IoT Solutions Integrated in Smart Cities

Concepts and Challenges

José António Portela Areia

May 2022

Abstract

IoT-Based Smart Cities are a concept that is gaining more popularity and attention throughout the last couple of years due to the fact of unceasing growth of urbanization and consequently population. This facts may seem irrelevant or maybe out of the scope of this research, but in fact, with an exponential growth of population, the need of controlling and make various city-sectors autonomous can add more quality to their lives. However, this type of concept, alongside with all the technological features, is still in a evolving process which means it has some barriers to overcome, such as cybersecurity, data privacy and the trust of its end-users. This document propose an overview of the basic concepts of an IoT-Based Smart City, alongside with their features and characteristics, architecture, real use-cases around the world and some barriers previously presented. Finally, it is closed with a brief chapter about some future challenges and opportunities in this wide and extensive area of knowledge and implementation.

1. Internet of Things (IoT)

The term Internet of Things (IoT) is used to describe a plethora of intelligent objects (e.g. sensors and actuators) connected through the Internet with the capability of exchanging information, resources, data and mostly important, acting and reacting according to different situations when needed.

1.1. Architectures

Because IoT is a vast and wide concept there is no proposed and uniform architecture. As shown in *Figure 1*, we can visualize what is proposed by the International Telecommunication Union (ITU) as the Architecture of IoT. It consists in four layers with distinct responsibilities and behaviours. These layers are (from the bottom to top) *Device Layer,* followed by the *Network Layer*, *Service and Application Layer* and finally the *Application Layer.*

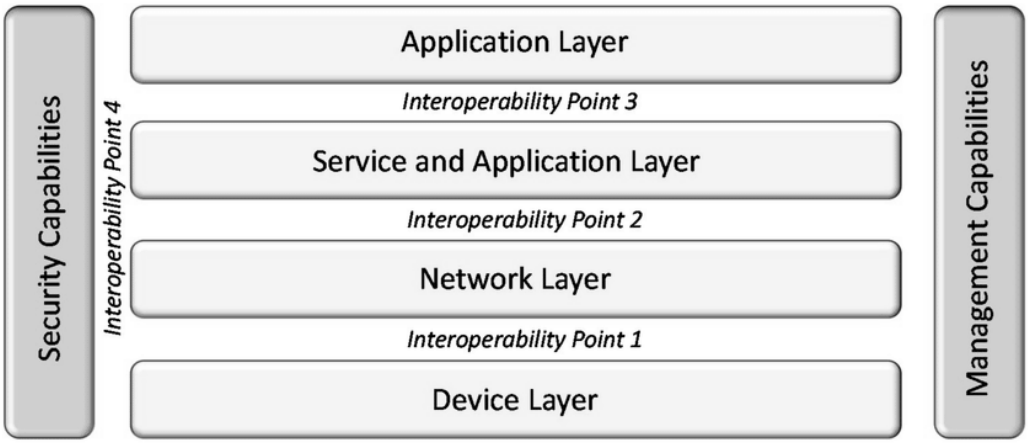

Figure 1 - IoT reference model (ITU-T Y.2060) and the points where interoperability solutions can be applied. (Kalatzis et al., 2019)

In *Figure 2* it's possible to see what is proposed by the IoT World Forum as their Reference Model. It's composed by seven layers and according to them it offers a clean, simplified perspective on IoT which includes edge computing, data storage and access (El Hakim, 2018).

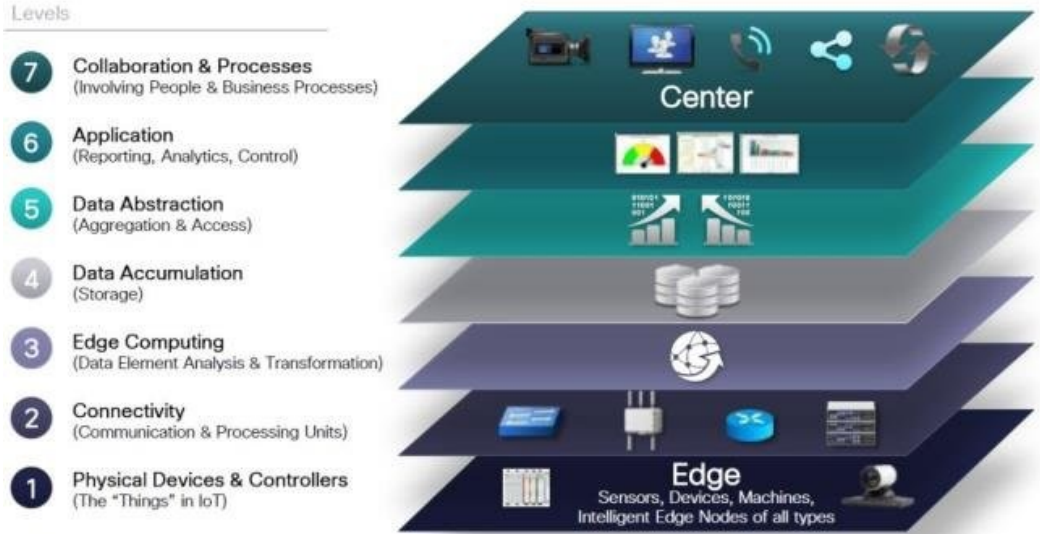

Figure 2 - IoT World Forum Reference Model. (El Hakim, 2018)

For considering it relevant, it will be explained below all the layers (from bottom to the top) that compose this architecture.

- **Physical Devices & Controllers** – According to this model, they define this layer as the "things" of the IoT. From a scientific perspective this "things" are the sensors, actuators and other devices that directly managed the IoT architecture. An interesting concept, known as Edge Intelligence, used to lower the latency reaction and consequently allow higher levels of autonomy and distributed processing, must be implemented at this layer.
- **Connectivity** – To ensure connectivity in this second layer of the IoT Reference Model, the focus is the reliable and timely transmission of data. More specifically, the exchange data between Layer 1 devices and the network or even between the network and the information processing that occurs at Layer 3.
- **Edge Computing** – Also known as "Cloud Edge" or "Cloud Gateway" this layer interfaces the data and control plains to the higher layers of cloud or enterprise software layers (El Hakim, 2018). Technologies like protocol conversion, "fast path" logic or even routing to higher layer software must be implemented at this layer.

- **Data Accumulation** – At this layer, the data generated by the layers below is stored for subsequent processing, normalization and preparation for upstream applications.
- **Data Abstraction** – The main purpose of this layer is to ensure data consistency in terms of semantics from various sources and organizes incoming data into appropriate schema and flows for the upper layer.
- **Application** – It interprets the data from the layer below using software applications. Some IoT applications can be: alarm management, control logic, logistics, monitoring and process optimization.
- **Collaboration and Processes** – The principal aspect of this layer is the human interaction with all of the layers of the IoT system. This layer must be leveraged the value of IoT and all of its layers for the greater-good of the economic growth, business optimization and social comfort and good.

Later in this document it's presented a typical IoT architecture composed with four layers and it's used in a specific cases of study such as smart cities, smart farms or even in intelligent logistics.

1.2. Communication protocols

There are many communication protocols associated with IoT systems. Usually these protocols are divided by layers accordingly to an OSI-based model. In *Table 1* are presented some protocols from the bottom layers (Physical, Data Link and Network) of the model.

It's important to notice that in some cases, just like the one present in this document (smart cities), this protocols must ensure some requirements in order to achieve success in the area that they are implemented. Some of this requirements are the following: low cost, low energy consumption, wider coverage (specifically for this case of study), reliability, high quality of service (QoS) and high security and privacy.

Communication Protocols	Spectrum	Data rate	Coverage	Power usage
Low Frequency RFID High Frequency RFID Ultra-High Frequency RFID	30 – 300 kHz 13.56 MHz 300 – 3000 MHz	4 – 8 kbps	10 cm 30 cm 25 – 100 m	Low
Bluetooth	2.4 GHz	25 Mbps	10 m	Low
Wi-Fi	2.4, 5.8 GHz	54 Mbps 6.75 Gbps	140 m 100 m	Medium
ZigBee	2.4 GHz, 900 MHz	250 kbps	50 – 100 m	Low
LoRaWAN	433, 868, 780 MHz	50 kbps	2 – 5 km	Low
GSM/GPRS	850, 900, 1800 MHz	80 – 394 kbps	5 – 30 km	High
LTE/LTE-A	700, 750, 800, 1900, 2500 MHz	1 Gbps, 500 Mbps	5 – 30 km	High
WiMAX	2 – 11 GHz	70 Mbps	50 km	High

Table 1 - Bottom layers communication protocols

However this bottom layer protocols ensure communication between IoT devices, there is a need that is the communication between the gateways, public Internet and the final applications. This need can be resolved with the help of application layer protocols which can be used to send the latest values of the end-devices sensors to an online server and consequently send information or commands from a applications to the end-devices actuators.

Examples of application layer protocols are MQTT, CoAP, XMPP, AMQP and DDS. For considering it important, this protocols will be briefly explained, accordingly to the works of (Glaroudis et al., 2020), (Li et al., 2015) and (Karagiannis et al., n.d.).

1. **MQTT:** *Message Queue Telemetry Transport*

This protocol targets a lightweight M2M communication and it runs on top of the TCP stack.

In MQTT there is a broker, which has the function of a server, that contains topics and each client can play the role of a publisher, that sends information to a broker at a specific topic, or it can be a subscriber, that receives subsequent messages that the publisher has posted to the topic that he subscribed. In *Figure 3* it's possible to visualize a more user-friendly design to understand better the MQTT protocol architecture.

MQTT also ensure a certain level of reliability by providing three levels of QoS (Quality of Service), which are QoS 0, 1 and 2. In QoS 0, also known as "Fire and Forget", the message is sent but it's not stored nor acknowledged by the receiver. With QoS 1 the messages are sent at least once and the it will arrive one or more times at the receiver which will acknowledge the communication. Finally, in QoS 2, a message is deliver exactly once and it's received once and only once by the receiver, using a four-way handshake to ensure reliability, although it is the slowest method since it needs to exchange four messages between the client (publisher/subscriber) and the server (broker).

In order to ensure security, MQTT relies on security protocols like TLS/SSL (Secure Sockets Layer), which make the brokers required username/password authentication for protection proposes.

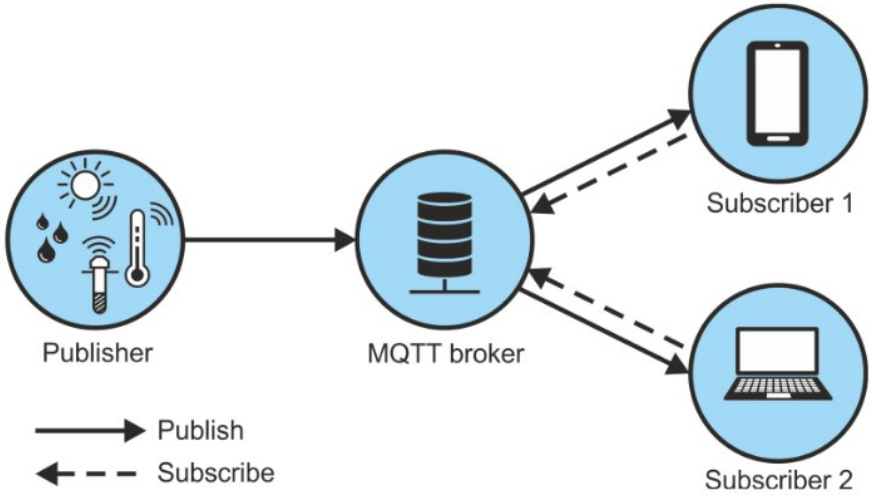

Figure 3- MQTT protocol architecture

2. **CoAP:** *Constrained Application Protocol*

CoAP is a protocol used by devices with limited computing resources. It runs over UDP to keep the implementation lightweight and consequently reduce bandwidth requirements.

This protocol follows a standard client/server model very similar to HTTP, but unlike HTTP, CoAP aims for a more constrained-recourse environments.

Because this protocol relies on a unreliable protocol (UDP), CoAP blended its own mechanisms for achieving reliability. These mechanisms are incorporated in a sub-layer called message sublayer and it consists in four different type of messages: CON (confirmed), that represents a request message that requires and acknowledgement (ACK), NON (non-confirmable) which represents a message that doesn't need an acknowledgement, ACK (acknowledgement) that confirms the reception of a confirmed message and RST (reset) that confirms the reception of a message that could not be processed.

Like in every protocols security measures are important and CoAP relies on Datagram Transport Layer Security (DTLS) to ensure the necessary security. DTLS runs on top of UDP and provides the same assurances as TLS but for data exchange over UDP. Although this protocol (DTLS) provides strong security measures like authentication, confidentiality, cryptographic algorithms and data integrity, it's an open issue while working with IoT systems, since it isn't a lightweight protocol since it requires additional packets because of his handshakes and primarily it does not support multicast which is an advantage of CoAP compared to other protocols. However, in the last couple versions, DTLS are focused to on a optimization that aims lightweight devices and the use of IPv6 over Low-power Wireless Personal Area Network (6LoWPAN). Still, it all this considerations and updates, DTLS utilization in IoT networks continues to be argued.

3. **XMPP**: *Extensible Messaging and Presence Protocol*

The XMPP protocols runs over TCP and provides asynchronous and synchronous communication. This protocol was designed for chatting, message exchanging, voice and video calls. It is also based in text messages that uses XML (Extensible Mark-up Language) which is a disadvantage because it leads to long messages that consumes a great amount of bandwidth and XML also requires parsing which needs additional computational capability that consequently leads to an increase in power consumption.

However, one of the greatest advantages of this protocol, unlike other protocols such as MQTT and CoAP, is that XMPP has a built in TLS mechanism

that provides reliability in data integrity and confidentiality. It also uses a SASL (Simple Authentication and Security Layer) to provide identification of individuals.

4. **AMQP:** *Advanced Message Queuing Protocol*

AMQP is an open protocol for business messaging and interoperability between different systems and applications. It relies on a TCP connection and provides three Quality of Service (QoS) levels that are in line with the ones previous explained in the MQTT protocol.

Above the transport layer, this protocols includes a layer called message layer. Hence, this layer includes two types of messages: *bare messages*, that are sent by the sender and includes the body of the message, system functionalities, and the properties of the application and *annotated messages* which are messages sent to the recipients after adding some more additional information.

Concerning security, AMQP supports and offers Simple Authentication and Security Layer (SASL) for client authentication and TLS for ensuring confidentiality and integrity.

Finally, it's important to notice that although this protocol offers many different capabilities, it's heavy in terms of network resources and computational power and because of it, it's mainly used between servers and strong autonomous nodes in a IoT network.

5. **DDS:** *Data Distribution Service*

DDS is a decentralized, based on peer-to-peer communication, real-time publish/subscribe protocol for M2M type communications that uses multicast. It is generally used to manage data exchange between large high-performance sensors and lightweight devices. It's important to notice that this protocol isn't a typical IoT solution, but it's used in many areas of application such as industrial deployments, smart grids, autonomous vehicles and healthcare services.

The architecture of this protocol consists in two distinct layers: Data-Centric Publish-Subscribe (DCPS) layer and Data-Local Reconstruction Layer (DLRL).

DCPS layer is responsible for exchange information between subscribers and DLRL facilitates the sharing of data between distributed objects.

DDS runs over UDP by default but can also run over TCP and because of that, this protocol provides several options regarding security measures. DTLS and TLS can be used depending whether the protocol is running with UDP or TCP.

Overall, DDS is an extremely powerful protocol that can support heavy and low-capacity simple devices, looking like an auspicious solution for IoT.

1.3. Applications

IoT enables information gathering, storing and exchanging between devices through the network. This "simple" process enables various areas to use IoT systems in order to help them in their daily basis functions. Some of the most common applications sectors are the industrial area, healthcare, infrastructure, security and surveillance.

The industrial applications based in IoT systems are able to improve the business transactions with smarter services networks, which will significantly improve the efficiency of real-time information processing and manage fine-grained applications, such as online-payment, critical data storage, aggregated QoS, and associated performance indicators (Li et al., 2015).

Healthcare is one of the most important areas of application in terms of IoT systems. If correctly applied these systems can help the end-users in order to make their lives a lot easier and peaceful in terms of medical concerns. Monitor medical parameters such as body temperature or even blood pressure are some examples of the capability of this applications.

IoT-based systems in infrastructure has been increased in the last couple of years. Some of the areas affected by this increase of interest in IoT systems are smart cities, which will be developed in more detail in Chapter 2, smart homes, farms, grids and building. Despite being different in terms of location and purposes to our daily lives all of these areas having something in common when it comes to IoT-based systems. They want to make the life of the end-users more easier, reduce wastes and improve the quality of their services.

Because IoT devices (sensors and actuators) are interconnected via network, these connections might bring some security issues, so a strong security protection is necessary in order to avoid malfunctions and malicious attacks. However, protecting millions of intelligent devices is a very challenging task and to join this difficult task, the heterogeneity of these devices also affects the security protection of network that might suffer treats (Li et al., 2015). Hence, privacy protection mechanisms in order to protect information should be implement taken into consideration data privacy.

1.4. Challenges

In the past few years, IoT has been developed rapidly and an enormous amount of architectures and technologies has been proposed. Although this type of technologies still have some problems and challenges to suppressed in the future.

Some of this challenges consist in finding the right technology or architecture to provide to this systems a good relation between a good performance and a low cost in term of energy.

Other current problem is the heterogeneity of the system. As said before, IoT-Based systems have several different technologies alongside with different types of sensors and actuators. Because, every technology method is different from each other there is no "right" way to manage this type of systems. This can problem can escalate quickly in terms of security too, because different technologies are built different in terms of software and they can compromise the entire network with a bad functional software.

Finally, other common problem is the security and data privacy that is exchange between devices in an IoT-Based system. From a developer perspective all software must have implemented the necessary protections in order to protect and not compromise the entire network. Some basic measures that help the security of an IoT-Based system are, for example, two-factor authentication, anti-malware solutions and data backup and recovery. Tiny Encryption Algorithms (TEA) or Advance Encryption Standards (AES) are also other low-cost symmetric-key cryptography algorithms to protect data exchange in a IoT network.

Privacy, although, is another important aspect to take in consideration. There is a giant amount of data exchange in an IoT network, and this data must not be accessed by third-party agents. This is a very serious requirement, because this data can expose private information about the end-users of the IoT network. So, take this in consideration, the traffic that flows through the network must be encrypted in order to protect the privacy of the end-users and consequently gaining their trust.

2. Smart Cities

A smart city is a complex ecosystem characterized by the intensive use of Information and Communications Technologies (ICT), aiming to make cities more attractive and more sustainable. This includes different services and application areas such as transport, environment, government, community, education, economy, lifestyle and transport.

2.1. Architecture

Defining an universal architecture for a smart city can be a tremendous challenge since exists drastic variations from a city to a another, so it's impractical and far from reality to accept a general architecture for the purpose.

However, there is a common architecture illustrated in *Figure 4* proposed by the majority of works that is composed by four layers i.e. sensing layer also known as perception layer, transmission layer, data management layer and application layer.

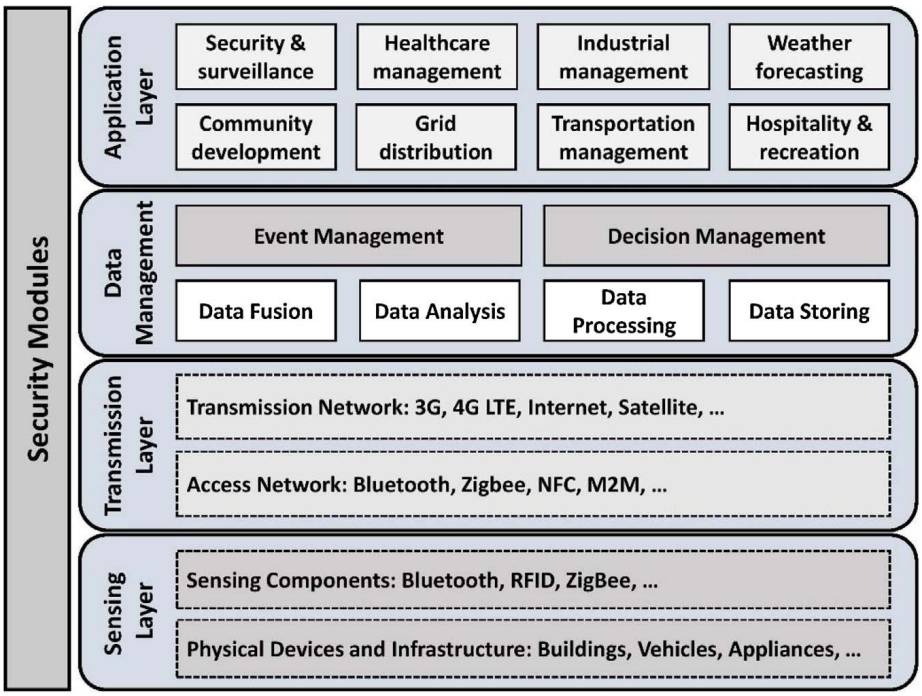

Figure 4 - Generic four layers architecture of a smart city

To a fully and simple understanding of this architecture there is below a bare list that explains all layers.

- **Perception layer -** Its main objective its to obtain/collect data from devices and sensors.
- **Network layer -** This layer is crucial in the IoT structure since it transmits the data collected in the perception layer and it sends it to servers or other network devices.
- **Support Layer -** It supports any type of requirement that any application must need and it uses intelligent computing techniques such as cloud computing, edge computing or even fog computing.
- **Application layer -** This layer's only responsibility is to provide intelligence and services to applications that have custom requirements.

Although all this layers have distinct responsibilities and purposes, what truly matters is the fact that together they can exchange and process the necessary data to a correct functioning of the system embedded.

2.2. Composition of a smart city

A composition of a smart city can differ from one smart city to another depending on the areas that is interesting to invest (Silva et al., 2018). However, there is some components that can be generally used in a smart city i.e. smart community, smart energy, smart transportation, and smart healthcare (Group et al., 2015). Following the list below, it will discuss some of the components presented earlier.

2.2.1. Smart Energy

Energy, without any doubt, is one of the essential elements in a smart city. Following a simple thought, we can say that a smart city includes a plethora of devices, such as sensors and actuators, and theses devices, when working together, they have a large power consumption. So, with this problem in mind and in order to solve that, news ways of creating energy must be implemented.

Currently, green energy is, perhaps, a solution to this problem, since it aims for a consuming energy with the minimal impact on the environment that we currently live on. However, the term smart energy is more alluring among others as it consolidates green energy, sustainable energy and renewable energy (Silva et al., 2018).

Adaptions of this technology like advanced photo voltaic (PV) generators that are incorporated in energy management systems for a microgrid (Kanchev et al., 2011) or a home energy management system (HEM) based on power line communication (PLC) to optimize power optimize power consumption (Boynuegri et al., 2013) are some examples of application and study cases proposed in order to apply components of a smart energy environment.

2.2.2. Smart transportation

A way of transportation has been a need of the human begins since the early days of the civilization. Hence, technological evolution has increased in the last years

in this particular area in order to make transportation more reliable, comfortable and economic to the end-users.

As a result, in modern days, technological evolution in this area has increased exponential to the point that vehicles and other ways of transportation are embedded with various types of navigation and communication systems, which means that every "particle of a particular transport type is connected with each other" (Silva et al., 2018).

VANET, also known as vehicular ad hoc networks has been gained some attention in the last couple of years with the concept of intelligent transportation systems (ITS) and it has been used to manage traffic congestion using vehicle-to-vehicle (VV) communication alongside with vehicle-to-infrastructure (VI) communication.

According to (Mohanty et al., 2016) intelligent road networks, protected pedestrian paths, protected cycle routes, safety embedded public transportation, subway and metro train networks and intercity train networks are some of the applications of a smart transportation system with the some necessary safety and security measures.

2.2.3. Smart healthcare

Smart healthcare plays an important role in today's society since the number of healthcare challenges have been growing exponentially due to the fact of a tremendous increase of population.

In order to face this problem, smart healthcare systems were introduced to reduce the gap between demand and supply, while maintaining efficiency, accuracy and sustainability.

The term "smart healthcare" is known as the junction between medical practices with medical intervention approaches such as medical equipment, wearable devices, emergency services and sensors. Nowadays, modern intelligent healthcare services uses sensor networks, ICT, fog and edge computing, smartphone applications and other powerful data processing mechanisms (Catarinucci et al., 2015; Roy et al., 2007).

2.3. Use cases

2.3.1. London, United Kingdom

London is consider one of the most advanced smart cities in the world. What contributes to this decision is the use of various technologies with the purpose to ensure a better life to his citizens.

Intelligent roads, transportation systems to avoid traffic congestion, Wi-Fi connectivity on the Tube, cycle renting schemes, exchange of digital money are some examples of the technological applications used in this city (Silva et al., 2018).

London's data are linked to an iPad wall at city hall which enables a better visualization of the performance in real time for the citizens. Furthermore, citizens are even welcome to give their feedback and rate their experiences with the city in which helps the developers and researches to understand in which way the technology should follow to keep the end-users satisfied and increase a better performance and trust among them.

The architecture used in London's smart city project aligns with the generic architecture presented in the section 2.1.

2.3.2. Barcelona, Spain

Despite of his down fall in 2008, Barcelona is still a reference when it comes to smart cities. The usage of ICT (information and communication technologies) is one of the goals for this city, special in areas such as business processes and public administration to improve the efficacy of services, transparency and accessibility.

The district project 22@Barcelona is an opportunity that some districts of Barcelona engaged in order to attain smart city standards in green infrastructure, science and technology, quality of life, mobility and economics (Bakıcı et al., 2013). This type of opportunities and interventions have a great importance in order to keep the communities aware of the existence of the concept of smart cities and everything that surrounds them. It also provides great standards and knowledge in these areas to the districts or communities that participate in this type of projects.

Barcelona smart city is equipped with a corporate fiber optical connection, Wi-Fi mesh network, a multipurpose and multivendor sensor network, and a public Wi-Fi network for the use of the population (Bakıcı et al., 2013; Silva et al., 2018). In brief, this type of model used in Barcelona has improved public services and administration, infrastructure plan, accessibility to knowledge, etc.

Various applications of technological improvements in this city are for example in areas such as smart transportation, with the use of lighting system for energy saving or the use of sensors in parking lots for helping citizens finding park, smart healthcare, smart energy and grids, and smart community.

It's important to refer that the architecture used in Barcelona smart city is, once again, extremely similar to the architecture presented in section 2.1.

2.3.3. Nice, France

Historically speaking, Nice was the first European smart city that adopted NFC (Near-field communication) to execute payment transactions in trains, buses, shops, galleries, etc (Anttiroiko et al., 2014).

The smart city project of Nice offers to his population four main areas of service i.e. smart transportation, smart waste management, smart environment monitoring and smart energy (Silva et al., 2018).

Smart transportation is used for and efficient parking management of the city. Various sensors are attached in public roads which are used to collect data from the different vehicles passing by. These information are conveyed to drivers and then direct them to the best route via GPS based mobile application (Daniel & Doran, 2013).

Another important component of this smart city project are the smart grids. Also known as Nice grids, this technology permits the development of a smart solar neighbourhood in city areas by converging distributed electricity, thermal storages and power generation forecasts (Michiorri et al., 2012; Silva et al., 2018).

The deployment of an expanded network of sensors also creates the possibility of an environment monitoring i.e. air, sound, humidity and energy.

Gathered all these information together on real-time basis offers to the citizens a more accurate and precise forecasting analysis.

In terms of electricity consumption and environment take care, Nice provides a schedule of electricity consumption at residential and business premises, and an optimizations of trash collection process (Grimaldi & Fernandez, 2019).

2.4. Challenges and opportunities

Addressing issues and exploring challenges and opportunities in this area has become crucial to achieve further improvement. There are many areas of interest to be more explored and consequently achieve new knowledge about them and solutions to make them more viable. Such areas are, for example, sustainability, security, data collection and analysis, interoperability, connectivity, and cost of design and operation (Mohanty et al.; Silva et al., 2018).

Sustainability is one of the challenges addressed and it's crucial to have a greater focus in this area to promote better solutions to minimize the carbon footprint and preserving the city environment for future generations. The use of renewable energy, ensure the sustainability of city operations and improving the efficiency of power networks are examples of measures that have been applied by GLA (Greater London Authority) in the London area (Giest, 2017).

Another important challenge that must be approached is the security, privacy and trust. It is extremely important for any smart city to ensure these three concepts in order to make the population more secure about the network that surrounds them. We must not forget that a smart city exchange a big amount of data, and this data is related to information about the citizens of that smart city. Hence, it's important to ensure that their information is secure and private, and consequently the they will gain trust and welcome better the solution that is a smart city.

Interoperability is a real challenge to approach if we want to develop a smart city. Different devices – mostly vendor locked-in – must communication with other devices in order to exchange the necessary data for the correct functioning of the

network. The realization of any smart city relies on the integration and communication of all these different devices (Mehmood et al., 2017).

For a more realistic implementation of a smart city, the design and maintenance cost must be taking in care. Cost is categorized in design and operational cost, and according to (Silva et al., 2018) design cost is the financial capital of deploying the smart city while operational cost are the daily operations and maintenance tasks. If both of this costs are minimal the more probable is a real-world implementation. However, this type of costs, while being carefully analysed and optimized throughout the lifetime of a smart city, they still are a quite challenging task.

3. IoT-Based Smart Cities

The correct deployment of a smart city full depends on several IoT structures. This structures usually are divided in four layers. The *perception layer*, also known as *sensing layer*, followed by the *network layer*, the *support layer*, also known as *middleware layer*, and finally the *application layer*.

- **Perception layer -** Its main objective its to obtain/collect data from devices and sensors.
- **Network layer -** This layer is crucial in the IoT structure since it transmits the data collected in the perception layer and it sends it to servers or other network devices.
- **Support Layer -** It supports any type of requirement that any application must need and it uses intelligent computing techniques such as cloud computing, edge computing or even fog computing.
- **Application layer -** This layer's only responsibility is to provide intelligence and services to applications that have custom requirements.

Although all this layers have distinct responsibilities and purposes, what truly matters is the fact that together they can exchange and process the necessary data to a correct functioning of the system embedded.

4. Communication Protocols in IoT-Based Smart Cities

The most prominent protocols used in IoT-Based Smart Cities are the short-range wireless technologies. This includes ZigBee, Bluetooth, Wi-Fi, WiMAX and IEEE 802.11p which are mostly used in smart metering, e-healthcare and vehicular communication.

There are also other alternatives to wide-range communications. Protocols used in this type of communications are the Global System for Mobile Communication (GSM), General Packet Radio Services (GPRS) and Long Term Evolution (LTE) and they are commonly used in ITS such as vehicle-to-infrastructure (V2I), mobile e-healthcare, smart grid and infotainment services.

Other protocols used are LoRaWAN - to support smart city applications and ensuring interoperability between several operators – and SIGFOX – an ultra narrowband radio technology that offers highly scalable with extremely low power consumption.

5. Cybersecurity, Data Privacy and Trust

The security of a smart city depends on a plethora of variables like strong security protocols, two-factor authentication or even the privacy between data exchange. In fact, according to HP, about 70% of IoT devices in a smart city were at risk of attack due to sufficient vulnerabilities such as insufficient authorization, inadequate software protections and weak encrypted communication protocols.

There are some cybersecurity-related processes or methods that are relatively easy to implement such as updating systems, making backups or even installing antivirus tools. However, in a wide-scale applying cybersecurity mechanisms can be a tough challenge since there is an abundance of different attacks and targets to protect. Below there's a table with the most common threats and their correspondent protective measures in different sector targets in a smart city.

Sector	Common Threats	Protective Measures

Smart Building	• Malware attack • System failure • Unauthorized access • Unauthorized control of resources • Disable access to resources	• Two-factor authentication • IoT forensic systems • Data backup and recovery
Smart Transport	• False message sending • Unauthorized access to braking/acceleration systems • Disable unauthorized systems (GPS)	• Public key systems • Anomalous behaviour arrest solution
Smart Governance	• Identity theft • Disable of critical systems • Text fraud • Unauthorized update of files	• Leak prevention systems • Threat analysis
Smart Health	• Change of medical reports • Exposure of sensitive data • Sending false information	• Secure Wi-Fi networks • Threat scan
Smart Energy	• Unauthorized access to control systems • Zero-day attacks • DDoS	• Intrusion detection services • Threat analysis • Risk analysis
Smart Finance	• Loss of privacy • Fraud • Unauthorized access to data • Trojan • DDoS	• Anti-malware solutions • Encrypted files • Risk analysis

Another point to breakdown is the data privacy aspect. All data that is exchanged in a smart city must be protected in order to gain the needed trust to end-users. If data privacy can't be achieved in a smart city, the end-users will not gain the trust that is needed to use and integrate these smart devices in their lifestyle. Therefore, security, data privacy and data protection are a must when it comes to an IoT-Based smart city.

6. Future Challenges

According to security aspects, computing requirement and energy consumption there are several challenges in this area that must be confronted in the future. With this aspect in mind, several papers and identities propose some solutions like fog computing, edge computing, blockchain, machine learning, intrusion detection systems and cryptographic techniques in order to increase the needed security, privacy, computing requirements and other important aspects.