for domestic users*.

Severino, A. J. (2014). *Metodologia do trabalho científico [livro eletrônico]*.

Talavera, L. E., Endler, M., Vasconcelos, I., Vasconcelos, R., Cunha, M., & Da Silva Silva, F. J. (2015). The Mobile Hub concept: Enabling applications for the Internet of Mobile Things. *2015 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom Workshops 2015*, *March*, 123–128. https://doi.org/10.1109/PERCOMW.2015.7134005

Vasseur, J., & Dunkels, A. (2010). Chapter 16 The 6LoWPAN Adaptation Layer. *Interconnecting Smart Objects with IP - The Next Internet*, 230–249. https://doi.org/10.1016/B978-0-1237-75165-2.00035-1

Yin, X., Liu, J., Cheng, X., Zeng, B., & Xiong, X. (2020). A low-complexity design for the terminal device of the urban IoT-oriented heterogeneous network with ultra-high-speed OFDM processing. *Sustainable Cities and Society*, *61*(March), 102323. https://doi.org/10.1016/j.scs.2020.102323

Zhang, S., Zhang, S., Chen, X., & Huo, X. (2010). Cloud computing research and development trend. *2nd International Conference on Future Networks, ICFN 2010*, 93–97. https://doi.org/10.1109/ICFN.2010.58