Article **Journal of Technology and Innovation**
December 2020, Vol.7 No.21 1-18

Intelligent mobility: a review of the cybersecurity of IoT in smart cities

Movilidad inteligente: una revisión sobre la ciberseguridad de IoT dentro de las ciudades inteligentes

VÁZQUEZ-DEL RÍO, Jorge Rubén†*, CARDEÑA-MORENO, Sergio Alejandro and VILLAFAÑA-DÍAZ, Luis Gerardo

Universidad Popular Autónoma del Estado de Puebla (UPAEP), Mexico.

ID 1st Author: *Jorge Rubén, Vázquez-Del Río* / **ORC ID:** 0000-0003-4620-9099

ID 1st Coauthor: *Sergio Alejandro, Cardeña-Moreno* / **ORC ID:** 0000-0001-5459-3743

ID 2nd Coauthor: *Luis Gerardo, Villafaña-Díaz* / **ORC ID:** 0000-0002-4130-9595

DOI: 10.35429/JTI.2020.21.7.1.18 Received July 10, 2020; Accepted December 30, 2020

Abstract

Objectives - This research aims to explore the various challenges of cybersecurity in the Internet of Things in a Smart Mobility framework within Smart Cities by reviewing the academic literature. Methodology - Through the review and analysis of the academic literature available in different databases to generate an empirical study, the prospective knowledge on strategy and technology that concatenates the concepts of the Internet of Things, Smart Mobility, and Smart Cities is derived. Contribution - Cybersecurity schemes in today's Internet of Things still present significant challenges arising from the lack of clarity in policies and strategies regarding the reliability of data collection by the various services present in the Smart Mobility framework.

Smart Cities, IoT, Smart Mobility

Resumen

Objetivos - El objetivo de esta investigación es explorar los distintos desafíos en materia de ciberseguridad en el Internet de las Cosas en un marco de referencia de la Movilidad Inteligente dentro de las Ciudades Inteligentes mediante la revisión de la literatura académica. Metodología – A través de la revisión y análisis de la literatura académica disponible en distintas bases de datos para generar un estudio empírico, se derivan los conocimientos prospectivos en materia de estrategia y tecnología que concatenan los conceptos de Internet de las Cosas, Movilidad Inteligente y Ciudades Inteligentes. Contribución – Los esquemas de ciberseguridad en el Internet de las Cosas actuales todavía presentan importantes retos derivados de la falta de claridad en las políticas y estrategias en materia de la confiabilidad en la recolección de datos por los diversos servicios presentes en el marco de referencia de la movilidad inteligente.

Ciudades Inteligentes, Internet de las Cosas, Movilidad Inteligente

Citation: VÁZQUEZ-DEL RÍO, Jorge Rubén, CARDEÑA-MORENO, Sergio Alejandro and VILLAFAÑA-DÍAZ, Luis Gerardo. Intelligent mobility: a review of the cybersecurity of IoT in smart cities. Journal of Technology and Innovation. 2020. 7-21:1-18.

* Correspondence to Author (Email: jorgeruben.vazquez@upaep.edu.mx)
† Researcher contributing as first author.

Introduction

The new fuel of the modern economy is artificial intelligence, the internet of things, and the processing of many data. This research presents a bibliographic review of scientific articles related to cybersecurity in Smart cities through the IoT and its implications on smart mobility. To analyze this problem, the factors implicit in the architecture of the IoT applied in smart cities are described by reviewing current cybersecurity mechanisms and their long-term challenges.

Smart mobility poses challenges in smart cities in terms of cybersecurity due to the increased use of Information and Communication Technologies (ICT), in this research we intend to explore these challenges by asking the following questions:

- Q1: What are the main challenges in cybersecurity for Smart mobility within Smart cities?

- Q2: How does cybersecurity influence the adoption of Smart mobility in Smart cities?

- Q3: Which security strategies should be adopted to facilitate the implementation of smart mobility?

This research is structured as follows: first, it is described the importance of new technological trends in industry 4.0 with a prospective focus on mobility and security, from the evolution of the internet into hyperconnectivity, remote cloud storage, to its wireless application in broadband in the smart cities. Later, an insight on smart mobility within smart cities is presented. Finally, the challenges of cybersecurity in smart mobility within smart cities' framework are described.

The goal of this research is to analyze the main scientific contributions published about the smart mobility on IoT cybersecurity within smart cities.

Strategic and technological prospective

Over time the technological evolution has incorporated different inputs for industrial processes; for example, in the first industrial revolution, the consumables were water and steam to mechanize production, followed by the second industrial revolution electric power used to create mass production. In the third industrial revolution, electronics and information technologies were incorporated to automate production. In the fourth industrial revolution, processes were digitized through the Internet, now the new fuel in the fifth industrial revolution is artificial intelligence, big data and, the Internet of Things (Kodama, 2018).

Mikulic & Stefanic (2018) mentioned that industry 4.0 represents the development and use of technology in its traditional model. They pointed out the trends that globalization sets by putting new challenges with existing resources and generating new concepts such as smart factories, cyber-physical systems, Internet of things, and smart products. With this, companies are lead to embrace new technologies to achieve compliance in consumers demanding high quality and added value. They presented an article identifying advantages and disadvantages of the implementation of technology considering the impact of the human factor, defining the relationship between industry 4.0 with efficient management, and its necessity to include the human element in all phases from design and implementation of technology.

Likewise, Kodama (2018) mentioned that the innovations required by the fourth industrial revolution would be characterized by the accumulation of innovations, the evolution of technology instead of disruptive innovations, and merging the lines between the physical-digital, as well as the biological.

The Japanese government proposed the phrase Society 5.0 to refer to the combination of social problem solving and the economic progress made by industry 4.0.

Dash et al. (2019) conducted a study highlighting the development of skills of the fourth industrial revolution and the internet of things. The authors mentioned that technological advances are marked by the acceleration of innovation and artificial intelligence estimating 30 billion devices in the year 2025.

ISSN 2410-3993

The data was obtained through a comparison of standards, theoretical evidence, and challenges in the assimilation of new technological trends. It was found that India's innovation policies are based on digital empowerment through the adoption of emerging technologies, making the workforce more efficient and productive.

In recent years technological trends have driven the growth of the smart city concept (i-city). Smart cities are a model of economic development through the use of information and communication technologies (ICT) that seek to improve society's quality of life through sustainable processes lasting over time.

In the research by Bran & Rendón (2016), they described the key elements to implement a smart territory in Colombia, from a technology-based perspective. The methodology used was technology watch and competitive intelligence by economic activity, entrepreneurship, and innovation, region, and population. The results detected two segments for its implementation; the first are national and international public policy factors that facilitate the link between technological development, economy, and social welfare. The second segment is the technical and financial socio-cultural adoption factor. The study concludes with a proposal of technical, strategic, and financial requirements to implement an i-city in Bogotá, Medellín, Cali, or Barranquilla.

Thus, Pise (2019) presented a study of trends in Information and Communication Technologies (ICT) in remote cloud storage. A literature review methodology was used. The results were four types of cloud according to use: public, private, hybrid, and community cloud. These are composed of three primary services containing infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

The work concludes with the various benefits offered by this trend in reducing operating costs and global hyperconnectivity.

Serrano Cobos (2016) described technological innovations and trends on the Internet, using a methodology of holistic analysis in automation, computerization, and digitalization through the adoption of technology.

The booming technology segments are: a) artificial intelligence and machine learning, b) quantum computer, IoT, c) virtual reality, multi-channel (dialnet), d) partitioning (walled gardening), e) immediacy, f) personalization and, g) big data. The work concludes by highlighting the inexhaustible opportunities in the tools as well as services of the Internet.

Lee et al. (2018) analysed the growth of computer systems, the importance of generating data with higher reliability in computer infrastructure, and finally described trends in open science and big data. They used a methodology based on the analysis of the genome in the material through machine learning, statistics, data mining, and artificial intelligence. The research provided a scheme between metadata, security, search, and analysis in the IT infrastructure trend.

The high demand for wireless communications and personalized services has experienced exponential growth in recent years. Sethi & Paramita (2016) analyzed the trends in next-generation, describing the opportunities in architecture and infrastructure IoT and D2D as the development of hybrid satellites with less fluctuation delay, due to the increase of traffic in applications of over the top (OTT) content for management and minimum human intervention.

The clear example of the development of wireless technology is the 5G mobile broadband, in the research proposed by Lawrence & Barnes (2019) they describe the advantages of the technology, such as the improvement in the speed of data transfer without delays and without failures as well as the increase of capacities in connectivity. On the other hand, the 5G network will boost the exploitation of the IoT industry, since it contains integrated sensors that collect and share data through closed private Internet connections. The 5G network, like the IoT, is expected to transform the world into smart cities to drive economic growth, increase operational efficiency, improve government services, and public welfare through the use of information and communication technologies.

One application in smart mobility in smart cities is the AV drive is based on sensor systems and processing capacity to extract, transform, and load data systems.

ISSN 2410-3993

It is predicted that the introduction of autonomous vehicles will reduce the number of accidents and environmental pollutants, through three streams, the development of autonomous vehicle driving systems, the adoption of transport sharing services, and the switching of vehicles to electric power (OECD, 2019).

Another application in the mobility of intelligent cities is cybersecurity, the protection of computer infrastructure that aims to minimize possible external attacks on servers, software, metadatabase, and files. Thanks to artificial intelligence, it allows monitoring and real-time security (Obeidat et al., 2015).

Smart Mobility through IoT in Smart Cities

The increase in population in cities has presented challenges in mobility within cities. Thus, urban researchers and developers seek to provide cities with a technological breakthrough to generate an interconnected environment, commonly through IoT (Faria et al., 2017). Faria et al. (2017) provided a review of Smart Cities and Smart Mobility concepts through IoT. They first offered the elements that the idea of Smart Mobility should contain. The definitions provided by different authors recognize that it is necessary to include fields of study in (ICT), Intelligent Transport Systems, Automotive Technology, and Embedded Systems.

Similarly, they identified different areas of interest within Smart Mobility: driving safety, urban mobility and collective transport, electric mobility (electromobility), green mobility, and intelligent payment systems.

Benevolo et al. (2016) carried out, from an (ICT) perspective, a holistic analysis of the actions to be taken by intelligent mobility initiatives to try to define the goals that the these should establish; they considered three items: a) the main actors of the efforts, b) the intensity of use of ICT in the initiatives and c) the goals and benefits of the actions. The analysis of the initiatives approached from four viewpoints: a) public mobility (mass transport), b) private and commercial mobility, c) mobility support (infrastructure and policies), and d) intelligent transport systems.

The results obtained established a correlation between the maturity of smart mobility systems and ICTs; i.e., ICTs are not necessarily representative during the implementation stage of smart mobility initiatives. However, they become essential when intelligent mobility systems become more complex and extensive.

A flexible transport system provides better transport performance in rural areas due to cost efficiency and technological development. Porru et al. (2020) presented a study of sustainable mobility models in rural areas of Central Europe based on public transport as part of the Interreg Central Europe's "RUMOBIL" project. The study focused on mobility solutions through IoT by analysing ten previous projects including a) recent unfinished projects for defining the state of the art of the subject, b) projects with an investment of millions of Euros for differentiating from smaller mobility projects, c) projects covering rural and urban contexts for establishing a point of comparison and d) pilot projects within the meaning of "RUMOBIL." Thus, the authors identified an opportunity for improvement by adjusting and balancing the service within the operational area of the public transport through the comparison of various IoT applications for users and designers in rural and urban contexts, as well as the complexity of urban mobility in the same.

On the matter of technologies, Dey et al. (2016) evaluated different wireless communication technologies (Wi-Fi, DSRC, and LTE) applied to Connected Vehicle Technology (CVT), mainly to communications between vehicles (vehicle-to-vehicle - V2V) and vehicles and infrastructure (vehicle-to-infrastructure - V2I). Two pilot case studies were taken as a framework: data collection and collision detection, both on a heterogeneous network. In the first case study, data collection was carried out by V2I communication; in the second case, V2V communication was used to alert vehicles in the vicinity. The two case studies demonstrated the benefit of using a heterogeneous network in V2V and V2I communications where the use of Wi-Fi and LTE extends communication coverage. Likewise, the combination of different communication protocols generates higher reliability in data transmission.

ISSN 2410-3993

Intelligent mobility in Smart Cities involves the implementation of technologies related to the use and interpretation of information and communication systems so that the elements that move in a particular area remain connected to each other. Ning et al. (2017) described the concept of the Vehicular Social Network (VSN) and its relationship with the Internet of Vehicles (IoVs). The authors indicated that a VSN not only involves conventional V2V and V2I communications, but they interrelate it with IoVs and social networks to interconnect vehicle users. A case study was presented in which the detection of traffic anomalies employing mass detection through the mobile devices of public transport users was analysed. The results obtained showed some problematic aspects to be overcome, such as the technological and human challenges (i.e., use of resources and apathy from users to participate), the existence of a large amount of data and analysis overhead, and security and privacy aspects.

Advances in V2V and V2I connectivity developments allow transport systems to be conceived beyond their mobility function. Rambow & Rambow-Hoeschele (2018) examined the vehicle's transformation into what they called a "third living space." The authors identified four technological trends in transport in an IoT framework: a) electrification, b) autonomous driving, c) services and, d) connectivity. Once the trends were identified, the authors focused on the connectivity characteristics that enable vehicle transformation. They recognize that with the increase of connectivity standards, it will be necessary to increase the requirement of user identity data (passwords, keys and, biometrics) so that computer security standards will have to increase as well.

Once the user is identified, the authors distinguish five fields of application. The first field is personalized user assistance based on artificial intelligence, which gives rise to the second field, monitoring passengers' physical and mental (emotional) health parameters through different on-board sensors. The third field concerns user comfort; biometric data can be used to make automatic adjustments within the vehicle and to serve as an authentication system.

The development of vehicle connectivity covers security issues, so it is possible to reduce vehicle theft as the fourth field of application. Finally, the fifth field contemplates the legal aspects since it is an application that collects personal data from users so that it seeks to avoid any fraud.

While vehicle IoT connectivity applications to improve mobility in urban and rural contexts are advancing and becoming more and more a reality, technologies that improve the energy efficiency of transport are emerging in response to the need to reduce dependence on fossil fuels and the generation of polluting gases. By 2016, more than 700,000 electric vehicles have been identified worldwide with a growth trend in sales (Kaldellis et al., 2017). This growth trend allows for the concatenation of intelligent transport systems and efficient energy management. In this way, electric vehicles (EVs) can act as agents of electricity generation responding to consumer needs in the network under a vehicle-to-grid (V2G) scheme (Nikitas et al., 2017).

Sechilariu et al. (2017) proposed an energy model for electric vehicles based on smart charging stations. The proposed model is based on the existence of a smart grid and renewable energy sources. One of the smart charging systems' objectives is to control and optimize the flow of energy with the instantaneous demand of the public (general users of the network). With this in mind, the authors define three strategies: a) V2G (Vehicle-to-grid), b) V2B (vehicle-to-building) and, c) i2B (intelligent charging station-to-building). The first two strategies are based on the discharge of the vehicle's batteries into the public grid and into buildings, respectively. The third is aimed at supplying electricity to buildings from the recharging stations.

The authors recognized several implementation challenges: urban scaling, infrastructure scaling, associated public services, social impact, and research. Thus, they identified innovative contributions to energy management in renewable energy systems, electromobility, public services and planning, regional analysis, social acceptance and, experimentation; within the context of smart cities.

ISSN 2410-3993

Internet of Things (IoT)

In a globalized world, Information and Communication Technologies (ICT) represent the backbone of countries and organizations. Nord et al. (2019) considered the Internet of Things (IoT) as a disruptive technology that integrates connectivity, infrastructure, applications, and security services within its ecosystem.

A first definition of the IoT, according to Nord et al. (2019), has to do with the interconnection of computer equipment and devices through the Internet, which facilitates the generation of data and its subsequent analysis. This connectivity makes it easier for people and devices to establish communication at any time, place, network, and service (Samih, 2019).

Following the previous definition, we express the following concern: establishing clear operating limits and standardizing criteria to establish the integration of devices in the network.

We find another type of definition for the IoT, according to Obaidat et al. (2019) describes it as a social network of connected devices, with an interaction between people and these, but also between themselves. Alam (2018), based on information from statistic, estimated a total of 75 million devices interconnected to the IoT for the year 2025.

Making an association with the above, the inclusion of the 5G network in the countries will be of great help to support first the enormous number of devices connected to the IoT, second that the data transmission and reception speeds will increase considerably allowing an improvement in communications online and within Smart cities.

However, and as we address it later, there is great concern in the field of cybersecurity due to the variants of existing attacks to compromise the information and interconnected infrastructure in the IoT.

For example, there is currently a portal where we can locate any device connected to the network or IoT, identifying the geographical location, vulnerabilities, and other vital information that serves as an element to establish an attack.

According to Zeadally et al. (2019), IoT is a real-world (physical) integration with computer equipment that allows the execution of systems connected to the internet, providing better efficiency with less people participation.

Architecture

This research work makes a model proposal to exemplify the IoT architecture, based on the reviews made of the articles consulted where the existence of three layers is mentioned as seen in Figure 1.

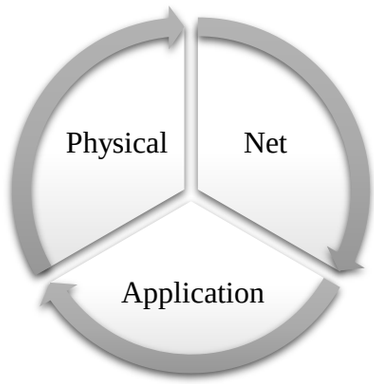

Figure 1 Internet of things architecture model
Source: Own elaboration according to the references consulted, 2020

The previous scheme is based on Open System Interconnection (OSI) to identify the most commonly used layers. The physical layer is in charge of the connections, the network layer for data processing, and the application layer in charge of offering services.

Another way to classify the structure of the IoT is through the proposal of Pratap et al. (2020), who considered domain, layer, and commercial or industrial architectures in the modern era.

The current architecture models start from an initial base; according to Gubbi et al. (2013), the first IoT architecture model considered the following layers: base layer (sensors), information processing layer (cloud), and an application layer (user interaction).

ISSN 2410-3993

Various literature exemplifies 3, 4, 5, or 7 layer architecture models for the IoT; finally, each one will adapt the best scheme to exemplify their infrastructure. Our research will base ourselves on the proposal made in a three-layer model, considering it sufficient for this work.

In this sense, the IoT ecosystem is made up of users who use the network, information systems, and devices that are tangible or intangible, communicating with each other using a standard protocol. The IoT architecture scheme proposed by Zeadally et al. (2019), comprises application layer (intelligent traffic and processing), network layer (4G, internet and WLAN) and sensing layer (sensors and WiFi).

As can be seen in the lower layer, we find tangible (physical) devices, such as the sensors that collect and send data, an essential part of the IoT concept, subsequently communication between the application layers is established through an interlocutor (network layer) and the physical one allowing the processing of all the data sent making use of means in the cloud, equipment located in the organizations and/or government agencies specifically for the interpretation of the information of the vehicles, their drivers or any other factor related to the mobility in Smart cities.

Application in smart cities

Smart cities involve the use of collective intelligence (Qian et al., 2019), connecting physical, information technology, social and, business infrastructures. Likewise, something important in the interconnection of infrastructures, is the implementation of sensors for permanent monitoring of services, sending data in real-time for decision-making. Rogers (1983) mentioned that the adoption and diffusion of technology is the use of innovation through communication between the members of society.

According to Atzori et al. (2010) and Obaidat et al. (2020), the IoT applications are classified into four domains: transport and logistics, medical care, homes or offices, and personal or social. For the present work, we focus on the first one, describing the application environment of the IoT in mobility, security, and how societies coexist in a smart city.

In this sense, it is mentioned that the implementation of the IoT in public transport generates remarkable efficiency; however, special attention must be paid to the risks that may arise from the replacement of people in certain activities (Brous et al., 2020).

It is important to mention that the Smart City concept is not unique to the main cities of the countries. The implementation and adoption of technology (IoT) that allows automation and monitoring of services are permeable to communities and/or municipalities, according to Hassan & Awad (2018).

According to Satyakrishna (2018), the IoT is used for better use of technologies in Smart cities, improving vehicle mobility, mitigating accidents, optimizing the transfer times of people, and having a higher quality of life compared to current problems in big cities. The boom in autonomous mobility has seen growth in recent years thanks to the implementation of IoT and technological innovations. According to Chen & Englund (2017), drivers experienced a reduction in driving times of approximately 50 million hours per year.

Something important to mention with the implementation of technology in-vehicle control has to do with response times in the emergency services Satyakrishna & Sagar (2018) and Jamjoom et al. (2018), through better-coordinated action taking advantage of the information provided by the sensors.

Security and privacy

It is essential to guarantee the reliability, integrity, and availability in a Smart city. As mentioned, the concept involves the interconnection of devices through the Internet; for this situation, people's information and data must be kept safe (Lee & Lee, 2015). The above was based on their survey in which they identified challenges in security and privacy issues.

The IoT is a vast field of action, for this reason, attackers (hackers) find an up-and-coming and attractive niche of opportunity, also considering what was indicated by Frustaci et al. (2018) that devices for this technology hardly They are updated, and even less have security patches Yu et al. (2018).

ISSN 2410-3993

Another important aspect has to do with the encryption of data stored and/or sent over the network because the capabilities of hardware and software are limited in most cases, we find one more problem to mitigate a security incident and, is that according to Obaidat et al. (2020) the capacities to perform cryptographic protocol processing are limited.

In this sense, Guoet et al. (2018) proposed a security model made up of five layers: end-user, perimeter and central network, service, and storage to end the administration model, however, according to Obaidat et al. (2019) his proposal considered six layers: application, cloud, information transmission, link information, internal communications and finally that of the final device. Based on the two architectures proposed below, we present (Figure 2) the following proposed security model for the IoT.

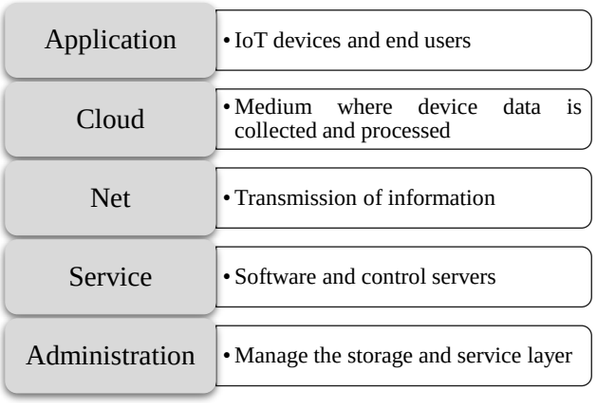

Figure 2 The security model for the internet of things
Source: Own elaboration according to the references consulted, 2020

The above also makes sense in the aspect of mobility; if there are no security mechanisms in networks and applications, motorists would be likely to be monitored or suffer an accident caused, according to Ali et al. (2018).

According to Stellios et al. (2018), we must bear in mind that IoT devices will sometimes be the target of an attack. However, in other cases, they will be the means to escalate an attack towards another device and/or target user. The above makes sense since one of the techniques used in hacking is the so-called man in the middle, through which an attacker compromises a device of no importance to them, but allows them to enter the network and/or environment to channel his attack towards the infrastructure that will make a user a profit.

Given the scenarios described above, we do not have an end-to-end encryption process (Sridhar & Smys, 2017), considering that most of the devices in the IoT will be under wireless connectivity. Users, organizations, and other instances of the society under the concept of Smart city will be more prone to an attack derived from the exploitation of existing vulnerabilities in hardware and/or software.

Over the years, the concept of transportation has taken on various meanings and applications. Implementing strategies to meet the needs (moving from one place to another) of people has generated a particular interest over the years.

In our times without a stable implementation of autonomous transport, the trends in technological innovation are closer to that futuristic reality, however, there is another area (cybersecurity) in which intense work must be done to prevent cyber-attack vulnerabilities.

The aforementioned by Mahdi et al. (2020) becomes vital to maintain security strategies in topics such as cryptography, detection of vulnerabilities in devices, applications, and malicious programs (Malware).

Every cybersecurity scheme starts from three fundamental aspects, confidentiality, integrity, and availability (CID), under international standards and frameworks. Taking the above as a reference and implementing cybersecurity within Smart cities considers the three CID concepts.

Confidentiality. All data that travels through the network in Smart cities must have a high degree of confidentiality, i.e., no other person may have access to personal and sensitive information about them, motorists must not be monitored, tracked or video recorded within out of or out of their vehicles.

Integrity. The data collected by the various sensors and devices connected to the IoT in Smart cities should not be altered during transmission over the network and within each device, therefore the importance of having cryptographic mechanisms to guarantee its integrity.

ISSN 2410-3993

Availability. The information in Smart cities must be permanently online, perhaps considering an interruption limit that does not imply a high impact situation in processes, strategies, vehicle control, among others.

The previous concepts involve the subject of this research work, the connectivity of V2V, V2I, and vehicle to the user (V2U), as mentioned by Mahdi et al. (2020).

It should be mentioned that the purpose of the investigation does not imply describing in detail each cyber-attack technique and/or implementation mechanism to mitigate a critical situation to the IoT infrastructure.

Considering the architecture model (physical layer, network, and application) proposed in our research, Obaidat et al. (2020) identify attacks and challenges to consider within the defined infrastructure. In the first layer (physical), we have unlimited resources and a free access environment within the interconnection of the devices, which presents us with a vulnerable scenario (without protection) to any type and technique of attack using exploits to compromise a car and the information it contains.

Perhaps we wonder how they could compromise a vehicle (device considered in our research), a coffee maker, a server, an end-user computer, a smart TV or any other means connected to the IoT, to exemplify the available scopes, just Make a query on the Shodan portal, where an analysis is made of everything that is connected in the world of the Internet, which is why it is the first search engine in the world for devices connected to the IoT. Here we find the existing vulnerabilities in hardware and software, being an opportunity gap for attackers and also for those dedicated to cybersecurity.

As we have mentioned in the second layer (network) is the point of intercommunication between the first layer and the last one of our provided model. This layer is where the data flow is captured by the various sensors that compile everything that occurs within a vehicle, between users or vehicle monitoring means in Smart cities. The attacks that hackers can carry out at this layer are denials of service (DoS) or distributed denials of services (DDoS).

The difference mainly lies in the number of computers or IP (Internet Protocol) addresses that make service requests simultaneously consuming the medium's resources, causing saturation in the capacity of response and rejection of the requests made in the application of the vehicles or their users.

Finally, in the third layer (application) in charge of processing the data provided by the devices (vehicles), it can receive targeted attacks in the applications in charge of the process initially mentioned. Focusing again on the Shodan portal, for example, we can observe open ports, enabled services, and detected vulnerabilities in servers that contain all the information of the users concerning vehicle control; such as vehicle data, user data, videos, and/or images that are generated in the IoT and Smart cities.

Das et al. (2019) defined eight actions to help mitigate cybersecurity risks in Smart cities through the implementation of the IoT; below, we refer to some actions incorporating technical and methodological aspects.

First, a threat assessment must be carried out through a mechanism based on international methodologies, the use of documents prepared by countries in Europe and our American continent is known. For example, the use of methodologies to carry out a risk analysis (Magerit), Identification of possible threats through reference guides from the National Institute of Standards and Technology (NIST), or the use of the ISO 27000 family of standards, documenting the existing risks and identified gaps.

Implement a permanent cybersecurity monitoring mechanism, also supporting itself through the methodologies mentioned above and standards, but incorporating security governance through the Control Objectives for Information and related Technology (Cobit).

Security in vehicular communications presents a significant opportunity and challenges to solve, according to Zeinab et al. (2019) Automobiles now integrate technology that equates them with a computer (advanced operating system) and is not just mechanical systems.

ISSN 2410-3993

A fundamental part of their technological innovation is that they are now able to interconnect with other vehicles, synchronize with cell phones, provide aspects of the weather, traffic, and other services provided by the new networks and the IoT.

Among the security incidents that have occurred in vehicles interconnected to the network, are remote unlocking, brake sequestration, and access to the Controller Area Network (CAN) bus to send illegal messages. Therefore, below, present the four vehicle cybersecurity challenges, according to Onishi (2012):

• Limited connectivity: refers to the ability to update the vehicle's software over the air, ensuring its protection because it will have the latest security patches for its applications.

- Limited computational performance: vehicles have limited performance, compared to a computer, as they have a longer service life, withstand higher temperatures and vibrations; therefore, some cybersecurity solutions will be unlikely to be implemented.

- Scenarios of attack and unpredictable threats: the vehicle architecture presents multiple entry routes to it; for example, there are vehicle databases, remote communications, and spare parts. These scenarios hardly controlled by the vehicle owner can generate security incidents using vulnerabilities through any of them.

- Risk to the lives of drivers and/or passengers: any physical and/or applicative means of the uninsured vehicle represents a critical scenario for any of its occupants, even considering external persons such as pedestrians.

Onishi (2012) defined three additional layers representing the Autonomous Vehicular Sensing-Communication-Control (AutoVSCC) framework, considering as part of the detection layer the sensors (inertia or radar) that would be vulnerable to a counterfeiting attack and/or espionage. The communication layer (automotive network or in-vehicle network) is vulnerable to communications between and within vehicles (people) through message manipulation.

Finally, a control layer that can initially be affected by the previous two, where the speed, direction, and other control processes of the vehicle takes place.

In this vehicular architecture, there is an ad hoc network called VANET (Vehicular Ad-Hoc Network), made up of two wireless nodes: on-board units (OBU) and road units (RSU).

The OBU represents a wireless transmitter installed in the vehicle, which enables V2X communication (vehicle-to-vehicle V2V and vehicle-to-infrastructure V2I) and with RSUs, which are roadside devices that provide internet connectivity by providing traffic information. The security part in this architecture is carried out by trusted authorities (TA), which carry out processes to confirm the authenticity of incoming and outgoing messages from the vehicle and remove malicious nodes within the VANET.

Due to the aforementioned, concepts related to confidentiality, integrity, and availability become of new importance. There is a controller area (CAN) that is part of several protocols such as the local interconnection network (LIN), the transport of media-oriented systems (MOST), and the Ethernet network itself. Part of the obstacles with CAN has to do with sending messages with relevant data from the medium to all existing nodes (Zeinab et al., 2019) without making a comparison, differentiation, or perhaps a risk analysis that they could present before sending the information. Thus, the medium is insecure since there may be man-in-the-middle attacks capturing the information traffic to direct it to another place, compromising its integrity or merely reading the messages sent to harm users.

A variant of attack in CAN is a denial of service (DoS), according to Liu et al. (2017), this becomes evident when several important messages block those messages sent in a legitimate. However, a low priority, manipulated by attackers that allow them to have control of the vehicle.

ISSN 2410-3993

According to Choi et al. (2018), another measure to mitigate a security incident has to do with the implementation of an Intrusion Detection System (IDS), which allows the system to defend against attacks such as masking, denial of service, among other techniques mentioned in the present work.

Through IDS, we can visualize an Artificial Intelligence application since modern systems include implementations that allow training of the vehicle system to identify malicious signals and/or messages. The inclusion of algorithms in Machine Learning, such as supervised or unsupervised, allows the establishment of classification criteria to identify possible attacks on the security of the vehicle infrastructure and its applications, mitigating the risks and guaranteeing the confidentiality, integrity, and availability of the information that web trip.

Precisely entering this work into disruptive technologies (Machine Learning) to improve cybersecurity mechanisms, these application models require variables in large quantities, as explained below. For a Machine Learning-based model to work efficiently, part of its achievement has to do with establishing the algorithm to be used. The tests carried out in its training using part of the information in the formation of the development environment and the other proportion for validating in a means of productivity or real implementation, making comparisons independently of the trained model to confirm that its performance is correct.

However, the algorithms must integrate as many variables and data as possible; without this, it would be challenging to implement an AI-based mechanism to mitigate security incidents.

In this context, Liang et al. (2019) and Ye et al. (2018) mention that the amount of information generated in new-generation vehicles, by incorporating the interconnection of devices in the IoT and Smart cities, will generate a large number of terabytes of operational data and automotive diagnostics, allowing the implementation of security strategies for vehicle platforms and the cloud.

As in any implementation of a solution based on Machine Learning, it is essential to have three elements, specify the type of situation (classification or regression), define what learning model will be used (supervised, unsupervised and reinforcement), to conclude with an architecture (decision trees) that provide greater confidence in the analysis and predictions that are needed (Zeinab et al., 2019).

Next, we present the following international standards and frameworks that must be considered in cybersecurity in Smart cities. Table 1.

Standard or framework	Application
BS 10012: 2009 - Specification for a personal information management system.	Manage the personal information of individuals in an organization, regarding data protection.
ISO / IEC 27000: 2016 - Information technology, information security techniques, management systems, overview, and vocabulary.	Providing definitions of commonly used terms describes how an information security management system (ISMS) should operate.
ISO / IEC 27001: 2013 - Information technology, information security techniques, management systems, and requirements.	Cover areas beyond cybersecurity.
ISO / IEC 27002: 2013 - Information technology, security techniques, code of practice for information security controls.	Provide detailed descriptions of the controls listed in Annex A of ISO / IEC 27001: 2013.
ISO / IEC 27003: 2017 - Information technology, security techniques, implementation guidance for information security management systems.	Guide planning and information security management system aligned with ISO / IEC 27001.
ISO / IEC 27004: 2009 - Information technology, security techniques, information security management measurements.	Apply metrics and measurements of ISO / IEC 27001.
ISO / IEC 27005: 2011 - Information technology, security techniques, information security risk management.	Apply a risk management program in the information.
ISO / IEC 27006: 2015 - Information technology, security techniques, requirements for bodies that provide auditing and certification of information security management systems.	Guides those bodies that provide ISO / IEC 27001 certification.

ISSN 2410-3993

ISO / IEC 27007: 2011 - Information technology, security techniques, guidelines for the audit of information security management systems.	Guides those bodies that provide ISO / IEC 27001 certification.
ISO / IEC 27010: 2015 - Information security management systems, information security management for communications between organizations or dependencies.	Exchange information securely between organizations and / or dependencies.
ISO / IEC 27011: 2008 - Information technology, security techniques, information security management guidelines for telecommunications organizations based on ISO / IEC 27002.	Comply with the ISMS reference requirements of confidentiality, integrity, availability, and any other relevant security property of telecommunications services.
ISO / IEC 27014: 2013 - Information technology, security techniques, information security governance.	Make decisions on information security issues in support of strategic organizational objectives.
ISO / IEC 27017: 2015 - Information technology, security techniques, code of practice for information security controls based on ISO / IEC 27002 for cloud services.	Apply to organizations that want to become cloud service providers, identifying their responsibilities to ensure the certification of security controls related to cloud services by integrating necessary security policies, practices, and controls.
ISO / IEC 27018: 2014 - Information technology, security techniques, code of practice for the protection of personally identifiable information (PII), in public clouds acting as PII processors.	Apply to all types and sizes of organizations, including public and private companies, government entities, and non-profit organizations, that provide information processing services through cloud computing.
ISO / IEC 27032: 2012 - Information technology, security techniques, guidelines for cybersecurity.	Invest in protection against cybersecurity issues.
ISO / IEC 27033 1: 2015 - Information technology, security techniques, network security, overview, and concepts.	Visualize the main problems that organizations may face.
ISO / IEC 27033 2: 2012 - Information technology, security techniques, guidelines for the design and implementation of network security.	Define the network security requirements that are likely to be required and provide a checklist.
ISO / IEC 27033 3: 2010 - Information technology, security techniques, network security, reference network scenarios, threats, design techniques, and control problems.	Consider the design of safety nets and examine the threats and possible controls associated with them.
ISO / IEC 27033 4: 2014 - Information technology, security techniques, network security, protection of communications between networks through secure gateways.	Guide how to protect communications between networks using security gateways and firewalls and introduces the concept of intrusion detection systems.
ISO / IEC 27033 5: 2013 - Information technology, security techniques, network security, protection of communications through networks through virtual private networks (VPN).	Protect network interconnects and how to connect remote users by providing a VPN.
ISO / IEC 27034 1: 2011 - Information technology, security techniques, application security, overview, and concepts.	Set the stage for secure application development, and in particular deals with the application security management process.
ISO / IEC 27034 2: 2015 - Information technology, security techniques, application security, the regulatory framework of the organization.	Provide more detailed instructions on implementing application security, including a detailed description of the application security life cycle reference model.
ISO / IEC 27036 1: 2014 - Information technology, security techniques, information security for supplier relations, overview, and concepts.	Examine the security requirements for the relationship between organizations and their suppliers.
ISO / IEC 27036 2: 2014 - Information technology, security techniques, information security for supplier relations, requirements.	Establish the technical security requirements that must be agreed and managed between an organization and its suppliers.
ISO / IEC 27036 3: 2013 - Information technology, security techniques, information security for supplier relations, guidelines for the security of the information and communication technology supply chain.	Guide managing the complex risk environment.

ISSN 2410-3993

ISO / IEC 27036 4: 2016 - Information technology, security techniques, information security for supplier relations Part 4: Guidelines for the security of cloud services.	Provide guidance to cloud service providers on information security risks associated with using cloud services and responding to the specific risks of acquiring or providing cloud services that may have an impact on the information security in organizations that use these services.
ISO / IEC 27039: 2015 - Information technology, security techniques, selection, deployment, and operations of intrusion detection and prevention systems (IDPs).	Provide an analysis of host and network traffic and/or audit trails for specific attack signatures or patterns that typically indicate malicious or suspicious intent. This standard provides guidelines for the effective selection, implementation, and operation of IDPs, as well as fundamental knowledge of IDPs.
ISO / IEC 27040: 2015 - Information technology, security techniques, storage security.	Apply to all data owners, IT managers, and security officers, from small businesses to organizations, as well as general and specialized data warehouse owners, and is particularly relevant to data destruction services.
ISO / IEC 17788: 2014 - Information technology, cloud computing, overview, and vocabulary.	Provide information on your application.
ISO / IEC 17789: 2014 - Information technology, cloud computing, reference architecture.	Apply from small businesses to organizations, and all kinds of cloud providers and partner organizations, such as software developers and auditors.
ISO / IEC 29100: 2011 - Information technology, security techniques, privacy framework.	Provide a high-level framework for the protection of personally identifiable information within IT systems.
ISO / IEC 29101: 2013 - Information technology, security techniques, privacy architecture framework.	Guide the entities involved in the specification, acquisition, architecture, design, testing, maintenance, administration, and operation of IT systems.

Table 1 ISO / IEC standards for the protection of the privacy of information in the IoT media in Smart cities
Source: Own elaboration according to the references consulted, 2020

The standards and specifications indicate clear procedures on what must be done to mitigate cybersecurity incidents in Smart cities that use the IoT. International recommendations are the responsibility of the International Organization for Standardization (ISO). The publication of updates and/or new recommendations can take several years and are carried out by specialists in cybersecurity issues.

Finally, to complement the recommendations we make in this research to mitigate cybersecurity incidents, it has to do with business continuity (that vehicle control data and information remain available, complete, and reliable) and recovery from a disaster.

The first business continuity standard (BCP) was PAS 56 of the BSI (United Kingdom) in 2003; it was later replaced by BS 25999 Part 1: Business Continuity Management in 2006 and later by BS 25999 Part 2: Business continuity management one year later. In 2014 both were obsolete due to the implementation of ISO / IEC 22301 and ISO / IEC 22313, their most current versions being those of 2014.

The National Institute of Standards and Technology (NIST) provides guides, manuals, and guidelines to guarantee the protection of information and other aspects implicit in the IoT and its processes within the scope of the study of Smart cities and risk scenarios in cybersecurity that we have described.

The NIST SP 800-53A is a guide for evaluating security controls on the information systems of organizations. On the other hand, there is the NIST SP 800-83 that provides information regarding the prevention of security incidents caused by malware. In addition, NIST SP 800-153 mentions guidelines for the protection of wireless local area networks (WLANs).

Methodology

The method used is highly relevant for empirical studies and the construction of the theory, databases such as IEEE, MDPI, SPRINGER, EBSCO, CONRICYT, THOMSON REUTERS, SCIENCE DIRECT, SCOPUS and WEB OF SCIENCE were used.

ISSN 2410-3993

A total of 157 articles were analyzed, of which 54 objectively fulfilled the field of study in strategic and technological foresight, intelligent mobility through the IoT in intelligent cities, security, and privacy in the application in intelligent cities. Likewise, different Boolean combinations AND, OR, and truncation * were applied for the filtering of relevant information? helping to gather specific information.

Figure 3 Search analysis structure
Source: Own elaboration, 2020

The search was carried out in a period from 2015 to 2020, with the following combinations of keywords: strategic and technological perspective in smart cities, technology trends in smart cities, technological intelligence in smart cities, security in smart cities, strategic and technological perspective, smart mobility through IoT in smart cities, security and privacy applications in smart cities, smart mobility, smart city, electro-mobility, IoT, vehicle communications, v2v, v2i, smart grid.

Results

The development as well as the use of technology in the new economic model within intelligent cities is strengthened by the accumulation of technological goods, the acceleration of innovation and the estimation of artificial intelligence.

At first, in the context of IoT and vehicle connectivity technology, the most used communication coverage technologies are identified as Wi-Fi, DSRC, and 5G. Once these technologies are established, communication forms in the framework of intelligent mobility correspond mainly to vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I).

On the other hand, there are other forms of vehicular communication from the perspective of electromobility (electric vehicles), which mainly involves vehicle to grid (V2G) and vehicle to building (V2B). These schemes, in addition to providing information on vehicle fleets, contribute to energy management strategies.

The great challenges presented by cybersecurity in Smart cities applied to mobility is undoubtedly the confidentiality of all the data collected by the various devices and sensors, added to the integrity of these to mitigate that users and vehicles are compromised in the three layers of architecture for the IoT established in this work.

As observed in the work carried out, the current cybersecurity schemes present important gaps, due to the importance that has been given to hardware and software without considering clear policies and strategies that provide an overview of cybersecurity.

It is important to remember that the interconnection between vehicles, vehicles, and people, and the people among themselves generate, together with the other schemes, a large amount of data that travels over the IoT network. Due to the foregoing, in the absence of a clear cybersecurity strategy backed by international norms and frameworks, security breaches will be more evident, increasing risks in the IoT environment, creating a niche of opportunity for attackers who will find diversity. of vulnerabilities in hardware and software.

The revised architecture models for IoT security show homogeneity, the proposals refer to three layers (physical, network, and application), the second being important because it distributes the data collected by the devices. In this sense, the inclusion of controls under the ISO / IEC standard becomes relevant, for example, considering those related to security techniques and architecture, using private networks, implementation of intrusion detection and prevention systems, storage security for the cloud and the organizations own data center and the telecommunications part in which the service providers must guarantee the confidentiality, integrity, and availability of the information.

ISSN 2410-3993

Considering the technology that integrates a vehicle in Smart cities, a fundamental part is the inclusion of embedded operating systems which carry out specific activities, that is, the cybersecurity of an autonomous vehicle should be centralized in the systems it integrates, telecommunications (networks), connection protocols and regulations that manufacturers must consider to offer their customers an environment of security and technological innovation, allowing interconnection through the IoT architecture in a secure manner.

Conclusions

By definition, smart cities take advantage of advances in digital technology to generate a communication infrastructure between various devices for the benefit of their inhabitants. This bibliographic review shows, in the first instance, various interconnectivity schemes through ICTs between different actors in the mobility scheme within intelligent cities. The purpose of this interconnectivity is to provide mobility solutions in a context where cities are increasingly saturated. Specifically, the interconnectivity of sensors in mobile systems through the IoT, together with the processing of the data collected, provide the information needed to generate mobility strategies.

The 5G technology in conjunction with the Internet of things and artificial intelligence, will revolutionize the application in the new generation of smart cities, for that reason the governments in connection with the private sector must necessarily invest in public policies and infrastructure that allow the deployment and adoption of technologies, it is an entire challenge but at the same time it is an opportunity for the benefit of the society.

It is a priority to establish IT governance strategies to guarantee the confidentiality, integrity, and availability of data and its treatment through the IoT. The application of international standards such as the ISO / IEC in its 27000 families, the Control Objectives for Information and related Technology (COBIT), the guidelines of the National Institute of Standards and Technology (NIST), to name a few, is fundamental in cybersecurity.

Complementing the above in any cybersecurity strategy, business continuity (BCP) and a disaster recovery mechanism (DRP) must be considered; as well as the inclusion in the architecture of an intrusion detection system (IDS) and an intrusion prevention system (IPS) that will strengthen the implementation of the cybersecurity strategy through the IoT in Smart cities.

References

Alam, T. *A Reliable Communication Framework and Its Use in Internet of Things (IoT)*. IJSRCSEIT 2018, 3, 450–456.

Ali, Q.; Ahmad, N.; Malik, A.; Ali, G.; Rehman, W. *Issues, Challenges, and Research Opportunities in Intelligent Transport System for Security and Privacy*. Appl. Sci. 2018, 8, 1964, doi:10.3390/app8101964.

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

Benevolo, C., Dameri, R. P., & D'Auria, B. (2016). Smart mobility in smart city. *Empowering Organizations. Lecture Notes in Information Systems and Organisation, 11*. https://doi.org/10.1007/978-3-319-23784-8_2

Bran, W. M., & Rendón Acevedo, J. A. (2016). Ciudades y territorios inteligentes desde la perspectiva de la vigilancia tecnológicai. *Dimensión Empresarial*, 17(4). DOI: 10.15665/17.4.2107.

Brous, P., Janssen, M., & Herder, P. (2020). *The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations*. International Journal of Information Management, 51, 101952.

Das, A., Sharma, S. C. M., & Ratha, B. K. (2019). The New Era of Smart Cities, From the Perspective of the Internet of Things. In Smart Cities Cybersecurity and Privacy (pp. 1-9). Elsevier.

ISSN 2410-3993

Dash, D., Farooq, R., Sankar, P., & Sandhyavani, K. (2019). *Internet of Things (IoT): The New Paradigm of HRM and Skill Development in the Fourth Industrial Revolution (Industry 4.0)*. The IUP Journal of Information Technology.

Dey, K. C., Rayamajhi, A., Chowdhury, M., Bhavsar, P., & Martin, J. (2016). Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network – Performance evaluation. *Transportation Research Part C: Emerging Technologies*, *68*, 168–184. https://doi.org/10.1016/j.trc.2016.03.008

Faria, R., Brito, L., Baras, K., & Silva, J. (2017). Smart mobility: A survey. *2017 International Conference on Internet of Things for the Global Community (IoTGC)*, 1–8. http://doi.org/10.1109/IoTGC.2017.8008972

Frustaci, M.; Pace, P.; Aloi, G.; Fortino, G. *Evaluating Critical Security Issues of the IoT World: Present and Future Challenges*. IEEE Internet Things J. 2018, 5, 2483–2495, doi:10.1109/JIOT.2017.2767291.

Guo, H.; Ren, J.; Zhang, D.; Zhang, Y.; Hu, J. *A scalable and manageable IoT architecture based on transparent computing*. J. Parallel Distrib. Comput. 2018, 118, 5–13.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). Internet of things (iot): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7):1645 – 1660. Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services & Cloud Computing and Scientific Applications Big Data, Scalable Analytics, and Beyond.

H. Ye, L. Liang, G.Y. Li, J. Kim, L. Lu, M. Wu, Machine learning for vehicular networks: recent advances and application examples, IEEE Veh. Technol. Mag. 13 (2018) 94–101.

Hassan, A.M.; Awad, A.I. *Urban Transition in the Era of the Internet of Things: Social Implications and Privacy Challenges*. IEEE Access 2018, 6, 36428–36440, doi:10.1109/ACCESS.2018.2838339.

J. Liu, W. Sun, Yongpeng Shi, In-vehicle network attacks and countermeasures: challenges and future directions, IEEE Netw. 31 (2017) 50–58.

J. Satyakrishna and R. K. Sagar, "Analysis of smart city transportation using iot," in 2018 2nd International Conference on Inventive Systems and Control (ICISC), Jan 2018, pp. 268–273.

Jordaan, C. G., Malekian, N., & Malekian, R. (2019). Internet of Things and 5G Solutions for development of Smart Cities and Connected Systems. Communications of the CCISA, 25(2), 1-16.

Kaldellis, J. K., Spyropoulos, G., & Liaros, S. (2017). Supporting electromobility in smart cities using solar electric vehicle charging stations. *Mediterranean Green Building & Renewable Energy*. https://doi.org/10.1007/978-3-319-30746-6_37

Kauffman, M., & Soares, M. (2018). *Intellectual Property Law In The Fourth Industrial Revolution: Trade Secrets Risks And Opportunities*. Revista Juridica Curitiba.

Kodama, F. (2018). Learning mode and strategic concept for the 4th industrial revolution. *Journal of Open Innovation: Technology, Market, and Complexity*, 4 (32), 1-16.

L. Chen and C. Englund, "Choreographing services for smart cities: Smart traffic demonstration," in 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), June 2017, pp. 1–5.

L. Jamjoom, A. Alshmarani, S. M. Qaisar, and M. Akbar, "A wireless controlled digital car lock for smart transportation," in 2018 15th Learning and Technology Conference (L T), Feb 2018, pp. 46–51.

L. Liang, H. Ye, G.Y. Li, Toward intelligent vehicular networks: a machine learn-ing framework, IEEE Int. Things J. 6 (2019) 124–135.

Lawrence, W. M., & Barnes, M. W. (2019). 5g mobile broadband technology— america's legal strategy to facilitate its continuing global superiority of wireless technology. *Intellectual Property & Technology Law Journal*, 31 (5), 3-16.

ISSN 2410-3993

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

Lee, S., Ahn, S., Joo, W., Yang, M., & Yu, E. (2018). A data-driven approach for computational simulation: trend, requirement and technology. *Journal of Internet Computing and Services*, (19) 1, 123-130.

Mahdi Dibaei, Xi Zheng, Kun Jiang, Robert Abbas, Shigang Liu, Yuexin Zhang, Yang Xiang, Shui Yu, Attacks and defences on intelligent connected vehicles: a survey, Digital Communications and Networks, 2020.

Mikulic, I. & Stefanic, A. (2018) *The Adoption of Modern Technology Specific to Industry 4.0 by Human Factor,* 29TH DAAAM International Symposium on Intelligent Manufacturing and Automation.

Nikitas, A., Kougias, I., Alyavina, E., & Tchouamou, E. N. (2017). How can autonomous an connected vehicles, electromobility, BRT, hyperloop, shared use mobility and mobility-as-a-service shape transport futures for the context of smart cities. *The Future of Urban Transportation and Mobility Systems*, *1*(4), 36. https://doi.org/10.3390/urbansci1040036

Ning, Z., Xia, F., Ullah, N., Kong, X., & Hu, X. (2017). Vehicular social networks: Enabling smart mobility. *IEEE Communications Magazine*, *55*(5), 16–55. https://doi.org/10.1109/MCOM.2017.1600263

Nord, J. H., Koohang, A., & Paliszkiewicz, J. (2019). *The Internet of Things: Review and theoretical framework*. Expert Systems with Applications.

Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. (2020). *A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures*. Computers, 9(2), 44.

Obaidat, M.; Khodiaeva, M.; Obeidat, S.; Salane, D.; Holst, J. *Security Architecture Framework for Internet of Things (IoT)*. In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile.

Obeidat, M., North, M., Richardson, R., & Rattanak, V. (2015). Business intelligence technology, applications, and trends. International Management Review, 11 (2), 47-56.

OCDE. (2019). Artificial intelligence in society. OECD Publishing, Paris, https://doi.org/10.1787/eedfee77-en.

Onishi, H. (2012, June). Paradigm change of vehicle cyber security. In 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 1-11). IEEE.

Pise, V. H. (2019). Cloud computing - recent trends in information technology. *International Journal of Management and Information Technology*, 4 (1) 27-29.

Porru, S., Misso, F. E., Pani, F. E., & Repetto, C. (2020). Smart mobility and public transport: Opportunities and challenges in rural and urban areas. *Journal of Traffic and Transportation Engineering (English Edition)*, *7*(1), 88–97. https://doi.org/10.1016/j.jtte.2019.10.002

Pratap Singh, S., Kumar, V., Kumar Singh, A., and Singh, S. (2020). A survey on internet of things (iot): Layer specific vs. domain specific architecture. In Smys, S., Senjyu, T., and Lafata, P., editors, Second International Conference on Computer Networks and Communication Technologies, pages 333–341, Cham. Springer International Publishing.

Rambow, N. G., & Rambow-Hoeschele, K. (2018). The connected vehicle and its impact on the development of electromobility. *2nd E-Mobility Power System Integration Symposium*.

Sechilariu, M., Locment, F., Martell-Flores, H., Molines, N., Baert, J., Richard, G., Henriot, C., & Pronello, C. (2017). Smart microgrid and urban planning for better electromobility. *2017 IEEE Vehicle Power and Propulsion Conference (VPPC)*, 1–6. https://doi.org/10.1109/VPPC.2017.8331030

ISSN 2410-3993

Serrano Cobos, J. (2016). Tendencias tecnológicas en internet: hacia un cambio de paradigma. *El Profesional de la Información*, 25 (6) 843 - 850.

Sethi, S. K., & Paramita, S. (2016). Network technology trend for next-generation wireless communication. *The IUP Journal of Telecommunications*, 8(2), 12-24

Qian, Y., Wu, D., Bao, W., & Lorenz, P. (2019). *The internet of things for smart cities: Technologies and applications*. IEEE Network, 33(2), 4-5.

Rogers, M. E. (1983). *Diffusion of innovations*. The Free Press.

Samih, H. (2019). *Smart cities and internet of things*. Journal of Information Technology Case and Application Research, 21(1), 3-12.

Sridhar, S.; Smys, S. *Intelligent security framework for IoT devices cryptography based end-to-end security architecture*. In Proceedings of the 2017 International Conference on Inve ntive Systems and Control (ICISC), Coimbatore, India, 19–20 January 2017; pp. 1–5.

Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. *A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services*. IEEE Commun. Surv. Tutor. 2018, 20, 3453–3495, doi:10.1109/COMST.2018.2855563.

W. Choi, H.J. Jo, S. Woo, J.Y. Chun, J. Park, D.H. Lee, Identifying ECUs using inimitable characteristics of signals in controller area networks, IEEE Trans. Veh. Technol. 67 (2018) 4757–4770.

Yu, S.; Wang, G.; Liu, X.; Niu, J. *Security and Privacy in the Age of the Smart Internet of Things: An Overview from a Networking Perspective*. IEEE Commun. Mag. 2018, 56, 14–18, doi:10.1109/MCOM.2018.1701204.

Zeadally, S., Das, A. K., & Sklavos, N. (2019). Cryptographic technologies and protocol standards for Internet of Things. Internet of Things, 100075.

Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan, Cybersecurity challenges in vehicular communications, Vehicular Communications, Volume 23, 2020, 100214, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2019.100214.

ISSN 2410-3993