T.C.

ALTINBAS UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

EFFICIENT ENERGY MANAGEMENT IN SMART HOMES USING IOT- BASED LOW-POWER WIDE-AREA NETWORK (LORAWAN) PROTOCOL

Bushra Fuaad KHMAS

Master of Science

Supervisor

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Istanbul, 2021

EFFICIENT ENERGY MANAGEMENT IN SMART HOMES USING IOT-BASED LOW-POWER WIDE-AREA NETWORK (LORAWAN) PROTOCOL

by

Bushra Fuaad KHMAS

Electrical and Computer Engineering

Submitted to the Institute of Graduate Studies

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2021

The thesis titled “EFFICIENT ENERGY MANAGEMENT IN SMART HOMES USING IOT-BASED LOW-POWER WIDE-AREA NETWORK (LORAWAN) PROTOCOL” prepared and presented by “Bushra Fuaad KHMAS” was accepted as a Master of Science Thesis in Electrical and Computer Engineering.

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Supervisor

Thesis Defense Jury Members:

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	School of Engineering and Architecture, Altinbas University	_____
Asst. Prof. Dr. Mesut ÇEVIK	School of Engineering and Architecture, Altinbas University	_____
Asst. Prof. Dr. Tareq MOHAMMED	Computer Science and Information Technology, Imam Ja'afar AL-Sadiq University	_____

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Approval Date of Institute of Graduate Studies
____/____/____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Bushra Fuaad KHMAS

DEDICATION

I devote and pledge this research work to my supervisor who is salient for guiding me through whole research work as well as my family for always assisting me in my hard time.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my supervisor Asst. Prof. Dr. Abdullah Abdu IBRAHIM for guiding and helping me along the way in writing this dissertation. Discussing my progress, problems, and ideas with my supervisor Asst. Prof. Dr. Abdullah Abdu IBRAHIM a couple of times every week helped me tremendously in understanding the logic behind the research. It made me better realize the technical need for this research work.

ABSTRACT

EFFICIENT ENERGY MANAGEMENT IN SMART HOMES USING IOT-BASED LOW-POWER WIDE-AREA NETWORK (LORAWAN) PROTOCOL

Bushra Fuaad KHMAS

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Date: 09/2021

Pages: 66

In this research, a concept for efficient energy real smart housing was built using IOT-based Decreased large network (LoRaWAN) and Sigfox software, and a research on potential user engagement strategies was conducted using Python 3.7 and different Iot official websites. Other goal was met, which was to equate the Sigfox model to Iot applications., It cannot be the only innovation used in a connected device given the scarcity. Although Mac layer provides more flexibility, it is more difficult and complicated to introduce, and it lags behind Sigfox projects such as the construction of usability. The main aim of this project is to build a functional housing system based on LPWAN Ai devices. The Iot is becoming a fact quicker than planned as more things become connected to the internet. Home automation, a framework in which the Internet of Things is expected to have a significant effect on the collective good of daily lives, is a hot subject. Other technological innovations, such as cloud technology, artificial intelligence, and miniaturisation, have aided in the development of this technology. The Internet is causing computers to shy away from demanding computing tasks. Close to zero broad channels are critical in this situation, since they include energy-efficient equipment at cheap prices. In this area, Sigfox and LoRa are dominant players. This work not only demonstrates an understanding of some of these debates as well as a detailed understanding of an IoT project, but it also adds

value by assembling an IoT-based proposal from its most basic form, the instruments that collect data, to its most advanced form, where a customer can use the material for their gait using the Python integration framework (IDE) and its production.

Keywords: IoT Networks, Internet of things, Home Security, Low Power and Lossy Web, Sigfox, LoRa.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

1. INTRODUCTION

1.1 INTRODUCTION

From how humans behave with one another to how they perform company, the advent of the desktop laptop into signal is modulated human lives. Computer systems are now ubiquitous, and they have ushered in a slew of new innovations that have changed the world. The Web would be one of those inventions. In 1991, Mark Brandt, a software engineer whom invented the term "significant development," which refers to tools to be used at any period, in any location, and in any layout, stated that "A most significant innovations are those that vanish. They become distinct from the structure of daily life when they insert itself into it." [2].

The Internet (IoT) is the next change on the horizon (IoT). And although term "big data" was coined in 1991, it was first used by Kevin Ashton in 1999 during a discussion on the use of Broadcast Id (RFID) [3]. Even, the Internet of Things (IoT) has only recently started gaining traction, both in terms of innovation., because of the introduction of technological developments, but also from a marketing standpoint It is currently available on the manufacturing, retail, and consumers. Its sense and description, though, still are hazy. It's known by a variety of names and is connected to a range of platforms, including the Internet of All (IoE), the Smart Manufacturing, and Business 4. 0.. [4], To mention few more, cloud hosting, Device (M2M) connectivity, and cloud computing. Much of these ideas and inventions are, in certain ways, a part of internet of things and a complex society. In the Information & Communication Technology (ICT) model, which would be concerned with reflecting all aspects of computer - based interaction, The Internet of Things introduces a new aspect: the "All Link." This new universe complements the current "Any Period" and "Any Location" relations [5], which relate to transactions that can be produced regardless of time or location, namely outside, inside, at night, during the day or. The modern "Any Issue" link allows human-to-human contact without using laptops.; Access points and people, as well as between IoT devices. A slew of new market prospects emerges as a result of this new dimension. With estimates of 20 to 30 billion iot devices by 2020 [6,] international investment of 1.4 trillion dollars by 2021 [7], and the reality that intelligent devices produce more than two Exabytes of information every day, the future looks bright. [8] confirm that IoT is quickly rising to a definite stay in our everyday lives.

According to a Verizon report, 2016 was the year that the IoT gained the most momentum and 2017 gave definite proof that IoT solutions are the next big step. In the same report, 73% of executives were either researching or deploying IoT related solutions in their companies [9].

A home automation, also known as e, automated residence, or core self, is a living space that is packed with sophisticated electronic computers, with the main goal of improving and simplifying the lives of its residents. According to a New poll, a traditional townhouse would have 500 mobile tvs by 2022, and the internet of things is currently one of the leading. IoT environments. A further survey conducted in the UK by Deloitte found that 66 percent of customers believed that iot systems had the ability to make their lives better. Intelligent aides, combined with AI breakthroughs are already being seen in the home automation context which are being promoted by big firms, allow for things like led products and home devices. Buyers are also bringing other gadgets into their homes, such as dimmers, door lights, data gathering, and animal gps tracking [11]. The Open iot market size has seen considerable growth as a result of home automation creation.as seen in a 2017 report which states that IoT platforms, in the IoT consumer segment, have a 21% focus on the smart home. Smart homes have very high market potential, but there are also many issues to overcome from the user point of view, such as:

Security: one of the most critical aspects for customers. It represents the steps taken to protect the home, either through hardware or software security, from such threats as Internet attacks, robberies or IoT device tampering.

Ease of Use: the system must be easy to understand and work with, offering a comfortable experience.

Cost: price stands as one of the most delicate aspects in all business areas and can hinder smart home device adoption.

Convenience: problems must be easy to solve; if possible, without user intervention. This makes monitoring, control and intelligence vital functions of the smart home.

Energy Efficiency: electricity represents significant costs in most countries, and it is where Low Power Wide Area Network (LPWAN) technologies are starting to take center stage as leading devices in energy consumption and battery life.

Privacy: the costumer expects that his personal and home information remain guarded. For example, in cases where the devices have a direct internet connection, it is imperative to guarantee that they have the necessary protection against possible security attacks.

In the years to come, the Internet of Things is sure to become a large part of society and will be incorporated in every setting possible, blending its way into cities, homes, hospitals and more, until it merges into the fabric of everyday lives just as Mark Weiser predicted. The most important feature of IoT is the impact on the daily lives of its users, in both the working and domestic fields.

1.2 PREVIOUS RESEARCH

Before 2013 the LPWAN term did not exist. LPWAN are technologies which focus on three main aspects:

Low power: few applications in IoT have the possibility to use a generator for power, so most devices are powered by batteries. LPWAN devices have a battery life with ranges in 5 to 10 years.

Long range: wireless networks need some kind of access point (gateway or base station). LPWANs generally have ranges from 2 to 10 km in urban settings, offering more mobility in deployment and the need for less gateways.

Low data rates: data rates are generally lower than 5 kbps and therefore LPWANs only send small packets of information ranging from 0 to 256 bytes.

One of the characteristics that separates LPWANs is the type of radio spectrum they use. Most operate in the sub-GHz band which are Industrial, Scientific and Medical (ISM) bands. These are public, open but regulated radio bands designed especially for use proposes other than telecommunications. The equipment in these bands are subject to all interference generated by ISM applications. The most used bands for LPWANs are generally: the 433 MHz and 902-928 MHz, in Asia; the 902-928 MHz in America; and the 863-870 MHz band in Europe. As the work focused on the 868 MHz band, only this band was reviewed. The 863-870 MHz band has a power limitation of 25 mW (14 dBm) and a duty cycle of 0.1%. In the 868-868.6 MHz band there is an extension to a 1% duty cycle and in the 869.4-869.65 MHz band an extension to 10%

duty cycle and 500 mW (27 dBm) power is possible, which is normally used for downlink messages.

Currently there is no adopted standard available in the LPWAN market and they are usually defined by the radio technology used:

Ultra-narrow Band (UNB): this type of technology uses modulation to achieve a very narrow bandwidth, reaching greater distances. It only supports low data rates, with a typical payload being around 12 bytes with its duration taking around 2s. UNB LPWANs are only used in applications where reliability and Quality of Service (QoS) are not very important.

Narrowband: this type of technology offers the best compromise between QoS, capacity, cost and network efficiency. With channel bandwidths around 12.5 kHz wide, they offer the best room of medium data payloads for uplink traffic from a vast number of terminal devices.

Wideband: the channel bandwidth of these technologies' ranges from 500 kHz to over 1 MHz.

1.3 PROBLEM STATEMENT:

The area covered by Sensor nodes, combined with advancements in computing that allow for the creation of contact lists, raises security issues, which are one of the key concerns with regards to the issues raised by Iot devices. It was discovered that 80 percent of Internet of things violated the secrecy of private details such as title and date of birth. More than 80% of respondents did not request credentials of sufficient scale and depth, and 60% had security holes in their web applications

Some of these issues have been addressed in federal studies over the past few years. Elements of the Belgian Organisation's privacy laws pertaining to the Internet of Things are debated. The Federal Trade Commission (FTC) in the United States faces similar rights and protections issues as it publishes reports on protection.

Start with private data, consumers of Iot systems will be regarding standard objects within European law, this indicates that if a computer contains private details about a person, that user will be considered an info object even though the computer doesn't really belongs to themselves. The parties involved, which are known as data managers, are in charge of the collection and use

of private information. Application producers, online media sites, data hosting services, and 3rd software developers are instances of shareholders [12]. Under EU law, that manner sensitive information is treated is often discussed, with the information participant's agreement about how the data is presented., which are known as data managers, are in charge of the collection and use of private information. Computer producers, online media sites, data hosting services, and 3rd programmers are instances of shareholders [12]. Under EU law, that manner sensitive information is treated is often discussed, with the software participant's agreement about how the information is gathered.. Often discussed is the equity of data collection and management. Parts such as intent restrictions are discussed, which specify that the information gathered must be used for clear, valid, and valid purposes.. Furthermore, data minimization aspects are mentioned as well, which discuss how the data should only be collected for the necessary use, and not stored by default [13]. In other points ranging from transparency, security, data subjects, rights, processing of sensitive data like health information and recommendations to stakeholders and device manufacturers are presented. However, all these challenges expressed previously represent only a small part of the problems facing IoT and the prospect of a connected world. For example, legal issues also encompass problems such as: cross border data flows; data discrimination; the case of IoT in the aid of law enforcement and public safety, which leads to questions of mass surveillance systems; the liability of IoT devices; and the proliferation of legal actions in regards to IoT [14].

1.4 AIM OF THESIS:

The main goal of this project is to create a smart house device that includes LPWAN Internet of things. Clear goals were set in order to realize this.:

To study IoT, its challenges and technologies with a focus on LPWAN.

To analyze the two most significant LPWAN technologies in the market, Sigfox and LoRa, while also studying their differences in the smart home context.

To study the various IoT platforms that have a focus on the smart home setting.

To create a prototype using Sigfox technology and to synchronize it with IoT platforms chosen, to obtain a user-friendly smart home system.

To create a prototype using LoRa technology and, like Sigfox, to synchronize it with the IoT platforms chosen.

And finally, to compare the technologies and analyze the results from both experiences.

For each topic discussed in the following chapters there are several papers addressing each subject at length, whether it be IoT, security, rights, LPWANs, Sigfox and LoRa technologies. In fact, for each of the latter, a different thesis could be written, covering the subject with a more in-depth focus. This thesis includes an overview of some of these concepts as well as a proper definition of an Iot application, and it means raising through creating an Iots project of its most primitive form, the sensors that gather data, to the very end, where a consumer can use the details for their benefit with the use of Iot systems..

1.5 THESIS CONTRIBUTION

We will design and develop a smart home system for energy efficient management using LoRaWAN IoT technologies. To achieve this, specific objectives were defined like IoT, its challenges and technologies with a focus on LoRaWAN. LORAWAN technologies in the market, Sigfox and LoRa, while also studying their differences in the smart home context. Various IoT platforms that have a focus on the smart home setting. Creating a prototype using Sigfox and LoRA technology and to synchronize it with IoT platforms chosen, to obtain a user-friendly smart home system. This thesis includes an overview of some of these concepts as well as a proper definition of an Iot application, and it means raising through creating an Iots project of its most primitive form, the sensors that gather data, to the very end, where a consumer can use the details for their benefit with the use of Iot systems..

1.6 THESIS OUTLINE

Chapter 1: Introduction

This section includes a description of the thesis and a quick description of each chapter.

Chapter 2: Theoretical Background

This chapter continues the introduction to the dissertation by reviewing previous studies on catastrophe relief and mitigation using wireless ad-hoc systems, as well as their implementations.

Chapter 3: Methodology

Theoretical outline of the approach proposed in this study is presented in this chapter. It describes the theory's framework as well as the proposed system for execution and reference, as well as several post for implementations. The framework will be trained and evaluated using a database of these. This information will be discussed as well..

Chapter 4: Results

The results and lab practice are presented and compared in this chapter.

Chapter 5: Discussion

This chapter discusses the findings, as well as the thesis's implications and consequences, as well as a summary of possible studies that may be done to further investigate the topics discussed..

Chapter 6: Conclusion

The thesis is summarized and concluded in the final chapter.

2. THE INTERNET OF THINGS

In this chapter, the basic concepts and other fundamental aspects of IoT are addressed. Challenges faced by IoT, such as security, privacy, standards, rights and legal issues are also reviewed.

2.1 DEFINING IOT

In recent years the IoT has become a favorite topic of discussion, an industry buzzword but also a clouded term. There are several advances in technology fields which prompted the appearance of IoT [15]. These technologies continue to evolve alongside it, providing it with new ways for implementation. Among them are:

Ubiquitous Connectivity: more devices at lower costs coupled with new technologies and faster connection speeds, are slowly connecting the world to the internet.

Widespread adoption of IP-based networking: more devices connected to the internet and better software programs enable an IoT connected world [16].

Miniaturization: computers with better performance while, at the same time, diminishing in size, price and power consumption, speed the advance of computer technologies.

Advances in Data Analytics: new algorithms capable of solving more complex tasks, better and bigger data storage and higher computing power enable new ways for data analysis that can generate added value, information and knowledge.

Cloud Computing: allows for small and distributed devices to use more powerful servers capable of advanced analytic and control capabilities for the processing, management and storing of information [17].

As the figure 2.1 shows, in IoT there are physical and virtual things. The physical things are objects which can be sensed, actuated and connected. Examples include machines, goods, appliances, buildings, vehicles, animals, plants, soil and even people. The virtual things are movies, music, books, tickets and application software, among others, which can be stored, processed and accessed.

Physical things are connected to devices which in turn can be represented in the information world by one or more virtual things, with the latter being able to exist without being associated with a physical thing. The devices are hardware equipment capable of communication and, if necessary, with sensing, actuation, data capture, data storage and data processing capabilities. They collect information from the physical world and send it to the information world. They can communicate between themselves in three ways: through communication networks, shown in the figure by the "b" connection; without communication networks, shown by the "c" connection; or with gateways, which can be compared to bridges responsible for ensuring that the information arrives at its proper destination, shown by the "a" connection. Virtual things

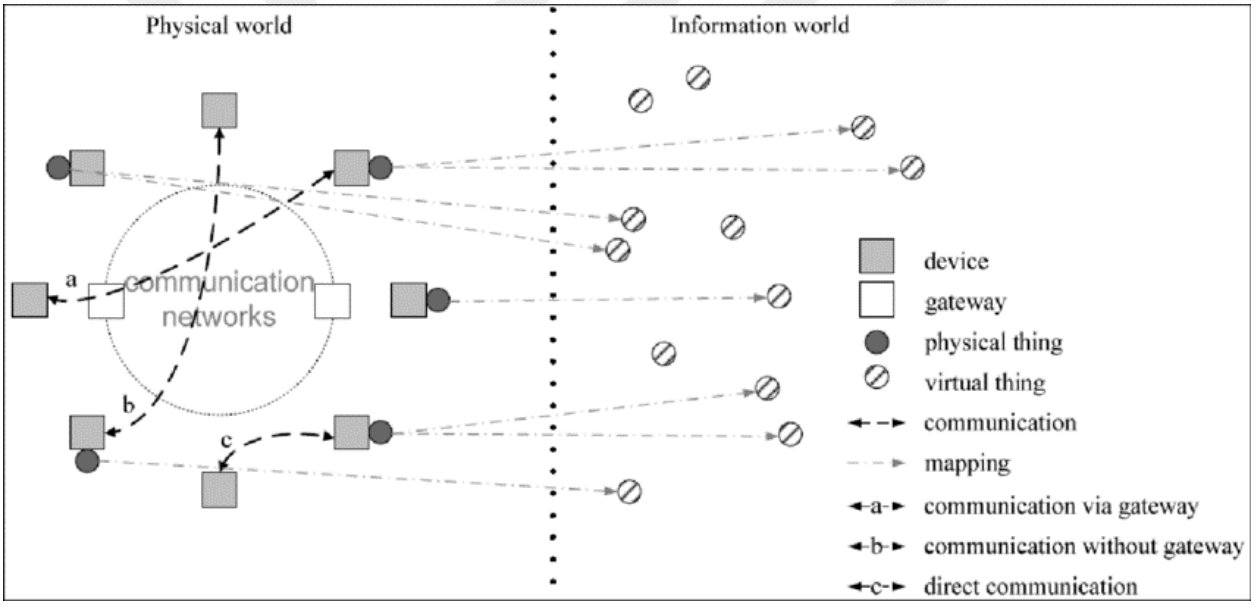


Figure 2.1: Technical overview of the IoT [18].

can also exchange information without the need of the physical things they are connected to. The devices in figure 2.1 can be categorized into four different types.

Data-carrying devices: they connect to physical things in order to bridge the gap between the latter and communication networks, for example RFID tags.

Data-capturing devices: they have the capability to interact with physical things, for example devices capable of reading QR codes, bar codes and RFID tags.

Sensing and actuating devices: they interact with physical things in the environment. They detect and measure information or convert signals into operations, respectively.

General devices: with processing and communication capabilities such as smart phones, home appliances and industrial machines.

The devices, described previously, are used in many different applications. These applications can be grouped into several categories. However there is not a consensus on these classifications. In [19] the IoT segmentation is presented in table 2.1.

In table 2.1 the consumer segment is directly related to an individual or family. Normally devices in this segment have shelf lives between months and years with limited maintenance, with an individual capable of having numerous of these devices. The commercial segment shares characteristics of both the consumer and industrial IoT[20]. It deals with inventory, tracking, management and data analysis. In some cases this segment is grouped with the industrial segment. Lastly, the industrial IoT, is the area where solutions are custom tailored for each application [21].

Table 2.1: The Internet of Things three main segments.

Consumer IoT	Commercial IoT	Industrial IoT
Smart Appliances	Retail	Heavy Machinery
Wearables	Asset Tracking	Transportation
Auto-Industry	Medical Equipment	Power Plants
Smart Homes		Smart Cities

2.2 THE IOT REFERENCE MODEL

There is no standard architecture for IoT. Depending on the communication technology used, or re-quirements for the project, the architectures may use a different number of layers [21]. Some differ in their abstraction levels, going into considerable detail on the layers used. Other go

beyond IoT to include business layers [22], manufacturing and logistic details, while others focus on the industry aspects. Reference models proposed for the IoT, with the status on their development can be found in [23]. One of the most critical technologies for IoT architecture [24], that finds itself under the IoT umbrella, its Machine-to-Machine (M2M) communications, sometimes referred as Machine Type Communications (MTC). Considered a key enabler for IoT, M2M communications is how mechanical or electronic devices communicate and share information with each other and with other applications, most of the time without the intervention of a human counterpart.

The International Telecommunication Union (ITU) proposed reference model for IoT is the one that better applies to a higher number of solutions, because of its level of abstraction. Figure 2.2 presents this architecture consisting of four layers: the device, the network, the service and application support and the applications layer. Present in all these layers are management and security capabilities.

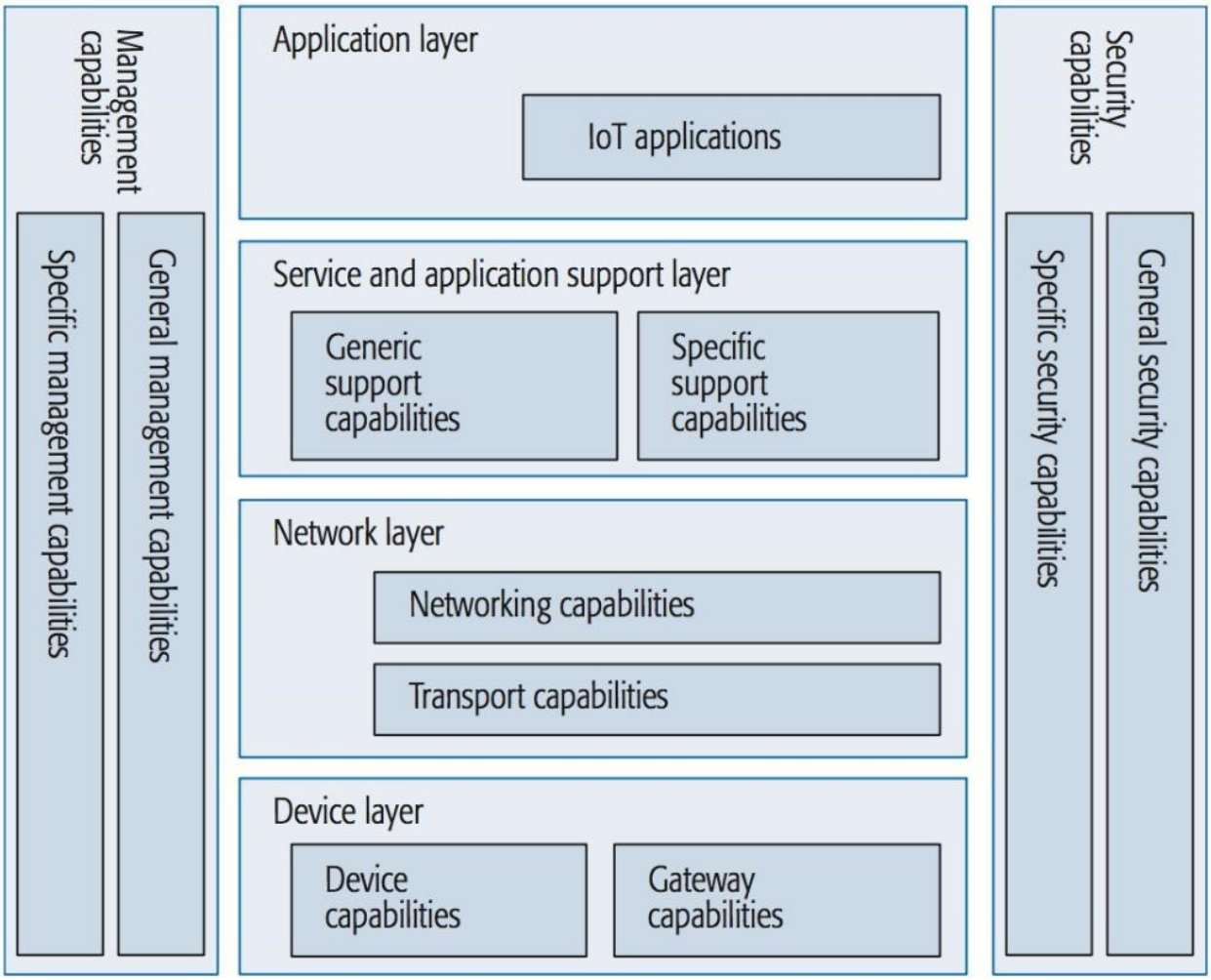


Figure 2.2: IoT reference model [28].

The device layer, sometimes referred to as the perception or sensing layer, is composed by devices and gateways. The device capabilities are responsible for tasks such as identification, gathering and uploading information from the environment or from the thing they are connected to.

2.3 DISASTER MANAGEMENT USING CLOUD COMPUTING

Cloud computing is way to store, manage and process data in a network server, which is hosted on the Internet, instead of using a local server or personal computer. It eases the process of collecting and processing the information from the IoT devices, and also enables the rapid setup of new ones, lowering the costs for the deployment of IoT solutions and complex data processing.The cloud handles the data flow to and from the client, data synchronization between

devices and data processing . It is in the cloud that all the information from the billions of IoT devices is stored, processed and analyzed [25].

The advantages offered by the cloud to IoT are better seen when one considers the complementary aspects of both technologies. The cloud acts as a centralized manager that can see all the applications requiring computational effort, and therefore reallocate its resources to better manage its demands.

For LPWAN technologies, cloud computing takes an even bigger role as report [26] shows. In it, IoT devices are separated by their computational abilities where LPWAN solutions were found to rely heavily on the cloud, due to their low computational abilities, for data storage and management, focusing only on data acquisition.

The cloud can also offer opportunities to implement applications and services that exploit the things and the data they produce, for example, IoT platforms. These platforms aim to reduce development risk and cost so that companies can bring products to the market faster and more easily. They are capable of displaying the information sent from the devices in a easy to use and appealing way, giving users a new way to interact with their devices and companies a way to manage their fleet. In [27] a list of 450 IoT. Platform companies is presented, where big technology companies, like Microsoft [29], Amazon [30] and Google [31] already offer IoT platform solutions. Big Data is another new term born from the continued expansion of cloud computing and IoT. It represents not only the large amounts of data that the cloud stores, but also what can be gained by managing that data, labeling, processing and analyzing it. IoT is expected to generate most of the information for big data, which coupled with the benefits of the cloud will enable the possibility to perform extremely complex analysis, data driven decision making and develop better prediction algorithms at low costs [32].

IoT cloud computing solutions bring some challenges as well [33], such as: the cost of the transfer may be high, depending on the amount of information; storing large amounts of data on the cloud may be expensive; Internet access may be unavailable, unreliable and slow, or congested by big data transmissions; Internet transmissions may increase the probability of information leakage; the devices that do not have the necessary security measures may be

targeted for Distributed Denial-of-Service (DDoS) attacks; and others. Fog computing, sometimes referred as edge computing, solves most of aforementioned problems.

2.4 INTERNT OF THINGS STANDARDS

Standardization brings a lot of benefits to technology areas but it can also be a very slow process, hindering rapid success or adhesion. There are several organizations currently working on IoT standards, such as: the European Telecommuni-cations Standards Institute (ETSI) , the Institute of Electrical and Electronics Engineers (IEEE) [40], the International Organization for Standardization (ISO) [34], and the International Telecommunication Union (ITU) [35]. The European Commission is also working in IoT standardization, launching a paper [36] on the standardization requirements for IoT technologies where the current standards are reviewed, the gaps are discussed and recommendations for the future are presented. A table with all organizations working on IoT standards and their standardization activities can be found in [37].There were not found any standards from ETSI specifically relating to IoT. However the organization has various standards under development which relate to technologies associated with it. Most of these are about M2M communications and, for example, the impact that smart city activity could have on IoT environments.

IEEE was the organization found with most standards associated to IoT, but like with ETSI, specific ones for IoT, were not found. It has eighty IoT related standards, such has wireless access in vehicular environments, health informatics and others like Ethernet standards which, although under the IoT umbrella standard division, are not about IoT.

ISO has a technical committee, the ISO/IEC JTC 1/SC 41, with a scope on the IoT and related technologies. These include sensor networks and wearable technologies. It has fifteen published standards focusing on sensor networks, underwater acoustic sensor networks and IoT use cases. Nine others are currently under development, for example on IoT definition and vocabulary, the interoperability in IoT systems, underwater acoustic sensor networks and the IoT reference architecture.

2.5 PRIVACY AND LEGAL ISSUES

The amount of data generated by Iot., combined with advancements in computing that allow for the creation of contact lists, raises privacy risks, which are one of the key concerns with regards to the risks raised by Ai devices. According to [38], 80 percent of Sensor nodes breach personal data protection such as a person's name and date of birth. More than 80% of respondents did not request codes of sufficient complexity and difficulty, and 60% had security holes in their web applications [39].

Some of these issues have been addressed in legislative studies over the past few days. Facets of Euro Zone security laws relating to IoT are mentioned in [40]. The Federal Trade Commission (FTC) in the United States, which publishes papers on confidentiality and support, is also confronted with law and protection issues. [41].

Beginning with private details, users to Iot. will be considered data objects under EU law, which indicates that if a computer contains private information about than a user, that user will be considered a data target even if the device does not belongs to their. The parties involved, which are referred to as data controllers, are in charge of the collection and use of private information. Device producers, social networking sites, information server applications, and fifth app developers are instances of investors. Under EU law, the manner private information is treated is also discussed., with the case participant's agreement on how the decisions are made being a key factor, but bearing in mind that now the individual in question might be required for the terms of the contract or requirement whereby the individual in question accepted. Likewise, the very same data procedure might be required for the information pilot's core rights, unless it infringes on the data subject's constitutional protections. Often discussed is the equality in database collection and management.. Aspects like purpose limitations, which state that the data collected must have specific, explicit and legitimate proposes are addressed. Furthermore, data minimization aspects are mentioned as well, which discuss how the data should only be collected for the necessary use, and not stored by default.

In other points ranging from transparency, security, data subjects rights, processing of sensitive data like health information and recommendations to stakeholders and device manufacturers are presented. However, all these challenges expressed previously represent only a small part of the

problems facing IoT and the prospect of a connected world. For example, legal issues also encompass problems such as: cross border data flows; data discrimination; the case of IoT in the aid of law enforcement and public safety, which leads to questions of mass surveillance systems; the liability of IoT devices; and the proliferation of legal actions in regards to IoT .

2.6 SECURITY OF IOT DEVICES

There are several types of legal threats to which IoT is susceptible, all of which can be classified. Assaults, cyber - attacks, application assault, and authentication assault are the four intrusions. Only what else are labeled the very worst assaults in compliance with will be addressed in the following paragraph. Beginning with assaults, one of the most worrisome is the malicious software antimicrobial agentA newly virus gets added to computers or access points that carry a virus, or a handset is connected to the system that has been infected, in this means of violence. The affected computer will then transmit misleading data to other connected devices, causing them to become corrupted. The intruder could acquire access to the device and make the process inaccessible.. Safe security and boot up, intrusion prevention tools, or perhaps a filtering ssl cert, in which a control entity authenticates others for questionable activities and adjusts accordingly, are some of the defences against this type of assault. Other assaults in this group include nodes manipulation and specific physical damage, which refers to computers that were tampered with. Replaced or destroyed, as necessary. This makes the items on that computer vulnerable to theft, including encrypted data, port numbers, and contact keys, among some other things. As a result, the computer becomes a danger to the architectural design greater tiers.

The subsurface assault is among the most harmful in the media impacts chapter. In this assault, a computer is hacked and used to carry out the crime. The approach is carried out by misleading route discovery so that other computer networks believe the infected system is adjacent to an access point or firewall, diverting traffic to it, which can results in traffic being altered or even removed.. Encrypted data and reliable encryption are used to prevent the corrupted nodes from gaining access to the system, or security precautions are usually applied to the packages sent. Man-in-the-middle assaults, in which an armed robber deploys information between the modules over the Web, are another sort of violence., or Remote Rejection (DDoS) assaults, in which an intruder loads a device with traffic, rendering it inoperable..

Infections, parasites, malware, and ransomware are the most dangerous and popular types of malware attacks. Spyware based on self is used in these assaults, which are usually delivered via email or file downloads from the Net. Bashing, rightwing, and anti-adware applications, as well as sophisticated authentication, are all effective defences against these kinds of malware..

The left assault one of the most higher levels of psychological distress of encryption assaults. This method of assault employs cyphers, which are a set of cryptography more widely used in cryptography, to obtain informations, such as power saving, taken to finish tasks just on scheme, limited or complete additional payments, or even the key exchange.. Timer strikes, which calculate how long formulas take to complete, and differential damage detection assault, which reveal informations by introducing bugs in mathematical calculations, are two examples of side-channel assaults. Developed cryptographic keys are used to defend against such a means of violence.

We have discussed more attacks and their counter measures earlier in this chapter . These attacks endanger the perception and adoption of IoT, and there are already cases that have put IoT adoption into question due to particular attack cases. In the smart home setting, for example, ways to control personal assistants in the home through the use of ultrasounds imperceptible from humans have been found. By using normal voice commands and transforming them using programs, through the use of harmonics, that shift the signal into frequencies above the human hearing range. These attacks gained the term of "dolphin attack" because of the way dolphins use high pitched noises for echolocation. There are also worries that IoT devices with cameras represent a way to introduce a camera into peoples homes . Hardware hack techniques, called flash memory attacks, exploit software bugs that not only expose the hacked device but every other unit of that model . Other, more personal and concerning problems are hacked baby monitors , or being able to stop a pacemaker from working . To face these problems the Federal Trade Commission (FTC) and other organizations like the non-profit Internet of Things Security Foundation (IoTSF) have provided reports and studies to alert to the possible dangers that IoT may bring and the first steps to prevent them.

Precursor, rerouting traffic through it, which can resulted in data being distorted or even lost. Authentication and reliable protection are used to prevent the corrupted nodes from gaining access to the device, or safeguards are applied directly to the bytes received. Man-in-the-middle

attacks, in which an intruder communications information transmitted among nodes over the Web, and Remote Ignorance (DDoS) attacks, in which an intruder loads the channel with traffic, rendering it inaccessible or inaccessible, are two other forms of assaults.

Pathogens, parasites, adware, and ransomware are the most dangerous and popular types of malware attacks. Malware good at self is used in these assaults, which are usually delivered via email or file downloads from the Internet. Anti-virus, anti-spyware, even anti-adware applications, as well as sophisticated protection, are all effective defences against these forms of threats..

The left threat is one of the most higher levels of psychological distress of authentication threats. This form of attacks employs cyphers, which are a set of quantum cryptography most widely used in cryptography, to obtain informations, such as energy harvesting, data to perform processes on the structure, minor or total additional payments, or the key exchange. Scheduling threats, which calculate how long equations take to complete, and differential predictive control assaults, which reveal information about the system by introducing fault in arithmetic operations, are two examples of right side attacks. Developed security mechanisms are used to defend against all this form of attack.

2.7 WIRELESS TECHNOLOGIES

There are various wireless technologies which can be used in IoT projects, such as: cellular technologies; Wi-Fi; Bluetooth; Zigbee; Sigfox; LoRa; and Weightless. Figure 2.3 shows the relation between range and bandwidth offered by several IoT technologies. LPWANs offer the greatest range with very low bandwidth, which no other technology can match.

Figure 2.3: Range versus bandwidth [42].

There are several ways to classify these technologies, whether from short to long range or from low to high power. Table 3.1 represents nine technologies grouped from short range to long range, both LPWAN and cellular.

Table 2.2: Short and long range IoT Technologies [43].

Fixed & Short Range	Long Range Cellular	Long Range LPWAN
Wi-Fi	LTE-M	Weightless
Bluetooth	NB-IoT	Sigfox
Zigbee	EC-GSM	LoRa

The most used Wi-Fi protocol, is the 802.11. It works in the 2.4 GHz or 5GHz band and can handle speeds from 300 Mbps to 1.3 Gbps, with ranges up to 100 meters depending on the condition. New advancements in Wi-Fi continue to be made with the Wi-Fi Alliance planing to implement a program for testing and certification of the 802.11ah protocol by 2018. This new

protocol, nicknamed HaLow, is set to compete with IoT technologies by using lower bandwidth and power with frequencies below the 1 GHz band.

Bluetooth works in the 2.4 GHz band. It has different variants which offer different data rates, power levels and ranges. Normal data rate is 1 Mbps, with 2.1 Mbps and 3 Mbps possible. It has three ranges, the first reaches up to 100 meters, the second 10 meters and the third only has a reach of one meter. The last version, Bluetooth 5.0, offers a specific connection for long range, with the worst case being 200 meters outdoors and 40 meters indoors.

Zigbee is a technology based on IEEE 802.15.5 standard for low rate wireless personal area networks. It operates in the 2.4 GHz band but it also has the ability to be used in the sub 1 GHz bands. Data rates in the 2.4 GHz band are 250 kbps, and in the sub 1 GHz are 20 kbps. It has a reach of 100 meters in line-of-sight conditions.

LTE-M can be used to refer to all LTE based technologies for IoT. This includes LTE-Cat-1, LTE-Cat-0, LTE-Cat-M1 and eMTC. These represent simplified versions of LTE, especially designed for low power and low speed, with Cat-0 and Cat-1 solutions offering data rates of 1 Mbps and 10 Mbps respectively. They have battery life up to ten years and use licensed frequency bands. LTE IoT objects will use SIM cards for security .

NB-IoT, which stands for Narrowband IoT, is a new radio technology being standardized by 3GPP. It uses 14 different frequency bands with 10 of them in the sub-GHz range. It offers low complexity (close to 90% in comparison to Cat-1), low power consumption and long range, with data rates ranging from 100 kbps to 1 Mbps. This new standard can also be deployed in any LTE network as a software overlay , and depending on traffic and coverage needs can achieve a battery life close to ten years.

EC-GSM which stands for Extended Coverage GSM, is an evolution of EGPRS towards IoT, with data rate between 70 kbps and 240 kbps and like LTE-M and NB-IoT offers a battery life in the ten year range.This standard includes the latest enhancements to the GSM and EGPRS standards to support better coverage, with the possibility of being deployed in existing GSM networks .

Last but not least, 5G technology is expected to play a bigger role in the IoT future but is still a few years away, with its first specification released in the end of 2017 and a goal to complete Release 15 in mid-2018. These new cellular IoT solutions although still a few years away from being deployed are considered the biggest threat to LPWANs like Sigfox and LoRa.

2.8 LOW POWER WIDE AREA NETWORKS

Before 2013 the LPWAN term did not exist. LPWAN are technologies which focus on three main aspects:

Low power: few applications in IoT have the possibility to use a generator for power, so most devices are powered by batteries. LPWAN devices have a battery life with ranges in 5 to 10 years.

Long range: wireless networks need some kind of access point (gateway or base station). LPWANs generally have ranges from 2 to 10 km in urban settings, offering more mobility in deployment and the need for less gateways.

Low data rates: data rates are generally lower than 5 kbps and therefore LPWANs only send small packets of information ranging from 0 to 256 bytes.

One of the characteristics that separates LPWANs is the type of radio spectrum they use. Most operate in the sub-GHz band which are Industrial, Scientific and Medical (ISM) bands. These are public, open but regulated radio bands designed especially for use proposes other than telecommunications. The equipment in these bands are subject to all interference generated by ISM applications. The most used bands for LPWANs are generally: the 433 MHz and 902-928 MHz, in Asia; the 902-928 MHz in America; and the 863-870 MHz band in Europe. As the work focused on the 868 MHz band, only this band was reviewed. The 863-870 MHz band has a power limitation of 25 mW (14 dBm) and a duty cycle of 0.1%. In the 868-868.6 MHz band there is an extension to a 1% duty cycle and in the 869.4-869.65 MHz band an extension to 10% duty cycle and 500 mW (27 dBm) power is possible, which is normally used for downlink messages.

Currently there is no adopted standard available in the LPWAN market and they are usually defined by the radio technology used :

Ultra-narrow Band (UNB): this type of technology uses modulation to achieve a very narrow bandwidth, reaching greater distances. It only supports low data rates, with a typical payload being around 12 bytes with its duration taking around 2s. UNB LPWANs are only used in applications where reliability and Quality of Service (QoS) are not very important.

Narrowband: this type of technology offers the best compromise between QoS, capacity, cost and network efficiency. With channel bandwidths around 12.5 kHz wide, they offer the best capacity for uplink traffic of moderate sized data payloads from a large number of terminal devices;

Wideband: the channel bandwidth of these technologies range from 500 kHz to over 1 MHz.

As this thesis focus on Sigfox and LoRa, a more in depth discussion of these technologies will be presented in the following section. Another LPWAN technology is described, chosen for being an open standard.

Weightless is a LPWAN open wireless technology, from Weightless Special Interest Group, which includes three specifications, each catering to a different LPWAN need. Weightless-W operates in the TV white space, using channels 6 MHz wide in the 470-790 MHz band. It offers bi-directional transmission and the data rate is between 1 kbps to 1 Mbps. It has a range of 5 km and a battery life around 3 to 5 years. Weightless-P is a high performance bi-directional communication, using 12.5 kHz wide channels, that operates in the 169, 433, 470, 780, 868, 915 and 923 MHz bands. Data rates can range from 200 bps to 100 kbps, with a typical range of about 2 km and a battery lifetime of 3 to 8 years. Weightless-N uses UNB technology, operates in the 800-900 MHz band and only offers uplink transmissions. It has data rates of 100 bps and has a typical range of 5 km. Intended for low cost applications, it reduces the power consumption, with battery life up to 10 years .

2.8.1 Sigfox Use on IoT Applications

Sigfox has the objective to deploy a global cellular network with a focus only on IoT applications. It is the most mature LPWAN technology, with their first network deployed in 2012 in France, and currently present in 45 countries throughout the world. In a move to become a

more active player in the development of IoT standards, Sigfox has joined ITU as a member in 2017 .

Technology Characteristics

Sigfox uses a proprietary technology offering low power, low data and long range solutions. It is both a wireless technology and a network service. It is a UNB technology, works in the ISM band, and in Europe uses 192 kHz, in the 868-868.2 MHz band . In the rest of the world it uses the 902-928 MHz band, with restrictions according to the regulations of the country.

Sigfox messages can be bi-directional. The uplink uses Binary Phase Shift Keying (BPSK) modulation and has a data rate of 100 bps in Europe and 600 bps in America. Each message is 100 Hz wide, and is 0 to 12 bytes long, with the latter taking 2.08 seconds over the air . Europe regulations only permit the use of the 868 MHz band 1% of the time, which equates to 36 seconds air time in an hour, corresponding to 140 messages, per day, per device, or roughly six messages per hour. Although messages that use fewer than 12 bytes would be sent faster, making it possible to send more messages in a day, Sigfox does not allow it. Sigfox uses the honor system to ensure the users comply with these limitations, saying that it is the responsibility of the country's telecommunications authorities to ensure the regulations are followed, but also saying that if a user abuses the system they can blacklist devices . All Sigfox messages are sent in hexadecimal format. The Sigfox protocol overhead uses and additional 14 bytes making the Sigfox frame 26 bytes in total. When a device sends a message, it uses a random frequency and then sends two replicas on different frequencies and time. The maximum range achieved by Sigfox is in the thirty to fifty kilometers in the countryside, or three to ten kilometers in an urban setting [17], with battery life usually in the 10 year range.

The downlink uses G-Frequency Shift Keying (FSK) modulation with a data rate of 600 bps. The downlink frequency is the frequency of the first uplink message plus a known delta, which puts the frequency generally 1 MHz higher where the regulations on the band are 10% duty cycle. Downlink messages are static eight bytes and only four, per device, per day are permitted. If, for example, more than four messages are sent a best effort will be made to see if more can be received but devices which have not received the four message daily limit will take precedent.

The downside of Sigfox downlink messages is that they can only be initiated by the devices following an uplink message. There is a twenty second delay between the first frame and the reception window, that lasts for twenty five seconds maximum . Following the reception of a downlink message, the device has to wait a minimum of six seconds before sending another uplink message [18].

Architecture

Figure 2.4 presents the Sigfox architecture, which consists of devices, base stations, the Sigfox cloud and the interfaces used to access the information on it. These are all essential functions for

Figure 2.4: The Sigfox architecture [44].

the deployment, operation and monitoring of the network. Also on this layer are the tools to analyze the data collected or generated by the network.

There are three ways to interact with the Sigfox cloud, as shown in figure 2.4:

Internet: access to a web portal, through a web browser, made for end-users to access all Sigfox cloud functions.

APIs: access to the cloud functionality using APIs in pull mode, permitting the integration of some of the Sigfox cloud functions in third party applications.

Callbacks: enable the reception of new events automatically, such as messages in push mode, which means getting data directly, without asking, by being notified by the Sigfox cloud when a new messages comes in.

Access to these interfaces and tools depends on the type of profile the user has on the Sigfox cloud. For example, a user can be only authorized to view messages, manage users and device

fleets, see service maps or check contracts. A distributor will be able to create contracts, while an operator will be able to access radio planning tools and network monitoring solutions.

Callbacks can be custom made or use simplified bridges, with Sigfox currently supporting bridges for Amazon AWS, Amazon AWS Kinesis, Microsoft Azure Event Hub and IoT Hub. There are three types of callbacks: data, service and error . Data callbacks can be uni-directional, offering three types of channels: email, URL and batch-URL. Or they can be bi-directional, offering URL and batch-URL channels.

Security

Sigfox implements security on all aspects of its architecture, from devices, to data, to radio and the cloud. At the device level, devices do not have internet connectivity, which ensures that they cannot be hacked through the internet. Each device has a different key unique to it, which guarantees that the compromise.

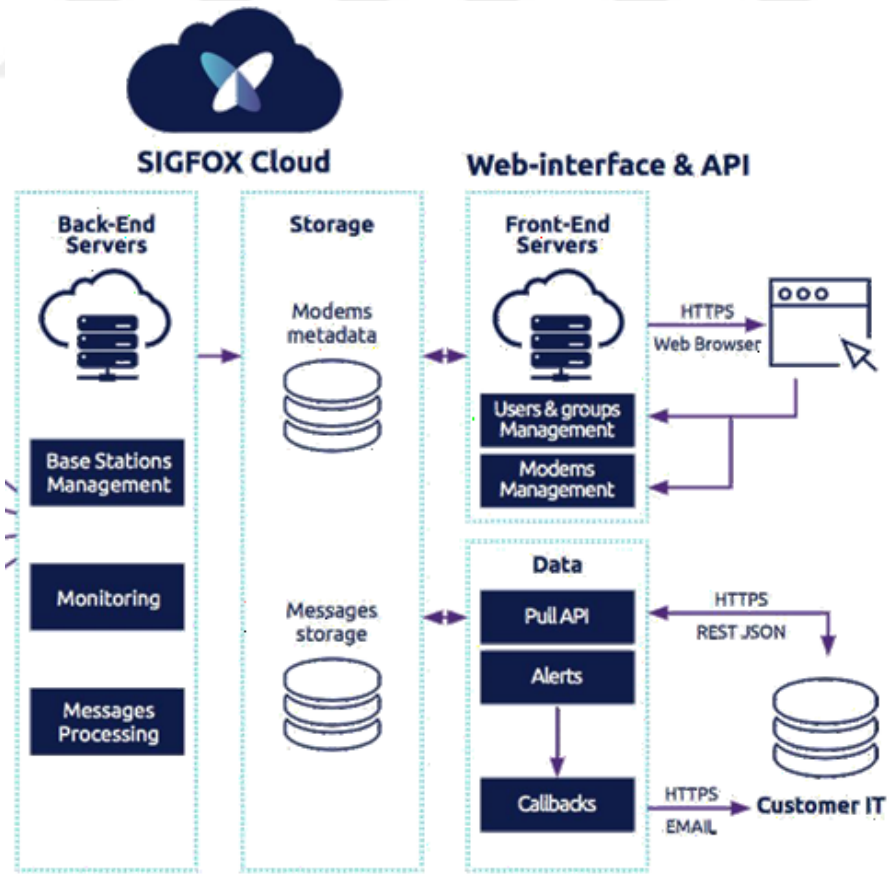


Figure 2.5: A detailed view of the Sigfox cloud [45].

of one device has a limited impact on the system. Also, Sigfox devices have dedicated resistance to interference available through secure elements, which are microcontrollers that secure applications and their confidential data.

2.8.2 Smart Home Using LORA

LoRa (LOng RAnge) technology was designed and developed in 2009 by Cycleo , and later acquired and patented by Semtech in 2012. It is an established LPWAN technology, focused on IoT applications. Semtech expected it to be present in more than 60 countries around the world at the end of 2017 . LoRa has two distinct aspects. The first is the LoRa physical layer and the second, an open MAC layer protocol called LoRaWAN, that provides access to the LoRa architecture . To talk about LoRa one has to address the LoRaWAN protocol, an open standard communication, and the proposed MAC layer defined by the LoRa Alliance consortium, a non-profit association led by IBM, Actility, Semtech, Microship and many other members, which drives the advancement of LoRa and the LoRaWAN protocol. However, LoRa can use other MAC layers protocols.

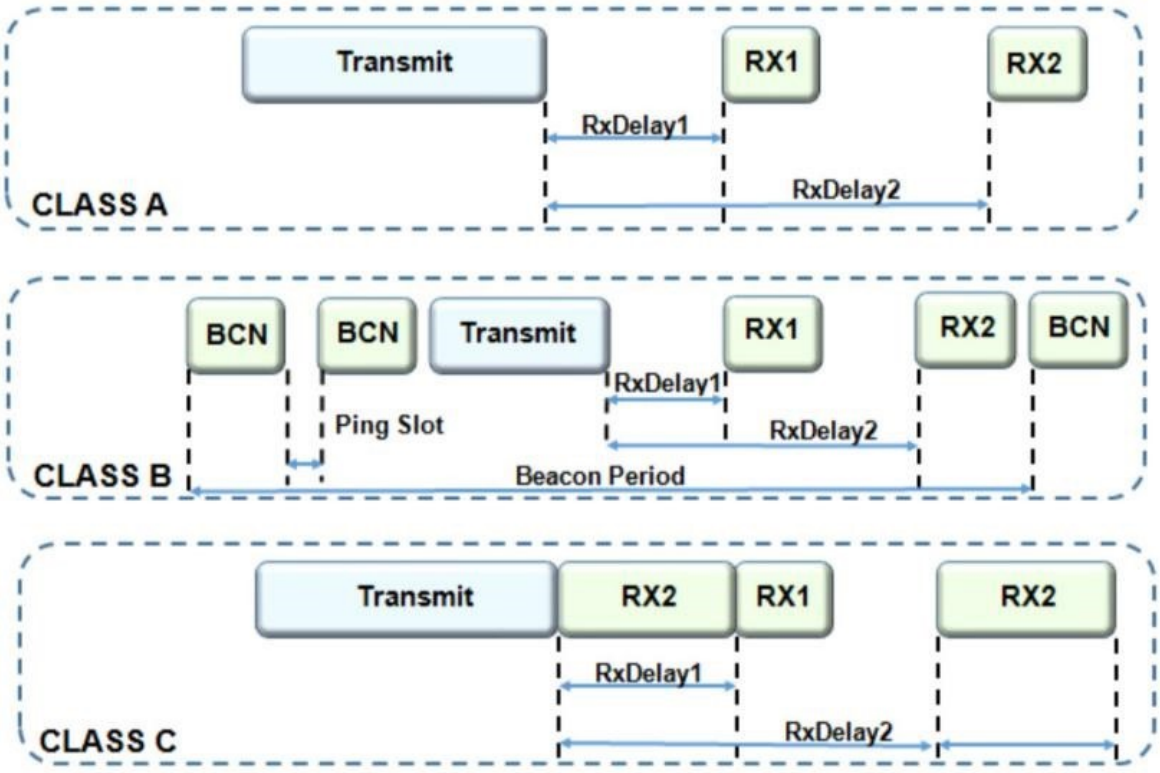


Figure 2.6: LoRaWAN device classes [46].

2.8.3 Differences between Sigfox and LoRa

Table 2.2 presents some the differences between the most important technical aspects of both technologies.As LoRa only represents the physical layer, the differences to Sigfox were made with LoRa using LoRaWAN. Both technologies use the same frequency band in Europe and their ranges are very similar. Sigfox uses ultra-narrowband technology, with very small bandwidth. LoRa, on the other hand, uses modulation based on Chirp Spread Spectrum (CSS), with a wider band .

The technologies also differ in the amount of messages that can be sent in the up and downlink transmissions, as well as the size of the payload. Therefore, Sigfox is better suited for applications that do not require constant exchange of messages, but only a handful of messages per day. LoRa has more leverage in the amount of messages it can send daily. For example, it does not send two replicas of the same message every time one is sent. It can manage higher transmission speeds, which equate to less time on air, therefore, account for even more messages. As referenced before, Sigfox takes 2.08 seconds to send a twelve byte

Table 2.3: Differences between Sigfox and LoRa/LoRaWAN.

	Sigfox	LoRa/LoRaWAN
Frequency	867 MHz (EU) 901-928 MHz (USA, AS)	868 MHz (EU) 915MHz (USA), 470 MHz (AS)
Range	3 - 10 km (urban) 30 - 50 km (rural)	2 - 5 km (urban) 15 - 45 km (rural)
Data Rates	90 bps (Up), 610 bps (Down)	250 bps - 27 kbps
Topology	STAR	STAR
Modulation	DBPSK (Up), GFSK (Down)	CSS
Payload	12 Bytes (Up), 8 Bytes (Down)	19 - 250 Bytes
Power levels	0 - 14 dBm	0 - 14 dBm
Battery Life	10 years	10 years
Messages/Day	140 (Up), 4 (Down)	Unlimited
Bandwidth	100 Hz (Up), 1.5 kHz (Down)	125 kHz, 250 kHz, 500 kHz

message but, even if only a six byte message is sent, which would takes less time, Sigfox continues to only allow the 140 daily limit, while on LoRa, different sized messages will have an impact on the air time and consequently on the number of messages that can be sent.

Another difference is in the base stations from Sigfox and the gateways from LoRa. Sigfox deploys and manages its own base stations, while LoRa gateways can be bought or made. LoRa gateways can be found at varying price levels with some costing 1600 e, others 800e , or even 150 e, with the use of a raspberry pi.

Regarding devices, both technologies also differ. Sigfox does not design any hardware, opting instead to share their design and license its software to vendors, such as, Texas Instruments, Samsung, Telit and Axcem. It uses a certification scheme on the hardware, called "SIGFOX Ready", with devices getting sorted by class 0, 1, 2 or 3 based on their radiation performance rating. More information on Sigfox certification and devices classification can be found in. This type of model means that is necessary to work directly with Sigfox because there is no other option.

2.9 STATE OF THE ART DEVICES FOR SMART HOMES

Through the Sigfox partner solutions site, Sigfox offers transceivers, System on a Chip (SoC), modules, devices and developer kits. Five transceivers are currently available from Texas Instruments and Silicon Labs. They are: the AX5043; S2-LP; CC1120; CC112; and the SI446X transceiver family. These transceivers are all capable of working in the ISM frequency bands at 433, 868 and 902 MHz and at additional programmable frequencies. The prices vary between the 0.5 to 5 erange. Also available at the Sigfox site are 10 system-on-chip, 54 modules, 374 devices and 66 developer kits.

For LoRa, Semtech currently has five transceivers available. They are: the SX1272 and SX1273 for frequencies between 860-1000 MHz; the SX1276, for 137-1020 MHz; the SX1277, for 137-1020 MHz; the SX1278, for 137-525 MHz; the SX1279, for 137-960 MHz; and the SX1268, the SX1262 and the SX1261 for 150-960MHz . These devices are currently all within the 4 to 10 eprice range. Also available are two chips for LoRa gateways: the SX1308 for indoor gateways and SX1301 for outdoor gateways.

Lora deployment has continued to advance as networks are set up all over the world. In Korea and the Netherlands, the telecom companies responsible for the deployment of LoRa network in their respective countries were both members of the LoRa Alliance.In London The Things Network (TTN) launched fifty LoRaWAN base stations free to use across the city for IoT devices.

Because cellular IoT technologies are still in their early stages of development products which use these technologies are hard to find. However, for NB-IoT the first roll-outs of the technology are expected for 2018. In 2017, u-blox, a Swiss company in the natural gas market announced their successful field trials on their NB-IoT network . At the start of 2018 Cisco was the first company to launch a global NB-IoT platform solution that, in conjunction to NB-IoT, will also allow for enterprises to manage cellular devices .

IoT is also seen entering commercial areas. For example, the Amazon Go is a new generation of shop where through the use of sensors, machine learning, artificial intelligence and computer vision, shoppers can enter the store, take the products they want and leave, effectively eliminating queues. After leaving, the user will be notified of the purchase and the price of the products will be deducted from their account.

Mobile phones, incredibly clever aids, are one way that the Internet of Things has made its way into in the lifestyles and, by definition, into the homes. Digital assistant like Android Now, Amazon Alexa, Voice Commands, and Virtual Assistants, as well as tech giants' drive towards quantum computing, would be a crucial step to a more unified IoT environment. Many smart devices, such as Amazon Alexa Echo with Amazon echo, have indeed made their way into the market. These voice assistants now can opening and lock the door when used in combination with IoT devices. The Ebay key, or example, allows you to unlock doors remotely by installing an intelligent deadbolt. With a set of security devices, items will open up the door with only an order, allowing them to drop parcels from the inside of the property when the buyer is not present.

Other smart devices, such as the window birds phone, are already on the market. This is a keyless entry system, similar to the Kindle key, that alerts the user via telephone someone who is at the backdoor, allowing they to see, talk to, and open doors anywhere in the universe.. Since in

the house, it uses Wi-Fi connectivity, and when travelling abroad, it uses 3G/4G services. The Eve Level is a system that displays the latest relative humidity in a recipient's homes and arrives with a smartphone app for quick permissions. Home appliances can also be made purely from ground up, with an emphasis on flexibility and the Internet of Things. Kasita is a small home that helps in controlling any part of it with the help of voice recognition from digital sensors..

There are also Sigfox apps for the connected home. The Sens'it 2.0 unit can measure humidity levels, as well as luminance in a house. The "bttn," the Sigfox tool, is a little multifunction system that allows users to order goods or items with a single push. Sigfox has also collaborated on a baggage monitor with Ralph Lauren..

LoRa has based smart gadgets as well. Centered on LoRa technology, Eddy Home offers a moisture control and utilization tracking device. It has an unique screen that allows people to see your water consumption and information at home, either on a mobile using eddy home screen or on a desktop using a web..

The IoT is also dominated by vulnerabilities. Cryptocurrency is one approach that is now being researched to address these issues. It's already showing up in products like the Open Iot System.

This tech's developments have already made their way into the connected home.

Figure 2.7: Smart Home Devices[47]

3. METHODOLOGY

We have gone over smart home solutions in great detail in this literature review. The measures to synchronise the tools with different Iot applications are addressed next, followed by the encounters for Sigfox and the changes in the measures and indicators. Next, the LoRa encounters with configuring the firewall and plugins, as well as the measures for synchronising them with their very own operating systems and 's output. A connected home IoT design balance can be achieved in two different ways. Figures 3.1 and 3.2 show 2 major systems that could be used to achieve the intelligent home development's preferred result..

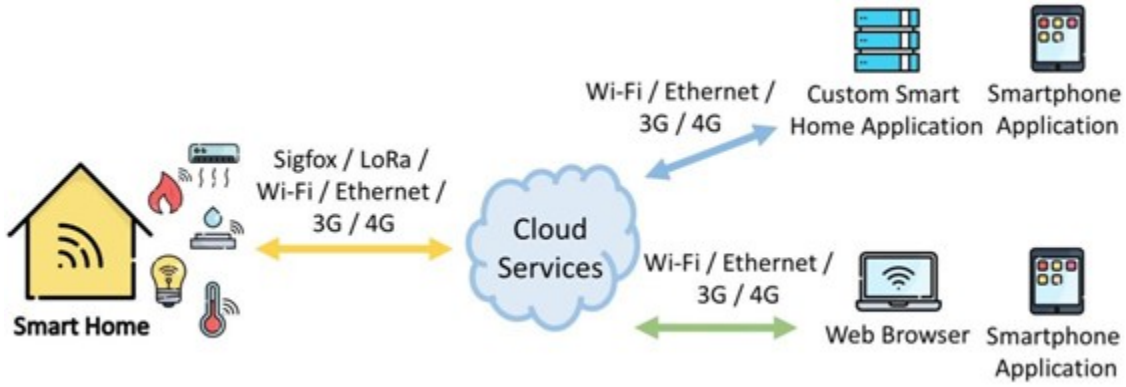


Figure 3.1: Smart home architecture solution using only cloud services.

The apps will submit the data to their corresponding cloud computing in the first implementation (shown in figure 3.1). The data could've been used in one of 2 ways: through an unique home automation and smartphones app, or through a browser and a mobile app. An installed central web server in the technology, typically called to as a node, will be the personalized voice controlled device.. This framework would collect smart devices and send it to the server, which would then be displayed on individual console games that could be placed on wall or in tablet with different professionals. Users will be able to use a mobile companion request for the customizable smart tv, or provide house details when on the go. The other option is to use a website with a webpage, a laptop computer, phone, or device, or an iphone app created by the

cloud provider on its own to gain user data from the cloud provider.

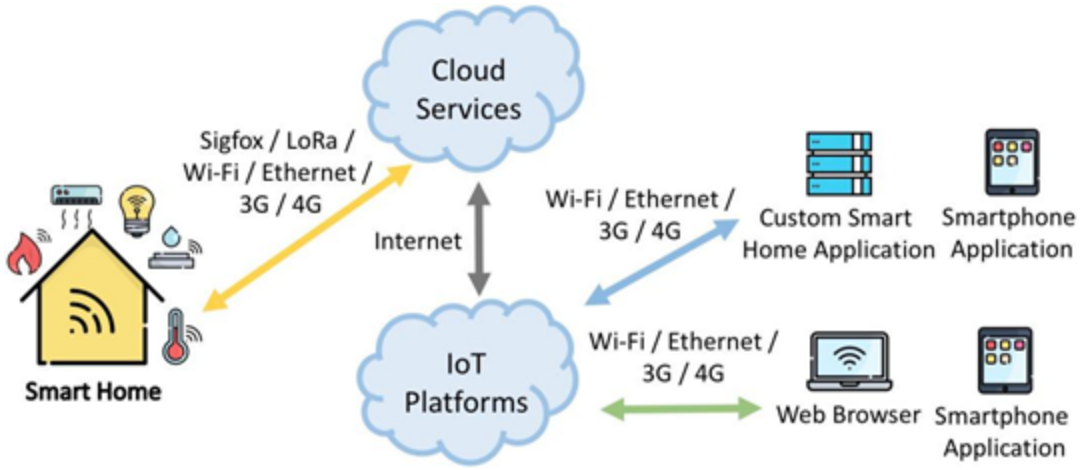


Figure 3.2: Smart home architecture solution using IoT platforms.

The systems will still send data to their different cloud service providers in the second step (shown in Figure 3.2), but the data will be forwarded to an IoT network. The data could now be processed using a tailored connected home programme or a phone app, much as in the proposed methods.. The main difference is that IoT systems get a more client layout and are much more browser in total. This indicates that, in the this scenario, a new homekit device will only have to explain things sent to the network, rather than getting its own applications designed for use by the. The Electronic resource may also have a dedicated phone device..

In the case of Sigfox, the cloud has a very basic and not user friendly interface, because it is not meant to be used as a platform, and the options for device analytics are limited. So, the better solution would be to use the architecture in figure 3.2. This way the information from the devices could be parsed and better presented by the IoT platforms, offering more statistics and history about the home devices, for a better understanding of their home use.

In the case of LoRa, because some of the network servers also serve as IoT platforms, the better solution, would be to implement the architecture in figure 3.1.

3.1 SIGFOX SOLUTION

For the Sigfox smart home solution, the architecture used in this work is presented in figure 3.3. To achieve it, several steps were taken.

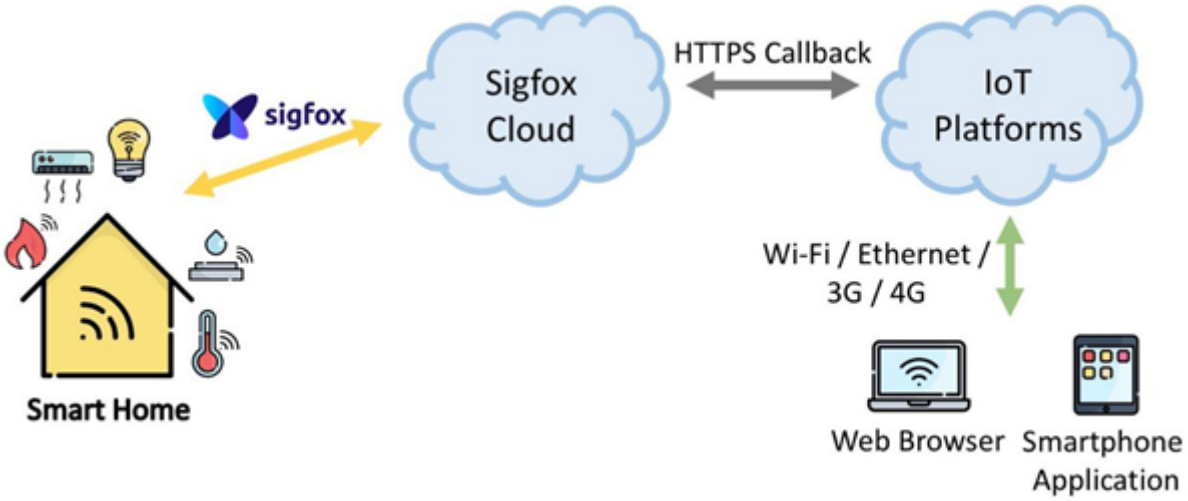


Figure 3.3: Proposed smart home architecture using Sigfox technology.

The first step was to make and program a prototype using Sigfox technology. The second was to register the prototype with the Sigfox cloud and successfully receive the Sigfox messages at the back-end. The third was to synchronize the prototype with several IoT platforms to see which one would be better suited for the smart home architecture designed. The fourth, and last, was to build a dashboard, so that a user could access it by way of a web browser or smartphone application. Three hardware developer kit modules were used. The Telecom Design TD1208 Evaluation Board Kit , which was given by Narrownet, the Sigfox operator in Portugal. The Smart Everything evaluation board, and finally an Arduino UNO R3 equipped with a shield and Sigfox module from Cooking Hacks .

The modules used the Arduino IDE software with C programming language, aside from the TD1208 Evaluation Board Kit. Programs using Arduino are generally called sketches. They use two basic functions: the setup, and loop functions. The setup function is called once upon the device turning on or resetting. It is mainly used for initiating variables, addressing input and output pin modes and other possible libraries needed in the program. The loop function, as its name implies, is a continuous loop, only stopping by turning off or resetting the device.

3.1.1 TD1208 Evaluation Board

This kit from Telecom Design was used in the first experiences with the Sigfox network and IoT platforms. It includes a breakout board with the Sigfox module, a twenty centimeter 868 MHz

antenna, a FTDI serial cable, one-year subscription to the Sigfox network and one year access to the TD developer back-end, which gives access to a Telecom Design IoT platform where the Sigfox messages can be visualized.

This board works by sending Sigfox messages with the use of AT commands from a command-line interface. "AT" commands, short for attention, are simple instructions used to communicate and control a modem. They are the lowest level of interaction available with a Sigfox module, except when using a Software Development Kit.

As the board was already registered at the Sigfox back-end only the token for it, which is a one year Sigfox contract, had to be renewed. After sending the first Sigfox message with the command AT$SS=414243444546, corresponding to ABCDEF, it was possible to confirm on the Sigfox back-end that the messages had been received.

To test the callback feature, an email callback was created. It was necessary to select the device name at the Sigfox back-end, and choose the create NEW callback option. In that callback sub-menu it is possible to select between a custom or dedicated bridge callback. Figure 3.4 presents the options necessary for an email callback. The email recipient, the subject and the body of the message were filled as the figure shows. The time sent from Sigfox is represented in a Unix time stamp.

The second data callback, was made to the Carriots platform . This type of callback has an URL channel, with the HTTP method selected as POST. After creating a Carriots account, an URL address was available to use, which was filled on the designated field for the callback, with the respective API key generated on the platform.

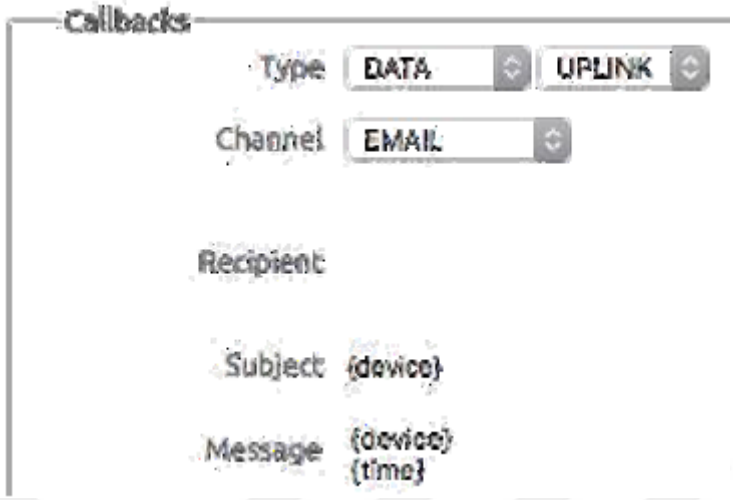


Figure 3.4: View of a Sigfox email callback.

3.1.2 Smart Everything Board

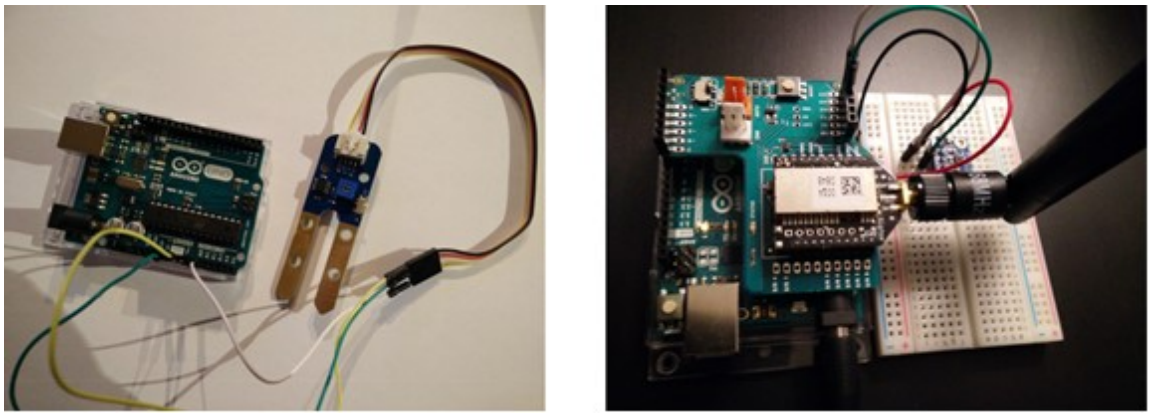
The Smart Everything evaluation board comes with a Sigfox module, has Bluetooth and NFC connectivity, a GPS receiver, a cryptography authentication chip, an absolute barometer and altimeter, proximity and ambient light sensors, a 3D accelerometer, a 3D gyroscope, a 3D magnetometer, and a temperature and humidity sensor. The board comes with a one year subscription to the Sigfox network.After installing the necessary drivers, board support and libraries in the Arduino IDE, the board was not recognized by the software. Searching for an answer through forums and help guides proved unsuccessful, although the problem seemed to be related to the fact that the computer used was a Mackintosh. However, this could not be confirmed. When the use of this board was beginning to seen impossible a beta version of the Arduino IDE was made available to solve this problem. This software version solved the problem of the board being recognized by the computer, but introduced another one. The software was now unable to create new sketches, rendering it useless. After installing the old version of the Arduino software, the board was now recognized and sketches could be created.

After solving the problem of the installation, all sensors of the board were tested, with the GPS receiver taking a long time to locate the device. To test the Sigfox network the board had to be registered at the Sigfox back-end. After registering, the Sigfox connection was tested as well. Other experiments were conducted by using sketches found for the board, for example, one

which sent a test message every ten minutes to the Sigfox network . Further experiments with this board were not possible because the token expired.

3.1.3 Sigfox Radio Shield for Arduino

Baking Modifications included an Arduino UNO R3 with a shell and Sigfox board. It was the droid x for the home automation system and the panel where most Sigfox studies were performed. Two relative humidity detectors (model DHT11 and SHT31) were used on the Arduino ide, and so were two rainfall communication elements (no clear marking upon on frameworka humidity detector (model IM121017001); three Vibration motor detectors (model PTR004226); and an activity tracker extension panel (model LIS344ALH). All detectors were reviewed, and the required library was built for each of them, with several getting large experiments with digital sources. The heat are shown by the Arduino microcontroller. There are three scenarios presented by the weather detectors: no storm, a rain alert, or a severe storm. Figure 3.5a shows how the water level sensor calculates the relative humidity. The twin wearable devices are capable of detecting intensity up to a distance of seven metres. Relative humidity measurements were also shown by the SHT31 detector.. Finally, the sensor was put to the test many times. The Arduino uno is attached to the firewall and Sigfox device in figure 3.5b, and the SHT31 sensor is linked with the aid of a circuit board. For all of this model, a new service was developed., as seen in Annex A, that used only the Arduino's loop feature to transfer drawings, a precaution taken to avoid possible errors by unplugging and reconnecting the Sigfox unit..



(a) Moisture sensor experiment. (b) Temperature and humidity sensor experiment.

Figure 3.5: Experiments conducted on the moisture and temperature sensors.

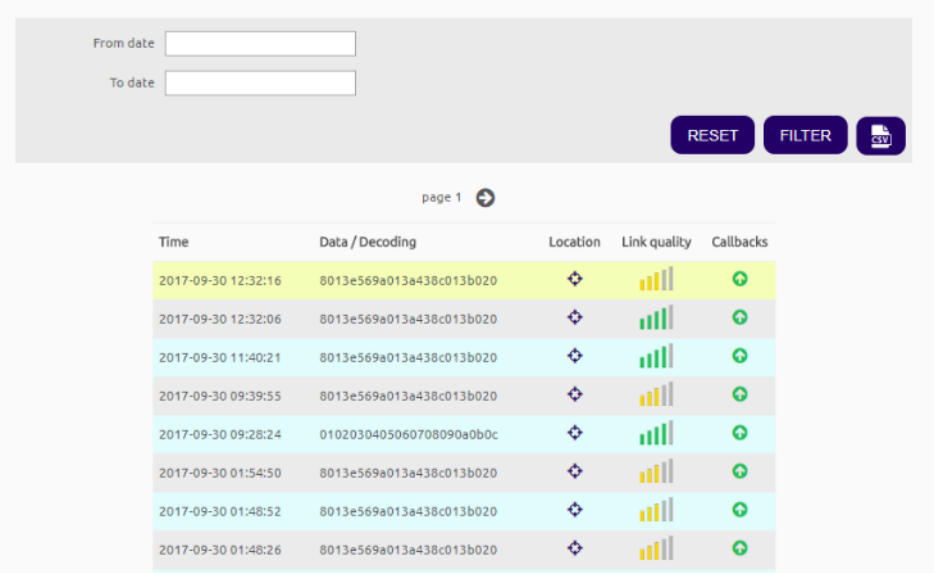


Figure 3.6: Example of a Sigfox message at the back-end. [3]

The schematic produced first initialised the thermometer, then the Sigfox subsystem; secondly, the temperature and pressure value are extracted and then sent to the Sigfox rear in an 8-byte text, with 4 bytes for warmth and 4 bytes for sulfur; and third, a 21 wait is released. Figure 3.6 displays a customized package view of the signal source just at Sigfox rear., It was made to decode byte info. To modify the sender electronic services, go to the Sigfox rear and modify that System Subtype information. It was appropriate to select the correct language alternative and enter the custom post config in the message decoding area..

Since the Arduino is a power-hungry device, a nap catalog labeled "Narcoleptic" was included in the software to see if the device can run on batteries for long durations. The "Narcoleptic" library lowers energy usage by using features of the Arduino board. It's great for simulating a power-off state while the system is in hold state.

3.2 SIGFOX IOT PLATFORMS

To finish the home automation framework we previously mentioned, we needed to use Sigfox callbacks to synchronise the systems with Iot systems. Some many technologies were listed, and six were put to the test using the Arduino design. The Cloud thing, the Tago, the Wia, the Thinger, the Data boom, React Native, and Google Cloud were among them.. We use Python again for deployment in our study, and it was deemed the most critical and will be discussed.

The rest of application studies, and some of the the challenges faced, are covered in the following sections.

The Thinger framework was used in 3 stages: one was to establish the data box, which holds the collected data from Sigfox as well as a figure had increased, which had been required for the details to be authorized by the website; the first was to design the Sigfox connection with the requisite encryption to the portal; and the third was to build the console at the portal for easily accessible to the product.

(a) Data callback example using URL channel. (b) JSON data.

Figure 3.7: Callback configuration for the Thinger Platform.

3.3 LORA SOLUTION

For the Lora smart home solution, the architecture used was different from Sigfox, and is presented in figure 3.8.

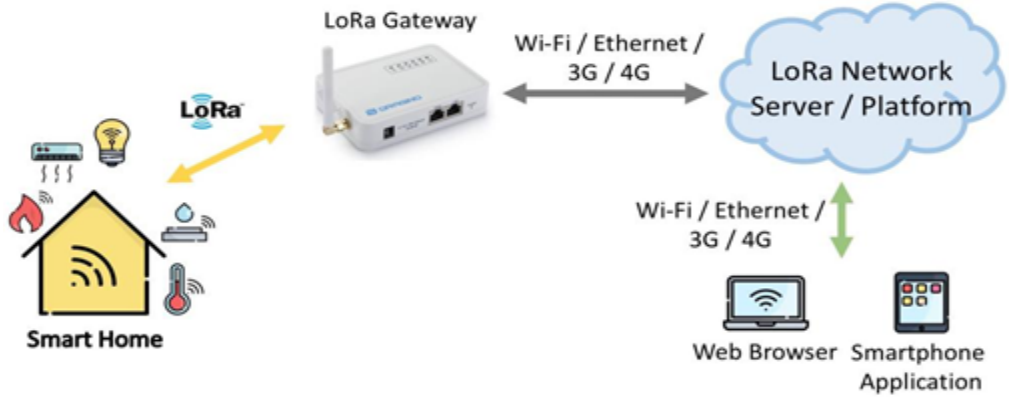


Figure 3.8: Proposed smart home architecture using LoRa technology.

A experimental system based on Lora was found to take this design to life. Following that, a converter was entitled to accept the LoRa notifications from the system and route them to the desired LoRa server computer. Some many firms provide LoRa internet services, with some also providing IoT development tools Finally, the details will be retrieved through data backup interface, which would have been accessible thru a browser on a device, laptop, or mobile. A specific phone programme may be available for the server computer.

A first step in this approach was to purchase a LoRa firewall system, which was needed because the Network Switch doesn't really build its own portals like Sigfox can. The Dragino LoRa portal set was discovered to be the solution. This package included a LoRa Gateway-LG01 P (see figure 3.9 a), which can be configured with 3G and 4G modules. Two Dc motors UNOs, a LoRa shield, a LoRa/GPS safeguard, three 868 MHz microphones, a fire detector, a buzzer, a photoconductive camera, the alarms, a loop, and a humidity levels detector were also included in the package.

(a)The Dragino LG01 Gateway . (b) The Arduino LoRa Shield.

Figure 3.9: Dragino devices.

3.4 RADIOHEAD PROTOCOL

The LG01 portal, an Arduino LoRa cover, and one DHT11 temperature and humidity sensor were used in the studies to use this procedure. By design, the portal is set up as a Wi-Fi hotspot. When enabled, it creates an unsecured hub in its immediate vicinity to which users can bind. The required platforms was mounted first to check the back door..

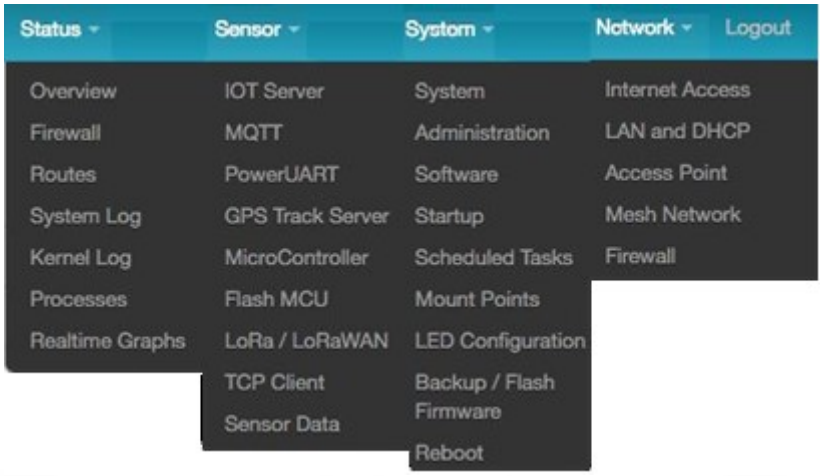


Figure 3.10: A compressed view of the LG01 gateway interface.

After configuring the gate, it was time to set up an account on the Quirky. A dashboard was built on the project with humidity levels field that produce a unique ID and API key. The Arduino IDE programme was then updated to include the Thing Speak catalog. The LoRa shield was attached to the DHT11 sensor, and an Arduino sketch was uploaded.

The ID channel numbering or API key created in Micro - controller are loaded in the firewall sketches. The sketches listen for details from the LoRa node, verifies that the LoRa client ID is right, delivers an acceptance response to the device, and then transmits the signal to the server.

It was appropriate to setup a new computer with the Arduino LoRa/GPS shield. No changes were made because the gate already had been reported and there was no need to alter its specifications. At the current model, only the measured terms for "DevAddr," "NwkSKey," and "AppKey" had to be written in.. With the LoRa/GPS shield, numerous drawings were used, and the installation for this experiment had many difficulties, which will be followed in this study. A design that could be submitted to the Atmega LoRa/GPS shield was discovered. This new outline necessitated the deployment of two new libraries, one for GPS and the other for LoraMAC-in-C (LMIC). The contact to the TTN service was verified after the sketch for the LoRa/GPS shield was downloaded, which sent the distance, ° e, and atmosphere as the load.

4. RESULTS

The results collected will be discussed in this chapter, driven by the collected data and based on the procedure mentioned in the Research Methodology. The effects of the smart devices project from the preceding part are covered in this chapter. The chapter begins with an overview of the Sigfox forums and the home automation program's out comes.. The effects of the synchronisation with the Connected devices, as well as an overview of their efficiency, are provided. The LoRa kit is investigated, and the findings are addressed. Python is used to conduct the experiment..

4.1 SIGFOX BOARDS

Only one device was regarded as the template for Sigfox. On an Arduino, Microcontrollers, or Wifi module panel, the device could be used a shield. Table 4.1 shows the three protection choices from Cook Hackers for the system, along with their costs, including the Sigfox protection.. The Akeru from Snootlab and the Smart Everything board were also considered, with values of about 90 e and 85 er, meanwhile. Taxes and delivery costs are not included in any of the rates

Table 4.1: Shield solutions for the Sigfox module.

	Arduino	Raspberry Pi	Wasp mote
Shield Price	65 e	90 e	160 e
Board Price	23 e	40 e	+160 e

The Smart Everything panel was chosen for its link to the Radio transceivers and for establishing a bunch of sensor devices, while the Raspberry pi was selected for its lower cost. The TD1208, the very first boards used, were already purchased prior to the beginning of this task.

TD1208 Board

The tests were performed with this board where meant to test the Sigfox network. It's also the first panel to work with a Cloud network, thanks to the development of a callback which sent the system ID and date as information.. The board is no longer available, but Telecom Design offers other Sigfox devices.. The tests using this board, both with Sigfox and the Carriots platform, proved successful and the results were good. The board proved a good starting point for the project and through it, it was possible to see how the Sigfox back-end worked. It also provided a better insight at how the callback process was made.

Smart Everything Board

The tests using this board were made using code from examples, in order to understand how the board worked and how to program it. All tests using the board were made connected to a power supply and never using batteries because, although the board uses a Sigfox module, that is very energy efficient, the board is not. All Sigfox tests were successful. This board, shown in figure 4.2, ended not being used to its full potential. Additional tests were envisioned for it, such as, using the gyroscope to attach the module to a door or drawer. In the test envisioned, the user could be alerted that the front door, or a drawer, of their house had been opened. As the token for this board expired and because the steps taken to synchronize the Arduino board with shield and Sigfox module to the IoT platforms presented difficult challenges, the planned tests for this board were not achieved. The problem faced where the uploads were not possible was not identified and even the beta version of the Arduino IDE used was not found after, leading to believe that the problem had been resolved with a new software update.

Although the full use of the board was not possible, the tests conducted with it allowed to see that this board had a greater learning curve than the Arduino with the Sigfox shield, and sketches designed for it would be harder to code, mainly because it had its own Sigfox library, it its own set functions.

Figure 4.1: The Smart Everything board [37].

Sigfox Radio Shield for Arduino. The Arduino with shield and Sigfox module, shown in above figure, was the board used as the prototype for the smart home project and the one used with seven IoT platforms. The objective with this board was to be able to send messages to the Sigfox back-end and to redirect them to IoT platforms. It was the board with the faster learning curve. The sensors tested worked as expected, except for the rain sensor which with a single drop of water accused a flood warning. The accelerometer was tested several times but it was not possible to make it work, or conclude if it even worked. Although all sensors described in section 3.2.3 were tested with the Arduino, the SHT31 sensor and the PIR motion sensor were the ones chosen to be used with the Sigfox module. The SHT31 sensor was preferred to the other temperature sensor, the DHT11, because it had more accurate readings for both temperature and humidity. The decision to first use the SHT31 sensor for the prototype was made to ensure that the smart home solution could be implemented, before starting to add more sensors to the prototype.

The tests to the Sigfox back-end were successful, but the messages could only be viewed in hexadecimal. As the temperature and humidity values were an eight byte hexadecimal value, the display information was created. It was found that the first code used to convert the float values to hexadecimal, needed to send the information to the Sigfox back-end, was not working correctly, as shown in figure 4.2. A new way to send the data, by using a union, proved successful.

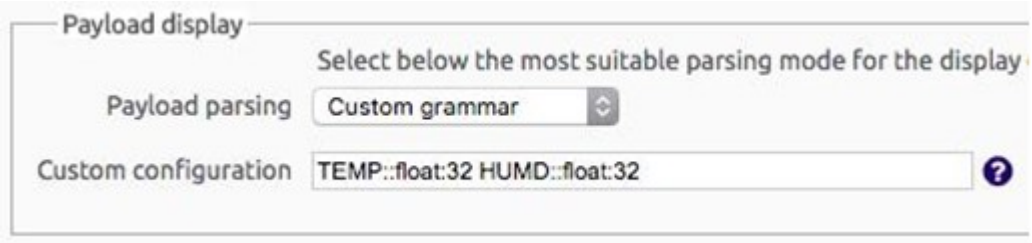


Figure 4.2: Custom payload configuration at the Sigfox back-end.

The Cooking Hacks Sigfox module presented a problem which could not be solved throughout the work relating to the upload of sketches to the Arduino. Theoretically, once assembled, the Arduino Sigfox shield with the Sigfox module, should be able to connect to the Arduino IDE software for sketch uploading. The Shield used to connect the Arduino board to the Sigfox module has a switch that selects the serial connection (USB or XBEE). After researching the problem thoroughly in forums and help guides, several attempts were made to solve it, starting with the switch on the shield, to switching the software serial ports on the sketch. After several failed attempts, and finding that this was a common problem with the shield, the solution found was to upload the sketches when the Sigfox module was not connected to the shield.

While this method worked, it is believed to be the cause for the Sigfox module to sometimes report not being switched on successfully. Sometimes when the module gave the packet sent error the message still arrived at the Sigfox back-end. This is believed to be the reason for receiving an event message warning at the Sigfox back-end This warning is sent when the message counter number is not the same as the one expected by Sigfox as shown in figure 4.4, meaning that some message might have been lost. To solve this problem the sketch created for the prototype did not use the setup function, only using instead the loop function, which meant that every time the prototype would send a message it would re-initialize the sensor and Sigfox module to avoid any errors. The sketch used sent information to the back-end every twenty minutes to ensure that the daily limit allowed by Sigfox would not be broken. The temperature and humidity values were 4 bytes each, making the payload 8 bytes total. This was not the most efficient way to send the temperature and humidity as both can be sent using only 2 bytes each.

```
Sensirion SHT31 - Humidity - Temp Sensor
ATATS304?Switch ON OK
Humidity        Temp
43.06 %         24.78 *C
AT$SF=TEMPPacket sent ERROR
ATSwitch ON ERROR
Humidity        Temp
42.89 %         24.84 *C
AT$SF=TEMPPacket sent OK
```

Figure 4.3: Sigfox module fails to switch on.

page 1

Type	Severity	Source id	Description
Break in message sequence	WARN	1AD924	Break in message sequence from Device #1AD924

Figure 4.4: A Sigfox warning event for a break in message sequence.

The Narcoleptic sleep code used in the Arduino sketch did not prove very effective. Two tests were conducted to see how much time the device would last only powered by batteries. In the test with the 9V battery the sketch was made to send data in twenty minute intervals, but after further studying this type of battery with Arduino solutions it was found that this type of battery drains fast. After a few hours a change to a two hour interval between messages was made. Based on the last message received at the Sigfox back-end, the device was powered by the battery for sixteen hours with the twenty minute interval plus an additional fifteen more hours with the two hour interval, reaching a total of thirty one hours using the 9V battery. The test with the eight 1.5V batteries used from the beginning a two hour interval between messages and managed to stay on for four days before losing power.

The second sketch created, which used the PIR sensor to detect movement, had the message received at the Sigfox back-end successfully, but its implementation was not further developed due to time constraints. The downlink test made was successful, but because there was not a need for downlink messages in the smart home system designed, further tests were not performed.

Only one email callback was created for the prototype where the custom fields for the temperature and humidity, already parsed by the Sigfox back-end were sent in the payload. In figure 4.5 the message received at the email client is presented.

Figure 4.5: Example of an email received using a Sigfox data callback.

The most successful IoT platform tested was the Thinger platform. Through the documentation from this platform, not only was it possible to have a functioning and complete IoT dashboard, but also gain a better understanding of how the process of synchronization between the Sigfox back-end and the IoT platforms worked. It was through the use of this platform that most problems faced with the others were resolved. In figure 4.6 the Thinger dashboard is shown, with widgets for the temperature and humidity, the SNR, the RSSI, the device ID, and a map showing the location of the base station, based on the latitude and longitude values. Widgets for the latitude, longitude, time and base station ID were also created. The widgets are the result of the data bucket created at the platform. This was the most successful dashboard implementation, completing the smart home architecture designed for the project, marking the success of the Sigfox solution implementation.

Figure 4.6: Custom signals received at the Data boom platform.

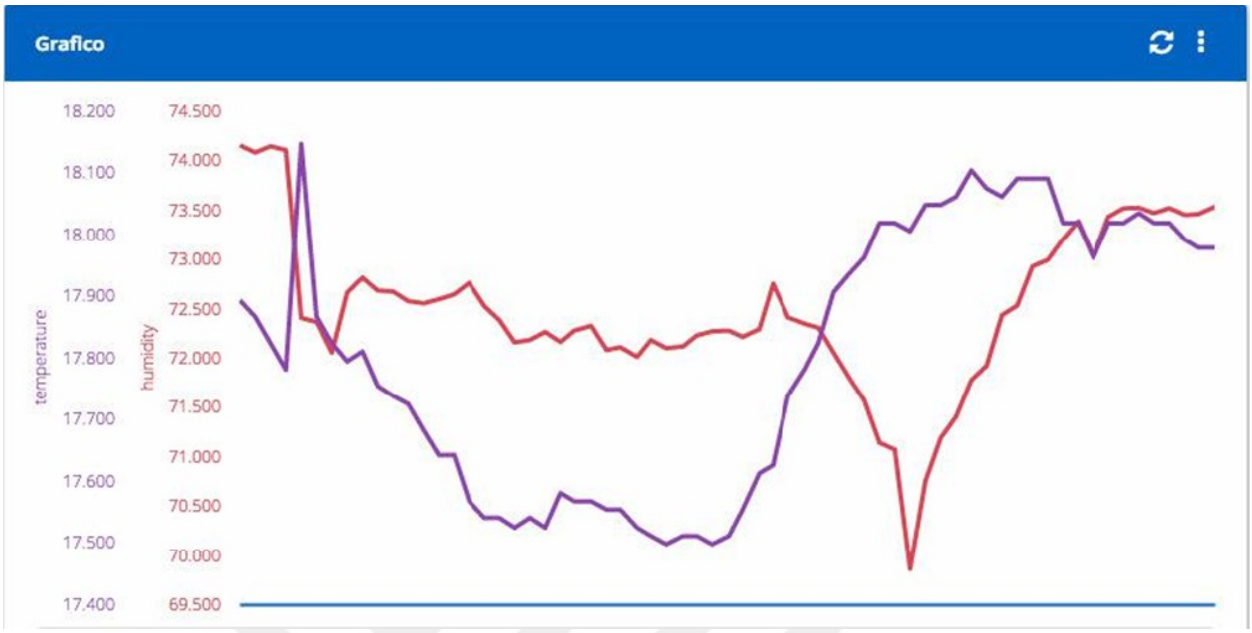


Figure 4.7: Custom IoT dashboard built at the Data boom Platform.

Through the use of all seven platforms a better understanding of the Sigfox architecture was achieved. The Sigfox back-end was considered difficult to navigate and the options for device management hard to find. Still, the Sigfox architecture solution for the smart home, initially proposed, was achieved. However, from the seven platforms used, the solution was only possible on two of them, the Thinger and Data boom. Although on the other platforms a dashboard was not able to be created, the synchronization with them was still achieved, except for the Cloud Thing platform.

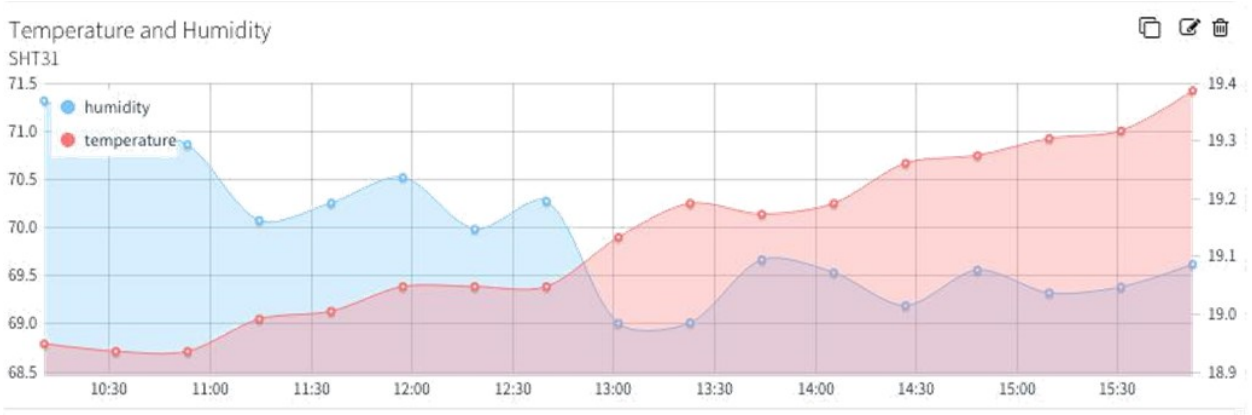


Figure 4.8: Temperature and humidity check in Thinger platform custom dashboard.

For the LoRa solution, two modules were considered, both for LoRa and LoRaWAN. The modules, from Cooking Hacks, were to be used with a shield on a Arduino, Raspberry Pi or Waspmote board. Table 4.2 shows the six Cooking Hacks shield options and their prices. This solution would also need a gateway. As LoRa gateways are very expensive, the two options considered were: to build one, using a Raspberry Pi; or to find an already built gateway solution which would not be very expensive. The custom Raspberry Pi gateway had a price around 150 e, and the cheap gateway solution found was the Dragino kit which had a price around 90 e. All prices do not include tax or shipping costs.

Table 4.2: Shield solutions for the LoRa module.

	Arduino	Raspberry Pi	Waspmote
LoRa Shield Price	75 e	85 e	147 e
LoRaWAN Shield Price	90 e	95 e	163 e
Board Price	23 e	40 e	+160 e

The model chosen for the LoRa solution ended up being the Dragino kit. This decision was made based on the study of LoRa gateway implementation, which after the time spent with Sigfox, was deemed to complex and difficult to implement in the time available for this work. As the Dragino kit already possessed a LoRa gateway, two LoRa nodes, and several sensors, it was found to be a better alternative for the LoRa tests.

Radio Head Protocol Tests

In the Radio Head tests two other ways to connect the gateway to the home network were tried. The first by connecting the gateway directly to the home Wi-Fi router, through its WAN port. The gateway would then act as a Wi-Fi access point for the home network, sharing its Internet connection through its access point or by connecting to its LAN port. And the second by connecting the gateway to a Wi-Fi range extender. Both tests proved unsuccessful.

To be able to monitor both the device and the gateway in the first LoRa experience, a new program, ZTerm, was installed. This was due to the Arduino IDE only being able to show the

serial monitor of the device connected to the PC. The experience was successful and the result of the connection can be seen in figure .

Figure 4.9 and figure 4.10 shows the result of the Thing Speak platform test. At the platform two widgets were created, one for the temperature and another for the humidity.

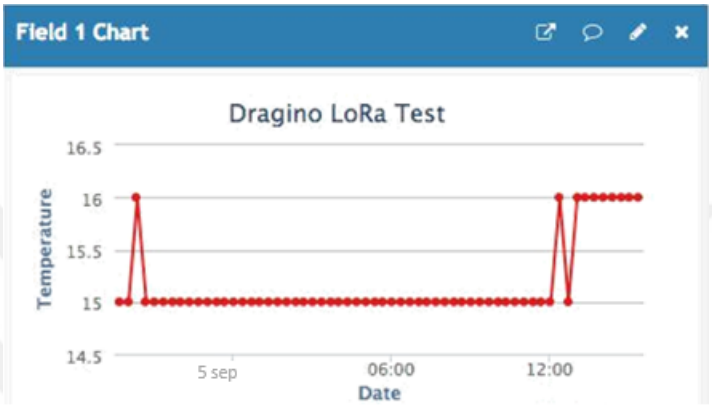


Figure 4.9: Temperature values in Thing Speak platform.

Figure 4.10: Humidity values in Thing Speak platform.

5. DISCUSSION

This thesis focuses on the use of IoT solutions for the smart home, with a particular focus on two LPWAN technologies, Sigfox and LoRa. A detailed study is done on both technologies and a prototype solution for a smart home project is developed. several topics relating to IoT, such as its meaning, definitions and architecture are discussed. Some of the most important technologies which enable the IoT are addressed, such as M2M communications and cloud computing, while others that might be implemented in the future, like fog computing, are touched upon. Also addressed are some of the challenges the IoT currently faces, such as security, privacy, standards and rights. Each of these topics is studied in light of the challenges that IoT faces today.

Different Technologies which enable the IoT are reviewed and their most important features explained, ending with a focus on LPWAN technologies. A more in depth discussion is given for the two technologies used in the research work, Sigfox and LoRa. Their characteristics, architecture and security are reviewed. A discussion on their main differences is presented, followed by an analysis on the state of the art. In the latter a look at the current hardware offers of both Sigfox and LoRa is given, and examples of current IoT applications are presented.

We have also developed the smart home project using Sigfox and LoRa technologies. Two architectures for Sigfox and LoRa are proposed and the steps to achieved them explained. With Sigfox, three developer kits are tested, with their experiences detailed, and a temperature and humidity prototype is used to simulate a smart home IoT device. The prototype is then synced with several IoT platforms to be viewed by a customer for a better user friendly experience. The experiences with the LoRa gateway and devices are detailed, and their synchronization with a network server and a platform is explained.

An analysis of the challenges faced during the various tests is presented along with the results of the IoT platforms solutions. An analysis is done on the experiences with Sigfox and LoRa.

Most of the objectives defined in the thesis are achieved, starting with the study of IoT, its challenges and technologies, specifically Sigfox and LoRa. The prototype for Sigfox is created successfully and the results obtained at the Sigfox back-end are the ones which were initially desired. Seven IoT platforms are used: one, which failed to be implemented; four, that do not

achieve the desired result; and two more, which achieve the objectives first established. The technologies are compared and their results analyzed. The four platforms using Sigfox that do not achieve the smart home solution desired are synchronized with the Sigfox prototype successfully. One of the successful results, the Thinger platform, proved to be the most suitable choice for a smart home project. With LoRa, a prototype as not achieved because the technology proved to complex and time consuming to implement mainly because of the study necessary to understand and use its gateway and devices. Although the gateway proved effective in the work done, the fact that it did not support the full LoRaWAN protocol was found to be lacking. The tests conducted were made to better understand the technology and how to implement it. Only one dashboard is used with this technology and successfully implemented. A network server is also used with two tests conducted, one which worked and the other did not.

CONCLUSION & FUTURE WORK

5.1 CONCLUSION

Based on the experiences of this work it is concluded that both Sigfox and LoRa technologies can be used in smart home devices and both can have a future in the market. However, through the study and use of both, it was also possible to conclude that neither can be used as the sole technology in the smart home, mainly due to their limitations and low level interaction, meaning most devices will adopt a passive stance, which goes against the normal use of devices in a home, where users like to interact with their surroundings. After implementing Sigfox and LoRa on a smart home prototype system using python, the best solution for the smart home was found to be Sigfox. Sigfox offers much more support for their customers, while LoRa is a much more independent technology. This relates, for example, to the fact that Sigfox base stations are deployed and managed by the company, meaning that users only need to focus on the devices and the platforms for those same devices. It also offers support through the Sigfox back-end. On the other hand, for LoRa, it is necessary to deploy and build a gateway or pay to use one from a telecommunications operator which has deployed it. But solutions like this could not be found today. LoRa also has the disadvantage of not offering a network service, meaning that one has to be used by third-party companies.

During the study and tests conducted with both technologies, the objectives defined at the start of the work were found to be too many to achieve, specially relating to LoRa. As neither technology had been used before, the study and implementation of the prototypes took longer than expected.

It is wished that this thesis will hopefully be of value and could serve as guidance for future smart home projects. It showcases the possible problems an IoT project can face and provides a deeper understating on the technologies which power the IoT.

5.2 FUTURE WORK

Throughout the course of the work several ideas were thought of for future continuation of the smart home project.

With Sigfox a possible prototype which made use of downlink messages could be made. Another possibility would be to synchronize various devices with IoT platforms. Using those same platforms services like Twitter, Slack and others could be implemented. A smartphone application could also be developed.

With LoRa technology, a gateway capable of supporting the eight LoRaWAN channels could be used to test several devices to better compare it with Sigfox. The newly released LoRaWAN specification capable of supporting Class B devices could also be tested. Other experiences like using IoT platforms to manage more than one device, while also using services like Twitter, Slack or smartphone applications could be made.

REFERENCES

[1]. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application:Areas, Security Threats, and Solution Architectures. IEEE 2019, 7, 82721–82743.

[2]. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises.Bus. Horizons 2015, 58, 431–440.

[3] Avaialbe Online: https://jacksonng.org/zoe-helper-sigfox-sos-device-part-1

[4]. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT Express 2019, 5, 1–7.10.1016/j.icte.2017.12.005.

[5]. Ayoub, W.; Samhat, A.E.; Nouvel, F.; Mroue, M.; Prévotet, J. Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility. IEEE Commun. Surv. Tutor. 2019, 21, 1561–1581.

[6]. Carvalho, D.F.; Depari, A.; Ferrari, P.; Flammini, A.; Rinaldi, S.; Sisinni, E. On the feasibility of mobile sensing and tracking applications based on LPWAN. In Proceedings of the 2018 IEEE Sensors Applications Symposium (SAS), Seoul, Korea, 12–14 March 2018; pp. 1–6.

[7]. Mekki, K.; Bajic, E. Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT 2018. In Proceedings of the 2018 IEEE International Conference on Pervasive Computing and CommunicationsWorkshops (PerComWorkshops), Athens, Greece, 19–23 March 2018; pp. 19–22.

[8]. Casals, L.; Mir, B.; Vidal, R.; Gomez, C. Modeling the energy performance of LoRaWAN. Sensors 2017, 17.

[9]. Sultania, A.K.; Zand, P.; Blondia, C.; Famaey, J. Energy Modeling and Evaluation of NB-IoT with PSM and eDRX. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, UAE,9–13 December 2018; pp. 1–7.

[10]. Gomez, C.; Veras, J.C.; Vidal, R. A Sigfox Energy Consumption Model. Sensors 2019, 19, 681.

[11]. Mahmoud, M.S.; Mohamad, A.A.H. A Study of Efficient Power Consumption Wireless Communication Techniques/Modules for Internet of Things (IoT) Applications. Adv. Internet Things 2016, 6, 19–29.

[12]. Finnegan, J.; Brown, S. An Analysis of the Energy Consumption of LPWA-based IoT Devices. In Proceedings of the 2018 International Symposium on Networks, Computers and Communications (ISNCC), Rome, Italy, 19–21 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.

[13]. Ismail, D.; Rahman, M.; Saifullah, A. Low-Power Wide-Area Networks: Opportunities, Challenges and Directions. In Proceedings of theWorkshop Program of the 19th International Conference on Distributed Computing and Networking, Varanasi, India, 4–7 January 2018.

[14]. Costa, M.; Farrell, T.; Doyle, L. On Energy Efficiency and Lifetime in Low PowerWide Area Network for The Internet of Things. In Proceedings of the 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, 18–20 September 2017; pp. 258–263.

[15]. Lpwan, A.D.; Callebaut, G.; Leenders, G. A Deployable LPWAN Platform for Low-Cost and

Energy-Constrained IoT Applications. Sensors 2019, 19, 585.

[16]. Hernandez, D.M.; Peralta, G.; Manero, L.; Gomez, R.; Bilbao, J.; Zubia, C. Energy and coverage study of LPWAN schemes for Industry 4. 0. In Proceedings of the 2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and Their Application to Mechatronics (ECMSM), Donostia-San Sebastian, Spain, 24–26 May 2017; pp. 4–9.

[17]. Augustin, A.; Yi, J.; Clausen, T.; Townsley, W. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. Sensors 2016, 16, 1466.

[18] Jazayeri, Mohammad Ali & Liang, Steve & Huang, Chih-Yuan. (2015). Implementation and Evaluation of Four Interoperable Open Standards for the Internet of Things. Sensors (Basel, Switzerland). 15. 24343-24373. 10.3390/s150924343.

[19]. Bouguera, T.; Diouris, J.F.; Chaillout, J.J.; Jaouadi, R.; Andrieux, G. Energy consumption model for sensor nodes based on LoRa and LoRaWAN. Sensors 2018, 18, 1–23.

[20] Cheong, P.S.; Bergs, J.; Hawinkel, C.; Famaey, J. Comparison of LoRaWAN Classes and their Power Consumption. In Proceedings of the 2017 IEEE Symposium on Communications and Vehicular Technology (SCVT), Leuven, Belgium, 14–14 November 2017; pp. 8–13.

[21] Peta, J. Evaluation of LoRa LPWAN Technology for Indoor Remote Health and Wellbeing Monitoring. Int. J.Wirel. Inf. Netw. 2017, 24, 153–165.

[22]. Popli, S.; Jha, R.K.; Jain, S. A Survey on Energy Efficient Narrowband Internet of Things (NBIoT):Architecture, Application and Challenges. IEEE Access 2020, 7, 16739–16776.

[23] Lee, H.; Chung, S.H.; Lee, Y.S.; Ha, Y. Performance Comparison of DASH7 and ISO / IEC 18000-7 for Fast Tag Collection with an Enhanced CSMA / CA Protocol. In Proceedings of the 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, Zhangjiajie, China, 13–15 November 2013; pp. 769–776.

[24] Purkovic, D.; Hönsch, M.; Raphael, T.; Karl, M. An Energy Efficient Communication Protocol for Low Power, Energy Harvesting Sensor Modules. IEEE Sens. J. 2019, 19, 701–714.

[25] Joulescope: Precision DC Energy Analyzer. Available online: https://www.joulescope.com

[26] Singh, R.K.; Berkvens, R.;Weyn, M. Synchronization and efficient channel hopping for power efficiency in LoRa networks: A comprehensive study. Internet Things 2020, 100233.

[27] Guo,W.; Healy,W.M. Power Supply Issues in Battery ReliantWireless Sensor Networks: A Review. Int. J.Intell. Control. Syst. 2014, 19, 15–23.

[28] H. H. Ved P. Kafle Yusuke Fukushima, “Internet of Things Standardization in ITU and Prospective Networking Technologies”, IEEE Communications Magazine, pp. 43–49, 2016.

[29] Bor, M.; Roedig, U. LoRa Transmission Parameter Selection. In Proceedings of the 2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS), Ottawa, ON, Canada, 5–7 June 2017; pp. 27–34.

[30]. Singh, R.K.; Aernouts, M.; De Meyer, M.; Weyn, M.; Berkvens, R. Leveraging LoRaWAN Technology for Precision Agriculture in Greenhouses. Sensors 2020, 20, 1827.

[31] J. J.P.C. R. Jonathan de Carvalho Silva, “LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities”, Computer and Energy Science (SpliTech), pp. 1–6, 2017.

[32] A. Z.M. Z. Marco Centenaro Lorenzo Vangelista, “Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios”, IEEE Wireless Communications, pp. 2–7, 2016.

[33] U. R. Martin Bor John Vidler, “LoRa for the Internet of Things”, International Conference on Embedded Wireless Systems and Networks, pp. 361–362, 2016.

[34] A. Orange, “LoRa Device Developer Guide”, Orange, 2016, pp. 5-11.

[35] V. P. Alexandru Lavric, “LoRa Wide-Area Networks from an Internet of Things Perspective”, Electronics, Computers and Artificial Intelligence (ECAI), pp. 1–3, 2017.

[36] R. Miller, “LoRa Security Building a Secure LoRa Solution”, MWR Labs, 2016, pp. 5-8.

[37] Available Online: https://partners.sigfox.com/products/smart-everything

[38] L. Labs, “Low Power, Wide Area Networks For ’Internet of Things’ Engineers and Decision Makers”, Link Labs, 2016, pp. 2-15.

[39] S. Tabbane, “IoT Network Planning”, ITU, 2016, pp. 18-107.

[40] G. T. Santhosh Krishna B V, “A Systematic Study of Security Issues in Internet-of-Things (IoT)”, I-SMAC (IoT in Social, Mobile, Analytics and Cloud), pp. 107–110, 2017.

[41] F. S. Report, “Internet of Things: Privacy & Security in a Connected World”, FTC, 2015, pp. 7-18.

[42] L. Labs, “Low Power, Wide Area Networks For ’Internet of Things’ Engineers and Decision Makers”, Link Labs, 2016, pp. 2-15.

[43] S. Tabbane, “IoT Network Planning”, ITU, 2016, pp. 18-107.

[44] Dash, Anshuman & Pal, Satyajit & Hegde, Chinmay. (2018). Ransomware Auto-Detection In IoT Devices Using Machine Learning.

[45] Sigfox, “Sigfox Technical Overview”, Sigfox, 2017, pp. 4-25.

[46] J. J.P.C. R. Jonathan de Carvalho Silva, “LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities”, Computer and Energy Science (SpliTech), pp. 1–6, 2017.

[47] Available Online:https://design-milk.com/8-smart-home-devices-will-make-life-easier/