Cybersecurity and Privacy in Smart Cities for Citizen Welfare

Bernardo José Ribeiro Figueiredo[1], Rogério Luís de C. Costa[2],
Leonel Santos[3], and Carlos Rabadão[4]

[1]ESTG, Polytechnic of Leiria, Leiria, Portugal 2202295@my.ipleiria.pt
[2]CIIC, Polytechnic of Leiria, Leiria, Portugal rogerio.l.costa@ipleiria.pt
[3]CIIC, ESTG, Polytechnic of Leiria, Leiria, Portugal leonel.santos@ipleiria.pt
[4]CIIC, ESTG, Polytechnic of Leiria, Leiria, Portugal carlos.rabadao@ipleiria.pt

ABSTRACT

In smart cities, technologies and systems of various types, from manual sensors to data collection devices, cooperate to improve citizens' wellbeing. They take advantage of information technologies and the Internet of Things (IoT) to increase citizens' welfare, through the implementation of services with distinct objectives, like reducing energy consumption and improving transport routes and health services. Due to their functionalities and characteristics, IoT devices work interconnected and collect large amounts of data.

In this context, cybersecurity and privacy arise as topics of central interest, as security breaches can lead to personal data exposure and service interruptions and malfunctions, thus directly affecting citizens' welfare and the implementation of sustainable development goals.

This chapter discusses how cybersecurity risks affect smart cities' operations and citizens' welfare. It presents some current cybersecurity techniques and how to apply them in the smart cities' context. It also reviews some open issues and future directions.

Keywords— Privacy, Smart Cities, Cybersecurity, Welfare, Internet of Things (IoT), Security threats

1 INTRODUCTION

In recent years, the implementation of smart cities has attracted the interest of organizations from the most diverse areas, including government and academic institutions and even large industries. The transformation of a city into a smart city brings benefits to citizens and multiple entities. But it also requires new applications and services, which introduce new techniques and technologies that would have a direct role in revolutionizing the city.

In 2050, around 68% of the world's population would live in an urban environment (Nations, 2018), which would lead to a high excess of collected data and high resource utilization due to the immensity of existing services that there will be. On the other hand, climatic problems and over-population would change the population way of life, thus having the opposite effect that one intends with smart cities (Nations, 2018). To overcome such challenges, improving the well-being of the cities' population, city governments should adopt specific measures, like creating sustainable environments and applying intelligent systems. Currently, there are massive investments in the development of smart cities, e.g., there are more than 200 projects in progress only in China (Cui et al., 2018).

The deployment of intelligent services often occurs in a long-term project. For instance, consider the case of Rio de Janeiro, Brazil. Rio de Janeiro has approximately 6.5 million inhabitants and (partially or fully) hosted a series of relevant international events over ten years (between 2007 and 2016), including the 2007 Pan American Games, the Rio+20 United Nations Conference on Sustainable Development, the 2014 FIFA World Cup, and the Olympic Games Rio 2016. Several strategic actions were taken to prepare the city for the events (Gaffney & Robertson, 2018). One of the most relevant was the creation of the Rio Operations Center (COR). The initial motivation for the creation of COR in 2010 was the real-time monitoring of rains and storms. But with the need to prepare the city to host major events, COR was turned into a central operation point, integrating agencies and utilities of several services, including the ones related to areas like incident management and responses to emergencies, transport and mobility, citizen safety, and energy efficiency (Schreiner, 2016). Then, in 2013, the Smart City Expo World Congress awarded the Smart City of the Year award to Rio de Janeiro, with COR being among the long-term initiatives that judges valued (Fira de Barcelona, 2013).

Smart cities are highly dependent on the Internet of Things (IoT). They comprise the use of thousands of interconnected devices, which collect information. Specialized systems and applications apply this data for the interest of the citizens by performing data analysis and predictions. Thus, they help in the decision-making process in various areas such as transport and health services, besides facilitating the management of the city. Although there are several types of applications and systems, a common characteristic is that they need large amounts of data to work adequately. Such data is collected, processed, analyzed, and usually shared between different systems, making it necessary to apply cybersecurity and privacy maintenance techniques in all operations related to the data (Cui et al., 2018).

People often consent to applications and devices to monitor their habits, preferences, and activities. Then, search engines would use such data to present results targeted to the person's location and profile. Social networks would use those data to show relevant information according to each person's interests, and streaming tools would advertise products that suit the person's tastes and needs. Hence, people often give up privacy in exchange for the comfort and supposed well-being that intelligent customizations would offer. If the monitoring of one person and the sharing of collected data with certain service providers (e.g., applications) can promote a supposed increase in well-being and simplification at a personal level, then the broader monitoring of the entire population of a city with data sharing between city services, and the use of artificial intelligence to process such data and to provide intelligent services, would have the potential to promote substantial simplification and welfare to citizens life.

But the massive interconnection and sharing of data in smart city systems also increase the risk of cyberattacks. In 2015, one of the first publicly acknowledged incidents caused by cyberattacks in power grids occurred: a large blackout in Ukraine that affected approximately 225,000 customers for six hours (Liang et al., 2016). In Ukraine's blackout, the coordinated attack compromised three electric power distribution companies and thirty substations. Attack strategies used in Ukraine could also have been used successfully in other countries (Sullivan & Kamensky, 2017). Indeed, that incident caused great alarm and interest, but although there is a research effort in creating defenses for smart grids against cyberattacks (e.g., Gunduz & Das, 2020; Zhang et al., 2021), the risks remain. Besides that, cyberattack risks remain a reality in several systems and services of smart cities, but are even increasing with the use of Artificial Intelligence (Kaloudi & Li, 2020).

Usual attacks and vulnerabilities include unauthorized access, DoS (Denial of Service), and DDoS (Distributed Denial of Service). Such attacks and vulnerabilities can degrade the quality of services and data integrity. Several sophisticated protection methods based on encryption and biometric services are not applicable for city systems, as sensors have limited computational power. But the variety of devices, the great scalability, and the characteristics of the service dynamics aggravate the problem and increase security needs (Verkruisen, 2017).

The following section reviews concepts and applications related to smart cities. Then, Section III presents security challenges in such a context. Section IV describes cybersecurity techniques and solutions. Section V discusses open issues and future directions. Finally, Section VI concludes the chapter.

2 SMART CITIES

Technological advancement is something real. One can verify technological advancements in several aspects of daily life, including the evolution and presence of new paradigms in urban scenarios. Cities are in a moment of redefinition. For instance, the digital advance changed the construction of new buildings. Smart buildings became a reality. But before applying any technique, there must be an intensive investigation by entities such as governments, private services, and others.

Digital Cities, *ICT (Information and Communications and Technology) Cities* and *Wired Cities* are among the concepts related to the smart city concept. The main objective of Digital Cities is to make information available in a digital way. Through a mobile device or an internet platform, it would become possible to access a large volume of data, analyze it, and make decisions based on such data. Besides making information available in a digital way, ICT cities also focus on the interconnection of existing services in the city and the way they interconnect. Wired Cities are a union of *Digital cities* and *ICT cities*. Their objective is to collect large amounts of data from the countless interconnected city services and use such data to assist systems. The previous identification of the existing connections of the cities' services is required to take advantage of the information in such a way (Cui et al., 2018). Such concepts are somewhat convergent but have their priorities and objectives. So, it is necessary to identify the areas that change with the evolution of smart cities.

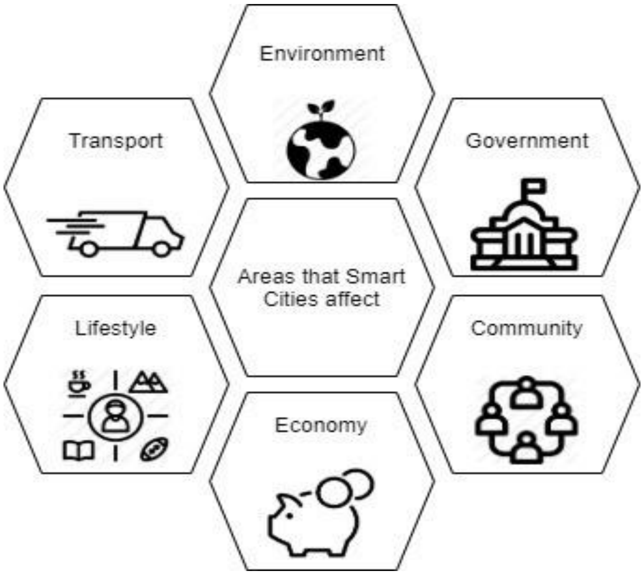

Figure 1 - Areas influenced by smart cities

The implementation of a smart city influences six areas (Cui et al., 2018), as represented in Figure 1. Each of these areas is associated with specific applications developed to improve the area's services:

- Smart economy - Using the Internet to support services, the economy took a new step and is evolving positively. With the advancement of technology implemented in smart cities, it will be possible to develop economic growth due to the new services created and the cost reduction of various tasks. For example, an application that promotes this growth is the dynamic pricing services, whether for restaurant reservations or even airline ticket reservations. These are tasks that become easier. Also, because it is simpler to carry out the actions, the demand to carry them out increases. Directly or indirectly, the city will evolve according to its economy.
- Smart governance - To achieve smart governance, one must minimize the probability of failure in several decisions related to standards, policies, and laws. The applications and services that a smart city can involve allow actions such as making somewhat simpler decisions.
- Smart environment - The environment can evolve into a Smart Environment parallel to city evolution, depending on several factors, including consumption management and applied intelligence levels. Considering the several types of data sources (which can include Bluetooth devices, physical sensors, sensors embedded in systems, smartphones, and wearables) is necessary to carry out all this management and improvement. Also, environmental sustainability benefits the environment and improves the community's lifestyle (smart lifestyle) and well-being (smart health);
- Smart transport - This area covers several factors, from city traffic routes to emergency services. A smart city should be able to assess areas of higher traffic and areas that, when damaged, have a major impact on city traffic and people's movement. Through control of these routes, it is possible to prepare emergency routes and alternative routes to traffic flows and find new ways to improve the city's traffic systems. Besides routes' management, part of the technology serves the sector through cargo tracking. This makes it possible to increase efficiency in several transportation processes (Sookhak et al., 2019).

2.1 IoT and Smart Cities

The development of a smart city depends on several IoT (Internet of Things) structures. However, the best approach is not uniform for all cities because the IoT structure depends directly on the requirements.

IoT architectures usually have a structure divided into the following four layers (represented in Figure 2):

- **Perception Layer -** Also known as the sensing layer, recognition layer, or even edge layer, such layer is the lowest one in the IoT architecture. Its main objective is to obtain/collect data from devices and sensors. It sends the collected data to the next layer for further transmission and processing.
- **Network layer -** Network connections that involve services such as the Internet, WSN's (Wireless Sensors Network), and communications networks are essential in the IoT. Thus, the network layer is fundamental in the IoT structure as it transmits the data collected from the perception layer and sends it to services, servers, and network devices.
- **Support Layer -** The support layer is the layer closest to the application layer. It supports any requirement that the numerous applications need through intelligent computing techniques such as cloud computing and edge computing.

- **Application Layer -** The application layer is responsible for providing intelligence and services to applications that have customized requirements. Because after processing this information, an analysis takes place, the results of this action allow application users to understand what is happening (Elmaghraby, 2013).

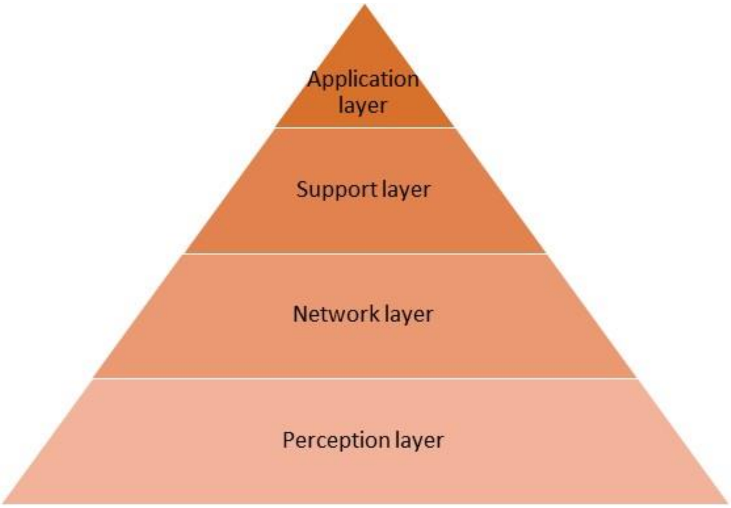

Figure 2 – The layers in the IoT structure of a smart city (adapted from [Cui et al., 2018])

The IoT structures implemented in such a layered model consider a variety of services. Several cities already adopted this IoT data collection structure (e.g., Barcelona, Singapore, Boston, London, Dubai, and Hamburg). These cities have large datasets to process and extract knowledge that can improve welfare. For instance, city systems may use data on road traffic, empty places in parking lots, and noise levels to prevent traffic congestion and increased noise, thus increasing the city efficiency and sustainability (Elmaghraby and Losavio, 2014).

When implementing such a system, one should be careful about the granularity used to store and process the collected data. Usually, such systems manage aggregated data, making it impossible to relate certain information to specific individuals. If it is possible to associate the data with a certain person, then privacy problems may arise.

Let us consider a real example with data privacy-related issues. In Singapore, the government once wants all vehicles to install a satellite navigation system, which would transmit data like speed and direction. So, it would be possible to check and monitor each vehicle’s location at any time (Mashable, 2016). Such a scenario is the perfect example of the IoT, with several devices connected to a network and providing data, which is processed to improve various services. That said, the idea of making the city more and more intelligent is conceivable. But this system contains privacy risks and may affect citizens' trust, especially if the data is used for commercial benefits or sold to third parties.

2.1.1 Heterogeneity

A system based on the 4-layer IoT structure is a very heterogeneous and highly independent and distributed system, as evidenced by the wide variety of nodes in the network, with different communication protocols, technologies, hardware devices, and platforms. These characteristics vary so much that smart cities are not uniform. The architecture of the IoT is unlikely to be identical between cities. Also, the lack of a formalized and standardized structure may make that security services adapted to a city but not to another, thus requiring additional measures to ensure security in the latter.

Hence, heterogeneity is one of the characteristics of smart cities, as represented in Figure 3.

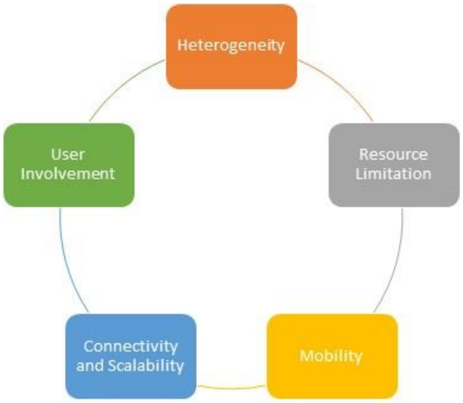

Figure 3 - Features of smart cities.

2.1.2 Resource limitations

IoT devices have several resource limitations, from memory limitation to battery capacity and even task processing and execution capacities. In addition to these limitations, there is still a restriction on the interfaces present on the network. Also, access to the storage platforms of these devices is usually limited. For example, the smallest, cheapest, and energy-efficient appliances are the most used in smart cities, because they allow the use of all the necessary rules for proper functioning.

2.1.3 User Involvement

Users (city population) are an integral and crucial part of smart cities, as a smart city involves more than just emerging technologies and new infrastructures. The creativity and learning of the population are essential for smart city development (Biswas and Muthukkumarasamy, 2016).

2.1.4 Mobility

Urban mobility is essential for the progress of cities. Smart cities need to obtain a form of real-time monitoring and wireless communication. Thus, all route systems in a smart city require customization due to such characteristics. In this way, it is possible to guarantee a communication system and an infrastructure that satisfies all the requirements and has an adequate recovery of extreme events.

2.1.5 Connectivity and Scalability

In a smart city, almost the entire city's equipment is interconnected. Hence, network connections and equipment interconnectivity are basic functionalities. Without them, it would not be possible to achieve success in the development of a smart city. Besides interconnectivity, it is also crucial to care about the solution scalability in a real scenario. Smart cities are developing rapidly, resulting in an explosion of growth in the volumes of data collected and permanent traffic on the network. Understandably, a smart city cannot evolve without highly scalable solutions.

2.1.6 Data Processing Characteristics

Data privacy is a challenge and a concern for any smart city, the method of collecting, storing, sharing, and analyzing data needs to be carried out carefully and correctly. That said, the effectiveness present in smart cities depends on the application carried out around Big Data (Elmaghraby, 2013).

With so many concepts and complexity of the themes involved in smart cities, there are several challenges related to processing methods. Some manage to be better than others:

- **Bach processing**: it is a method of processing and analyzing large amounts of data, collected in a given period and stored in a data phase.
- **Near Real-Time Processing**: there is a need to receive data and process it in a very short time. Processing and analysis of the received data occurs almost in real-time.
- **Data management**: allows the development of architectures, policies, and procedures to manage the data received.
- **Network**: without an understandable infrastructure that allows the transfer of data between the different layers and components of a city, there is no smart city that can evolve without this type of network.
- **Algorithms**: algorithms have a huge responsibility because they are the ones that allow the processes to evolve and improve the city's analysis process (Verkruisen, 2017).

2.2 Infrastructures

Smart cities are based on infrastructures (Shahidehpour et al., 2018). Building intelligent infrastructures also arises as an alternative to help and improve the lifestyle of the population. Considering that the initial challenge is to understand the needs and concerns with the population safety, finding the strategy that achieves better results in the different city parts is fundamental.

Figure 4 presents the main infrastructures:

- Institutional Infrastructure - It is based on fundamental activities, from management, to the governmental and planning part of the city. There is also an objective to include the population in these decision-making processes, so that decisions are not taken arbitrarily or discriminatory. Since it is essential to the process to have a method that in real time and exercising certain rules and agreements, it is possible to provide an efficient, responsible and transparent method of making decisions for the system.
- Physical Infrastructure - Through the application of communication systems, it is possible to verify the efficiency and intelligence applied to the infrastructure. But there are still other actions to take, like wastewater management, energy resource management, communications management, etc. For example, the management of roads, routes, and transit systems would benefit the population's quality of life. Also, it would let people look for alternatives to walk, ride a bicycle, or even use urban transport services. In a smart city, pre-planning solutions should make it easy to find alternatives.
- Social Infrastructure - The social infrastructure involves several mechanisms that promote the human and social development of the city. Intelligent services are linked to infrastructures that provide social services to the population, including education, health services, and various environment-related activities.

- Economic Infrastructure - This point refers to basic services that help and promote the production and distribution processes of economic activities, whether developing a specific structure that creates job opportunities and attracts investments. Even if these activities do not produce services or goods, they have a direct impact on the economy and persuasion in production, whether, in agriculture, industry or business (Gharaibeh et al., 2017).

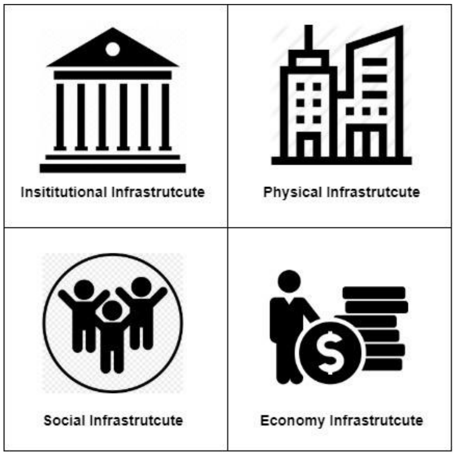

Figure 4 - Existing infrastructures in smart cities

It is indisputable that the concept of the smart city transforms and changes several daily tasks of society. The result of involving applications smart in smart cities is to improve the existing connectivity and communications, allowing data collection and interpretation of a large amount of information. Governments may analyze this data and use the information in intelligent methods, having a direct impact in several areas (Kitchin, 2016). Keeping, analyzing, and processing this information will also increase tasks to ensure security in services and all infrastructures.

2.3 Application Examples

The smart city is an innovative concept that involves several applications that promote the city itself and the environment. Figure 5 presents some of such applications, which are discussed in this section.

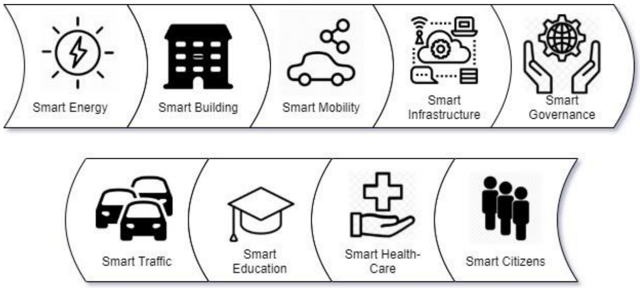

Figure 5 - Existing applications in smart cities.

2.3.1 Smart Energy

One of the smart cities' objectives is to provide its citizens an accessible, comfortable way of life in a neutral environment. The purpose of smart energy is to allow efficient control of energy and resource consumption, increasing the use of renewable energy sources through emerging approaches and planning strategies (Wilson, 2020). The smart energy concept consists of seven elements:

- **Resource integration system -** It indicates the physical and digital control plans, being possible to test methods that benefit the system. The benefits that these plans bring are the optimization of energy levels and increased effectiveness.
- **Access to energy services -** It suggests that all citizens should be able to obtain energy services in an accessible, reliable, and sustainable way.
- **Resilience -** It refers to methods that allow preserving the communities and the economy of the city, following the plans, performing various functions in the city's area.
- **Efficiency -** It is considered the key element of smart energy due to the existing scarcity of natural resources.
- **Renewable -** Over time, one of the objectives of smart cities is to encourage companies to focus on the area of renewable resources to prevent unexpected climate change.
- **Active to users -** Smart energy strategies' effectiveness depends directly on business evolution. It will depend on the interaction of the population and the way they operate daily.
- **Sustainable Economy -** Government should use smart energy systems sustainably to provide services, so the population's economy will not be affected.

Applications that aim to improve energy efficiency and its use:

- **Smart Grid -** A smart grid is a network infrastructure based on standard and interoperable communication transceivers, gateways, and protocols. Smart grids allow a real-time balance between the local and the global generation and storage capability with the energy demand. They will also allow a high level of consumer awareness and involvement (Thakrit Panklib, 2016).
- **Residential building Ecosystem -** This provides an innovative concept for power distribution, energy storage, grid monitoring and communication (Thakrit Panklib, 2016).
- **Hydrogen Solutions -** Hydrogen is a clean and safe energy option, that can be used as a fuel in transportation and electricity production (Dincer and Acar, 2018b).

2.3.2 Smart Building

Smart building refers to how one manages, measures, monitors, and optimizes the maintenance of buildings and infrastructures. It involves various automatic processes and the integration of different technologies. Sensors and system controllers collect and process data, which support several services, like climate control, management of energy equipment, and monitoring of the building's structural health. Apanaviciene et al. (2020) describe a framework that evaluates the integration of smart buildings into smart cities through the verification of statistics about operations in the city.

2.3.3 Smart Mobility

Through tasks that allow the planning of the transport of people and materials, it is possible to make these services more efficient and sustainable, which is the objective of smart mobility applications.

One can obtain this system through the road networks construction and the development of processes that analyze transport systems data. Such structure includes some layers:

- **User Experience Layer**: allows users to return transport information.
- **Transport Services Layer**: contain the transport services provided by companies.
- **Data Collection Layer**: mode of collection on the use of services.
- **Information Management and Control Layer**: service verification mode that confirms the efficiency of the services provided.
- **Transport Coordination Layer**: responsible for optimizing the transport system through the analysis and collection of data from companies.

2.3.4 Smart Infrastructure

It consists of automatic systems distributed in smart cities. Such systems communicate with each other, managing and integrating the distinct components of a smart city, such as smart mobility, energy, and economy applications. The main objective of smart infrastructure is to optimize the use of resources and improve performance in general. However, there are several difficulties to implement such a system, including choosing the system location, the lack of technical knowledge, and poorly evolved and inefficient business models.

2.3.5 Smart Governance

One of the components of cities involves the political system that must be understandable and support all necessary planning and decision making. The advantage of having a smart governance methodology is that it helps evolve into a smart city through the connection between public, private, civil, and national organizations. The main concerns of smart governance include the expression of appropriate policies and strategies, supporting capital investment, providing opportunities for the population to interact in decisions, and involving technology in these actions, allowing the city to evolve.

2.3.6 Smart Education

It has very high relevance in the efficiency of a city and the progression through the generations. The use of services based on new technologies or social networks can support the education system's improvement. One must also introduce (in the education system) smart cities-related topics such as energy control and management in systems, addressing security levels, forms of communication, and transport, thus facilitating the population adaptation to smart services.

The Students Career Assistance System is an example of a smart education application. It is a framework to support students in learning and career development (Dincer and Acar, 2020).

2.3.7 Smart Healthcare

Smart healthcare systems collect patient and health infrastructures data, processes, and analyzes such data to make predictions and corrective actions. Smart healthcare systems should be part of the context of the city's network of systems of telecommunications and information. The smart healthcare concept is an innovative concept that in different contexts has the following effects:

- **Society**: promotes health services to allow the population to become healthier, focusing on nutrition and physical activities, reducing the treatments' costs.

- **Government**: applying the smart healthcare system will reduce the costs that governments apply to healthcare.
- **Research**: adopting smarter techniques for the health model and population of a city will develop results that become more accurate as the amount of data is collected.

The RFIDLocator developed at the University of Fribourg (CH), in collaboration with Sun Microsystems, is an example of a smart healthcare application proposed to improve the quality of hospital services (Dincer and Acar, 2018a). This application successfully uses the passive for equipment localization in hospitals (Dincer and Acar, 2018a). Another technology applied in the smart hospital context is the CoAP (Constrained Application Protocol) protocol, which connects and monitors medical sensors. The CoAP adoption in healthcare scenarios is relevant due to some CoAP built-in features, such as resource observation (useful for real-time monitoring of vital signs) (Dincer and Acar, 2018a).

2.3.8 Smart Citizens

Smart citizens are considered a prerequisite for any smart city. They force the system to become more comprehensive, revolutionary, and sustainable. By smartly using available solutions, citizens drive creating more smart products and services, all through information sharing. The population may still participate in decision-making depending on the method of the city administration.

Cell phones, wearable devices, and home-based IoT devices provide many services to citizens. But such devices also collect and share data (e.g., weather, traffic, and route-related data) with other cities' services and systems. Then, they would process and analyze the data to provide smart services to citizens.

2.3.9 Smart Traffic

Among the biggest challenges that cities face are the planning and implementation of an efficient traffic management system. In some cities, the number of traffic accidents is very high. Traffic accidents lead to material losses at the most diverse levels, including many directly related to the accident itself. But the high number of accidents increases the number of traffic congestions, which significantly impacts urban mobility and increases pollution levels. Citizens lose time in traffic congestions, which affect them both economically and in terms of their quality of life.

Intelligent traffic is a concept that seeks to deal with these problems efficiently, making quick and efficient decisions based on the collection of data from mobile devices, sensors, and cameras.

Currently, there are traffic control approaches that enable dynamic responses to disasters and uncontrollable or even unexpected changes through the management of information sent in real-time. Existing solutions may also change the city's urban system based on the data collected to reduce the intensity of traffic (Rizwan et al., 2016).

MobiTraS (Manolopoulos et al., 2010) is an example of a smart traffic application. In MobiTraS, a mobile application communicates to a traffic server where a traffic prediction algorithm reconstructs the traffic model from gathered data and provides near real-time guidance to the driver.

3 CYBERSECURITY AND DATA PRIVACY CHALLENGES

Smart cities are the evolution of cities as one knows them today and will impact the lives of the entire population worldwide. The smart cities concept aims to improve the quality of life, reduce the environmental impact in urban areas, make the population healthier and more productive, boosting the local economy.

However, these are complex initiatives and present several challenges, as discussed in the previous section. The logistics and complexity of the interaction between services hamper the city's evolution. Besides the implementation challenges, there are also issues related to cybersecurity and privacy.

In smart cities, intelligent systems monitor and record citizen movements and interactions. Maintaining privacy and cybersecurity for the population in such a context is a complex challenge. Recently, several states and countries created regulations that impose constraints on what data may be collected and recorded. Also, such legislation usually specifies requirements on how/where to store such data to ensure citizens' privacy.

Despite the evolution of technology implemented in smart cities, smart applications have vulnerabilities that cybercriminals may explore. Examples of the possible attacks include background knowledge attacks, collision attacks, Sybil attacks, eavesdropping attacks, and spam attacks (Ijaz et al., 2016a).

3.1 Security and Privacy

The technologies involved in smart cities connect several (critical) services, providing increased efficiency and greater convenience to the population. But they also expose the city infrastructures to extensive cybersecurity risks and threats (Shahidehpour et al., 2018). Therefore, cybersecurity-related processes, methods, and systems are even more critical in smart cities than in non-smart cities.

Some of them are somewhat easy to implement, such as updating systems, making backups, and installing antivirus tools. But on a city-wide scale, applying cybersecurity mechanisms is challenging. Also, smart cities have complex interconnected systems, made up of thousands of devices, which increases the seriousness of the risks. So, governments must adopt even more digital measures than in a non-smart city. Therefore, high investments are necessary to apply good standards, firewalls, policies, and procedures that respond to cyberattacks.

Table 1 presents examples of cyber-risks and protection and measures for different application areas in a smart city. The challenges that smart cities face are based on the management of distinct industries and technologies. Methods that involve Big Data dictate how the city will evolve into a smart city.

The integration and coordination of different technologies and systems also increase the cybersecurity challenges. Currently, the security implemented is in systems that impose themselves through smart grids. These systems focus on control centers, industries, systems that integrate different services and are essential for the city. However, a smart city is not only about the industry. It also involves citizens and their daily lives, from their homes to the means of transport (Elmaghraby, 2013). Also, continuously monitoring and data collection, increase the amount of data to be processed, stored, and protected.

The lack of security can lead to the invasion of privacy. For instance, several applications and extensions are constantly collecting data from browsers, including search data and authentication information, which leads to privacy-related concerns. In a smart city, where several IoT devices and services are interconnected, and citizens are constantly monitored, privacy-related issues become even more relevant. Indeed, in some situations, maintaining privacy goes in the opposite direction to the implemented features. Let us consider the example of the traffic monitoring system of Singapore discussed previously in this chapter. The government requested that all vehicles share real-time information on their speed and directions. Although that information may be extremely useful in traffic and route management, a breach of privacy would expose data about individuals (e.g., when and where they have been) that they may not want to share.

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

Table 1 - Threats and protection measures (adapted from [Aileni et al, 2020])

Data collected by IoT services may be available to companies and governments. Besides the risk of unintended privacy exposure, there is the risk of using data for economic and marketing benefits (e.g., through the intentional sale of private data to third parties). Then, there is the need to protect and monitor the data communications and storage. So, it is mandatory to have methods that implement security in the global system.

In general, if there is no investment in this area of cybersecurity, smart cities may never go from a concept to real implementations. It is essential to have security processes in this type of system. Also, governments must agree and build privacy rules and regulations on it. Maintaining digital data privacy is the central concern of several laws established in the last few years. But this type of agreement on what is public and what should be private will continue to exist in the future, just as systems evolve with technology. So, there should always be studies on the privacy and security risks for the collected data.

Also, in a complex environment like smart cities, following a traditional system is not realistic because it does not have the necessary security. It is then required to develop methods for predicting attacks and recovery, which may be possible through intelligent systems that can automatically predict and recover from attacks.

3.2 Cybersecurity-related requirements in smart cities

Figure 6 presents the main security and privacy requirements in smart city systems (Cui et al., 2018). To fulfill such requirements, one should consider the characteristics of the IoT devices and how smart city applications use them:

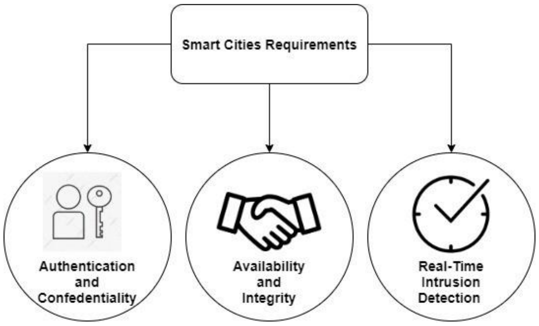
Smart Cities Requirements
Authentication and Confedentiality
Availability and Integrity
Real-Time Intrusion Detection

Figure 6 - Requirements for smart cities applications

- Authentication and Confidentiality: authentication and confidentiality control mechanisms must exist in the various services of the entire system. As there are several distinct entities using authentication methods, it is necessary to use an authentication management system. Confidentiality appears in the sense of preventing the disclosure of data in an uncontrolled way, preventing passive attacks. Therefore, it is crucial to have communication with a base of encryption systems throughout the network. Encryption coupled with authentication will increase the data confidence of the implemented system (Cui et al., 2018).
- Availability, Integrity, and Confidentiality: these characteristics allow services to share data and to consume shared data to make decisions, relying on data sources. Critical services must remain functional even when under attack. Hence, the system must identify when a device is functioning abnormally. Also, there should be protection and robustness mechanisms that allow the adaptation when under attacks. Without that, the data shared between services may become invalid. The cybersecurity methods currently applied to maintain availability, integrity, and confidentiality include firewalls, protocols on data traffic management, and communication between IoT devices.
- Intruder detection and attack prediction: there must exist mechanisms to predict and monitor risks and anomalies in the systems considering the specific vulnerabilities of the IoT devices and characteristics of the city network. Traditional measures include the use of fault detection and anomaly detection mechanisms.

3.3 Vulnerabilities related to government, technological, social and economic factors

This section considers three of the smart-cities dimensions: governmental, socioeconomic, and technological. It presents the links between such dimensions and a set of risks and vulnerabilities, which Figure 7 summarizes. The combined dimensions influence the information that is collected and the possible security problems that are involved in a smart city. The technology has the function of managing the system's security and can implement solutions and prevention mechanisms to cyberattacks.

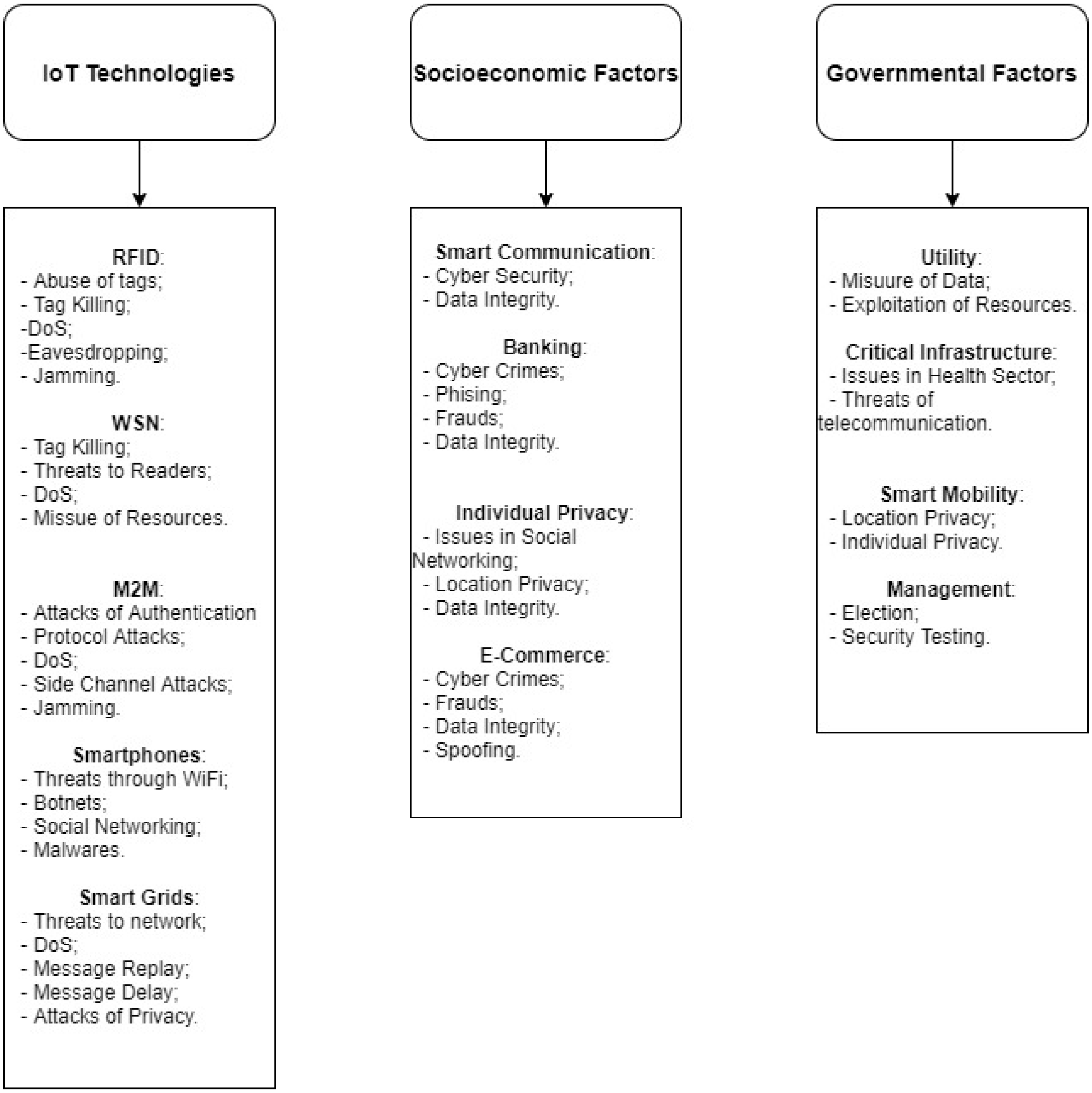

Figure 7 - Security and privacy issues in a smart city

3.3.1 Government Factors

In smart cities, systems should manage and maintain all the infrastructures and help solve the obstacles of a city. But bad implementations of smart technologies will encompass even more problems such as attacks and fraud. These malicious attacks can cause damage to a city's functional core.

- **Security Testing Required -** One of the problems in government entities is that companies that obtain technology do not waste time due to testing security in systems. Therefore, indicating and advising these entities on the security problems that exist is a priority.

- **Critical Infrastructure Threats -** Critical structures usually include smart grids and IoT services. Attacks on infrastructure critical to the city functioning are the points that need the most protection since they can cause everything from delays in the responses to the total loss of control of the system. Therefore, it is necessary to protect such infrastructures and services from malicious attacks and to guarantee the security, resilience, and integrity of the data they consume.
- **Smart Mobility Security and Privacy -** As discussed earlier, this is a crucial system for the functioning of a city, but the collection of information from services covered by smart mobility can cause privacy problems due to the availability of personal information. Information from techniques such as GPS, GSM, WiFi, Bluetooth, and RFID may not relate information to IDs or individuals when stored in centralized systems.
- **Energy and Optimization of Use -** Devices and implemented services usually use electricity. In a smart city, services and devices are diverse and in great quantity. To save resources, these devices depend on smart grids, which use bidirectional communication between users. There is effective energy management and distribution.

3.3.2 Social and Economic Factors

In a smart city, technology manages all requests made by people. It provides a platform with services that allow urban planning, the management of emergency services, and the community.

Social and economic factors in smart cities include communication, individual identity, banks, and finance. These systems are crucial for the proper functioning of a smart city, but these also systems have security vulnerabilities and privacy problems.

- **Communication difficulties -** The communication sector is an integral part of the whole system. There are several vulnerabilities, attacks, viruses, fraud, and privacy attacks that can impact communications. Several (government and financial) activities use telecommunication and wireless services, so the need for security and authentication increases. Therefore, security threats are related to M2M communication (machine to machine). The use of smartphones and tablets opened new horizons in the area of communication. Although they provide new applications, they also require new security measures.
- **Privacy of individuals -** Citizens' privacy is essential, and a smart city must guarantee it. Individuals use different services that communicate with each other through a heterogeneous network. Cybercriminals wanting to attack these systems and succeed will have access to large amounts of private data. Therefore, these communication services also need robust security components.
- **Banks and Finance -** Banks and financial services are part of the smart economy, which is a fundamental component of smart cities. Smart cities promise economic growth, but it is a system very vulnerable to attacks behind financial information. Usually, these attacks intend to sabotage the economy of some organizations or even the entire city.

3.3.3 Technological Factors

Technology has a crucial role in the sense that smart cities can achieve everything they propose. Smart cities depend on technology to provide the best possible services, improve the economy and the decision-making method, and develop new services.

It is a very generous promise, but there are concerns about security and privacy that can dictate the solution's credibility.

- **IoT** involves many different devices, which services that smart cities' systems. Therefore, the IoT has a fundamental role in the development and maintenance of information collection services.
- **Smart Grids** is one of the fundamental technological pieces. Smart grids influence the energy management method. These infrastructures are communication instruments that include sensors that communicate in a network with real-time data. When data sharing occurs in real-time, a secure source of energy is needed, as users and services may need the information at any time. If the system allows attacks that influence this mode of operation, many users and services will encounter uncertainties and flaws in the system.
- **Smartphones** are a component that allows easy access to information from services and smart applications. This mobile service allows the management and development of a better smart city, due to ease access to information.
- **M2M Communication** allows applications and services to communicate with citizens smartly. The protocols used in the machines arrange communication rules between nodes in the network. In this context, the Internet Protocol (IP) is a standard for communication processes.

3.4 Problem Examples

Several risks identified in previous sections are directly related to smart cities' infrastructures. For instance, monitoring grids and smart mobility applications with access to data on the residents (including habits and schedules) may become targets of direct attacks. To these problems are added others that involve the evolution of smart applications, as several applications that promote the city and improve its quality of life are the target of exploits. Some examples of such situations are:

- Botnet activities - Introducing botnets to IoT services causes severe risks to the system. These systems affect devices such as cameras, printers, and even routers. If they manage to infect multiple devices, that would be like a DDOS attack on the system's servers. The interconnected use of computers, mobile devices, and IoT devices can hamper techniques for applying security to the system.
- Automatic driving cars - Several companies are working on developing automatic driving cars to reduce the number of road accidents. However, such vehicles involve several different technologies. Thus, they may become vulnerable to different types of threats. For instance, cybercriminals can exploit bugs in the system to control the vehicle remotely, intercepting and changing the behavior of any vehicle function (including accelerating and brake, shut down, for example). Therefore, it is necessary to implement severe security measures.
- Virtual reality - Technology like virtual reality has been implemented in several cases in the industry with the integration in digital twin environments. In smart cities, this technology is implemented to improve planning services, visually assisting services (e.g., health services). However, these applications involve lots of sensitive data collected from different devices and shared through third parties. Since there may be a disclosure of this type of data without authorization, it is a privacy issue.
- Artificial intelligence - To understand the everyday actions in smart cities, one needs an intelligent system. Artificial intelligence came to assist the applications to work smartly. But as the other examples presented, the use of this technique has certain risks. For instance, device manufacturers and service providers may use machine learning and data mining over collected data for their benefit. Machine learning algorithms are highly dependent on the data they train.

Hence, cybercriminals can create techniques to influence the training of machine learning models and alter the effects of training algorithms.

4 CYBERSECURITY TECHNIQUES AND SOLUTIONS

This section presents some key concepts (cryptography, blockchain, machine learning, and data mining) and their application for cybersecurity and data privacy in smart cities.

4.1 Cryptographic Techniques

Cryptography algorithms are a fundamental security measure to guarantee the privacy and protection of services for smart applications. These algorithms are well referenced because there is no need for third-party access during the data storage and processing process.

Currently, several cryptography tools that use even innovative techniques are available for smart city systems. IoT computational power limitations, smart cities' complexity, and energy consumption requirements make most traditional cryptography tools and algorithms inadequate for smart cities. New encryption techniques are considered lightweight and contain authentication mechanisms for a given IoT scenario that can protect communication between users from DDoS attacks. Recently, these protocols have become easy to implement in the security schemes of smart cities.

Techniques found in these systems also include encryption, which allows computer systems to manage and share data in an encrypted and secure way by a chain between various services. These systems protect private information from several services ranging from healthcare to computing services in cybersecurity (Rizwan et al., 2016). One of the problems of this type of system is the investment that is too high at the computational level, being a disadvantage that has a great weight when opting for a security service. So many organizations dismiss this type of service.

Another technique applied in real scenarios is Zero-knowledge proofs. It is a tool that applies cryptography services. These services can be used as a form of authentication and can implement protocols in smart cards.

4.2 Blockchain

Blockchain is being applied more and more to several areas, including in IoT systems, where it adds security, trust, and transparency to several processes (Khan and Salah, 2018). Blockchain is a decentralized solution that allows applications to operate in a distributed way, in contrast to centralized systems, such as cloud services, that do not guarantee total data integrity and have a greater possibility of information exploits. That is one of the reasons that attract so many to implement solutions using this technology,

The distributed P2P blockchain-based systems maintain a list of records with all transactions for a given service. This distributed system maintains security and privacy through methods that do not identify the transaction authors. Hence, using blockchain technology makes the system more efficient and resistant to failures. It also improves the solution's flexibility and adaptation to changes, thus ensuring high scalability and security.

Existing examples guarantee secure communication between the devices of the smart cities while improving the reliability and efficiency of the system. Also, regarding cybersecurity and data privacy in smart cities, blockchain technology guarantees and allows the system to be protected safely (Rizwan et al., 2016). An example on the use of blockchain is in the context of bank operations, where this type of system is implemented with smart contracts with transactions that maintain privacy (Khatoun and Zeadally, 2017). This system can also be applied to homes, thus allowing for the collection of information processes that maintain the confidentiality and integrity of the data, allowing them to be available in real-time.

4.3 Machine Learning and Data Mining

Machine learning and data mining techniques are based on practical situations. They apply and improve the models created during a training process to real-world conditions efficiently and effectively. The processes involved in this technology aim to predict intrusions, failures, or anomalies in the system.

These methods protect infrastructures from attacks. This system applies security to wireless sensors through a model based on machine learning. As it receives data, models are created that verify the operations that are taking place and detect any suspicion.

Systems based on machine learning detect and are programmed to make personalized decisions with the activity that is taking place. In addition to improving several steps in the processes of smart cities, it is also possible to apply the same methods to ensure security and privacy to the system. The main idea is to understand user standards and match that action to features in the environment. However, the data analyzed by the mechanism will always be a cause for concern for users and may not even portray the real-world situation. Therefore, it is necessary to create strategies that allow the evolution of the system.

The vast amount of data collected by sensors may be analyzed to find patterns and information to improve various services through data mining techniques (Lee et al., 2006). However, when dealing with private data, some concerns arise. For instance, data about location and behavior patterns are considered private, and it should not be possible to link the user to the data. Privacy-Preserving Data Mining (PPDM) protocols and technologies may mitigate the risks of private data exposure (Ijaz et al., 2016b).

5 OPEN ISSUES AND FUTURE DIRECTIONS

The increase in urbanization and the irregular cities' growth impose new challenges to governments at the most diverse levels. In smart cities, cybersecurity is an additional challenge. Implementing cybersecurity solutions in several services (such as transportation, housing, and health) is not trivial. Thus, as smart cities grow and new smart services emerge (increasing the volume of data and the number of interconnected devices), the challenges related to cybersecurity are also increasing. The use of machine learning in the most diverse contexts, and combined with other techniques, is seen as one of the most promising ways to overcome these challenges.

The use of machine learning techniques in smart cities has been studied for some years. Smart systems and services use machine learning to analyze data to assess the way the city operates. Machine learning models make predictions to optimize resource usage. Application areas in smart cities include smart transportation (Bacciu et al., 2017; Karami and Kashef, 2020), smart health, and healthcare (Rayan et al., 2019; Zahin et al., 2019) and smart homes (Liang et al., 2018; Popa et al., 2019). In Rudin et al., (2012), machine learning models use New York City historical data from the power grid to predict the risk of component and system failures. These models can then be used directly by energy companies to help prioritize maintenance and repair work. Machine learning may also help citizens with their daily choices, like choosing the best route to work.

There also exists much research on using machine learning to maintain cybersecurity and privacy, including in the IoT environment (Hussain et al., 2020; Singh and Singh Tomar, 2019; Xin et al., 2018). A promising approach is to combine machine learning with the more traditional concept of Intrusion Detection Systems (IDS).

Intrusion detection systems allow the identification of unauthorized accesses and unusual activity. Thus, they are both a way to identify cyber-attacks and system failures that lead to abnormal behavior. But traditional IDS systems are not entirely suitable for the IoT environment. Although there are some specific proposals for the IoT context, the integration of machine learning techniques with IDS systems is an opportunity for achieving better results.

Machine learning methods are categorized into supervised learning, unsupervised learning, and reinforcement learning. In supervised learning, one uses a dataset representative of a situation to train the algorithm. After the training, the algorithm is ready to be used in a real-world condition. When using unsupervised learning methods, there is no training phase, and the algorithm discovers data patterns by itself. In reinforcement learning, the algorithm uses feedback to try to achieve a goal. Choosing the best learning method for each situation is a challenge. Also, there is a lack of representative datasets to be used to train machine learning algorithms.

Machine learning models would consume large amounts of data collected by sensors to find patterns or make predictions. Machine learning-based programs usually need a computational power that is not available in IoT devices. Using a centralized architecture on which data should be transferred to a central place to be processed would pose problems such as network congestion. Also, processing such a volume of data is challenging regarding the required response time (which would be almost real-time in many situations). The development of distributed architectures for machine learning solutions that would use the available distributed resources in smart cities systems and services is another open issue.

6 CONCLUSIONS

A smart city has several interconnected systems and devices, which collect, process, analyze and share a large amount of data. This structure ultimately aims to provide intelligent services that improve the quality of life for citizens in a sustainable ecosystem. Smart services have been studied and developed for several areas, such as energy, mobility, infrastructure, health, education, and traffic. The number of available smart systems and the quality and effectiveness of made available services are related to the city's evolution. However, the high number of heterogeneous devices, systems, and services in smart cities, and the large volume of data collected, processed and shared, severely increase the risks of cybersecurity failures and private data exposure.

Maintaining cybersecurity and data privacy in smart cities involves protecting the various components of the ecosystem, from IoT devices to systems and services, through the interconnection network components. As there is no facto standard for the technological environment in this context, there is the need to study cyber protection vulnerabilities and the corresponding protection techniques before implementing new systems and services.

The security measures must detect anomalies, and guarantee data backups and security of the available services. However, each application has its vulnerabilities, and it is necessary to find the cybersecurity solution that presents the greatest advantages for each service. This chapter presents several characteristics, elements, and requirements of a smart city, relating them to possible cybersecurity problems. The chapter presents measures for preventing cyber-attacks and protecting privacy in this context using emergent technologies. It also discusses open issues and future directions. Currently, there are proposals for solutions to various types of vulnerabilities with the aid of specific techniques or emerging technologies, such as cryptography and blockchain.

Using machine learning techniques for security and maintenance of privacy in IoT and smart cities emerges as a promising future direction. Some of the challenges to overcome include choosing the best model for each situation, the lack of representative datasets for training machine learning models, and the need to develop distributed architectures that may take advantage of the distributed processing power available in the smart city ecosystem.

ACKNOWLEDGMENTS

This work was partially funded by National Funds through the FCT (Foundation for Science and Technology) in the context of the project UIDB/04524/2020.

REFERENCES

Aileni, R. M., Suciu, G., Serrano, M., Maheswar, R., Sakuyama, C. A. V., & Pasca, S. (2020). The Perspective of Smart Dust Mesh Based on IoEE for Safety and Security in the Smart Cities. In *Integration of WSN and IoT for Smart Cities* (pp. 151-179). Springer, Cham.

Apanaviciene, R., Vanagas, A., & Fokaides, P. A. (2020). Smart building integration into a smart city (sbisc): Development of a new evaluation framework. *Energies*, *13*(9). https://www.mdpi.com/1996-1073/13/9/2190

Bacciu, D., Carta, A., Gnesi, S., & Semini, L. (2017). An experience in using machine learning for short-term predictions in smart transportation systems. *Journal of Logical and Algebraic Methods in Programming*, *87*, 52–66. https://doi.org/10.1016/j.jlamp.2016.11.002

Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 1392–1393. https:// doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access*, *6*, 46134– 46145. https://doi.org/10.1109/ACCESS.2018.2853985

Dincer, I., & Acar, C. (2018a). An iot-aware architecture for smart healthcare systems. *International Journal of Hydrogen Energy*, *43*(18), 8579–8599. https://ieeexplore.ieee.org/abstract/document/7070665/

Dincer, I., & Acar, C. (2018b). Smart energy solutions with hydrogen options. *International Journal of Hydrogen Energy*, *43*(18), 8579–8599. https://doi.org/10.1016/j.ijhydene.2018.03.120

Dincer, I., & Acar, C. (2020). Smart education literature: A theoretical analysis. *Education and Information Technologies*, *25*(4), 3299–3328. https:// doi.org/10.1007/s10639-020-10116-4

Elmaghraby, A. S. (2013). Security and privacy in the smart city. *6th Ajman International Urban Planning Conference AIUPC*, *6*.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy [Cyber Security]. *Journal of Advanced Research*, *5*(4), 491–497. https://doi.org/10.1016/j.jare.2014.02.006

Fira de Barcelona, (2013). Smart City Expo World Congress chooses Rio de Janeiro as the best smart city of 2013. Retrieved June 21, 2021, from https://www.firabarcelona.com/en/press-release/uncategorized/smart-city-expo-world-congress-chooses-rio-de-janeiro-as-the-best-smart-city-of-2013/

Gaffney, C., & Robertson, C. (2018). Smarter than smart: Rio de Janeiro's flawed emergence as a smart city. *Journal of Urban Technology*, *25*(3), 47-64.

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., & Al-Fuqaha, A. (2017). Smart cities: A survey on data management, security, and enabling technologies. *IEEE Communications Surveys Tutorials*, *19*(4), 2456–2501. https://doi.org/10.1109/COMST.2017.2736886

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094.

Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys and Tutorials*, *22*(3), 1686–1721. https://doi.org/ 10.1109/COMST.2020.2986444

Ijaz, S., Shah, M. A., Khan, A., & Ahmed, M. (2016a). Smart cities: A survey on security concerns. *International Journal of Advanced Computer Science and Applications*, *7*(2). https://doi.org/10.14569/IJACSA.2016.070277

Ijaz, S., Shah, M. A., Khan, A., & Ahmed, M. (2016b). Smart cities: A survey on security concerns. *International Journal of Advanced Computer Science and Applications*, *7*(2), 612–625.

Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34.

Karami, Z., & Kashef, R. (2020). Smart transportation planning: Data, models, and algorithms. *Transportation Engineering*, *2*, 100013. https://doi.org/10.1016/j.treng.2020.100013

Khan, M. A., & Salah, K. (2018). Iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395– 411. https://doi.org/10.1016/j.future.2017.11.022

Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, *55*(3), 51–59. https://doi.org/10.1109/MCOM.2017.1600297CM

Kitchin, R. (2016). Getting smarter about smart cities: Improving data privacy and data security.

Lee, S. Y., Lee, J. Y., & Lee, B. I. (2006). Service composition techniques using data mining for ubiquitous computing environments. *International Journal of Computer Science and Network Security*, *6*(9), 110–117.

Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2016). The 2015 ukraine blackout: Implications for false data injection attacks. IEEE Transactions on Power Systems, 32(4), 3317-3318.

Liang, T., Zeng, B., Liu, J., Ye, L., & Zou, C. (2018). An unsupervised user behavior prediction algorithm based on machine learning and neural network for smart home. *IEEE Access*, *6*, 49237–49247. https://doi. org/10.1109/ACCESS.2018.2868984

Rayan, Z., Alfonse, M., & Salem, A. B. M. (2019). Machine learning approaches in smart health. Procedia Computer Science, 154, 361-368.

Manolopoulos, V., Tao, S., Rodriguez, S., Ismail, M., & Rusu, A. (2010). Mobitras: A mobile application for a smart traffic system, 365–368. https://doi.org/10.1109/NEWCAS.2010.5604010

Mashable. (2016). The singapore government wants to track cars using satellites and people are mad. Retrieved February 26, 2016, from https://mashable.com/2016/02/26/singapore-satellite-tracking-cars/?europe= true

Nations, U. (2018). World population projected to live in urban areas. Retrieved March 18, 2018, from https://www.un.org/development/desa/en/ news/population/2018-revision-of-world-urbanization-prospects.html

Popa, D., Pop, F., Serbanescu, C., & Castiglione, A. (2019). Deep learning model for home automation and energy reduction in a smart home environment platform. *Neural Computing and Applications*, *31*(5), 1317– 1337.

Rizwan, P., Suresh, K., & Babu, M. R. (2016). Real-time smart traffic management system for smart cities by using internet of things and big data. *2016 International Conference on Emerging Technological Trends (ICETT)*, 1–7. https://doi.org/10.1109/ICETT.2016.7873660

Rudin, C., Waltz, D., Anderson, R. N., Boulanger, A., Salleb-Aouissi, A., Chow, M., Dutta, H., Gross, P. N., Huang, B., Ierome, S., Isaac, D. F., Kressner, A., Passonneau, R. J., Radeva, A., & Wu, L. (2012). Machine learning for the new york city power grid. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *34*(2), 328–345. https://doi.org/10. 1109/TPAMI.2011.108

Schreiner, C. (2016). International case studies of smart cities: Rio de Janeiro, Brazil. *Inter-American Development Bank*.

Shahidehpour, M., Li, Z., & Ganji, M. (2018). Smart cities for a sustainable urbanization: Illuminating the need for establishing smart urban infrastructures. *IEEE Electrification Magazine*, *6*(2), 16–33. https://doi. org/10.1109/MELE.2018.2816840

Singh, K., & Singh Tomar, D. D. (2019). Architecture, enabling technologies, security and privacy, and applications of internet of things: A survey. *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018*, *4*(5), 642–646. https://doi.org/10.1109/I-SMAC.2018.8653708

Sookhak, M., Tang, H., He, Y., & Yu, F. R. (2019). Security and privacy of smart cities: A survey, research issues and challenges. *IEEE Communications Surveys Tutorials*, *21*(2), 1718–1743. https://doi.org/10.1109/COMST. 2018.2867288

Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the US power grid. The Electricity Journal, 30(3), 30-35.

Thakrit Panklib, T. V. (2016). Iot application for smart energy. *7*(2), 3–4.

Verkruisen, A. (2017). Privacy in smart cities. Retrieved December 6, 2017, from https://smartcityhub.com/collaborative-city/privacy-smart-cities/

Wilson, G. (2020). How smart cities can power a sustainability revolution. Retrieved October 14, 2020, from https://www.energydigital.com/smartenergy/how-smart-cities-can-power-sustainability-revolution

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*, 35365–35381. https://doi.org/10.1109/ACCESS. 2018.2836950

Zahin, A., Tan, L. T., & Hu, R. Q. (2019). Sensor-based human activity recognition for smart healthcare: A semi-supervised machine learning. In S. Han, L. Ye, & W. Meng (Eds.), *Artificial intelligence for communications and networks* (pp. 450–472). Springer International Publishing.

Zhang, H., Liu, B., & Wu, H. (2021). Smart grid cyber-physical attack and defense: a review. IEEE Access, 9, 29641-29659.