University of Piraeus
School of Information and Communication Technologies
Department of Digital Systems

Undergraduate Program of Study/Postgraduate Program of Studies
MSc Digital Systems Security

Privacy on Smart Cities

Master Thesis
of
Makrygianni Vasiliki

Supervisor Professor: Gritzalis Stefanos

Piraeus, [September 2021]

Η σελίδα αυτή είναι σκόπιμα λευκή.

Acknowledgments

I would like to take this opportunity to first express my gratitude to Professor Gritzalis Stefanos, who is my thesis advisor, for devoting time to reading and reviewing my work. His special interest and knowledge in issues related to privacy and new technologies enabled him to give me the right guidance and motivated me.

Finally, I would also like to thank my family for always being supportive of my education, without them none of this would indeed be possible.

Table of Contents

Abstract 6
Περίληψη 7
Image Index 8
Table Index 9
Chapter 1: Privacy on Smart Cities 10
Introduction 10
Structure of thesis 11
Chapter 2: Smart Cities 12
The architecture of Smart City 12
Categories of Smart Cities 15
Characteristics of Smart Cities 17
History of Smart Cities 18
Smart Cities Applications 20
Smart Energy 22
Smart Building 23
Smart Mobility 26
Smart Infrastructure 28
Smart Governance 29
Smart Education 29
Smart Citizens 32
Analysis of IoT 33
Chapter 3: Privacy 37
Privacy fundamentals 37
Privacy by design 39
Privacy issues 42
Cyberattacks 43
Types of attacks 46
IoT protocols related to security 48
Chapter 4: Challenges 50
Taxonomy of Challenges 50
Challenge of Mashup Data 52
Data Management and protection 53
Chapter 5: Solutions 57
Understanding of privacy 57

Security Requirements of Smart Cities 57
Enhancing Technologies 60
Chapter 6: Conclusion 66
Chapter 7: References 68

Abstract

This thesis deals with the need for privacy that has arisen from the rapid development and application of new technologies in all areas of our lives and especially in their use in smart cities, which are developing rapidly. Many of them around the world have launched and adopted technologies that improve the daily lives and living standards of their citizens while enhancing education, economy, environmental protection, quality of public transport, and medical care. However, many smart cities have not fully embraced the methods that define a city as “smart”, as they lack the necessary means, such as proper design, networking structure, storing large amounts of data, etc. For this reason, as in many other technological areas, in smart cities, there are frequent breaches, which aim either to steal data and damage the proper functioning of these systems or to cause moral or economic damage. The following paper analyses smart cities, present the fundamentals of privacy, discusses the challenges that arise with the emergence of smart cities, and identifies ways to eliminate the breach of personal data.

Περίληψη

Η παρούσα διπλωματική εργασία, ασχολείται με την ανάγκη για ιδιωτικότητα που έχει προκύψει από τη ραγδαία εξέλιξη και εφαρμογή των νέων τεχνολογιών σε όλους τους τομείς της ζωής μας και κυρίως στη χρήση τους στις έξυπνες πόλεις, οι οποίες πλέον αναπτύσσονται με γρήγορους ρυθμούς. Πολλές από αυτές ανά τον κόσμο, έχουν ξεκινήσει και υιοθετούν τεχνολογίες που βελτιώνουν την καθημερινότητα και το επίπεδο ζωής των πολιτών τους, ενώ παράλληλα ενισχύουν την παιδεία, την οικονομία, την προστασία του περιβάλλοντος, την ποιότητα στα μέσα μαζικής μεταφοράς αλλά και την υγεία. Παρόλα αυτά, αρκετές έξυπνες πόλεις, δεν έχουν ενστερνιστεί πλήρως τις μεθόδους που ορίζουν μια πόλη ως «έξυπνη», καθώς δε διαθέτουν τα απαραίτητα μέσα, όπως είναι η σωστή σχεδίαση, η δημιουργία δικτύου, η αποθήκευση μεγάλου όγκου δεδομένων κ.α. Για το λόγο αυτό, όπως και σε πολλούς άλλους τεχνολογικούς τομείς έτσι και στις έξυπνες πόλεις παρατηρούνται συχνές παραβιάσεις, οι οποίες έχουν ως σκοπό είτε να υποκλέψουν δεδομένα και να βλάψουν τη σωστή λειτουργία αυτών των συστημάτων, είτε να προκαλέσουν ηθική ή και οικονομική ζημιά. Στο πόνημα που ακολουθεί γίνεται ανάλυση των έξυπνων πόλεων, παρουσιάζονται τα θεμέλια της ιδιωτικότητας, αναφέρονται προκλήσεις οι οποίες προκύπτουν με την εμφάνιση των έξυπνων πόλεων, ενώ παράλληλα ορίζονται τρόποι για την εξάλειψη της παραβίασης των προσωπικών δεδομένων.

Image Index

Image 1: Architecture of IoT
Image 2: Smart City Applications
Image 3: Smart Building
Image 4: Smart Infrastructure
Image 5: Smart Education
Image 6: Top 10 Application areas 2020
Image 7: 7 Principles Privacy by Desing
Image 8: Smart City Challenges

Table Index

Table 1: History of Smart Cities

Table 2: Taxonomy of security attacks

Table 3: IoT protocols related to security

Chapter 1: Privacy on Smart Cities

Introduction

In today's modern society technology evolving faster every day and playing such a critical role in people's daily lives. One of the biggest changes in the last years is the appearance of the Internet of Things (IoT) and smart devices which constitute an integral part of everyday life. Their role is multiple, they improve the quality of life of people especially in the large cities, they facilitate their daily life with several applications and solutions for example smart home automation, they inform and entertain people by collecting data through sensors, they even can build a whole smart city with great applications such as smart energy, smart building, smart mobility, smart health-care, smart governance, and smart security. With 54% of the world's population are living in urban areas the smart city concept is necessary for humanity.

The way that IoT systems are working is based on sensors and devices which collect data and transfer them to the cloud or Internet through some kind of connectivity. Once the data gets to the cloud, software processes it and then might decide to act, such as sending an alert or automatically adjustings the sensors/ devices without the need for the user. It is commonly known that IoT devices are nothing without data, so that makes the data powerful. Data is now becoming the most valuable commodity on earth, recently surpassing fossil fuels like oil.

But how safe is this way of living? Do people know that there are cases where they are sacrificing their privacy to have a better way of living? The data that people provide to these types of devices are photos, videos of their personal life, information about their fitness and health, maps, emails, messages, and more. Several types of research show, as we will see below, that those data and information are not exactly private, and if they are stolen they can cause damage to the owner.

Moreover, we will make a detailed explanation of the challenges that exist in this new way of living, with one of the most major issues is be peoples' trust. As we already know, there are several cases in the past with collision of personal data, such as the case of Cambridge Analytics where over 80 million people's data were intercepted in violation of Facebook's terms of service to target voters with political ads in the 2016 selection.

However, we are focusing on the important impact that smart cities will have on our lives and how companies, organizations, and governments will corporate in order to overcome ethical dilemmas that arise before any major change.

This paper is concentrating on how important the existence of Smart Cities is especially in big cities, examines the benefits of living in a society that consists of IoT devices, how this type of technology can provide a better way of living for the citizens without encroaching privacy and the challenges and opportunities that exist behind of this way of life.

Structure of thesis

The structure of this master thesis is divided into the following seven chapters. In the first chapter, we describe the topic of the thesis by identifying the research area in which it is embedded and at the same time the contribution to the reader and subsequent researchers and more generally to the field of IoT and cybersecurity. In the second chapter, we analyze the architecture, the categories, and the characteristics of smart cities and also, the applications of smart cities, giving examples with the purpose to give the opportunity to the reader to perceive the usefulness of new technologies. In the third chapter, we inspect privacy and analyzing the privacy fundamentals, the importance of privacy by design, and also the privacy issues. Also, related to privacy issues are cyberattacks, which we have included in this chapter, with the purpose to help the reader to understand the link between the different types of attacks and the result that they have in our privacy. The fourth chapter is all about the challenges that come after changes, like smart cities. We taxonomize the challenges and also we reference two big challenges, which are the challenge of mashup data and the management and protection of private data. In the fifth chapter, we refer to solutions, such as the understanding of privacy, the education of individuals around privacy issues and dangers, and also we list the security requirements of smart cities and potential enhancing technologies. In the sixth chapter, we conclude all the above, and lastly, on the seventh chapter, which is the last one, we list all the bibliographic and online sources that are used in the writing of the thesis.

Chapter 2: Smart Cities

The architecture of Smart City

There are several definitions of what makes a city “smart”, short smart city, uses a framework of information and communication technologies to create, deploy and promote development practices to address urban challenges and create a joined-up technologically-enabled and sustainable infrastructure. Moreover, smart cities combine automation, machine learning, and IoT to adapt technologies for a variety of applications. However, it is still difficult to distill a definition of the terminology “smart city”. Professor Mark Deakin in his article (From intelligent to smart cities) list four factors that contribute to the definition of a smart city, which are the below:

1. The application of a wide range of electronic and digital technologies to communities and cities.
2. The use of ICT to transform life and working environments within the region.
3. The embedding of such Information and Communications Technologies (ICTs) in government systems.
4. The territorialization of practices brings ICTs and people together to enhance the innovation and knowledge that they offer.

Smart cities are always related to the existence of IoT devices. Due to the complexity of their architecture, it is hard to create a uniform that will fit any system that includes IoT devices. However, the architecture can be divided into five layers, which are going to be described below:

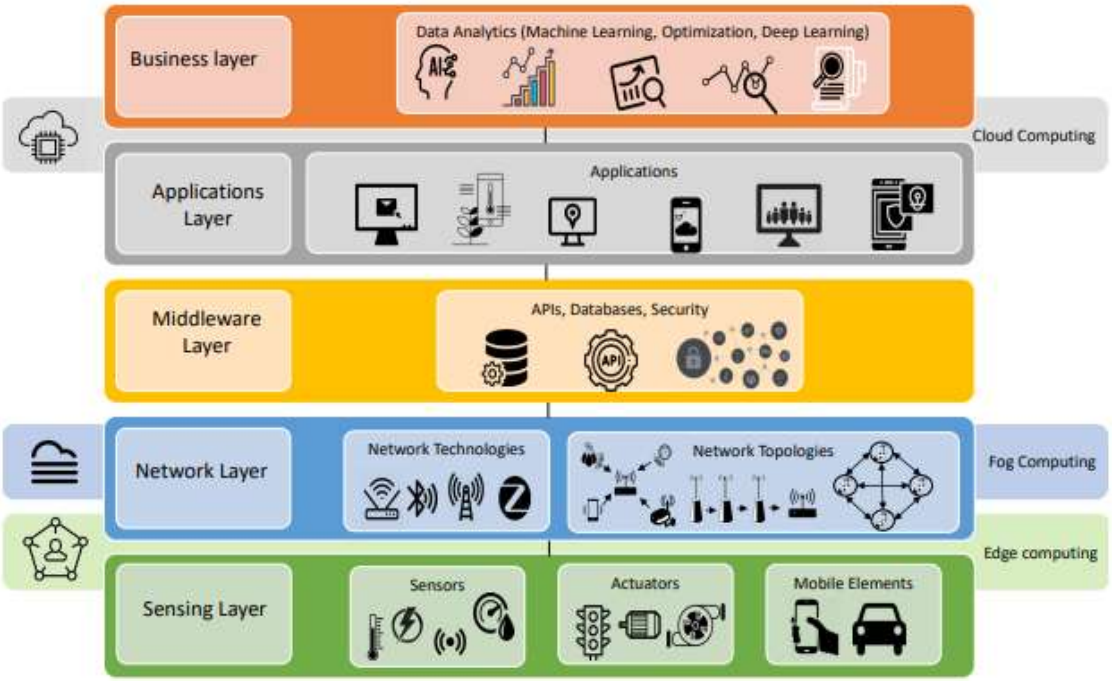

Image 1: Architecture of IoT

The sensing layer is the lowest layer of the architecture and it is mainly used for data collected from devices like sensors, cameras, etc. After collection, the data are going to be transferred for further processing to the next layer which is the network layer. This layer can be described as the core of IoT architecture because it can transfer the initial data to the devices that are connected to the network, either the connection is wired or wireless. To work properly the network layer, need support, which is the next layer and is called the middleware layer and it includes intelligent computing techniques such as APIs and databases. The next one is the application layer, which provides applications or services to users that are based on their personalized requirements. Above all is the business layer which is responsible to develop strategies and formulate policies that help manage the complete system.

However, beyond those five layers, smart cities architecture is based on three types of operations which respect to the stage of the IoT framework where the processing of data can be carried out, and these are Cloud Computing, Fog Computing, and Edge Computing. The main purpose of every IoT system designer is to combine with balance all the three layers keeping in view system costs and requirements.

Cloud is the space that hosts all the processing of data from the various components in the IoT system. As we already know, the advantage of the cloud is the remote accessing of uninterrupted shared sources, such as computing, storage, and services over the network, from a variety of different platforms. Basically, it is about centralized systems, that accommodate both hardware and software services and provide central management platforms to control the amount of receiving data, and also allows for cloud systems to have sufficiently large computing and storage capacities thereby allowing them to perform complex tasks of data mining, pattern extraction and making inferences from sensor data in smart cities to make use of it in the best manner possible. However, cloud computing appears some disadvantages most of the time because of the transmission of big amount of data. Transmitting all gathered data from different applications to the cloud increase the network traffic and direct the network costs. Moreover, due to the many applications, sensors, and data, there is data latency, especially when many devices start sending data at the same time because the sensing units exist at the sensing layer and the decision making/ data processing takes place in the cloud.

Fog computing provides a more diverse distribution of responsibilities than are dictated by the cloud computing architecture by moving some of the processing to devices on the local network. Due to the increased computational capabilities that fog computing offers, it is responsible for operations such as aggregation and collection of sensor data, simple processing operations, and decision-making that can be performed to reduce the amount of information flow towards the higher cloud layer. Moreover, the fog layer can provide the higher layers with decisions options rather than just data, thereby providing a better quality of information to the cloud layer thus resulting in better utilization of cloud sources. Also, the fog layer has access to the local state of a given region, so it can localize decision-making. Furthermore, devices can use different protocols on the local network, such as Zigbee, Bluetooth, or RFID in order to transmit data to the fog node, which is connected to the cloud. It is should be noticed, that the fog layer, rather than the above reasons, is responsible to solve the issues that exist on the cloud layer because it reduces costs for deployment of IoT systems, increases robustness as latency, data overhead, and transmission errors are reduced. This can improve the efficiency of the applications as a quick decision can be made on the received data, which is important in critical decision-making situations. Lastly, the fog layer is responsible to ensure smooth system operation and keeps a balance between the cloud and itself, and always keeping in view the costs that they are involved in.

Last but not least, is the edge computing model, which is also can decrease issues that appear on the lower level, such as reducing network and device costs even further. The main difference between the edge and the fog layer is that the first one edge nodes act as aggregation and decision-making units on a smaller scale compared to fog devices which act to provide seamless connectivity and data integrity throughout the IoT network. Once again, the purpose of the edge layer is to decrease the costs, by making the IoT systems decentralized and also increasing scaling.

Categories of Smart Cities

Smart cities can be categorized into two categories, which are IoT-based and cloud-based. In many surveys, it is possible to notice another category, which is Big Data. All of them are separate solutions and when they combining they can create a smart complexity, such as smart cities.

IoT-based describes the network of physical objects or things that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the Internet. The word “Things” in the terminology of the Internet of Things, is referring to the process of sending and receiving data using the internet and also it has the ability to training devices to make decisions and remember particular patterns and routines from an action that happened before. Also, IoT devices can include multiple appliances that need to be connected for reasons including automation and real-time control of devices. IoT devices can provide effective decision-making instructions to devices and control certain actions and aspects of when and how they function, due to the real-time and historical data stored that they have. Of course, IoT and cloud can combine and provide good communication, connection, and transference of data between devices. Moreover, it is recommended to use both systems because there are several benefits such as:

- Access data remotely
- Promotion on analysis and review of the status of connected IoT devices.
- Using cloud and IoT can enhance security, as regular updates can be sent and knowledge of any breach in infrastructure can be flagged up immediately.
- Scalability for device data.

- Quicker use and distribution of apps.

Big Data is about the process where structured and unstructured large quantities of data are analyzed to gain insight into business patterns. Most of the time, that referring to data that is also too vast or complex to process using usual methods such as volume, which is the amount of data collected from a variety of sources, velocity is the rate at which data is being processed, variety, which is the different types of formats of data that are transferring across systems and veracity which is the ability of Big Data tools to analyze and separate poor from high-quality data.

The last technology is the Cloud, which is a centralized system that delivers and transports data and various filed across the internet to data centers. The advantage of a Cloud system is that all the different data and programs can de be accessed easily from centralized systems. Moreover, cloud systems are economic solutions, because it does not require on-site infrastructure for storage, processing, and analytics. The scalability of Cloud Computing means that as businesses grow, technological and analytical capabilities can grow too. One of the most common types of Cloud services is Microsoft Azure Cloud.

IoT, Big Data, and Cloud Computing are linked because IoT is the source of data, Big Data is an analytics platform of data, and Cloud Computing is the location for storage, scale, and speed of access. In cases where we can combine all the three services, we can have great benefits such as scalability for device data, by using cloud-based solutions that can be scaled vertically and horizontally to meet the needs of Big Data hosting and analytics. For example, you can increase a server's capacity with more application, or expand hardware resources when necessary. Moreover, they offer scalable infrastructure capacity, and they can be used to store large amounts of data and provide scalable processing and improved real-time analysis of data. The lack of physical infrastructure needed to get Big Data, IoT, and Cloud up and running together reduces costs and means you can focus on the improved analytical capacity rather than worry about maintenance and support. Moreover, IoT and Big Data generate a large amount of data, and Cloud provides the pathway for the data to travel, so that's why they increase efficiency in daily tasks. Another important action is the quick use that they offer with several apps, worldwide, due to Big Data we can have access remotely, easily, and fast, from anywhere in the world and still carry out actions on devices when using the Cloud.

Furthermore, the big amount of connected devices on the internet, have created pressure and the need for intelligent systems to send data to the server for processing versus to the central server. With IoT devices, the processes and the access of the data can happen from many areas within the network, respond faster to downtime, and predict when errors may occur. Plus, using the Cloud with IoT helps to enhance security, as regular updates can be sent and knowledge of any breaches in infrastructure can be flagged up immediately. Last but not least, there are several economic benefits in business due to the built-in management tools of the Cloud.

Concluding, Big Data, IoT, and Cloud together can offer successful communication, connection, and transference of data between devices, effectively and efficiently. More specific, for industries and businesses, the combination of those systems is that it's a scalable, reliable, and agile solution.

Characteristics of Smart Cities

To develop any new security or privacy protection in smart cities, it is important to understand the characteristics and differences that it has with the traditional ones.

The first one and probably the most important is that IoT-based cities are heterogeneous, which means that the systems are independent, distributed, or can be used by different users. Moreover, the variety of IoT devices, different communication protocols and technologies, diverse hardware performances, and platforms have as a result that there is no one common uniform of smart cities, thus there is a lack of a common security framework and service.

As mentioned before, IoT devices should be budget friendly. To succeed that, suppliers should limit memory, battery capacity, processing capability, constrained network interfaces which means that the random-access memory and storage of these types of IoT devices are limited, most of the time with 8-bit or 16-bit microcontrollers. Due to the limit of possibilities of those devices, there are resource constraints on smart cities.

As will be mentioned below, one application of smart cities is called smart mobility, which is a characteristic of urban cities. It refers to the movement within a city the delivery of goods from one place to another but also means the technologies like citywide wireless

communication and real-time monitoring of the traffic flow. It is worth noting, that smart mobility is customized through a well-developed communication infrastructure.

One of the most basic features of smart cities is connectivity and scalability. Without connectivity, it is impossible to connect devices to the smart world, which is getting bigger and bigger every day. At the same time, scalability is an apparent feature in smart city scenarios. Both of them are a combination that helps smart cities to move forward.

Last but not least, humans are the mechanisms that make all the above things working and they are essential for the development of smart cities. Citizens that are living in those cities, should learning, creating, and educating into new features and most of the time to improve the quality of those applications.

History of Smart Cities

With the rapid growth of technology, as expected the big cities began to be affected and to redefine their needs. Developing modern technology directs the cities in the smart environment, which consents cites to intelligently optimize the scarce resources, save money, and provide pervasive resources for all citizens.

Looking back on the timeline of the smart cities, we can observe that the first smart city was in Los Angeles. The project “The State of the City: A Cluster Analysis of Los Angeles” was created in 1974 and it has been characterized as the first urban big data project in the history of smart cities. The purpose of the project was to used computer databases, cluster analysis, and infrared aerial photography to gather data, produce reports on neighbourhood demographics and housing quality and help direct resources to wars off blight and tackle poverty.

According to research, Los Angeles was the best choice to start a smart city because it had one of the best networks of streetcars and freeways, its flood control and water infrastructure, Southern California had a huge high-tech cluster in the aerospace industry and las but not least, Hollywood that they had their system.

Below we can see a timetable from 1974 until now major milestones events that will implement in the future.

Year	Fact
1974	Los Angeles created the first urban big data project: “A Cluster Analysis of Los Angeles” report.
1994	Amsterdam created a virtual ‘digital city’ – De Digital Stad (DDS) – to promote Internet usage.
2005	Cisco put up $25m over five years for research into smart cities.
2008	IBM Smarter Planet project investigated applying sensors, networks, and analytics to urban issues.
2009	IBM unveiled a $50m Smarter Cities campaign to help cities run more efficiently. American Recovery and Reinvestment Act (ARRA) provided funding for US smart grid projects. EU Electricity Directive required EU states to roll out smart meters to 80% of consumers by 2020.
2010	Japanese government named Yokohama as a smart city demonstrator project.
2011	IBM named 24 cities as Smarter Cities winners from 200 applicants. 6000 visitors from over 50 countries attended the first Smart City Expo World Congress in Barcelona. Barcelona deployed data-driven urban systems, including public transit, parking, and street lighting. China announced the first batch of pilot smart cities, comprising 90 cities, districts, and towns. Mayor of London created Smart London Board to shape London’s digital technology strategy.
2014	China launched the second batch of 103 pilot smart cities. Vienna City Council launched the Smart City Wien Framework Strategy until 2025.
2015	China announced the third batch of 84 smart cities, comprising 277 in all. India’s Prime Minister Narendra Modi launched the “Smart Cities Mission” for 100 Indian cities.

2016	Columbus won the US Dept of Transportation's $50m Smart Cities Challenge. UK government launched 5G testbeds and trials program. Hong Kong launched a smart city blueprint.
2018	Toronto and Google offshoot Sidewalk Labs announced a plan to develop a smart waterfront area. London updated 2013 plans with the launch of the 'Smarter London Together' roadmap. IESE Business School Cities in Motion Index ranked New York, London, and Paris as its top 3 cities. Singapore won the Smart City of 2018 award at the Smart City Expo World Congress.
2019	Ford committed to supporting Cellular Vehicle to Everything (C-V2X) standard. Sidewalk Labs' Toronto planning document fiercely criticized over data privacy implications. G20 nations picked the World Economic Forum as the secretariat for a G20 Global Smart Cities Alliance. US Federal Communications Commission picked New York and Salt Lake City as 5G testbeds
2020	Vietnam to start work on new $4.2bn smart city close to Hanoi, with completion target of 2028
2030	By 2030, the number of cities in the world with a population of more than 10 million will grow to 43.
2050	By 2050, up to 70% of the world's population is expected to live in cities.

Table 1: History of Smart Cities

Smart Cities Applications

In the last years, many applications have been developed, mainly in big cities, with the help of technology. Smart application is a big part of nowadays cities and they affect the life of the citizens in many daily activities. The main purpose of this application is to improve the standard of living and providing a liveable and affordable environment for citizens. As we can see below, a smart city can consist of :

- smart security for reducing the security risks and managed security services to protect people, properties, and information,

- smart building for independently controlling and managing the lighting and temperature system, security, and energy consumption throughout the large constructions
- smart mobility for enabling intelligent mobility by utilizing the innovative and integrated technologies and solutions
- smart technology for enabling intelligent network connectivity and edge processing solutions in cities across the globe
- smart healthcare for enabling intelligent systems and connected medical devices to promote wellness, provide health monitoring and diagnostics
- smart governance and education to provide policies and digital services from the government and facilitate the educational system through the modern technologies
- smart energy for optimizing the generation
- monitoring, and consumption of different types of energy
- resources by using digital technologies

and many other applications that they are going to appear in the next years.

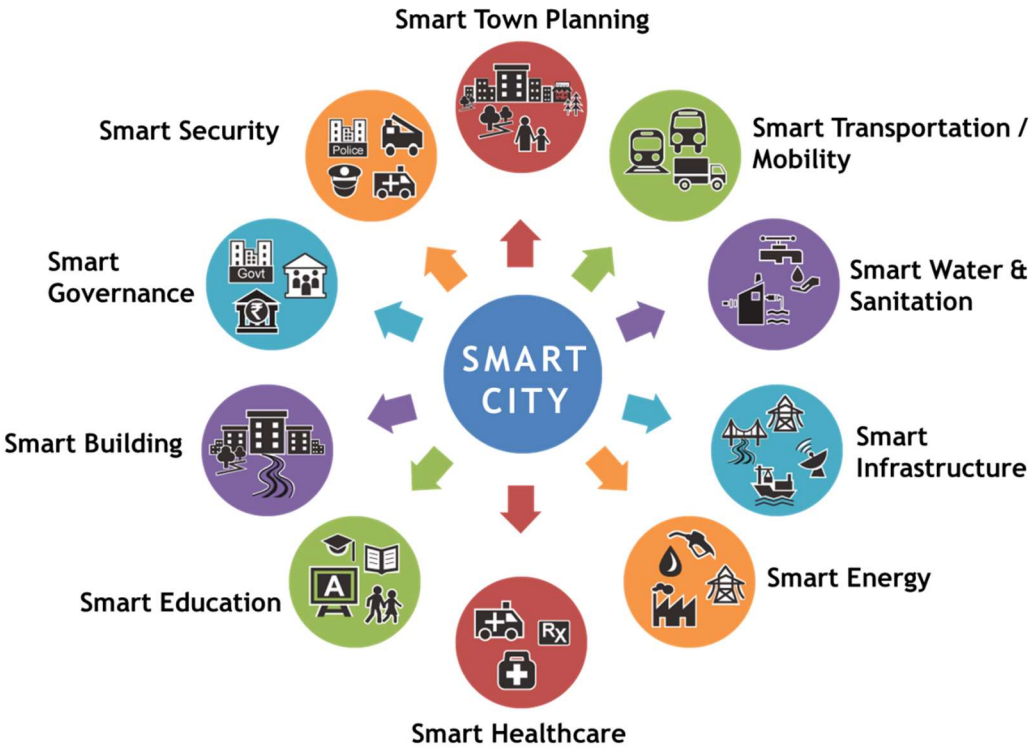

Image 2: Smart City Applications

Below we are going to analyze the most famous applications that they have the biggest impact on people's life.

Smart Energy

Smart energy focuses on efficient control of energy and resource consumption and increases the usage of renewable energy sources. Smart energy systems pose many benefits to consumers, the environment, and energy providers at large. Many pillars support the smart energy concept, such as:

- Resource system integration
- Access to energy services
- Resilience
- Energy Efficient
- Renewable energy
- Active and engaged users
- Sustainable economy

There are many types of smart energy but two of the most popular are solar energy and natural gas. Both of them are renewable energy options and they have already made an impact felt. Solar energy has become the fast-growing form of renewable energy in the United States and on the other hand, natural gas can be environmentally friendly when it burns in the proper facility.

In the last couple of years, smart energy grids have gained a lot of interest due to the changes in the climate and the new sustainability methods that bid cities are trying to pose. Smart Energy Grids are a complexity of advanced technologies, electronics, and microelectronics, high-performance computational platforms which have been developed by the use of innovative models, intelligent algorithms, and a series of new methodologies to produce and conserve energy. The systems that compose the smart energy grid, should be fault-tolerant, with high technology-based and able to improve the consumers' quality of services, guaranteeing the needs of consumers by minimizing cost, waste of resources, and environmental impact. Moreover, smart energy grids need high-performance telecommunications networks for the exchange of data between nodes, and of course a highly-designed automation and smartness network. The concept of Smart Energy is to describe a point of an intelligent network able to maximize the use of renewable energy resources and, at the same time, able to satisfy the energy demand from consumers. In

particular, smart energy may be considered as a simple home configuration where there is a photovoltaic production, a storage device, and a series of users such as household appliances, so this is why a smart energy grid can be defined as the next generation power grid. The difference between traditional smart energy and smart energy is that the first one the power is carried from central generators to a large number of users, and in the case of smart energy, there are two-way flows of electricity and information to create an automated and distributed advanced energy network that is clean, safe, secure, reliable, resilient, efficient and of course sustainable.

As mentioned, smart energy uses two-way flows of electricity and information, which offers the opportunity of monitoring every sensor that is assigned on the same network. Other features of smart energy are the real-time monitoring of the power system, the quick and accurate diagnosis of issues that can improve outage management performance, reduce system losses, and enables scenarios for automated maintenance and outage prevention. Besides those features, smart energy may solve issues that exist on the traditional energy grid, such as the overprovisioning of electric power induces frequency jumps, while under-provisioning implies frequency drops, which causes excessive frequency deviations. As a result of malfunction on both producer and consumers side, is the blackout or collapse of the grid. Another issue is the lack of renewable energy sources, which makes the traditional grid harmful to the environment.

Smart Building

Smart buildings application tries to keep everything under control by using sensors to collect data, monitors, and controllers. To make a building more efficient, cutting costs and lowering its environmental impact. The main applications of smart buildings are to manage energy equipment, reduce energy consumptions, and increase energy reliability. There are several benefits of smart buildings, such as:

- Saving costs
- Reducing energy consumption
- Improving efficiency
- Wellbeing

Smart buildings can be a small place i.e., an office or a big one like an university campus. One of the most famous examples is the National Grid, where they use technology in the

form of occupancy sensors to make their buildings smart and optimize their space utilization. They also gained valuable data on the time employees went for lunch, enabling them to choose quitter times to visit them, avoiding queues at the typically busier periods.

Below we can see an example of a smart building, that includes important technologies that they can facilitate people's life. The first one, and one of the most major, is high-speed Internet, which can allow all the other systems to work fast, and of course to the people, to complete their daily tasks. Moreover, access points can offer wireless internet in every corner of the building even when cable installation is not possible, methods such as mesh can be used and add wireless internet on places that UTP cables have been destroyed or were not provide. Needless to say, that wireless and wired internet, should be protected, for that reason, VPN is a secure method that can be used for the residents when they need extra safety (i.e., payments).

Furthermore, IP phones can offer HD voice quality, cheaper running costs, and advanced business phone features, unlike a regular telephone that uses landlines to transmit analog signals, IP phones connect to the internet via a router, so they are internet-based phone technology and they have improved by leaps and bounds.

Audio and Visitor conferencing allow connecting multiple people on different devices on the same phone or video call. For this scope, it can be used either a desktop phone or a smartphone, and all the participants can connect via the internet and attend real-time communication.

Visitor management is a method that has begun to be preferred by many owners of smart buildings because does not require physical presence. In many cases, visitor management is integrated with the system of access control, so it allows visitors to self-register when they are visiting a building. Moreover, this method gives the opportunity to have several entries and exist on the building without the presence of a concierge or a security guard. As we have already mentioned, visitor management can easily integrate with access control, and this can give to the operator the opportunity of total control of the building. The operators can control all the entries and the exits, for people or cars, the elevator, the elevator and execute reports on a daily basis regarding the movements of the people that they visit the building. Access control apart from the control can also be very useful as a safety system in cases of emergency, for example, a well-configured system, in case of a fire, can open the critical door, move elevators to the main level of the building, create a detailed report with the people

that they are on real-time inside the building, activate the fire system and inform via IP Telephone the local fire department.

All the above can be supervised 24/7 via IP smart cameras that can be located all over around the building and a video surveillance system can be located in the security room in order to record daily. Smart cameras can record under certain scenarios, such as when a light is turning on in a highly secured room a smart camera is start recording and at the same time is sends a notification to the security offices that someone, is inside this specific room. Surveillance gives a chance to the security to inspect the room from a distance before visiting it.

We can understand from the above example, that lights are probably the one thing that should always work inside a building, no matter what. Only imagine, that all the other technologies, by the end of the day, cannot efficiently work if there are no lights. This reason created the need for well-designed smart lighting solutions and the existence of backup systems.

Last but not least, there are many benefits of smart buildings, one of them is the saving costs, which came after reducing energy consumption. A sensor that controls the temperature inside the rooms of a smart building can help on this because again human presence is not necessary and when the temperature increased or decreased, sensors will restore it to the set point that it has been determined. Moreover, we can use sensors in order to control lights, for example, is it not necessary to turn on the lights 100% during the day, so that's why we can use sensors that are going to perceive the brightness and setting the lights in a specific point.

As we are going to discuss in the below chapters, to understand the importance of privacy in smart cities, we could imagine an attack in one of the major systems of a smart building, i.e., one the access control. Beyond the chaos that will come up after an attack like this, malfunction of those systems can cause, in rare cases, loss of human life.

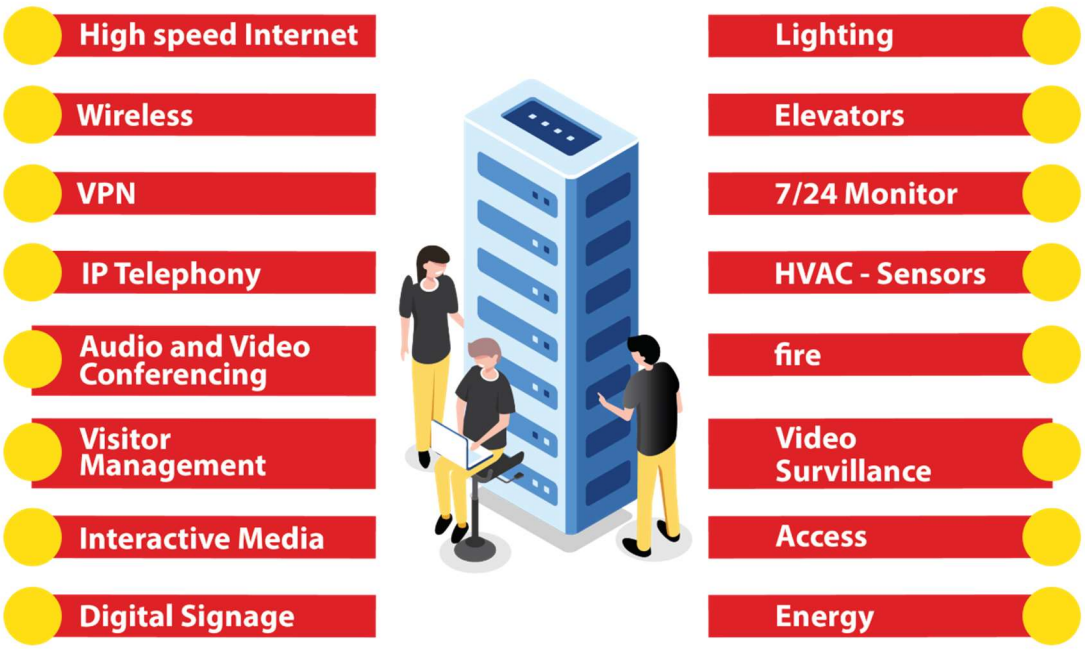

Image 3: Smart Buildng

Smart Mobility

The term smart mobility refers to the transport of people and goods to achieve a smooth and sustainable society. One way to achieve a smart mobility system for a city is to build a network for collecting, processing, and analyzing data from the transport systems of the existing organizations. Interesting is the research about American peoples show that they spent 42 hours/ year sitting in traffic and the 30% of the city traffic are people looking for parking, both of them have an economic cost of 124$ billion. A great solution for smart mobility is the smart cities of Hitachi which include the below 5 different layers:

- Transportation user experience layer: to deliver various information about transportation services to citizens
- Transportation services layer: that contains provided transportation services by organizations
- Information collection layer: to gather the information about the usage of services
- Information management and control layer: that check the services to confirm the smoothness of provided services by the organization

- Transportation company coordination layer: that is responsible for optimizing the city's overall transportation system by analyzing the collected information from all companies

In most cases, the term of smart mobility is referring to improve traffic. Indisputably this is an important issue, but smart mobility does not concern traffic alone. The special attention to traffic is a result of the expansion process in cities, which has led to a polycentric structured city with decentralized, dispersed, and fragmented links, causing a greater dependence on private cars due to increasing distanced and the lack of competitiveness in public transport in low population density areas. The importance of mobility and its impact on the other Smart City axes such as sustainability, economy, and lifestyle make this a vital issue for residents and local governments. The difference between mobility and smart mobility is public access to real-time information, this improves services by saving time, enhancing the journey, saving money, and reducing CO2 emissions. Smart mobility is the key to the smart transformation of cities and long-term to a smart environment.

Moreover, the smart mobility axis is closely related to environmental sustainability. Smart mobility includes numerous initiatives designed to improve the environment, such a reducing the use of private vehicles and integrating transport modes, which generally produce a decrease in emissions. The transformation of the environment by the urban development process generates impacts such as the consumption of natural resources and energy, atmospheric emissions, and waste discharge. It has been estimated that cities currently consume about 75% of the world's energy and generates 70% of global CO2 emissions, and these figures are expected to continue rising in coming years as cities grow even larger. The increasing intensity of urban metabolism and its effects on climate change are some of the most important sustainability challenges facing cities today.

The sustainability of the urban environment is analyzed from two approaches, the first is from the point of view of energy and the prevention of consumption, involving renewable energy, technological grids, pollution control, and management, green buildings, green urban management, efficiency, re-utilization and so on, and the second one linked to the urban grid and the management of resources, waste, street lighting, waste management, drainage systems, monitoring water resources, reducing contamination and improving water quality.

Basic on research that took place between 62 Spanish cities with a population of over 50.000 inhabitants, with 35% of the Spanish population and 43% Spanish Population living in municipalities more than 50.000 inhabitants and it also includes all Spanish cities with more than half a million inhabitants, shows that the smart mobility is a very important factor in smart cities and that the smart environment has poor results in Spanish cities.

Smart Infrastructure

Smart infrastructure is the result of combining physical with digital infrastructure, proving improved information to enable better decision making, faster and cheaper. Smart infrastructure is part of the fourth industrial revolution and the global opportunity of this type of technology worth £2trn-4.8trn.

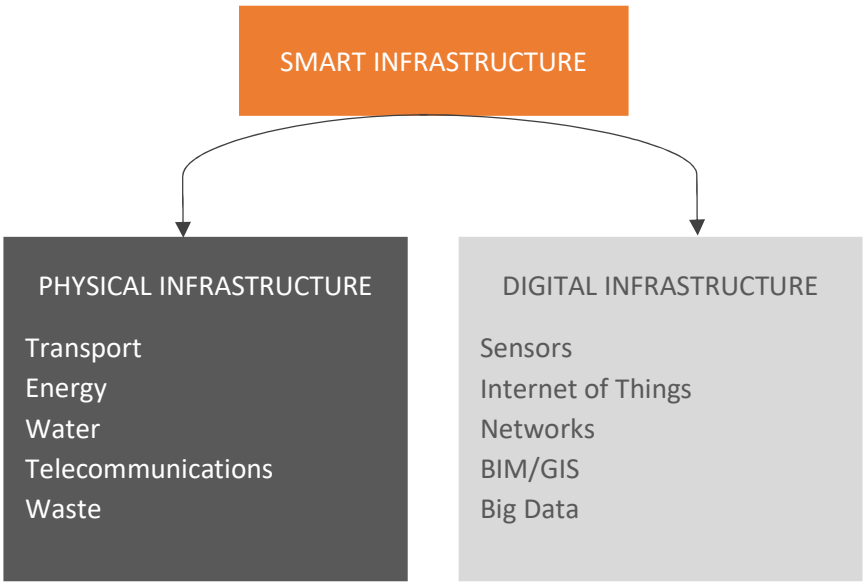

Image 4: Smart Infrastructure

A good designed smart infrastructure should take into consideration four different principles in order to be successful. The first one, and probably the most important is that a smart infrastructure is a people-centric approach which means that the requisites of citizens should be taken into consideration. Moving on a smart framework should be resilient and sustainable to prevent unpredictable internal and external shocks but also has to be flexible to

support future modifications and enhancements. Last but not least, risk-mitigating plans to protect the privacy of the citizens should have a major role.

Smart Governance

The influence of modern technology can be felt in every aspect of our lives, even in the way our government functions. Smart governance is the process of utilizing modern technologies and ICT to create a collaborative, communication-based, transparent, and sustainable environment for citizens and government. There are four different smart governance models:

- G2C model: Government to Citizen in this type of model government interact with citizens using communication media such as newspaper, radio, TV, and the internet.
- G2B model: Government to Business in this type of model government communicate with businesses to promote the growth of the economy. Moreover, assist online business practices to save time and costs.
- G2G model: Government to the government using ICT tools for a paperless, corruption-free, and sustainable system. This type of system tries to create better communication between government and government organizations.
- G2E model: Government to Employee, in this type of governance communicate with the employee and companies with a purpose to help at daily tasks such as payroll, bank loan, medical plans, etc.

Moreover, a smart government plays a crucial role in a smart city, because it allows citizens to get involved in public decisions and city planning.

Smart Education

It can be described as one of the most remarkable impacts of a Smart City. There are several advantages of smart education because it provides new facilities for students by engaging modern technologies or social media, such as virtual, online, and e-learning. The purpose of smart education is to support the teacher's job by using either hardware or software.

A great example is the case of Malaysian smart schools that aim to help their country to foster the workforce of the 21st century by utilizing and enabling leading-edge technologies into schools. Smart schools not only focus on stimulating thinking, creativity, and caring for the students, but also considering the individuals' differences and learning styles among the learners. Smart education in Singapore also emphasizes the role of technology. Their goal is to foster an engaging learning experience to meet the diverse needs of learners, through the innovative use of information and communications technology. In order to realize this, Singapore created an enriching and personalized learner-centric environment and additionally created a nationwide education and learning architecture for educational institutions and life-long learning.

Moreover, Korea carried out the smart education project to provide customized and adaptive learning for students to foster self-directed learning ability and have fun using various resources and technology. Individualized instructions and creativity-centered education is considered as the main keyword of smart education. Also, Australia aims to build a smart, multi-disciplinary student-centric education system using adaptive learning programs and learning portfolios for students, collaborative technologies ad digital learning resources for teachers and students, computerized administration, monitoring, and reporting, and online learning resources. New York is another great example because they trying to connect every school using a high-speed network, utilizing transformative technologies to embracing and expanding online learning, extending connectivity between inside and outside of the classroom, high-quality continuous professional development, and focusing on foster 21st-century skills.

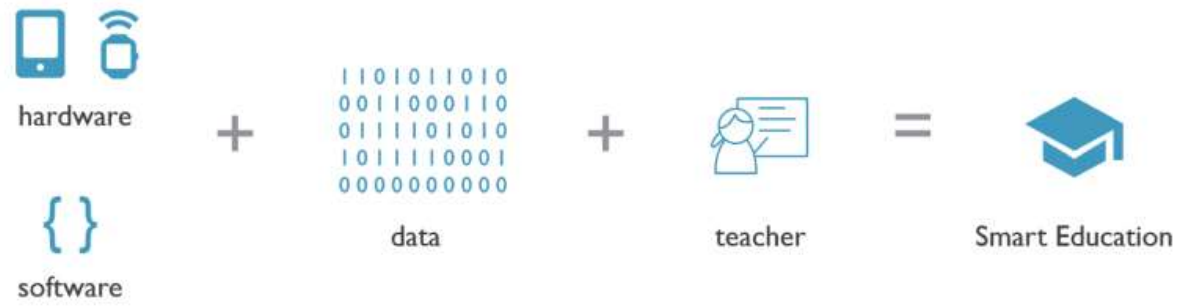

Image 5: Smart Education

By analyzing these smart education projects, we can find some generalities. The goal of smart education is to foster a workforce that masters 21st-century knowledge and skills to meet the need and challenges of society. Intelligence technology plays an important role in

the construction of smart educational environments. In smart educational environments, learning can happen anytime and anywhere. It encompasses various learning styles, such as formal and informal learning, personal and social learning, and aims to realize the continuity of the learning experience for the learner. In these learners are provided with personalized learning services as well as adaptive content, and according to their context and their abilities and needs. Generally, the smart thing on smart education refers to intelligence, personalized, and adaptive.

However, the term “smart” has a different meaning for different entities. In the case of smart education, “smart” refers to accomplish its purpose effectively and efficiently. The technology includes hardware and software. Smart hardware refers to smart devices that are much smaller, more portable, and affordable. It is effective to support users take to take place the learning anytime and anywhere with smart devices. And some hardware (i.e. smartphones, laptops, Google glass, etc.) has the function to recognize and collect the learning data to engage the learner into contextual and seamless learning. Regarding software, smart refers to adaptive and flexible. It is efficient to carry out personalized learning for the learner to their difference, with adaptive learning technologies (i.e. cloud computing, big data, learning analytics, adaptive engine, etc.)

Moreover, due to the development of new technologies, we can learn more effectively, efficiently, flexibly, and comfortably. With the development of mobile, connected, and personal technologies, mobile learning has become a major paradigm. Mobile learning emphasizes the utilizing of mobile devices and focuses on the mobility of the learner, in contrast to the static traditional educational typer. In addition to that, the support of ubiquitous technology has caused further changes that moving the learning style away from mobile learning toward ubiquitous learning which emphasizes learning and teaching can take place anytime and anywhere without the limitations of time, locations, or environments.

In order to situate students in authentic learning environments, it is important to design learning that combines both real and virtual learning environments. Seamless learning, which overlaps with some aspects of mobile learning and ubiquitous learning, is expounded as an oone-to-one model which learners can learn across time and locations, and they can convert the learning from one scenario to another conveniently encompassing formal and informal learning, individual and social learning through the smart personal device.

Also, other intelligent technologies such as cloud computing, learning analytics, big data, IoT, wearable technology, etc., promote the emergence of smart education. Cloud computing, learning analytics, and big data, which focus on how learning data can be captured, analyzed, and directed towards improving learning and teaching support the development of personalized and adaptive learning. With these adaptive learning technologies, the learning platform reacts to individual learner data and adapts instructional resources accordingly based on cloud computing and learning analytics, and it can leverage aggregated data across mass learners for insights into the design and adaptation of curricula based on big data.

In addition, the IoT and wearable technology support the development of contextual learning and seamless learning. The IoT can connect people, objects, and devices. Learners carrying smart devices can benefit from various related information that is pushed to them from their surroundings. Wearable technology can integrate location information, exercise log, social media interaction, and visual reality tools into learning.

Smart Citizens

Citizens can be described as the fuel and the foundation of smart cities. They are the supplies that can make a smart city works and develop. For a smart city to be successful, the designers must think about the people that they live in, because people are going to be the raw material and those that they are going to use all the equipment. Smart cities should communicate with smart citizens' care about them and don’t be technocratic, but they should try to provide a better and easier way of leaving. In order for the smart city project to be successful, organizations should take into account the role of technology in their cities and its impact on how they will travel, live eat, play, study otherwise the vision of a smart city, will fail.

Moreover, the city officials, if they want to gain the benefits of technologies in society, they need to interact with their citizens, through discussions, workshops, or surveys on how technology changes might impact their lives. Citizens have the right to know where technology will be applied in their cities and how their data will be used. Organizations should take into consideration the opinion of individuals and engage their thoughts in the process of a smart city project.

Last but not least, the education of smart citizens should be a priority, because everyone needs to understand the basics of privacy, technology and interpretation of data.

All the above classes, explain the link between technology, and people's daily life. Some of the above categories are important for the health and safety of people, for education, for privacy, so we can understand the damage that could be occurred if some of them stop working properly. Below we are going to analyze the popularity of each category, and also we are going to taxonomize them based on the percentage of resonance that they have on industries, companies, etc. Moreover, we are going to explain the reasons why each category is in a particular position.

Analysis of IoT

As discussed above, all the applications of smart cities are useful, however, some of them have a higher demand than others. On the top of the list, is the manufacturing/ industrial area. This is happening because there are large industrial automation companies that support this area, such as Microsoft, Siemens, or Rockwell Automation. Moreover, the industrial IoT has a wide scope of application both inside and outside factories, such as many IoT-based factory automation and control projects include holistic smart factory solutions with numerous elements such as production, floor monitoring, wearables, remote PLC controls, or automated quality control systems. Also, some projects include remote control of connected machinery, equipment monitoring, or management and control of entire remote industrial operations. Another reason that puts this category on the top of the list, is that there are several solutions with selected IoT platforms-enabled projects. In this case, also, there are several manufactures behind successful IoT platforms that provide efficient solutions to their clients. Those innovative solutions, allow their customers to ultimately save a significant amount of time and associated cost. Also, there are solutions that by the means of constantly improving strategies of maintenance, reduce costs of repair and maintenance scheduling, effectively reallocating resources, and decreasing production risks.

Below we can see a chart that captures the top ten application areas of the previous yes. In the last column, we can see that more than half of them tend to be trending in the next years. In the first position, we can easily notice the area of manufacturing/induction, which occupies the largest percentage.

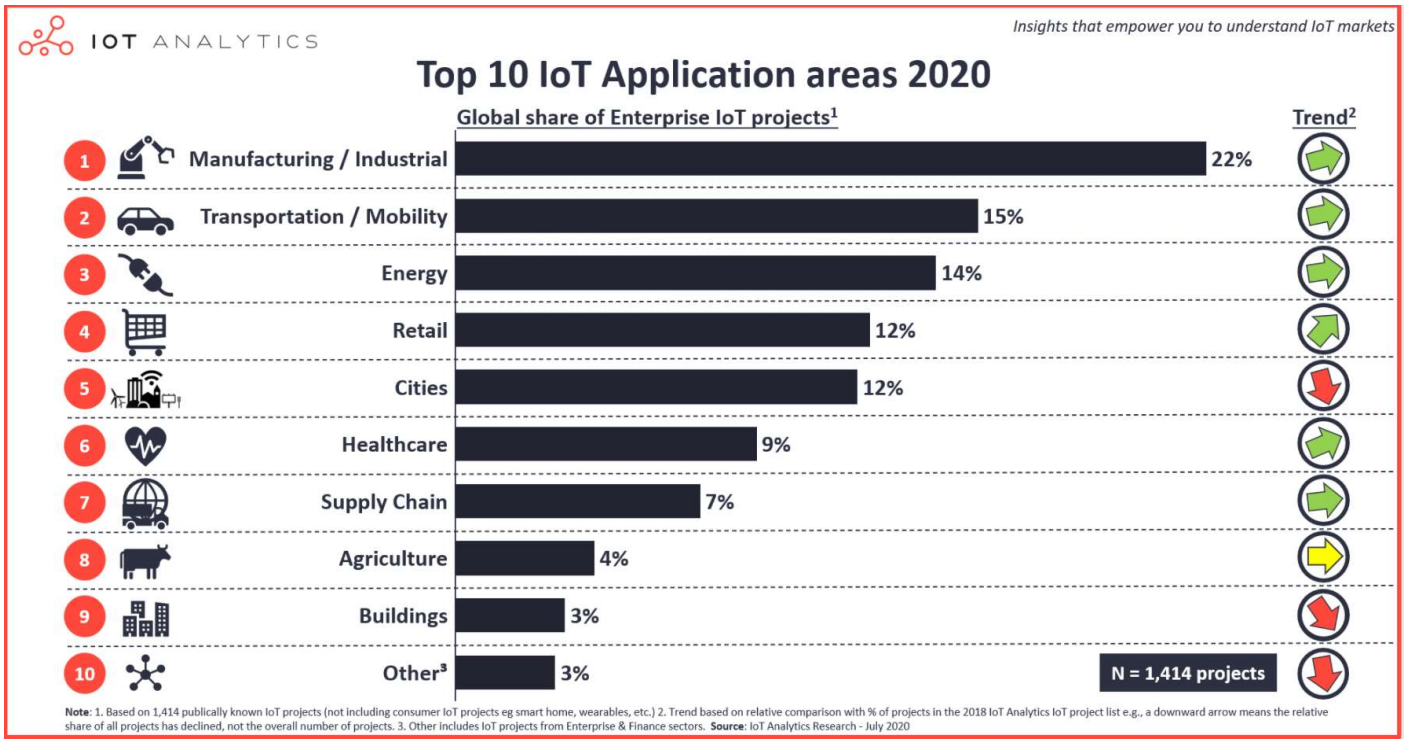

Image 6: Top 10 Application areas 2020

Transportation/Mobility is the second biggest IoT application area in 2020. As in the previous case, the manufacture Tesla is responsible for this change, because after the release of the latest car, pretty much every manufacture begins to follow suit integrating similar IoT technologies. This area includes applications, such as KWRL real-time fleet monitoring, OmniBus fleet operations optimization, and Caledonian driver behavior tracking. Among other features, those applications include telematics and fleet management solutions that connect with the local operating system within the car for vehicle diagnostic/monitoring such as battery monitoring, tire pressure monitoring, driver monitoring, and vehicle tracking.

The third application area is energy. Due to the large energy consumptions which are expected to grow by 40% over the next 25 years, the need for smart energy solutions is more necessary than ever. Smart energy is applicable in every part of the energy industry, from generation to transmission to distribution and changing how energy companies and customers interact. The main object of smart energy focuses on energy distribution, grid optimization, remote asset monitoring and management, predictive maintenance, and creating more transparency for better-informed customers.

Retail is the fourth application on the list, and it starts to rise because many companies have understood that they can improve their cost-efficiency and in-store customer experience through innovative IoT use cases. Moreover, there is a high interest in the retail market for digitizing stores to create a smart process, which is included in-store digital signage, customer tracking, and engagement, monitoring and inventory management, and smart vending machines.

As we have already examined in this chapter, smart cities starts to grow in the last years, and they are in the fifth position of this list. The top 3 smartest cities in 2019, was Singapore, Zurich, and Oslo but more and more cities are trying to accommodate this concept.

The sixth application is the area of healthcare, where unfortunately before the pandemic COVID-19 the concept of smart healthcare there was no remarkable development due to security issues that can occur. However, the last two years, after the appearance of COVID-19 has changed. Several applications were developed in order to offer solutions such as telehealth consultations, digital diagnostics, remote monitoring, and robot assistance. Hospitals and clinics, trust the technology and include medical devices for monitoring, such as in the case of Medisanté and Medtronic.

In the next position, which is the seventh position on the top ten, we can find the area of the supply chain. The rising of this area is a result of the changes that have occurred in retail, where goods are more complex to deliver, so logistics provides are increasingly integrating connected digital solutions to tackle the complexity. There are more than 56% of customers are planning to invest in IoT. A typical IoT platform for the supply chain includes the feature of asset tracking, condition monitoring, inventory and storage management, automated guided vehicles, and among others, connected workers. IoT platforms for the supply chain, are going to increase in the next few years because they help companies to stay in control, keep an overview, and react quickly.

The next one, the eighth position on the list, is the area of agriculture, which we will see in the coming years grow rapidly. As it is estimated, a population of almost 10 billion people will need up to 70% more food than we do today, so this challenge creates the need for fast and quick production in agriculture. Smart agriculture, include among others, sensors that can help farmers to make more informed decisions to achieve higher crop yield, better quality produce, and save costs by reducing the use of fertilizers and pesticides. Moreover, a

smart agriculture platform could also include features to monitor conditions of the weather, soil moisture, chemical compositions of the soil, and other environmental conditions at a much lower total cost.

In the ninth position, we can find the category of smart buildings, which has investments of more than 71% in the United States. Organizations that vest in smart building control systems improvements and over half have implemented an enterprise-wide smart building management system. The goal of smart building innovations is to increase productivity and efficiency while reducing operational costs through complete building life cycle management. There are several IoT platforms, the typical applications include facility-automation and monitoring for building systems, like HVAC, lighting, elevators, smoke and fire alarms, introduction system, audio, and video systems. All those features can make building more active, entities that they can understand their environment, interact, learn and adapt.

In the last position of this list, we can find random IoT applications, which are occupied 3% of the project of smart cities.

Chapter 3: Privacy

Privacy fundamentals

Privacy is the competence for a person or a group of people to insulate either themselves or information regarding them and to be able to express themselves optionally. Sometimes, the definition of privacy is confused with the definition of security, however, they are two different meanings with the second one to be mentioned on the concepts of appropriate use.

Privacy has ten fundamental aspects, that should be followed by everyone in society. Those aspects, which some of them have been established since 1890, are the bellow:

- The right to be let alone has been established in 1890 in the United States by jurists Samuel D. Warren and Louis Brandeis after they wrote an article for the "right to be let alone". This article describes the right of a person to choose seclusion from attention and the proper to be immune from scrutiny or being observed in a private area, such as one's own home.
- Limited access is the ability of people to be a part of a society without other organizations collect information about them. In the 19th century, the American journalist Edwin Lawrence Godkin wrote in one of his articles that "nothing is better worthy of legal protection than private life, or, in other words, the right of every man to keep his affairs to himself and to decide for himself to what extent they shall be the subject of public observation and discussion".
- Control over information means that the control of personal information belongs only to the person to whom the information relates.
- Sates of privacy can be separated into different experiences based on the Professor of Public Law & Government Emeritus Alan Westin: solitude, intimacy, anonymity, and reserve. All of them have a different impact on people's society because they separate their private social life.
- Secrecy and privacy have similar meanings and most of the time they have the same purpose, which is to protect personal information from third parties. However, secrecy is defined as an option for people to keep secret or private information, and if they choose, they can make it public. Most of the time, secrecy and privacy are identical terms and privacy can be described as secrecy.

- Personhood and autonomy are meanings that are related to privacy, so they have been defined by many professionals of Philosophy such as Jeffrey Reiman, Stanley Been, and Joseph Kufer. In the first case, Jeffrey Reiman has been defined privacy in terms of recognition of one's ownership of his or her physical and mental reality and a moral right to his or her self-determination. On the other hand, Stanley Benn defined privacy in terms of recognition of oneself as a subject with an agency—as an individual with the capacity to choose. Moreover, privacy is a state that enables autonomy, which is a concept closely connected to personhood. That's why, last but not least, Joseph Kufer defined autonomy as an autonomous self-concept that entails a conception of oneself as a "purposeful, self-determining, responsible agent" and an awareness of one's capacity to control the boundary between self and other—that is, to control who can access and experience him or her and to what extent.
- Self-identity and personal growth social psychologist, Irwin Altman argued that privacy barriers "define and limit the boundaries of the self" and thus "serve to help define". Moreover, privacy may be understood as a state that promotes personal growth, that urges individuals to feel free to express themselves, to engage in self-discovery and self-criticism. That is to say, privacy could be interpreted as a precondition for the development of a sense of self-identity.
- Intimacy can be described as the mean that people use to strengthen or intimate relationships with other humans. Human relationships are complicated, which means that intimacy should be defined with limits on individuals. Moreover, privacy and intimacy have a close association, according to the American philosopher James Rachels has been mention, "there is a close connection between our ability to control who has access to us and information about us, and our ability to create and maintain different sorts of social relationships with different people."
- Personal privacy can be described "as the right of people to be secure in their persons, houses, papers, and effects, against unreasonable search and seizures" as it has been said from the U.S. Fourth Amendment.
- Organizational most of the time does not refer to individuals, but a group of people, for example, government agencies, corporations, groups/societies, and others. Those organizations may desire to keep their activities or secrets private, and in order to achieve that, they accomplish various security practices.

All the above aspects have been established in the field of personal data and privacy for almost a century and they are taken seriously when personal information is compromised, published, processed, or exploited without the permission of the person to whom they belong. The invasion of privacy has been a legal issue since 1900, so as expected the rapid rise of technology complicates the situation because many solutions need personal information to work correctly. This circumstance forces lawyers in conjunction with technologists to find ways to secure personal data and to evolve new resolutions so that privacy and technology coexist. For that reason, in 2009 the framework of privacy by design has been published and in 2010 has been adopted by the Internation Assembly of Privacy Commissioners and Data Protection Authorities.

Privacy by design

Privacy by design has been established to systems engineering from Ann Cavoukian, which is the former Information and Privacy Commissioner for the Canadian province of Ontario. In 2010 the Internation Assembly of Privacy Commissioners and Data Protection Authorities recognize the concept of privacy by design as an essential component of fundamental rights and is a core part of the European Union GDPR.

Privacy by design has seven foundational principles, which are the below:

- Proactive not Reactive, preventative not remedial is the first approach of Privacy by Design and is the process that anticipates and prevents privacy-invasive events before they happen. Privacy by design should act proactively and be applied to information technologies, organizational practices, physical design, or networked information ecosystems and certainly, it begins with a recognition of the value and benefits of proactively adopting strong privacy practices early and consistently.
- Privacy as the Default Setting
  Protecting personal data should be an automatic default rule for any IT system of business practice by applying several standards during design. First of all, it is necessary to define the purpose of the specification, which means that must be recorded which personal information is collected, used, retained, and

disclosed shall be communicated to the individual at or before the time the information is collected. All purposes should be clear, limited, and relevant to the circumstances. Additionally, all the information that they are collected should be minimal and most of the time the collection of personal information must be fair, lawful, and limited to that which is necessary for the specified purposes. Moreover, use, retention, and disclosure limitation should be limited. Last but not least, in cases that where the need or use of personal information is not clear, there shall be a presumption of privacy and the precautionary principle shall apply: the default settings shall be the most privacy protective.

- Privacy Embedded into Design means that privacy by design should not be an add-on but an embedded system during the design and architecture of IT systems. Moreover, wherever is possible, detailed privacy impact and risk assessments should be carried out and published documenting the privacy risks and all measures taken to mitigate those risks, including consideration of alternatives and the selection of metrics. As importantly, the privacy impacts of the resulting technology, operation, or information architecture, and their uses, should be demonstrably minimized, and not easily degraded through use, misconfiguration, or error.
- Full Functionality – Positive-Sum, not Zero-Sum. However, privacy is such an important principle, when embedded into a given technology, process, or system, it should be done in such a way that full functionality is not impaired, and to the greatest extent possible, that all requirements are optimized. In other terms, systems after privacy rules should be fully functional and multi-functionality, for that reason all interests and objectives must be documented, the desired function, articulated, metrics agreed upon and applied, and trade-offs reject as ofter being unnecessary, in favor of finding a solution.
- End-to-End Security – Full Lifecycle Protection. End-to-End Security ensures that strong security measures are applied from the start to finish and that all data are securely retained as well as securely they will destroy at the end of the process. Although security and privacy are different meanings, without strong security, there can be no privacy, as a consequence, security standards should be applied to assure confidentiality, integrity, and availability of personal data.

- Visibility and Transparency – Keep it Open. Parts and operations of privacy by design should remain visible and transparent to both users and providers alike. For auditing purposes, three different practices are important:
    - Accountability means that the collection of personal information entails a duty of care for its protection. All privacy-related policies and procedures should be documented and communicated as appropriate and when personal information transferring to third parties they should be protected through contractual or other means
    - Openness when combine with transparency is the key to accountability. All information regarding the policies and practices relating to the management of personal information shall be made readily available to individuals.
    - Compliance is important for the protection of personal data. To succeed that, a redress mechanism should be established, and information communicated about them to individuals, including how to access the next level of appeal. It is necessary to create steps to monitor, evaluate, and verify compliance with privacy policies and procedures that should be taken.
- Respect for User Privacy – Keep it User-Centric. Research shows that the best Privacy by Design result are those that they take into account the interests and needs of individuals users. The purpose of this specific aspect is to respect user's privacy is particularly extends for human-machine interfaces to be human-centered, user-centric, and user-friendly so that informed privacy decisions may be reliably exercised by following the below:
    - Consent, this consent is indispensable for the collection, use, or disclosure of personal information. Consent should be clear and protect sensitive data and it can be canceled at any time if this is a user's aspiration.
    - Accuracy, all personal information should be accurate and up-to-date
    - Access, all users should have access to their personal information and they should be able to dispute the accuracy and completeness of the information.

- Compliance, all organizations that manage personal information should establish a compliant mechanism that should be published to all individuals. This mechanism requires also to include steps on how to individuals have access to the next level of appeal.

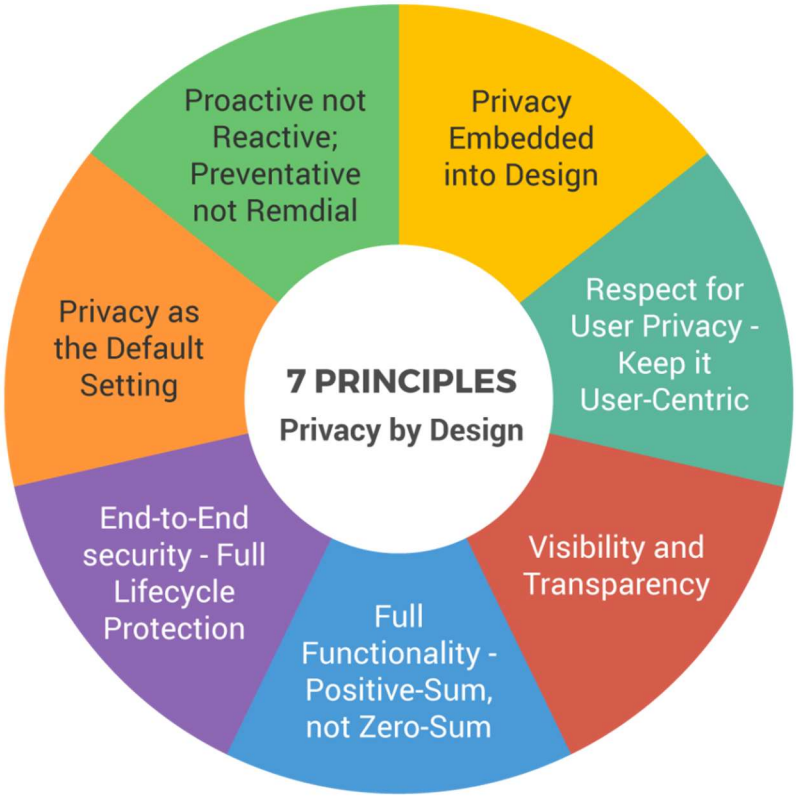

Image 7: 7 Principles Privacy by Design

Privacy issues

Privacy by design can be a solution to many threats because it can give the ability to engineers to design correctly from scratch and most of the time to predict as many privacy issues as possible. However, many other privacy issues arise some of them are not possible to prognosticate because they are based on humans.

Human behaviour is one of the biggest paradoxes in privacy and a lot of interesting research has been done. Studies show that however people are express concerns about their privacy, there is a lack of appropriate secure behaviour, for example, password “1234” is one of the most common combinations that people are using, or even worst a part of the population is using the same credentials for different accounts. Research of Pew Research Center (PEW) demonstrates that people despite the fact they do not feel comfortable or secure on social media, such as Facebook or Twitter, keep posting news or updates about their lives without concern them who is going to watch or edit those data, which constitute another enigma on about human behaviour.

From all the above, we do understand that people’s behaviour cannot predict, their reactions cannot be designed based on specific rules because every human being acts differently. However, many other threats such as attacks, arise from the rapid technology of IoT in people’s daily lives and as has already been said, data is one of the major things that have to be protected, because they are generating, processing, analyzing, sharing, and storing a huge volume of sensitive private information. This raises several concerns and challenges about the security and privacy of data and how to protect them against unauthorized parties during different steps.

Cyberattacks

In the world of cybersecurity, an attack is any attempt that happens from someone that desires to expose, alter, disable, steal, or even gain unauthorized access. This type of attack is called a cyberattack and the target of the assaulter are computer information systems, infrastructures computer networks, personal computers, or other devices that they connect to the network. Most of the time, an attacker can be a person or a group of people, that attempts to access data on restricted areas without authorization, potentially with malicious intent. Cyberattacks can also be used by sovereign countries, individuals, groups, society or organizations that’s why they have become increasingly sophisticated and dangerous in the last years.

We can measure a cyberattack by calculating three different factors, the fear factor which is the worry that a state or an individual has against the possibility to happen a

cyberattack, the factor of spectacularity, which is a way to measure the actual damage that an attacker achieved and last but not least the factor of vulnerability which can describe how vulnerable on the organization or a government is to cyberattacks.

Before we can fully analyze the types of attacks, for better understanding we will determine why cyberattacks happening, how is this possible, and the profile of who is behind a cyberattack.

A bug is a state when something unpredictable despite careful planning and execution, happened. Software and firmware have several bugs and often attackers exploit this weakness in applications, operating systems, application services, and networks. In order to be able to more easily manage bugs, we have separated them into two categories, the first one is the unexpected input and the second the unexpected combination. The unexpected inputs can happen by human error, and more specific if a programmer does not pay enough attention while coding and sets wrong input when a user enters a value that does not match can occur buffer overflow, which is a common attack that exploits inputs bugs. The unexcepted combinations are when the attackers send inputs to one of the multiple layers of a database (application, database, and operating system) but this input has another meaning to a different layer. This type of attack is called SQL injection, and it is also a rare method that can exploit unexpected combination bugs. The high demand for new technologies sometimes does not allow the system administrators to create a secure computing environment in cyberspace, because they should work fast to deliver all the amount of work, which means that there are several times where they skip the proper security checks and preparations. The default configuration in IoT devices and systems is one of the major mistakes that happened and when an attacker notices this type of weakness can have easy access due to the weak with no complexity password and network settings. Of course, there are other cases, when the system administrators forget to disable services that they were running for testing purposes.

However, due to automatic checks on devices and systems, codes of software applications can be perfect, and correctly working, but they still can be vulnerable as a result of TCP/IP protocols, which have been developed to support efficient communications between friendly parties. For example, the protocol of WEP (Wired Equivalent Privacy) even though it is recommended to not use it anymore, it constitutes another example of a design flaw that used CRC32 for integrity checking. The issues that appear on protocols are a result of misunderstanding some cryptographic methods.

The changes in cyber security are rapid, so every time we ask ourselves “How does an attacker gain access?” the answer could be different, and sometimes it is not easy to find a response. However, we can reply to the answer “What?” what is the reason behind every cyber attack? In most cases, there are three perspectives, motive, means, and opportunity. Motivation for an attacker can be hate, cyberpunks, cyberterrorism, or the theft of personal data, sensitive information, or credit cards. Also, terrorist and transnational criminals are aware of and using information exploitation tools such as computer viruses, worms, Trojan horses, logic bombs, and sniffers that can destroy intercept, degrade the integrity of, or deny access to data. Moreover, the available sources that exist nowadays on the internet, like a video that shown how to hack a wireless network, or IoT devices such as thermostat sensors, increase the curiosity of people that maybe have already a knowledge background regarding hacking. Currently, it is easier than ever for someone to start hacking even as a hobby because as we already know, not all hackers have the same intentions.

Also, only in the last year (2020), the number of vulnerabilities that have been recorded was 18.335 of which 4.380 were high severity, the largest number of high severity vulnerabilities recorded in any year tracked. Vulnerability of medium severity was 11,194 and low severity 2,761, as we can see on the below graphic. This means that currently there are abundant vulnerabilities. Each and every vulnerability represents a weakness in a product or in a system that an attacker can exploit in some way to achieve the objective of compromising a system.

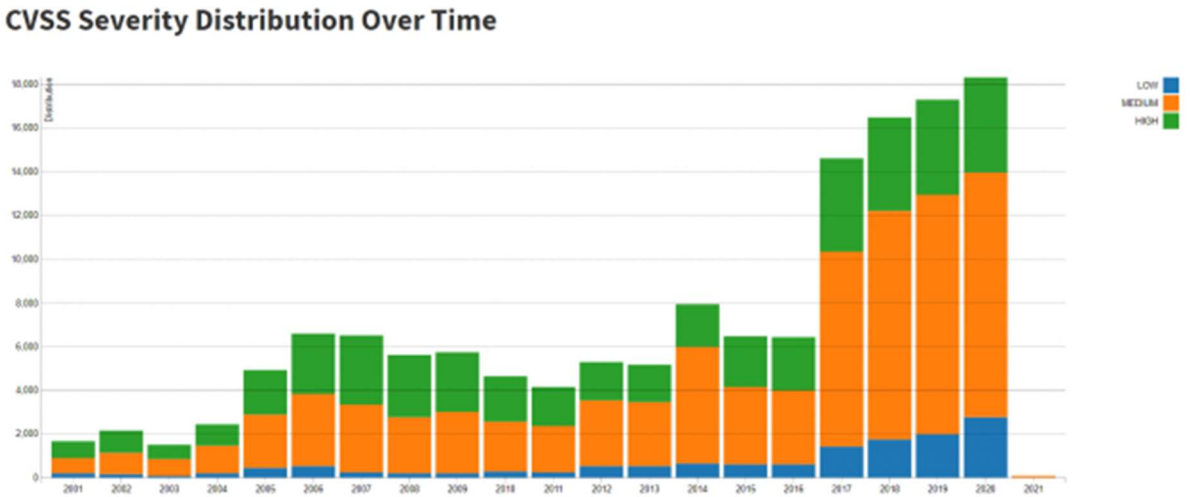

Image 8: Severity Distribution Over Time

Last but not least, we are going to analyze the profile of an attacker. As we have already mentioned above, a cyber attacker can be someone who starts hacking as a hobby or for fun and is not intended to harm or damage any software or hardware. On the other hand, there are malicious hackers (we can also call them dark hat hackers) who like to gain unauthorized access to cause damage. Malicious hackers can be categorized into insiders and outsiders. Insiders can be users that already have access to a system or a network and they use their internal system privileges to gain access to unauthorized information. These types of hackers have as an act of purpose revenge, financial or another personal gain.

On the other hand, outsiders come from the outside world, which is the Internet, and more specifically the wireless networks, dial-up lines, physical break-ins, or a partner network linked to the enterprise network, such as a vendor or a customer. There are several types of outside attackers but on the psychology of computer crime, we can notice seven different types, which are: the novice, usually young people with limited skills who tend to use pre-written software or exiting tools, the cyberpunk, mostly young people with some technical skills and programming capabilities, the petty thief, which can be described as the traditional thief who learns how to hack to expand their field of a target, the old guard, are highly skilled individuals who can write their one code and scripts, the virus writer, which are similar to the old guard attackers, they can write their code but they're usually motivated more by revenge or curiosity than notoriety, the professional criminal, which have sophisticated skills, and they are highly trained technical experts and last but not least, the information warrior, often motivated by patriotism and they use their advanced knowledge and skills to disrupt the command and control rival nations.

After we examine and analyze the means, the reasons, and who is behind attacks, we can move to the type of attacks, which also are separated.

Types of attacks

We can separate attacks into two big categories, active and passive attacks. In the first case, an active attack tries to modify resources or to affect by damaging operations of the systems. On the other hand, a passive attack does not affect the system's resources but attempts to learn or make use of information from the systems. Either the attacks are active or passive, we can distinguish them if they happened from the inside or from outside. An inside

attack is the one initiated by an entity inside the security perimeter, an individual who has been already authorized to access system resources, i.e. an employee of a company who is working by using resources of the group, and an outside attack is launched by someone from outside the secure perimeter, which is not authorized. The target, which is called threat can be either be for violation of security and it can be an action or an event that could breach security and cause harm. Below we can see a taxonomy of security attacks, which target they have, the weaknesses that they appear, and the techniques that are used in order to be implemented.

Attack	Target	Weakness	Technique
Denial of Service (DoS) attacks	IoT devices that connected via the Internet	1. Reduction in network's capacity 2. Disable the network	IP enables status contributes to pool things. The distributed attack utilized and auto shut the IoT system.
Wormholes	Locations of the packets	Problematic in checking the routing information	Record the packets at one location then tunnel them to a different location
Spoofed, alter, or replayed routing information	1. Routing information 2. Detectable of IoT devices	1. High end to end latency 2. Routes sources might be extended or shorten	First, the spoofer only listens. Only act when the transmitter stops sending a signal, then an unreliable signal sends.
Sybil	The integrity of data security and resource utilization	1. Launch threat to the geographic routing protocol 2. Costly network	Propagate malware to a website. The adversary is masquerading the normal users.

Table 2: Taxonomy of security attacks

Other than the above, in recent years, we have found many different attack application scenarios, such as the Mirai botnet. Mirai is a Japanese word which is means "future", practically is malware, it was found in August 2016, and we can categorize it on white hat types. This type of malware can convert into remotely controlled bots the network devices that they are running Linux. Those devices can be used as a part of a botnet in large-scale

network attacks. Most of the time, the targets are devices such as IP cameras or home routers, IoT devices that are often designed with poor security or even at none at all. One of the most famous DDoS attacks with Mirai malware took place on the 20th of September on computer security journalist Brian Kerbs' website.

Another great example is the driverless cars in smart cities. Those type of cars has been designed from high-tech companies, aiming to reduce traffic accidents and build a cleaner and smarter society. However, the autonomous vehicles are one of the most major security issues, because if it is hacked, both life safety and data privacy will be threatened. If any security bug is exploited by hackers, they can take the remote control of the vehicle, applying the brakes, shutting down the engine, or controlling the steering. Apart from this dangerous behaviour, the computer system of a self-driving vehicle can cause significant privacy issues.

Furthermore, similar to autonomous vehicles is the technology of virtual reality which is used very frequently by many organizations and entities for city planning departments, healthcare service providers and the engineering industry sector. According to our understanding, any sensitive information that is shared with third parties, such as data that have been stored by sensors. Another drawback in this situation is that VR devices and applications are rushed to market, so designers and users have not made appropriate and comprehensive privacy considerations.

Finally, yet important are the AI systems in smart cities, that they are playing an indispensable role in many applications, such as automatic control of trading systems, home appliances, etc. AI systems have been designed to use personal data and extract sensitive information in order to provide services to customers. This can be a target for hackers because they can understand more easily how this technology works, what type of protection they are trained or designed, and this will allow them to adopt targeted approaches to weaken the training effects and to reduce the reliability of the algorithms.

IoT protocols related to security

As we have mentioned above, IoT covers a vast range of application products and the number of protocols that are adding to IoT are keep on increasing. Protocols used for high level are assigned to certain vendors which provide room for the selection of different

capabilities and features. In the below table, we can examine some certain IoT protocols that are used for the feature of security.

Protocol	Transport	Messaging	2G,3G,5G	LPL *	Compute Resources	Security	Success Storied	Arch
Azure-IoT	AMPQ or HTTPS/TCP	Rqst/Rsonse	Excellent	Good	10K-100Ks RAM Flash	High-Mandatory	Wearables	Client-Server
CoAP	UDP	Rqst/Rsonse	Excellent	Excellent	10Ks/RAM Flash	Medium Optional	Utility field area	Tree
Continua HDP	UDP	Pub/Subsrb Rqst/Rsonse	Fair	Fair	10Ks/RAM Flash	None	Medical	Star
DDS	UDP	Pub/Subsrb Rqst/Rsonse	Fair	Poor	10Ks/RAM Flash++	Hig-Optional	Military	Bus
DPWS	TCP		Good	Fair	10Ks/RAM Flash++	Loew-Optional	Web Servers	Client-Server
HTTP/REST	TCP	Rqst/Rsonse	Excellent	Fair	10Ks/RAM Flash	Medium Optional	Smart Energy	Client-Server
MQTT & MQTT-SN/S	TCP	Pub/Subsrb Rqst/Rsonse	Excellent	Good	10Ks/RAM Flash	High Optiona	IoT messaging	Tree
SNMP	UDP	Rqst/Rsonse	Excellent	Fair	10Ks/RAM Flash	High-Optional	Network monitoring	Client-Server
Thread	UDP	Rqst/Rsonse	Excellent	Excellent	10Ks/RAM Flash	High-Mandatory	Nest	Mesh
UPnP	UDP	Pub/Subsrb Rqst/Rsonse	Excellent	Good	10Ks/RAM Flash	None	Consumer	P2P Client Server
XMPP	TCP	Pub/Subsrb Rqst/Rsonse	Excellent	Fair	10Ks/RAM Flash	High-Mandatoty	Rmt Management	Client-Server
ZeroMQ	UDP	Pub/Subsrb Rqst/Rsonse	Fair	Fair	10Ks/RAM Flash	High-Optional	CERN	P2P
*Low Power and LossyFair								

Table 3: IoT protocols related to security

Chapter 4: Challenges

Taxonomy of Challenges

There are different challenges that the designers have to face when they deployed smart city applications. Below we can see a taxonomy of those challenges.

One of the most major challenges is the combination of security and privacy because it deals with services related to operations of the city's services. Those services, in case that they are not working properly it could bring inconvenience to citizens and in some cases to put human lives and properties at risk. Moreover, IoT devices can collect data without the approval of citizens for advertising purposes. As we understand, to be able to build a relationship of reputation, the trust of citizens in the new changes that are made is necessary, but on the other hand, the applicable solutions will require processes that anonymize data collections while retaining the integrity of the context of the measuring task.

Another basic issue is the smart sensors, which are the main hardware of a smart city. The main role of those devices is responsible to collect and exchange data and perform the scheduling of tasks. However, according to our understandings, there are several manufacturers how to create and design devices, so there is a big amount of different protocols that they follow. To overcome this diversity, manufacturers can develop a standard method or protocols and develop their products compatible with this way. Needless to say, smart sensors should provide robustness and reliability independently who manufacturers design them because they establish the backbone of future smart cities. Also, the smart sensor should work smoothly and continuously, which means that they have to be connected to the network infrastructure and always have access to power or battery. They are also responsible to measure, to transfer and sometimes collecting data. In case that we have a system that stores the measured data on smart sensors, we should predict how we can store a large amount of data, how we can compress those data, and last but not least, which database schemes are going to be developed.

For all of this to work, it is necessary to be connected to the network. This can be an easy process, but it depends on the capability of connected devices. The fast growth of smart cities requires that all smart devices should always remain connected. However, this is not

always possible, and in order to overcome this issue is a good design of the local network and many access points, that they provide a continuous network on those devices.

Finally, yet important, an upcoming issue is going to be the big amount of data that the IoT devices produce. Those data should execute specific services continuously and deliver particular data analytics that ensures the proper operation of a smart city.

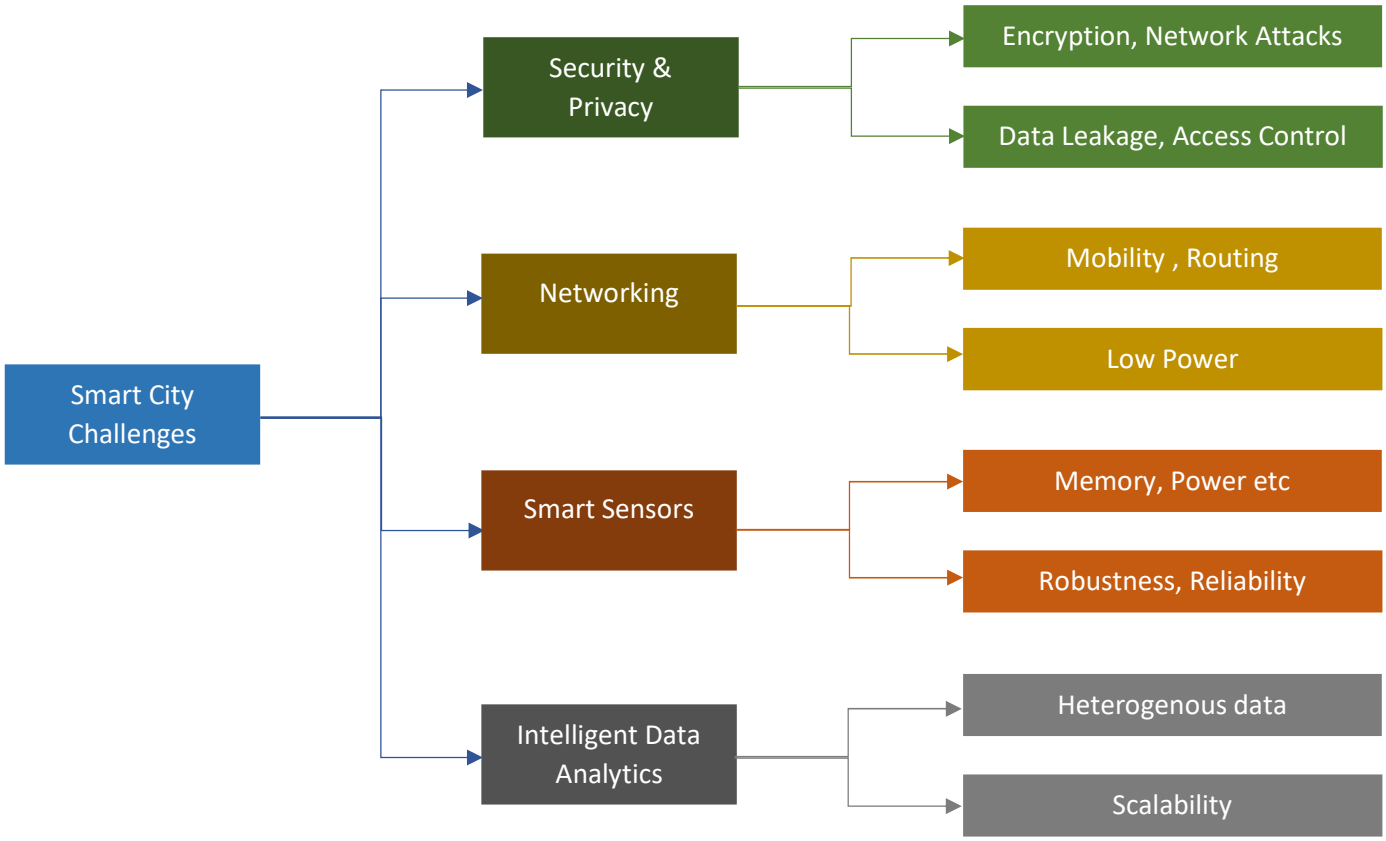

Image 9: Smart City Challenges

Challenge of Mashup Data

Smartphones are an integral part that serves citizens to control smart objects and IoT devices of the cities that they are living in. They are also one of the core components of IoT infrastructure in a smart city as they give access to various services and applications.

However, smartphones and other individual objects can be a big threat and pose a risk to the security of smart cities because is a rare target of vulnerabilities. When a hacker gain access to a smart network, can collect information about the security posture of the means that they are operating in the smart city, or can upload malicious smart applications into an unsuspecting user's phone to infect the device, in other words, this phone will have been hacked. So, even if there is a secure connection between all the smartphones and the network, a hacked smartphone could use this secure connection for malicious purposes. Those purposes could be several vulnerabilities that could compromise smart city security, such as malicious applications, hacks on Wi-Fi or Bluetooth, threats from social networks, botnets, locations, and GPS, or attacks on multiple smartphones that will launch simultaneous attacks on the network. Even worse, there are attacks that they can listen to a user's conversation, elicit their sensitive data like their address, steal personal's bank account credentials, and other acts that violate people's security.

Furthermore, the way to control objects into a smart city through a smartphone is called Machine to Machine (M2M) communication. M2M is direct communication between devices which is using any communication type to control wired or wireless objects, like sensors. However, M2M communication can pose risks to smart cities because of several types of attacks, like physical attacks which can be executed through configuration attacks utilizing malicious software to commit fraud by manipulating the integrity of existingM2M software. Other types of attacks on M2M communication can be on authentication tokens, protocols, or threats on network security that can cause a breach in privacy. For example, attacks on the network can be any Denial-of-Service (DoS) between smart devices, or protocol attacks most of the time occurred again against devices, such as man-in-the-middle. All of these types of attacks and many more can give access to unauthorized people that they want to damage a smart city.

However, there are also other challenges that smart cities have to face, like the vulnerabilities of radio frequency identification tags (RFID). RFID uses electromagnetic

fields to automatically identify, and track tags attached to objects. An RFID system consists of a tiny radio transponder, a radio receiver, and a transmitter. When triggered by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag transmits digital data, usually an identifying inventory number, back to the reader. This number can be used to track inventory goods. In smart cities, RFID can be used in a smart environment, smart industry, and smart mobility because it is very useful in real-time information visibility and traceability, however, RFID technology is prone to attacks and threats. An attack on RFID can give to an attacker unauthorized access to sensitive information, a fact that undermines data confidentiality and privacy. Attackers that have access to RFID readers or access to the Electronic Product Code (EPD), which is produced from RFID readers can intercept an RFID tag. Other ways to corrupt RFID tag is by tag killing, tag cloning, signal interference jamming, denial of service attacks and eavesdropping. In all the above, if there is an attack, the attacker can disrupt the frequency and guide the message away from the receiver.

In conclusion, there are several types of attacks that smart cities have to face. Security teams can predict some of them, but it is impossible to foretell all of them. New technologies always are going to bring new challenges to security and privacy, so engineers must pay attention to attacks that have the intention or ability to disrupt the entire smart city network. In other words, smart city applications should always be up and running, independently of the type of vulnerabilities or the security efforts.

Data Management and protection

As already mentioned, one of the three characteristics of a smart city, is Big Data, which makes a city smart, efficient, and convenient. Data are the sources of IoT, and smart city systems implement daily tasks in order to produce, collect, transmit, and mining them. Smart cities are composed of private cloud services which control critical services and infrastructure and manage the private data of the citizens. So, because the risk of cyber-attacks becomes much more dangerous and since privacy protection and security are paramount for the viability of a smart city, vendors that they manage the private cloud services should follow enhancing procedure to protect the data. Therefore, companies should try to find methods for privacy and security breaches and limiting the amount of risk but also

remain financially viable. This will guide the companies to uphold security and privacy goals but at the same time, companies should find balance and not fear the repercussions so much, that they are disincentivized from providing cloud services. Moreover, organizations that offer their services in smart cities, should take initiative and ensure their compliance with laws before a regulatory authority has to step in. Consulting services, that are related to the law firm would help heighten data security and ensure that they are following data laws.

Moreover, companies and organizations should try to win public trust, and in order to achieve that, they could follow transparent business practices when dealing with personal data. So, smart citizens could easily inform how their data was being utilized, how long they are stored, and when they are used. Also, organizations should inform the individuals regarding the second phase of their personal data. It is commonly known that data will be collected and utilized in smart city, and it is obvious that if individuals consent to provide their personal information for a specific purpose, then it's ethical for the provider to accept those data. However, there are situations that the personal data is utilized in a secondary manner, which does not directly benefit the data provide and is not ethical clearly. It is commonly known that we as individuals, offer our personal data to organizations with the purpose to raise the standard of living. Therefore, it is unclear whether privacy would be violated if smart city organizations monetized the personal data they collect. It is commonly known that companies already monetize the personal data they collect, and in many cases in services that they are not unavoidable aspects of daily life. A similar example is smart cities if they are managed by private companies and they decide to perform a fundamental task, it would become an unavoidable presence and the inhabitants would have no choice but to submit to it. Thus, monetization of personal data should be thoroughly examined if it is undertaken by a fundamental organization in a smart city.

A well-known fact is that changes to smart cities will affect the total amount of people, in other words, potential privacy and security challenges, could be the data that come from consenting individuals negatively affect nonconsenting individuals. For example, if smart cities are managing the data that they are receiving in the way that companies are managing the data that they already have from customers, they are going to have the ability to analyzing their locations, buying patterns, and personal information. Although this practice already occurs daily on the marketplace of the internet, if this happens in a smart city it would be an inescapable part of life that could artificially produce different experiences within the

smart city. This practice could be further complicated if the individuals consensually providing their data are compensated for doing so and essentially profiting from the detriment of others.

In the complexity of smart cities, we should add the influence that social media have and how important a role they have in human interactions. In the near future, social media will most likely be used to facilitate social interactions within the smart city. However, concerns inevitably arise about privacy, if social media accounts are used to verify or interact within certain smart city services. The question that arises, is if the government organizations should have access to inhabitants' social media profiles for a more socially integrated city experience or this method starts to be considered as domestic spying?

Moreover, we already know that social media accounts yield a wealth of information about a user, such as the date of births, phone number, emails, locations, data that would give an organization within a smart city a breadth of information. However, if social media integration is an unavoidable step to participating in smart city services, will occur many issues for privacy. It is commonly known that social media have issues with security and privacy methods, they are far from perfect when it comes to verifying identities in a secured network. A solution to this issue could be the use of biometrics as identify method, however, we already know that facial and body characteristics are the most personal information that we have, and in case of hacking those data will leak. In conclusion, securing the smart city through such effective means will be elusive without proper implementation.

Another major challenge is preserving citizen's trust, which is so important to sustaining the smart city. Organizations that will undertake to implement solutions in smart cities, should work to establish computational trust with the users that will interact with the smart network. The meaning of computation trust is that the trust levels surrounding interactions in information technology are crucial to facilitate interactions and cooperation through digital mediums. This is a type of motivation for organizations to abide by the laws of the smart city. Moreover, the technological organization could develop computation trust and reputation models in order to secure user confidence in the smart network. Also, rating systems could be implemented, so they will help users to treat each other with respect by holding individuals' reputations accountable for their actions. Furthermore, every time a new organization gains access to personal information a record system will be enabled and will register every move that new authority is doing. Also, it would be very handy, if a novel

software creates an environment within which data analysis can occur without allowing the organization to extract said data would allow smart cities to facilitate what organizations have access to the sensitive data.

As mentioned above, transparency will be important for fostering trust and confidence in the smart network. Users through data timelines and clear parameters for data privacy and security will have the opportunity to understand how their data is used and also this method will incentivize organizations to better serve their customers. For example, citizens of a smart city, state, or county could decide with democratic means, the frequency with which individuals providing data need to indicate that they consent to their data being used for secondary purposes.

As mentioned in the first chapter, the education of individuals is important, because they will understand how significant their personal data are. With the combination of knowledge and an application, that is will be a sliding scale of consent, the user can customize the amount of data they wish to provide the company or a specification of what their data can be used for. In addition, organizations should create some type of rewards for the users that are submitting personal data when that data is used secondarily. For example, subscribers to a ride-sharing service could be offered a percent discount if they allow the service provider to use their personal information securely for business intelligence purposes. This way organizations receive consent and users feel compensated for the extraction of their personal information.

We can conclude that, on the one hand, there are several challenges in smart cities, but on the other hand, there are also many solutions in order to overcome those issues and create secure, safe, and sustainable cities for everyone who lives in. Ultimately, decisions having to do with the whole of people should be determined clearly and democratically. Last but not least, organizations should enhance individuals to overcome ethical concerns about their privacy and trying to develop systems that will aim to develop secure cities and not exploit for their own profit people’s sensitive information.

Chapter 5: Solutions

Understanding of privacy

To provide proper privacy in the smart city environment, the level of privacy should be quantified and mapped by engineers and researchers to help them to design and evolve in terms of privacy protection. Regardless of technological means, people should understand the significance of privacy and how import is to respect it. As we had already described, there are seven principles of privacy by design, and apart from those, there are also seven types of privacy. Those types have been well defined by Finn R.L. and are the privacy of the person, privacy of behavior and habits, privacy of communication, i.e. messages, phones calls, emails, etc., the privacy of data and image refers to the need for the individual to have complete control over any of their personal information that has been collected, the privacy of thoughts and feelings refers to separate opinions, the privacy of location and space refers to need of not be identified as they moving and last but not least privacy of association which refers to the protection of a person, a group and community associations.

All the above areas can be exposed in smart city activities, such as technologies that they impose on physical privacy could be fitness trackers that measure heart rates and biometric authentication methods. Another example is the use of social media, which can easily uncover the privacy of association. For a smart city to be secure, privacy should be understanding as to the preservation of the information that is collected, processed, and disseminated that relates to an individual's person, behavior, habits, communication, location, associations, or feelings.

Security Requirements of Smart Cities

As we have already understood that most of the time it is difficult to protect smart cities due to the complex environment, new technologies, and new threats that appear every day. However, there are four requirements that they can fit in any smart city model, and they are applicable on different layers of a smart system. The below requirements have technical characteristics, and they offer solutions that have positive effects. However, governance

meanings, education of smart citizens, and updated policies should also be implemented in order to achieve the protection of the smart systems to the fullest.

Privacy and security are two different meanings that they have a similar concept and the one can overlap the other when it is necessary, in cases of smart cities, we should secure smart systems in order to protect the privacy of smart citizens. Threats such as packet interception, malware in mobile devices and applications, hacking on servers, data leakage are the main cause of privacy breaches. To avoids misuse by unauthorized people, adequate and effective countermeasures, such as encryption methods and anonymous mechanisms, and some techniques, such as differential privacy, should be applied. Although that the systems are secure, the privacy of citizens sometimes can be breached. One potential way for this to occur is the powerful data mining algorithms. With these mining tools, some services providers and third parties can easily discover consumers' personal information. It is also worthwhile to note that the adoption of only one technical solution is not enough and sufficient, although it has some positive effects. Other means of protection, such as governance, education, and policies, should also be implemented.

A smart system can be seen as secure only if it has the ability to monitor its operation conditions and detect any abnormal events in a timely manner. In other means, according to the statistics of the vulnerability of the devices and networks that have been deployed on a smart city, the traditional intrusion detection system is widely sued in three approaches which are misuse detection, anomaly detection, and specification-based detection. However, in the heterogeneous and complex smart city ecosystem, the simple adaptation of a global intrusion detection system solution is not flexible and is not realistic. One of the reasons is the way that the sensors have been created, most of the time are resource-constrained, so it is necessary for a lightweight intrusion detection method to be developed. Of course, prediction and knowing about incoming threats in advance is better than detection and recovery after an attack. After research, it has been found that many intrusion prediction systems failed to detect and prevent attacks, with a high failure rate, especially for web-based applications. Similarly, smart grids indicated that many harmful attacks are caught too late to take measured after detecting and the current security protection strategies are unable to provide sufficient protections for a smart grid. Therefore, it is necessary to develop intelligent intrusion prediction systems to achieve security situation awareness and to automatically predict various attacks on smart applications.

As we have mentioned in the above chapters, smart systems of applications should have the ability to maintain effective functioning even when under attack, because availability means that those devices and services should be available when needed. Smart devices are susceptible to attacks, so they have to be able to detect any abnormal conditions and have the ability to stop further damage to the system. Resilience is regarded as the attack-resistance ability of a system that can tolerate various faults and failures caused by attacks and large-scale disasters. Protection mechanisms should have strong robustness and the ability to continue learning adaptively to cope with the increasingly intelligent attacks. Furthermore, integrity is such important as availability, so it is crucial to ensure the integrity of both IoT devices and the data exchanged between devices and the cloud. Data are exchanged across many devices in an overall smart application, the data are easily tampered with during the transmission process if they are not well protected. Firewalls and protocols and manage data traffic in IoT communications, but they cannot guarantee the integrity at endpoints because of the low computational power of most IoT devices.

One of the most basic requirements is authentication, it is used in all different layers of a smart system and is needed to prove identities and ensure that only authorized people can access services across the system. IoT devices have been developed in a way that they can authenticate the network, nodes, and messages from management stations. The challenge is to develop advanced technologies that guarantee real-time authentication independently of the growing data of smart cities. Apart from authentication, confidentiality is important, because it is to prevent information from passive attacks or being exposed to the wrong source. To protect the confidentiality of information transmission between nodes should be applied encryption-based technologies that they can build reliable communication and storage systems. However, the design of identification and authentication is difficult due to transparency and reliability.

In other words, four different security requirements should exist in every smart city, and even in smart devices to protect the privacy of the users. However, for some of them, it is difficult to deploy them due to the complex design of the devices. For that reason, when all the above are not enough, numerous enhancing technologies can be used for a secure smart IoT environment.

Enhancing Technologies

As written in the above chapters, to build a smart city we have to invest in research for secure and good design. Nevertheless, it is also important to apply two important techniques, anonymization and security techniques.

The first one is when data are changing in that way so there is no connection between the anonymized and the original data and therefore there is not a link between the human being and the data, in other words, anonymization offers masking and perturbation of sensitive data. We can also describe anonymization as the method where sensitive information is been removing or hiding or replacing the actual data with noisy or otherwise altered data and encryption is reversibly disguising sensitive or confidential information. The security techniques are the second method, which includes the triad of the protected system, which are confidentiality, integrity, and availability, and techniques can be public-key encryption, symmetric encryption, and hashing. Therefore, to be able to apply the above techniques, we have to hierarchic a smart city into three categories of quality, the first one is the architectural layer, the second one is privacy methodology and the last one is the data type. To simplify the first category, which is the bigger one, we will separate it into other three categories, the sensor layer, the networking layer, and the application layer. Therefore, below we have cleared the below:

- Smart City Architectural Layer which includes:
    - Sensor Layer, which are devices that they collect data, such as IoT devices
    - Network Layer, which is the part of the architecture that is responsible to transfer data from the sensor layer
    - The Application Layer is presented as the final layer of the architecture because it is the application of the end-user.
- Privacy Methodology includes the below:
    - Anonymization, which is the technique of removing any sensitive attributes from receiving data. Technologies that use anonymization can also aid in protecting identifying information.

    - Perturbation is another technique that alters all the sensitive attributes while maintaining some statistical properties of the data set.
    - Encryption includes all the methods of symmetric and asymmetric encryption. Technologies that use encryption techniques can protect any data up to the strength of the encryption algorithm.
- Data type includes only two categories:
    - Numerical is the information that includes values such are height or weight
    - Categorial include information that they can be categorized, such as gender, postal code, etc.

Other than the above, which are the backbone of security in a smart city, there are also several technologies that we can implement, with the main purpose, on the one hand, the proper functioning of smart cities and, on the other, the protection of personal data and sensitive information of the citizens.

One of these methods is a substitution, which is the completely random replacement of identifying information in data and the final effect is incomprehensible results. So, in order to replace a name, for example, “Bob” they are using a random string with characters such as “AX05” and not another name, like “Peter”. In the case of Smart Cities, this could be very useful when data such as name, email, or addresses should be anonymized. Therefore, the method of substitution is an anonymization method that protects the data of the end-user. Another similar technology except for random replacement is the method of masking which is using very often in credit cards or phone numbers, this method reveals digits in specific positions, and last but not list in is the method of nulling out, also a form of substitution where all values of a particular attribute are removed.

The next one is the method of shuffling, which has the same purpose as the above, anonymization. Shuffling is the method of rearrangement of values and as a final result is not exist no link between the first attribute and the exported one. Shuffling can be implemented both on categorical and numeric information. On the other hand, sampling is another method in which from a set of data we select to release only partial data. The released data should be representative of the whole set. An important difference between shuffling and sampling is that the second one is not an anonymization technique that applies to the application layer

and the sensor layer for categorical and numerical data but it is a method that protects the identity of those who are excluded from the data set.

In cases of numerical data, we can use a perturbation technique which is the technique of variance, which distorts numerical data that is either correlated or uncorrelated to the distribution of numbers within all data. Other similar technologies with the variance method are synthetic data and differential privacy. Both of them have the purpose to change the final data in order to protect the end user from attackers who attempt to deduce an individual's private information by clever manipulation of a sequence of queries.

Another way to provide anonymization is to use the method of generalization, in which we decrease the granularity of some attribute in the data. This type of method can be used either on the sensor layer or the application layer. There are also some technologies similar to the generalization, which are called the "Top and Bottom Coding" and "Microaggregation". In the first case, the data that outline the threshold are more vulnerable and should be protected. In the second case, generalization is given by groups of data, if those groups are close to a specific value they should be protected.

One of the most famous methods of privacy is encryption. In simple terms, encryption is the method of hiding information in that way equal to the strength of the algorithm and cryptographic key used. Encryption is a technology that can be easily applied to many applications in a smart city, and it has many implementations that can protect privacy in many layers. All the technologies are based on encryption, and the most common are the below:

- Secret and Public Key Encryption: the secret key encryption uses the same key for encryption and decryption and the public key is using different keys.
- Biometric Encryption is one of the most interesting types of encryptions. The main distinction with other technologies is that the key encryption and decryption is generated using human inputs, like fingerprints, eye scans, facial structure, or any other feature that can be measured.
- Hashing is a method that replaces the original data with transformed data. A variable-length input can be accepted, and a fixed-length

output returned. Different from encryption, the transformation is completely deterministic and irreversible. This type of encryption can be used on the sensor and network layers in cases that messages required anonymity.

- Homomorphic Encryption is a method that uses a specifically designed cryptosystem that allows operations to hold the same effect on encrypted data as on unencrypted data. This method is very useful in cases with sensitive data because the data are never recorded unencrypted, such as applications in smart health, where a patient device may send periodic reports to a health provider and the second one wants to perform checks on this data without revealing sensitive information while still maintaining a level of service.

In this category, we can also add the encryption technique of mi networks, which provides anonymity of senders and receivers within a network. During the transmission of messages, information is revealed in the form of confirmation of the occurrence of that communication between parties. This method can be used in a health organization database, where the source or the destination of communication is preferred to be hidden or in many other applications because mixed networks can protect both categorical and numerical information in the network layer and also protect the identity of the participants in a way that the path cannot be traced back to the source. In cases that we want to provide anonymity to the sender and receiver during communication, we can also implement the technique of onion routing, with the only difference from the mixed networks is that the first one provides anonymous socket connections between a user and a server that can support different types of application data. The reason that this protocol having this name is because it adding layer upon layer of encryption for each hope.

Another famous technology of privacy is blockchain. Blockchain is a list of blocks that are linked together using cryptography, each block contains a cryptography hash of the previous block, a timestamp, and transaction data. An interesting thing about blockchains is that they are resistant to modification of their data because once recorded, the data in any given block cannot be altered. In the case of smart cities, blockchain can be used on some applications on IoT for automatic and

secure deployment. Also, like all the other technologies, blockchains offer security and anonymity in financial transactions.

Another interesting method, k-anonymity was introduced by Latanya Sweeney and Pierangela Samarati in a paper published in 1998 as a solution for the privacy of data. In this type of anonymization if the information for each person contained in the release data the k-anonymity, they cannot be distinguished from at least k – 1 individual whose information also appears in the release. Even if an attacker has some background knowledge, they will not be able to identify their target from among k – 1 other entry. Similar to this method, we can find the l-diversity and the t-closeness. The first one is an expansion of k-anonymity, but it is used in cases where the sensitive attribute does not vary within a group that has k-anonymized quasi-identifiers. l-diversity is responsible to improve the method of k-anonymity such that in a group of k-anonymized data there are l well-represented values. The second one is called t-closeness, which is also an expansion of k-anonymity improving on l-diversity, and it treats the values of an attribute distinctly by taking into account the distribution of data values for that attribute. This type of method preserves privacy in data sets by reducing the granularity of data representation.

In smart cities, we can also implement association rule protection or oblivious transfer. Both of them are useful and provide privacy and anonymity. The first one appears in open data initiatives, in cases that the released information might be vulnerable to data mining and machine learning algorithms to reveal private information, and there are two proposed solutions, the distortion and blocking. In the case of the second method, the oblivious transfer, a sender can deliver several messages at once, with one message being read by a receiver without the sender knowing which and without the receiver learning the other messages. This method can be used for location-based services, protecting the users that they want to discover a nearby point of interest without revealing their exact location, for example, if a smart city provides service for the nearest hospital. It can also be implemented at the application layer for categorical or numerical information on a smart city such as the method of Private Information Retrieval or PIR, which is a similar method to oblivious transfer, but it allows the transfer of a particular bit from a set of bits while preserving the secrecy of which bit has transferred. While PIR protecting simple

queries another method can provide privacy during the execution of online analytical processing, and it is called Private Data Warehouse Queries. This type of technology provides privacy during the execution of online analytical processing (OLAP) on a data warehouse. Typical data warehouse queries are usually generated by online analytical processing or data minim software components. Private data warehouse queries are categorized as an encryption technology that works at the application layer for both categorical and numerical data.

However, other than the above, there was a problem with transferring identifying or sensitive attributes during authentication. Those attributes can be usernames, email addresses, and passwords. This issue is solved with the Attribute-Based Credentials or ABC, which is a technique where an authenticating client can communicate only particular attributes that have been pre-authenticated, such as age, country of residence, or marital status. There are also some other additional benefits of ABC, such as unlikability, key binding, advanced issuance, pseudonyms, inspection, and revocation. ABC technology can be implemented in smart cards, for example, in a public library, where users can prove that they have an account without revealing any other information about themselves.

Zero-Knowledge Proof is a protocol that allows for participation in a system while providing a method of hiding any information beyond the fact that participation is allowed. This type of protocol can be implemented in smart city applications to provide authentication to the users to access a system without providing an actual key. One other different method is called Secure Multiparty Computation or SMP and has a purpose to compute a function over their inputs while keeping those inputs private. In smart cities can be used as an encryption method of securing application-layer services for numerical information.

Last but not least is the blind signature, which is a specific method for accomplishing the signing application shown above, in SMP. This method can be also used in smart cities in the application of e-Governance initiatives. Using this type of procedure, participants could deliver ballots or other feedback to the signing authority without the signing authority known any private information.

Chapter 6: Conclusion

After we have examined and analyzed all the above aspects regarding privacy in smart cities we can conclude that there are many ways that security can be breached but also there are many methods to be protected as smart citizens.

First of all, we should start accepting that changes in technology are necessary. Smart cities have come to make our lives easier, like offer us assets and services faster, encourage us to interact directly with issues concerning our cities, providing us education in any place from any device and for all ages, improving medical care, to protect our environment with finding ways to make sustainable ways for our buildings, and many more. Under no circumstances, the innovation of IoT would have a purpose to intercept personal data, spying on peoples' lives, and posing ethical dilemmas that can divide individuals if smart cities are worthwhile or not.

However, it is highly important for the influencers and the influenced to understand the meaning of privacy and why it is necessary for the principles of privacy to be implemented in technologies such as smart cities. Cyber security can also help in the development of smart cities. To make this possible, industries and manufacturers, and the designers of smart cities should corporate and take an advantage of the knowledge and the methods that already exist, and they can offer privacy and safety to their users. It is necessary to understand that privacy and smart cities can coexist.

As we have examined above, there are several invasions of privacy. Protecting is not always an easy way, first of all, requires educating, and a constant update regarding privacy issues. Nevertheless, there are methods that we can follow, without necessarily knowing, such as biometric security or two-factor authentication can provide privacy and protect the users at a satisfactory level. There are also multiple enhancing technologies based on cryptography and after they implement, they can offer more safety.

On the other hand, companies can invest in cyber security education in order to stay sustainable and gain people's trust. Nevertheless, as we have also examined, it is difficult to predict and detect attacks on the smart grid due to the complexity of the systems, so it is necessary to develop intelligent intrusion prediction systems to achieve security situation awareness and to automatically predict various attacks on smart applications.

In conclusion, if we want to answer the question “Are smart cities project worth it?” the response is yes. As long as people are informed about privacy, and clarity on the part of organizations, projects of a smart city can thrive. We have to realize that the knowledge we have about new technologies and privacy if combined in the right way, can improve our way of living.

Chapter 7: References

[1] A Critical Appreciation, by Mark Vallianatos, https://boomcaliforniablog.wordpress.com/2015/06/16/uncovering-the-early-history-of-big-data-and-the-smart-city-in-la/ Accessed 31 October 2020

[2] History of Smart Cities: Timeline, https://www.verdict.co.uk/smart-cities-timeline/ Accessed 31 November 2020

[3] What is Smart Energy? https://smartenergyusa.com/what-is-smart-energy/ Accessed 1 November 2020

[4] What is the Difference Between IoT and Cloud Computing? https://www.mckennaconsultants.com/what-is-the-difference-between-iot-and-cloud-computing/ Accessed 7 November 2020

[5] Smart Buildings: https://www.trueoccupancy.com/smart-building-guide Accessed 15 November 2020

[6] What's so 'smart' about smart governance?: https://www.allerin.com/blog/whats-so-smart-about-smart-governance Accessed 5 December 2020

[7] Privacy, Wikipedia, Wikimedia Foundation, 26 January 2021 [https://en.wikipedia.org/wiki/Privacy#Control_over_information] Accessed 10 December 2020

[8] Ann Cavoukian, Wikipedia, Wikimedia Foundation, 14 December 2020 [https://en.wikipedia.org/wiki/Ann_Cavoukian#Privacy_by_Design] Accessed 16 December 2020

[9] CAVOUKIAN, Ann. Privacy by design. *Take the challenge. Information and privacy commissioner of Ontario, Canada*, 2009. Accessed 17 December 2020

[10] 7 Principles Privacy by Design https://deviq.io/resources/articles/privacy-by-design/ Accessed 29 December 2020

[11] Van Zoonen, Liesbet. "Privacy concerns in smart cities." *Government Information Quarterly* 33.3 (2016): 472-480. Accessed 9 January 2021

[12] Cyberattack, Wikipedia, Wikimedia Foundation, 24 January 2021, [https://en.wikipedia.org/wiki/Cyberattack] Accessed 31 January 2021

[13] Nawir, Mukrimah, et al. "Internet of Things (IoT): Taxonomy of security attacks." *2016 3rd International Conference on Electronic Design (ICED)*. IEEE, 2016, Accessed 31 January 2021

[14] Cui, Lei, et al. "Security and privacy in smart cities: Challenges and opportunities." *IEEE Access* 6 (2018): 46134-46145., Accessed 7 February 2021

[15] Mirai, Wikipedia, Wikipedia Foundation 19 February 2021 [https://en.wikipedia.org/wiki/Mirai_(malware)] Accessed 28 February 2021

[16] BRAUN, Trevor, et al. Security and privacy challenges in smart cities. *Sustainable cities and society*, 2018, 39: 499-507. Accessed 21 March 2021

[17] CURZON, James; ALMEHMADI, Abdulaziz; EL-KHATIB, Khalil. A survey of privacy-enhancing technologies for smart cities. Pervasive and Mobile Computing, 2019, 55: 76-95. Accessed 21 March 2021

[18] Blockchain, Wikipedia, Wikipedia Foundation 03 May 2021 [https://en.wikipedia.org/wiki/Blockchain], Accessed 10 May 2021

[19] k-anonymity, Wikipedia, Wikipedia Foundation 25 December 2020 [https://en.wikipedia.org/wiki/K-anonymity], Accessed 15 May 2021

[20] t-closeness, Wikipedia, Wikipedia Foundation 11 July 2019 [https://en.wikipedia.org/wiki/T-closeness], Accessed 15 May 2021

[21] What is IP Telephony? https://www.nextiva.com/blog/what-is-ip-telephony.html

[22] Papa, Enrica, and Dirk Lauwers. "Smart mobility: Opportunity or threat to innovate places and cities." 20th international conference on urban planning and regional development in the information society (REAL CORP 2015). 2015. Accessed 20 May 2021

[23] ZHU, Zhi-Ting; YU, Ming-Hua; RIEZEBOS, Peter. A research framework of smart education. Smart learning environments, 2016, 3.1: 1-17., Accessed 20 May 2021

[24] AQEEL-UR-REHMAN, Sadiq Ur Rehman, et al. Security and privacy issues in IoT. International Journal of Communication Networks and Information Security (IJCNIS), 2016, 8.3: 147-157. Accessed 20 May 2021

[25] Explain the Relationship Between IoT, Big Data and Cloud Computing, [https://www.mckennaconsultants.com/relationship-between-iot-big-data-and-cloud-computing/] Accessed 28 May 2021

[26] LIU, Simon; CHENG, Bruce. Cyberattacks: Why, what, who, and how. IT professional, 2009, 11.3: 14-21. Access 28 May 2021.

[27] PIERONI, Alessandra, et al. Smarter city: smart energy grid based on blockchain technology. Int. J. Adv. Sci. Eng. Inf. Technol, 2018, 8.1: 298-306. Access 28 May 2021.

[28] Knud Lasse Lueth, Top 10 Applications in 2020, [https://iot-analytics.com/top-10-iot-applications-in-2020/], Access 30 May 2021

[29] Secure Multi-party computation, Wikipedia Foundation 07 July 2021 [https://en.wikipedia.org/wiki/Secure_multi-party_computation] Accessed 16 July 2021

[30] 2020's Record Numbers of Vulnerabilities [https://www.k2io.com/2020s-record-numbers-of-vulnerabilities/]. Accessed 21 July 2021

[31] SYED, Abbas Shah, et al. IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. Smart Cities, 2021, 4.2: 429-475., Access 20 July 2021