ISSN 2410-3993

Volume 7, Issue 21 – July – December 2020

# Journal of Technology and Innovation

ECORFAN®

**Journal of Technology and Innovation,** Volume 7, Issue 21, December - 2020, is biannual Journal edited by ECORFAN-Bolivia. Santa Lucia N-21, Barrio Libertadores, Cd. Sucre. Chuquisaca, Bolivia, http://www.ecorfan.org/bolivia/rj_tecnologia_innovacion.php, revista@ecorfan.org. Editor in Chief: BUJARI - ALLI, Ali. PhD. ISSN: 2410- 3993. Responsible for the last update of this issue ECORFAN Computer Unit. Imelda Escamilla Bouchán, PhD. Vladimir Luna Soto, PhD. Updated as of December 31, 2020.

# Journal of Technology and Innovation

## Definition of Journal

## Scientific Objectives

Support the international scientific community in its written production Science, Technology and Innovation in the Field of Engineering and Technology, in Subdisciplines of technology and technology in telecommunications, food technology, computer technology, technology in transport systems, technology in motor vehicles, energy technology, naval technology, nuclear technology, textile technology, systems engineering, electronics engineering, energy engineering, innovation.

ECORFAN-Mexico SC is a Scientific and Technological Company in contribution to the Human Resource training focused on the continuity in the critical analysis of International Research and is attached to CONACYT-RENIECYT number 1702902, its commitment is to disseminate research and contributions of the International Scientific Community, academic institutions, agencies and entities of the public and private sectors and contribute to the linking of researchers who carry out scientific activities, technological developments and training of specialized human resources with governments, companies and social organizations.

Encourage the interlocution of the International Scientific Community with other Study Centers in Mexico and abroad and promote a wide incorporation of academics, specialists and researchers to the publication in Science Structures of Autonomous Universities - State Public Universities - Federal IES - Polytechnic Universities - Technological Universities - Federal Technological Institutes - Normal Schools - Decentralized Technological Institutes - Intercultural Universities - S & T Councils - CONACYT Research Centers.

## Scope, Coverage and Audience

Journal of Technology and Innovation is a Journal edited by ECORFAN-Mexico S.C in its Holding with repository in Bolivia, is a scientific publication arbitrated and indexed with semester periods. It supports a wide range of contents that are evaluated by academic peers by the Double-Blind method, around subjects related to the theory and practice of technology and technology in telecommunications, food technology, computer technology, technology in transport systems, technology in motor vehicles, energy technology, naval technology, nuclear technology, textile technology, systems engineering, electronics engineering, energy engineering, innovation with diverse approaches and perspectives, that contribute to the diffusion of the development of Science Technology and Innovation that allow the arguments related to the decision making and influence in the formulation of international policies in the Field of Engineering and Technology. The editorial horizon of ECORFAN-Mexico® extends beyond the academy and integrates other segments of research and analysis outside the scope, as long as they meet the requirements of rigorous argumentative and scientific, as well as addressing issues of general and current interest of the International Scientific Society.

## Editorial Board

## Arbitration Committee

ARREDONDO - SOTO, Karina Cecilia. PhD
Instituto Tecnológico de Ciudad Juárez

ARROYO - FIGUEROA, Gabriela. PhD
Universidad de Guadalajara

BAEZA - SERRATO, Roberto. PhD
Universidad de Guanajuato

BARRON, Juan. PhD
Universidad Tecnológica de Jalisco

BAUTISTA - SANTOS, Horacio. PhD
Universidad Popular Autónoma del Estado de Puebla

CASTAÑÓN - PUGA, Manuel. PhD
Universidad Autónoma de Baja California

CASTILLO - TOPETE, Víctor Hugo. PhD
Centro de Investigación Científica y de Educación Superior de Ensenada

CORTEZ - GONZÁLEZ, Joaquín. PhD
Centro de Investigación y Estudios Avanzados

CRUZ - BARRAGÁN, Aidee. PhD
Universidad de la Sierra Sur

GONZÁLEZ - LÓPEZ, Samuel. PhD
Instituto Nacional de Astrofísica, Óptica y Electrónica

GONZÁLEZ - REYNA, Sheila Esmeralda. PhD
Instituto Tecnológico Superior de Irapuato

**Assignment of Rights**

The sending of an Article to Journal of Technology and Innovation emanates the commitment of the author not to submit it simultaneously to the consideration of other series publications for it must complement the Originality Format for its Article.

The authors sign the Authorization Format for their Article to be disseminated by means that ECORFAN-Mexico, S.C. In its Holding Bolivia considers pertinent for disclosure and diffusion of its Article its Rights of Work.

**Declaration of Authorship**

Indicate the Name of Author and Coauthors at most in the participation of the Article and indicate in extensive the Institutional Affiliation indicating the Department.

Identify the Name of Author and Coauthors at most with the CVU Scholarship Number-PNPC or SNI-CONACYT- Indicating the Researcher Level and their Google Scholar Profile to verify their Citation Level and H index.

Identify the Name of Author and Coauthors at most in the Science and Technology Profiles widely accepted by the International Scientific Community ORC ID - Researcher ID Thomson - arXiv Author ID - PubMed Author ID - Open ID respectively.

Indicate the contact for correspondence to the Author (Mail and Telephone) and indicate the Researcher who contributes as the first Author of the Article.

**Plagiarism Detection**

All Articles will be tested by plagiarism software PLAGSCAN if a plagiarism level is detected Positive will not be sent to arbitration and will be rescinded of the reception of the Article notifying the Authors responsible, claiming that academic plagiarism is criminalized in the Penal Code.

**Arbitration Process**

All Articles will be evaluated by academic peers by the Double Blind method, the Arbitration Approval is a requirement for the Editorial Board to make a final decision that will be final in all cases. MARVID® is a derivative brand of ECORFAN® specialized in providing the expert evaluators all of them with Doctorate degree and distinction of International Researchers in the respective Councils of Science and Technology the counterpart of CONACYT for the chapters of America-Europe-Asia- Africa and Oceania. The identification of the authorship should only appear on a first removable page, in order to ensure that the Arbitration process is anonymous and covers the following stages: Identification of the Journal with its author occupation rate - Identification of Authors and Coauthors - Detection of plagiarism PLAGSCAN - Review of Formats of Authorization and Originality-Allocation to the Editorial Board-Allocation of the pair of Expert Arbitrators-Notification of Arbitration -Declaration of observations to the Author-Verification of Article Modified for Editing-Publication.

**Instructions for Scientific, Technological and Innovation Publication**

**Knowledge Area**

The works must be unpublished and refer to topics of technology and technology in telecommunications, food technology, computer technology, technology in transport systems, technology in motor vehicles, energy technology, naval technology, nuclear technology, textile technology, systems engineering, electronics engineering, energy engineering, innovation and other topics related to Engineering and Technology.

## Presentation of content

In the first article we present, *Intelligent mobility: a review of the cybersecurity of IoT in smart cities*, by VÁZQUEZ-DEL RÍO, Jorge Rubén, CARDEÑA-MORENO, Sergio Alejandro and VILLAFAÑA-DÍAZ, Luis Gerardo, with adscription in the, Universidad Popular Autónoma del Estado de Puebla, in the next article we present, *Prototype of natural user interface applied to a robotic arm for medical attention preventing nosocomial infections in healthcare personnel*, by SERRANO-RAMÍREZ, Tomás, GUTIÉRREZ-LEÓN, Diana Guadalupe, MANDUJANO-NAVA, Arturo and SÁMANO-FLORES, Yosafat Jetsemaní, with adscription in the Universidad Politécnica de Guanajuato, in the next article we present, *Mobile app with reading speech-translated OCR images for visually impaired people*, by VAZQUEZ-GUZMAN, Francisco, OLGUIN-GIL, Liliana Elena, VAZQUEZ-ZAYAS, Eduardo and NICANOR-PIMENTEL, Brawhim Jesseth, with adscription in the Tecnológico Nacional de México/Instituto Tecnológico de Tehuacán, in the next article we present, *Comparative analysis of methods to determine deflection in steel beams: theoretical analysis, finite element and experimental*, by ALOR-SAVEDRA, Gabriela, ALAFFITA-HERNÁNDEZ, Francisco Alejandro, ESCOBEDO-TRUJILLO, Beatris Adriana and SILVA-ÁGUILAR, Oscar Fernando, with adscription in the Universidad Veracruzana.

## Content

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.

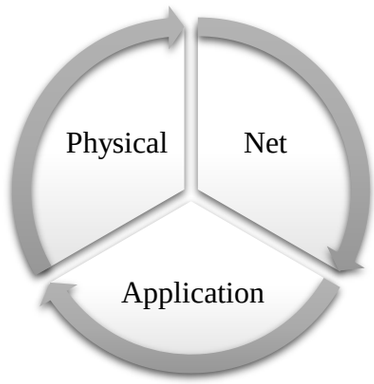



**Figure 1** Internet of things architecture model
*Source: Own elaboration according to the references consulted, 2020*

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.

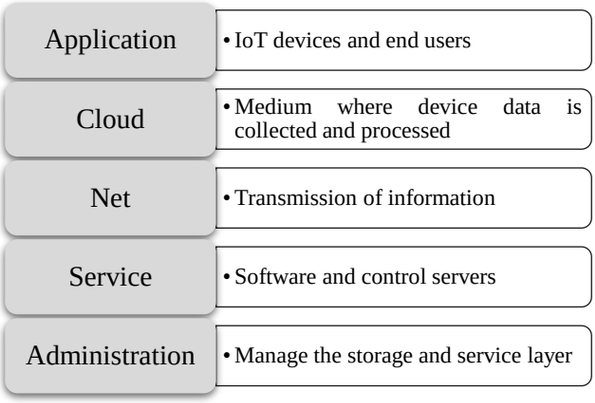



**Figure 2** The security model for the internet of things
*Source: Own elaboration according to the references consulted, 2020*

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

Article **Journal of Technology and Innovation**
December 2020 Vol.7 No.21 19-25

# Prototype of natural user interface applied to a robotic arm for medical attention preventing nosocomial infections in healthcare personnel

# Prototipo de interfaz de usuario natural aplicado a un brazo robótico para atención médica previniendo infecciones nosocomiales en personal sanitario

SERRANO-RAMÍREZ, Tomás†*, GUTIÉRREZ-LEÓN, Diana Guadalupe, MANDUJANO-NAVA, Arturo and SÁMANO-FLORES, Yosafat Jetsemaní

*Universidad Politécnica de Guanajuato, Automotive Engineering, Mexico.*

ID 1st Autor: *Tomás, Serrano-Ramírez* / **ORC ID**: 0000-0001-6118-3830, **Researcher ID Thomson:** G-6039-2018, **CVU CONACYT ID:**493323

ID 1st Coautor: *Diana Guadalupe, Gutiérrez-León* / **ORC ID**: 0000-0001-5051-880X, **Researcher ID Thomson:** G-6035-2018, **CVU CONACYT ID:** 443892

ID 2nd Coautor: *Arturo, Mandujano-Nava* / **ORC ID**: 0000-0003-2022-4397, **CVU CONACYT ID**: 270254

ID 3rd Coautor: *Yosafat Jetsemaní, Sámano-Flores* / **ORC ID**: 0000-0003-4173-6236, **CVU CONACYT ID**: 444850

**DOI:** 10.35429/JTI.2020.20.7.19.25 Received July 20, 2020; Accepted December 30, 2020

**Abstract**

In this work, an experimental prototype of natural user interface based on Kinect for the tele-operation of a robotic arm, was developed as a technological support to contribute in facing the global crisis of health generated by COVID-19, a dangerous and highly transmissible virus. Until now, it is causing thousands of deaths and growing of contagion rates around the world, involving a serious situation for healthcare personnel that works in hospitals attending infected population. This system was proposed with the aim to control a robotic arm for medical purposes to achieve a quality medical care to COVID-19 patients without risk implications for healthcare workers associated to nosocomial infections due to direct contact with infected patients, contaminated medical equipment, surgical objects and surfaces. The developed prototype is able of being manipulated in real time requiring neither physical controller nor any contact device to carry out its functions, but simply motion or gesture from the user's arm. It can be applied in areas such as tele-operation, tele-rehabilitation, telehealth nursing, assistive and therapeutic robotic devices, elderly care which are the last tendency in medicine at this time. Kinect V2, the Software Development kit SDK 2.0, Microsoft visual C# and Arduino were used for this purpose.

**Natural-user-interface, Robotic-arm, COVID-19**

**Resumen**

En este trabajo, un prototipo de interfaz natural de usuario basado en Kinect para la tele-operación de un brazo robótico fue desarrollado como soporte tecnológico para contribuir a hacer frente a la crisis global de salud generada por COVID-19, un virus peligroso y altamente transmisible. Hasta ahora, éste ha causado miles de muertes y altas tasas de contagios alrededor del mundo, involucrando una seria situación para el personal médico que trabaja en hospitales brindando la atención a las personas infectadas. Este sistema fue propuesto con el objetivo de controlar un brazo robótico para fines médicos para lograr una atención médica de calidad para los pacientes de COVID-19, sin que ello implique un riesgo para sí mismos, ya sea teniendo contacto directo con pacientes infectados, objetos quirúrgicos y superficies contaminadas. El prototipo desarrollado es manipulado en tiempo real sin requerir un control físico u otro dispositivo de contacto para realizar sus funciones, sólo movimiento y gesticulación del propio brazo del usuario. Esto puede ser aplicado en áreas tales como la tele-rehabilitación, cuidado médico a distancia, dispositivos robóticos terapéuticos y de asistencia, lo cual constituye las últimas tendencias en Medicina. Kinect V2, Software Development kit SDK 2.0, Microsoft visual C# y Arduino fueron usados para este propósito.

**Interfaz natural de usuario, brazo robótico, COVID-19**

**Citation:** SERRANO-RAMÍREZ, Tomás, GUTIÉRREZ-LEÓN, Diana Guadalupe, MANDUJANO-NAVA, Arturo and SÁMANO-FLORES, Yosafat Jetsemaní. Prototype of natural user interface applied to a robotic arm for medical attention preventing nosocomial infections in healthcare personnel. Journal of Technology and Innovation. 2020. 7-21:19-25.

* Correspondence to Author (E-Mail: tserrano@upgto.edu.mx)
† Researcher contributing as first author.

## Introduction

Worldwide, COVID-19 has been categorized as a novel, rising and highly infectious disease (Chang, Joob and Wiwanitkit, Hsia, 2020), which it is responsible to cause until now (May 8th, 2020), 3,767,744 confirmed cases and 259,593 deaths (WHOa, 2020).

Healthcare personnel is heavily exposed to infection risk during its working sessions due to direct contact with infected people and contaminated objects including equipment, medical instruments and supplies.

Natural user interface is a technology that can be used to control devices without establish a direct contact, specifically by gestures and human body motion that is correlated with the interface reaction (Sommerer *et al*., 2005).

The latest trends in natural user interfaces involve the control of artificial limbs using the own user's extremity movements and gestures. Natural user interfaces have several advantages including (Blake, 2012):

Instant expertise: The user takes advantage of the existing skills or abilities that most of the people domain such as the movement of his own body in order to interact with technological devices. It gives in the majority of cases an instant level of expertise letting the user to apply his natural abilities to control the device.

Progressive learning: Natural user interfaces imitate the way people learn physical skills, allowing them to start with basic tasks and move on to something more advanced step by step, in a steady increment. That is not the case with other interfaces that require a huge training by the user in order to begin the interaction with the device. Direct interaction: Natural user interface imitates the user's interaction with the physical world by having a direct correlation between user action and the natural user interface reaction. It means that the interface actions happen at the same time as user actions or that the motions of elements on the interface follow the motions of the user.

Low cognitive load: The mental effort to manipulate a natural user interface is minimum, due to the user takes advantage of his basic skills or abilities, such as the movement of body, letting him focuses on achieving a task.

As is shown, natural user interfaces represent the future tendency in the interaction among technological devices and human beings.

Kinect V2 is able to facilitate the interaction between human and robots, supporting non- expert users to control them with minimal training, in a more intuitive and natural way. Kinect V2, the Software Development kit SDK 2.0, Microsoft visual C# and Arduino are used for this purpose. Kinect V2 is an accessible but powerful motion sensing input device, capable to track the human body joints in 3D space and recognize hand gestures in real time (Microsoft b, 2014). The joint positions are displayed on screen (skeleton-tracking), converted into angles and sent to the microcontroller board (Arduino), in order to control the arm's position (servomotors). The hands gestures are used to open and close the hand grip or even turn on/off the interface.

By the other hand, the Software Development Kit (SDK 2.0) provided by Microsoft, is free and there will be no fees for runtime licenses of commercial applications developed with it. The interface was written in (C#/WPF), based on a free example provided in SDK2.0 and is capable to track 25 joints per person at 30 frames per second.

Robotic arms are part of this evolution, and many of them which have been successfully used with more conservative interfaces are migrating to the use of natural user interfaces, in areas such as: surgical robots, tele-operation, tele-rehabilitation, assistive and therapeutic devices, human augmentation, tele-skill transfer and soft robotics.

Some representative examples of the latest trends in the research of natural interfaces and robotic arms applied in medicine are as follows: a gesture control for the Da Vinci Robot developed by Laboratory for Computational Sensing and Robotics (LCSR) (Wang et al., 2012) and a soft exoskeleton jacket for human motion interaction carried out by The Biological Systems Engineering Lab at the University of Hiroshima (Vega and Kurita, 2018).

ISSN 2410-3993

Then, the aim of this work is developing a natural user interface for controlling a robotic arm in real time, without the requirement of a physical controller or any contact device, but simply by the motion or gesture from the user's arm. This technological application could help the medical staff to face the elevated risk of infection, generated by COVID-19, giving medical attention with high quality, without establish direct contact either infected patients or contaminated objects, in which could be included, the physical controller in a conventional robotic arm. Additionally, the implementation of advices for public issued by WHOb (2020) such as maintaining distance by yourself and others and, avoid touching contaminated surfaces with finger by healthcare personnel.

## Design and development of prototype

The natural user interface designed and developed to control a robotic arm is explained below.

The proposed project consists of four hardware modules: 1) motion sensing input device (Kinect V2), 2) computer, 3) microcontroller (Arduino mega 2560) and 4) robotic arm, whose block diagram and prototype are presented in Figure 1 and Figure 2, respectively.

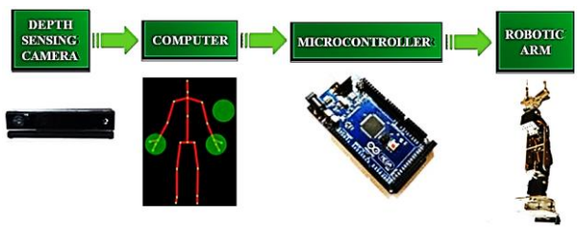



**Figure 1** Hardware flow chart for the remote-controlled robotic arm

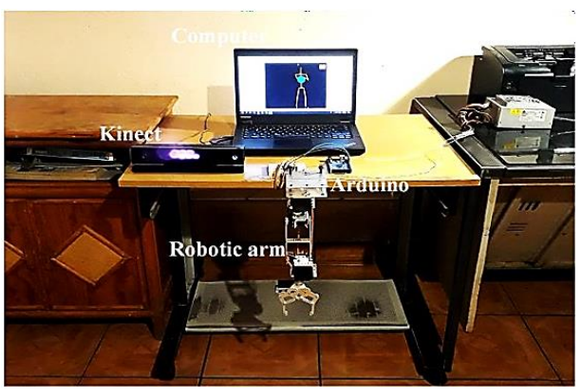



**Figure 2** Remote controlled robotic arm and the real position of the hardware modules

Hardware modules are explained as follows:

Motion sensing input device (Kinect V2): the Kinect V2 sensor by Microsoft is used as an input device. It features an RGB camera and a depth sensor (Time of Flight) which provide full-body 3D motion capture at 30 frames per second, sending the data to the computer via USB 3.0.

Computer: it is notebook or a personal computer (PC) which stores and executes the designed natural user interface. The natural user interface processes the Kinect information sent via USB by artificial intelligence (Decision Forest Classifier and Mean shift), obtaining the position of the 25 specific body joints from the user at 30 fps. Natural user interface displays the user skeleton tracking and at the same time, sends via USB the respective angles and hand states to Arduino for controlling the robotic arm.

Microcontroller: once the angles or hand states are sent from the computer using the USB port to the microcontroller board (Arduino mega 2560), it receives them, and for each one, generates a PWM signal to position the servo-motor (belonging to the robotic arm) into a specific angle. The servo-motor angle depends on the magnitude of the received angle from Kinect.

Robotic arm: the prototype is an articulated robotic arm, that tries to emulate the human arm, under the wrist and uses servo-motors to mimic the joints motion. For this prototype, the we emulate the movement from the right shoulder and the open and closed right hand state; three servo-motors mg996r are used for this purpose (0 to 180° turning radius).

ISSN 2410-3993

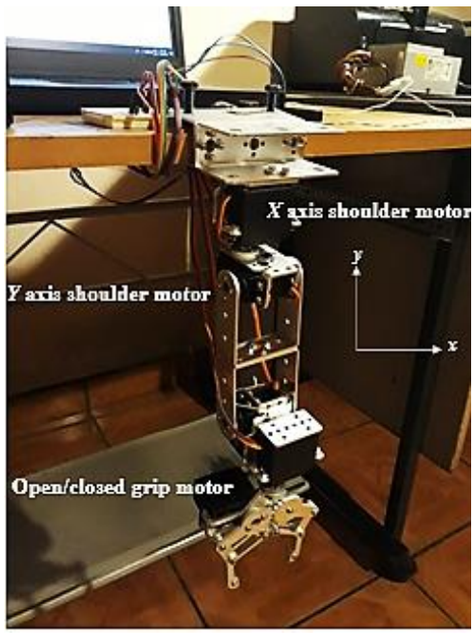



**Figure 3** The robotic arm used in this project

The proposed project consists of two software modules as is shown in Figure 4.

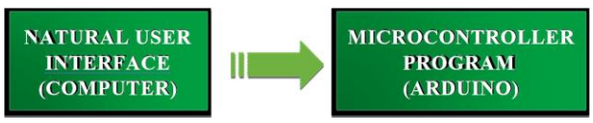



**Figure 4** Software flow chart for the remote-controlled robotic arm

## Natural user interface

In this section the proposed natural interface to control the robotic arm is explained in detail. The following operative system and tools were used to develop the natural interface:

– Windows 10.

– Kinect for Windows Software.

– Development kit 2.0 (SDK 2.0).

– Visual Studio 2017.

– Microsoft visual C#.

The Kinect sensor was developed by Microsoft Corporation, which provides a Software Development Kit (SDK 2.0) that lend to programmers generate applications supporting corporal motion and voice recognition.

SDK 2.0 carry out its functions with the operative systems Windows 8 and Windows 10 and it does not require fees for runtime licenses of commercial applications developed with it (Microsoft a,b, 2014).

We began the natural user interface development with a free basic skeleton-tracking sample code, provided by Microsoft SDK 2.0. This sample was written in (C#/WPF) and is capable to track 25 joints per person at 30 frames per second and identify open/closed hand gestures.

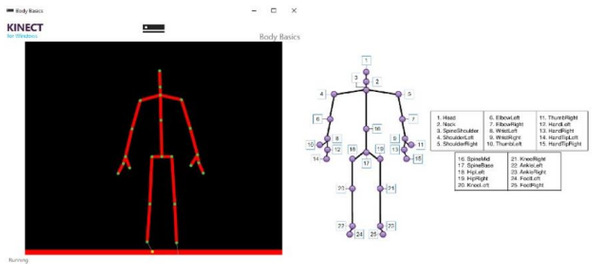



**Figure 5** Skeleton-tracking sample code, provided by Microsoft SDK 2.0, which detects 25 body joints (Ahmed *et al.*, 2015)

The free skeleton-tracking sample code, provided by Microsoft SDK 2.0 to demonstrate the Kinect capabilities, is used as a basis in the design and development of the Natural User Interface which controls the Robotic Arm. The first step is to calculate the angles from the user´s arm using the body Joints detected by Kinect. It is called forward kinematics and is explained in the next section.

## Forward Kinematics

Forward kinematics require the application of kinematic equations corresponding to a robot, to calculate the location of the end- effector from specified values for the joint parameters (Al-Ammri and Ahmed, 2018). In this case the Joint parameters are the body joints detected from the Kinect sensor and the end effector is the robotic arm. The robotic arm must be controlled by the right arm, therefore, two body joints from the user arm (ShoulderRight and HandRight, Figure 5) are used to calculate the arm angles. In specific two angles are needed to control the shoulder movement from the robotic arm: the angle between the arm and the XZ plane, and the angle between the arm's projection in XZ plane and Z axis (Figure 6 and considering ShoulderRight at origin.

ISSN 2410-3993

These angles will be used to control the shoulder servomotors from the robotic arm (Figure 3).

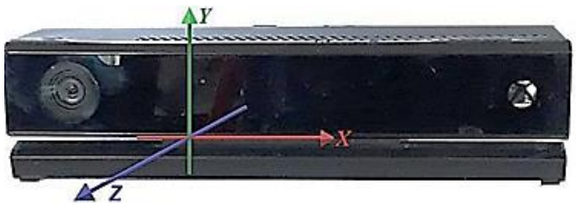



**Figure 6** Kinect V2 coordinate system

These angles must be calculated using vector calculus following the next steps:

- Get the coordinates ($x1$, $y1$, $z1$) from ShoulderRight and ($x2$, $y2$, $z2$) from HandRight joints.

- Move the vector formed by the union of these two joints (pointing from ShoulderRight to HandRight) to the coordinate origin:

$$\vec{A} = (x2 - x1,\ y2 - y1,\ z2 - z1) \quad (1)$$

- Calculate the vector magnitude an its projection in XZ plane magnitude:

$$\left[\vec{A}\right] = \frac{\sqrt{(X-X)^2+(y-y)^2+(z-z)^2}}{2\quad 1\quad 2\quad 1\quad 2\quad 1} \quad (2)$$

$$\left[\vec{P}\right] = \frac{\sqrt{(X_2-X_1)^2+(z_2-z_1)^2}}{} \quad (3)$$

Calculate the angle $\alpha$ between the arm and the XZ plane and the angle $\beta$ between the arm's projection in XZ plane and the z, applying the equations presented in Ec. 4 and Ec. 5

$$\alpha = sin^{-1}\left(\frac{\vec{A}_y}{|A|}\right) \quad (4)$$

$$\beta = sin^{-1}\left(\frac{\vec{A}_x}{|\vec{P}|}\right) \quad (5)$$

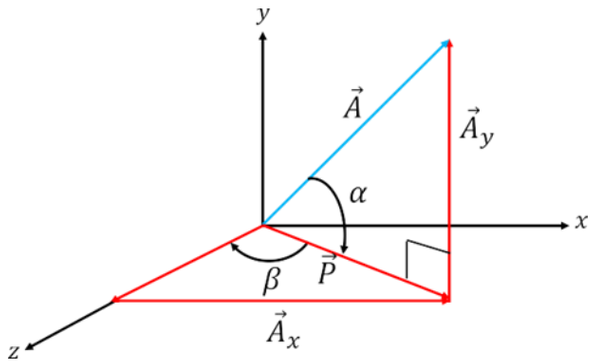



**Figure 7** 3D space interpretation for the robotic arm forward kinematics

Once the angles $\alpha$ and $\beta$ are calculated, they are sent via USB to Arduino for controlling two servomotors belonging to the robotic arm.

## Microcontroller program

The microcontroller board (Arduino) is programed to communicate with the natural user interface throughout USB port, receiving two angles (0 to 180°) from the user right-arm position and the right-hand state (open Close). These variables are converted to PWM (Pulse Code Modulation) and sent to the Arduino ports in order to control three servomotors mg996r. The servomotors control the arm movement and the grip from the robotic arm.

## Results

Interactive Functionality. At this moment, the robotic arm can be controlled by the natural user interface but it lacks of interactivity, or a dialog between the user and Computer, wasting the powerful functionality that Kinect offers in this category. For this purpose, three hand gestures detected by the improved Kinect V2 will be used in order to communicate with de computer these gestures are: open, closed and lasso as shown in Figure 8. When Kinect detects some of these gestures, it sends to the computer Boolean variables that can be read with the appropriate command in SDK 2.0.

ISSN 2410-3993

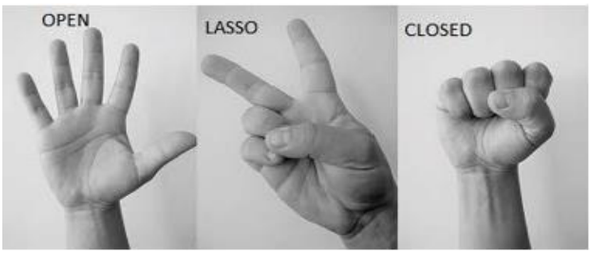



**Figure 8** Three hand gestures detected by the Kinect V2 sensor
*Source: (Arizpe, 2016)*

We improve the natural user interface in order to turn on and off the device at distance, using hand gestures as can be seen in Figure 9. It avoids undesired and unsafe movements for the robotic hand, in the transition between these two states (on/off) and facilitating the user switching.

**Figure 9** Natural user interface developed in this project

When a user is in front of the Kinect, the sensor only displays the skeletal tracking, but the robotic arm is turned off. When the user closes the left-hand, the user can activate the robotic hand guiding the right-hand position at screen over a green circle, once they match the device is activated. When the user wants to quit, he opens the left hand and guides the right-hand position over the green circle and the robotic hand is deactivated.

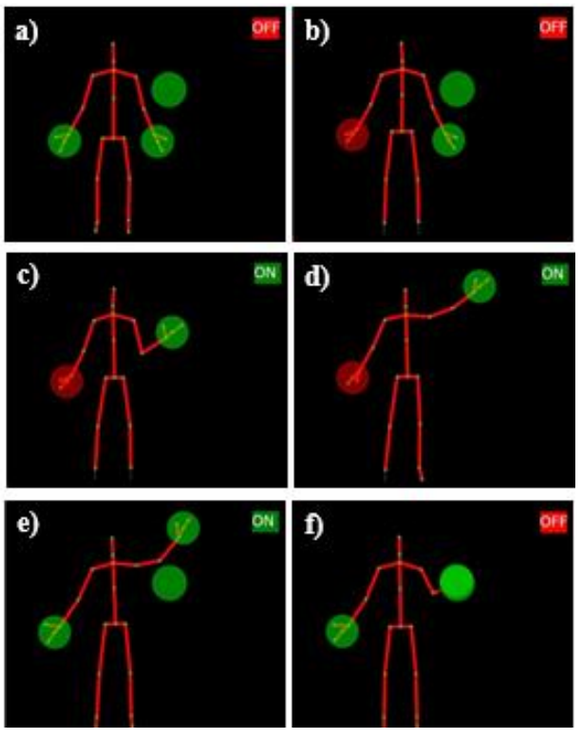



**Figure 10** a) User is in front of the Kinect with both hands open, the sensor only displays the skeletal tracking, but the robotic arm is turned off. b) When the user closes the left-hand, c) the user can activate the robotic arm guiding the right-hand position at screen over a green circle, d) once they match the device is activated. e) When the user wants to quit, he opens the left hand and f) guides the right-hand position over the green circle and the robotic arm is deactivated

## Conclusions

According to the objectives set in this project, a natural user interface for controlling a robotic arm in real time, without the requirement of a controller or any contact device, but simply by the motion or gesture from the user's arm was successfully designed. The fast response and easy operation in the control of a robotic arm, give our natural user interface important advantages over many proposed prototypes under the same budget. Our prototype can be easily escalated to a more complex natural user interface, which would let us to control a robotic arm with more degrees of freedom, fingers control and haptics, emulating the movement of a real arm more closely. Besides that, applying a remote control using a node to node communication in an Internet of Things (IoT) application, could transform this prototype in a tool for telemedicine, in areas such as tele-operation, tele-rehabilitation, telehealth nursing, assistive and therapeutic robotic devices, which are the last tendency in medicine at this time.

ISSN 2410-3993

**References**

Al-Ammri, A. S., Ahmed, I. (2018) Control of omni-directional mobile robot motion. Al-Khwarizmi, Eng. J. 6(4), 1-9.

Ahmed, F. Paul, P. and Gavrilova, M. (2015) Kinect-Based Gait Recognition Using Sequence of the Most Relevant Joint Relative Angles, Journal of WSCG, 23(2), 147-156.

Blake, J. (2012) The natural user interface revolution. In Natural User Interfaces in .NET. Manning Publications.

Chang, D., Huiwen, X., Reabaza, A., Sharma, L., Dela Cruz, C. (2020) Protecting health-care workers form buclinical coronaviros infection. Correspondence 8-3, E13. Published: March 01, 2020.

Hsia, W. (2020) Emerging new coronavirus infection in Wuhan, China: situation in early 2020. Case Study Case Rep 2020; 10:8e9.

Joob, B., Wiwanitkit, V. (2020) COVID-19 in medical personnel: observation from Thailand. Journal of Hospital Infection 104(4).

Sommerer, C., Jain, L. C., Mignonneau, L. (2005). The art and science of interface and interaction design / (ed. Springer).

Wang, X.L., Stolka, P.J., Boctor, E., Hager, G.D., & Choti, M.A. (2012). The Kinect as an interventional tracking system. Medical Imaging: Image-Guided Procedures. Robotic Interventions and Modeling, 8316, 1-6.

Vega A. and Kurita, Y. (2018). A soft exoskeleton jacket for human motion interaction. The 36th Annual Conference of the Japanese Robotics Society, At Chubu University.

Microsoft a (2014) Download the updated Kinect for Windows SDK public preview. URL: https://blogs.windows.com/windowsdev eloper/2014/08/26/download-the-updated-kinect-for-windows-sdk-2-0-public-preview/ Updated: August 26, 2014.

Microsoft b (2014) Kinect for Windows SDK v1.8 URL:https://www.microsoft.com/en-us/download/details.aspx?id=44561 Updated: October 21, 2014.

World Health Organization, WHOa (2020) WHO Coronavirus disease (COVID-19) dashboard. https://covid19.who.int/ Updated: May 8, 2020

World Health Organization, WHOb (2020). Coronavirus disease (COVID-19) advice for the public. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public Updated: April 29, 2020.

ISSN 2410-3993

Article **Journal of Technology and Innovation**
December 2020 Vol.7 No.21 26-31

# Mobile app with reading speech-translated OCR images for visually impaired people

# Aplicación móvil con lectura de imágenes OCR traducidas a voz para personas con discapacidad visual

VAZQUEZ-GUZMAN, Francisco†*, OLGUIN-GIL, Liliana Elena, VAZQUEZ-ZAYAS, Eduardo and NICANOR-PIMENTEL, Brawhim Jesseth

*Tecnológico Nacional de México/Instituto Tecnológico de Tehuacán, Mexico.*

ID 1st Author: *Francisco, Vázquez-Guzmán* / **ORC ID:** 0000-0002-3886-4774, **Researcher ID Thomson:** 4006862, **CVU CONACYT ID:** 1094851

ID 1st Co-author: *Liliana Elena, Olguín-Gil* / **ORC ID:** 0000-0003-4649-1434, **Researcher ID Thomson:** 4006628, **CVU CONACYT ID:** 410583

ID 2nd Co-author: *Eduardo, Vázquez-Zayas* / **ORC ID:** 0000-0002-6534-5582, **Researcher ID Thomson:** 4028090, **CVU CONACYT ID:** 1094961

ID 3rd Co-author: *Brawhim Jesseth, Nicanor-Pimentel* / **ORC ID:** 0000-0002-5512-9149

**DOI:** 10.35429/JTI.2020.21.7.26.31 Received July 25, 2020; Accepted December 30, 2020

**Abstract**

This research allows to have an overview of the different technologies that can be used to benefit people with visual disabilities. In the association "Sentir con los ojos del corazón" located in Tehuacán, Puebla, México, people with visual disabilities are served who do not have the technological tools available to understand their environment, such as restaurant menus, signs on doors, reading a book and any setting that contains a text, making life difficult in a world where most texts are oriented towards visual people. There are few applications for people with visual disabilities that allow them to improve their lives in the different areas in which they operate. Therefore, it is proposed to design a mobile application that interacts with a virtual assistant to translate the images into text to speech through optical character recognition (OCR), allowing them to function in different educational, work, social environments, among others. This project allows the Inclusion of people with visual disabilities to improve the quality of life using applications for mobile devices and to be self-sufficient in their daily life, later managing to translate in different languages, with different intensities and tone of voice, using different platforms.

**Visual impairment, OCR, App, Inclusion**

**Resumen**

Esta investigación permite tener un panorama de las diferentes tecnologías que se pueden utilizar para beneficiar a las personas con discapacidad visual. En la asociación “Sentir con los ojos del corazón” ubicada en Tehuacán, Puebla, México, se atienden a personas con discapacidad visual que no tienen al alcance las herramientas tecnológicas para comprender su entorno, como menús de restaurantes, letreros en puertas, leer un libro y cualquier escenario que contenga un texto, haciendo la vida difícil en un mundo donde la mayoría de los textos están orientados a personas visuales. Existen pocas aplicaciones para personas con discapacidad visual que permitan mejorar su vida en los diferentes ámbitos en que se desenvuelven. Por lo cual se propone diseñar una aplicación móvil que interactúe con un asistente virtual para traducir las imágenes en texto a voz mediante un reconocimiento óptico de caracteres (OCR), permitiendo desenvolverse en diferentes entornos educativos, laborales, sociales, entre otros. Este proyecto permite la Inclusión de las personas con discapacidad visual para mejorar la calidad de vida utilizando aplicaciones para dispositivos móviles y ser autosuficientes en su vida diaria, logrando más adelante traducir en diferentes idiomas, con diferentes intensidades y tono de voz, utilizando diferentes plataformas.

**Discapacidad visual, OCR, App, Inclusión**

**Citation:** VAZQUEZ-GUZMAN, Francisco, OLGUIN-GIL, Liliana Elena, VAZQUEZ-ZAYAS, Eduardo and NICANOR-PIMENTEL, Brawhim Jesseth. Mobile app with reading speech-translated OCR images for visually impaired people. Journal of Technology and Innovation. 2020. 7-21:26-31.

* Correspondence to Author (E-Mail: francisco.vg@tehuacan.tecnm.mx)
† Researcher contributing as first author.

## Introduction

López Delgado, A., Olmedo, E., Tadeu, P., & Fernández Batanero, J. M. (2019), p. 196) visual impairment as follows:

The World Health Organization in its descriptive note number 282 divides vision capacity into 4 levels: normal vision, moderate visual impairment, severe visual impairment, and blindness. Grouping the antepenultimate and penultimate into the descriptive of "low vision", which together with the term blindness represent cases of visual impairment.

On this subject, Cardona Mesa (2019) states that: "There are 285 million visually impaired people in the world of whom 39 million are completely blind and 246 million who have low vision".

And one thing we care about as a society is that: "In 2010, people who had some form of disability in Mexico exceeded 5 million, representing 5.1% of the population" (Esparza-Maldonado, A. L., Margain-Fuentes, L. Y., Alvarez-Rodríguez, F. J., & Benítez-Guerrero, 2018, p. 151).

According to the latest INEGI survey (INEGI, 2010),the state of Puebla is in fourth place nationally with a limitation in activity to see 63,575 people. Therefore, the ITTEH-CA-9 Academic Corps, in agreement with the association "Sentir con los ojos del corazón", is intended to benefit visually impaired people with this research.

The academic body has conducted three research related to visual and hearing impairment, which has allowed us to know the problems faced by these types of people.

In recent years the constant change of technology as a result of the different platforms and equipment that evolve rapidly, allow to develop research projects in different areas, thus implementing tools to be used in an important society improving the quality of life of people (Zambrano, D.M; Daza-Alava, Y. D; Pinargote-Zambrano, J.D; Lituma-Ramirez, 2019). There are several technological tools aimed at supporting the visually impaired. (Escandell Bermúdez, María Olga, Fortea Sevilla, María del Sol, Castro Sánchez, 2014, p. 490) state:

"In the case of visual impairment, ICTs made available to these people are quite diverse and extensive, ranging from visual adapters, text-to-sound converters, to the use of Braille-specific printers."

Today there are many conventional smartphones and tablets (Apple and Google) that allow low-vision users to adjust color, Contrast, size, brightness, visibility, readability, and blind users can turn on voice output (VoiceOver on Apple and Google Talk-Back on Android) that reads information aloud, from emails, messages to eBooks, plus voice-controlled digital assistants (SIRI and Alexa) are used to read text, open apps, search, online, send messages, and initiate a call. Also for writing activities, the application incorporates a dictation function that converts voice into text (Natalina Martiniello, Werner Eisenbarth, Christine Lehane, 2019, p. 2).

Due to the high use of mobile devices with high-resolution cameras and high processing capacity, the idea of applying OCR technology to mobile photos arises.

However, existing applications are geared towards visuals without hearing by the interface they present. When regular users require transcribing text on their smartphone that comes from contact cards, document identification, or lottery code, they will use one of the available text entry methods. Optical Character Recognition (OCR) technology can help reduce text transcription time and have been available on mobile devices for several years, in various commercial applications available, some applications recognize structured documents (e.g. business cards)(Bellino, A., 2019, p. 167982).

The goal of the project is to develop an easy and intuitive application with a simple interface that allows access through a screen reader, which uses the camera of the device to take a photograph of the text and translates to voice audibly.

## Methodology

Ilya Bibik (2018) states: "Scrum's approach is to divide the project into smaller logical fragments (mini projects) and execute them in short iterations of ideally one to three weeks.

ISSN 2410-3993

These iterations are called Sprints." Therefore, it was decided to use the Scrum methodology for this project.

In the release plan it was necessary to identify the user stories, which specify the software requirements and in which the customer describes the features that the software must possess.

User stories were based on two crucial aspects:

- Conversation: Between the client and the developer, to analyze and expand details, which is done verbally or documented if required.

- Confirmation: Performed by means of acceptance tests to verify and confirm the correct monitoring of the customer's requirements.

To track requirements and needs, a user story planning was structured with which each iteration was able to determine the necessary changes in the project.

Once the needs and requirements were contemplated through the user stories, the modules that the system would have were defined. The system modules were proposed according to the priority and order in which they would be developed for implementation, being as follows:

1. System functions
    a. Home
        i. Speaker's Welcome
        ii. Tutorial
    b. Data capture
        i. Approach to the input text
        ii. Processing using OCR
        iii. Translation and preparation of the output
    c. Exit
        i. Text storage
        ii. Playing text in speech

With the evaluation of the first user stories and the definition of the system modules, the first launch plan was made, estimating an average time for the elaboration of each module based on a week of 5 days and a day of approximately 3 hours, as shown in Table 1.

| Form | # | User history | Estimated time Weeks |
|---|---|---|---|
| System functions | 1 | Home – Welcome | 1 |
| | 2 | Home – Tutorial | 1 |
| | 3 | Capture - Digitization | 1 |
| | 4 | Captura – OCR | 2 |
| | 5 | Capture - Translation and preparation | 1 |
| | 6 | Output - Text storage | 1 |
| | 7 | Output - Voice playback | 1 |
| Total estimated time | | | 8 |

**Table 1** Launch plan

An iteration plan was made in which the communication of the actors (client and developer) was essential to follow up on the development of the modules and reallocate the risk and priority of the modules.

Depending on the user stories and their assessment, a three-iteration plan was developed to be revalued and if necessary restructured; at the end of each one a working meeting was held with the client to carry out the corresponding operational and acceptance tests.

| Form | # | User history | Iterations | | |
|---|---|---|---|---|---|
| | | | 1 | 2 | 3 |
| System functions | 1 | Home – Welcome | X | | |
| | 2 | Home – Tutorial | X | | |
| | 3 | Capture – Digitization | | X | |
| | 4 | Captura – OCR | | X | |
| | 5 | Capture - Translation and preparation | | X | |
| | 6 | Output - Text storage | | | X |
| | 7 | Output - Voice playback | | | X |

**Table 2** Iteration Plan

Depending on the proposed planning, iterations were constantly being reviewed through the participation of the product owner, the master scrum and the development team.

ISSN 2410-3993

**Results**

It is important to implement the necessary efforts to promote technological development in order to support visually impaired people to be included in society in a natural way.

This article proposes the application of the OCR feature on images in which text is captured using a mobile application to audiblely reproduce such information, to help visually impaired people.

For application development and speech, Google's OCR and Text-To-Speech libraries were implemented.

The project on Android is divided into the following points:

- Splash design. The application logo was designed, and the app input animation was programmed where it presents the project name while loading the application.

- Central design of the application. Added the app icon in the main view, as well as a button with an ImageView where camera preparation and text capture will be programmed. This photo will be viewed in the ImageView.

- Integration of Google's OCR library. After you have taken the photo and assigned it in the ImageView, the Google OCR library will be added to the Gradle repository; being a standalone library to Android, is compiled and made use of it and the TextBlock and Frame objects that are from the OCR library are installed. The Frame is instantiated which will take the contents of the bitmap so that with an array of type BlockText can be adapted and obtained the lines of text recognized by the device. Finally, the contents of the array are mapped in the TexView to show the user the detected text on the screen. At the end, the function that receives the obtained text is executed, and with the Tex-To-Speech class, an object of that class is instantiated so that it can initialize the event where it receives the Text, and the language setting to which it will read the detected text is assigned.

For the mobile app to work properly, the following requirements are required:

- Software specifications

  – Mobile device with at least Android 7 operating system
  – Space available for the application of at least 20 MB for installation

- Hardware Specifications:

  – Camera and speakers, on mobile device
  – Voice recognition sensor

The test was performed on a cell phone running Android 10 operating system. When you run it, the Splash screen is displayed, which presents the name of the application and its logo (Figure 1).


**Figure 1** Home screen

The data entry is then captured. The support of a person acting as an assistant must be supported to correctly capture the text to be translated by voice. Figure 2 shows the functions of the application. The Scan Text button opens your device's camera to capture the photo of the text you want to interpret audibly.

ISSN 2410-3993


**Figure 2** Data capture screen

Once the photo is captured, the application will interpret the text of the image and convert it to voice to play it automatically (Figure 3).


**Figure 3** Text-to-speech

The accessibility of the mobile application for reading text images was satisfactory, compared to other programs, due to its easy use on mobile devices with visually impaired people.

**Acknowledgment**

A scientific article is a work that is not only the result of the efforts of the members of the Academic Corps of Information Technologies of the Tecnológico Nacional de México / Instituto Tecnológico de Tehuacán, but needs the help of many people, both professionally and personally. With these lines we want to show our thanks to all of them.

To Tecnológico Nacional de Mexico, the central body of our national system, because thanks to its economic support programs we have managed to grow as teachers and discover that we can contribute to the development of knowledge and technology in research and inclusion.

To Master Yeyetzin Sandoval González, director of the Tecnológico Nacional de México / Instituto Tecnológico de Tehuacán, for her unconditional support in all our academic projects.

To Master Lucrecia Guadalupe Valenzuela Segura, who in addition to being our reference in the subject of inclusion and the "machinist" of this train, is an excellent person with us.

To our families, who usually do not understand our projects, our long sessions in front of the computer, or our delays at lunchtime, thank you for your patience.

**Conclusions**

This article has talked about visually impaired supports. In this same tenor, in correspondence with the needs, professionals are also required to take advantage of technology to develop typhotechnological tools, depending on the type or level of visual impairment.

It was shown that to develop mobile applications and projects in general, it is necessary to employ appropriate methodologies to ensure a reduced delivery time and quality, based on constant reviews with the customer, coordinators and the team.

ISSN 2410-3993

A portion of the application's execution was shown, detailing that the end result is the audible reproduction of text that might be in a magazine, sign, ad, notice, or real-life object, which a visually impaired person could not locate and understand. A simple yet understandable, voice-based and thoughtful interface was designed for the visually impaired.

Efforts to do this type of aid should not be spared, they are valuable and necessary. The inclusion of visually impaired persons could be achieved gradually if research and technological developments are increased. If this article provides a small grain of sand, then we will be satisfied.

**References**

A. Cardona, R. V. (2019). Mobility assistance devices in visually impaired people: a bibliographic review. Polytechnic Journal, 15(28), 107–116. Polytechnic Journal, 15(28), 107–116. https://doi.org/10.33571/rpolitec.v15n28a10

Bellino, A., & Herskovic, V. (2019). CameraKeyboard: A novel interaction technique for text entry through smartphone cameras. IEEE Access, 7, 167982–167996. https://doi.org/10.1109/ACCESS.2019.2954101

Bibik, I. (2018). How to Kill the Scrum Monster: Quick Start to Agile Scrum Methodology and the Scrum Master Role. In Apress Media LLC. https://doi.org/10.1007/978-1-4842-3691-8

Escandell Bermúdez, María Olga, Fortea Sevilla, María del Sol, Castro Sánchez, J. J. (2014). DIGITAL GAP IN VISUALLY IMPAIRED PEOPLE. International Journal of Developmental and Educational Psychology, 1(1), 489–497. DOI: 10.17060 / ijodaep.2014.n1.v1.396

Esparza-Maldonado, A. L., Margain-Fuentes, L. Y., Alvarez-Rodríguez, F. J., & Benítez-Guerrero, E. I. (2018). Development and evaluation of an interactive system for the visually impaired. Technological , 21(41), 149–157. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-77992018000100010&lng=en&tlng

INEGI, I.N. de E. and G. (2010). No Title. Health and Social Continuity (Disability). https://www.inegi.org.mx/app/areasgeograficas/?ag=21#tabMCcollapse-Indicadores

López Delgado, A., Olmedo, E., Tadeu, P., & Fernández Batanero, J. M. (2019). Propuesta de las condiciones de las Aplicaciones móviles, para la construcción de un Entorno de Accesibilidad Personal para usuarios con discapacidad visual en las Smart Cities. Aula Abierta, 48(2), 193. https://doi.org/10.17811/rifie.48.2.2019.193-202

Natalina Martiniello, Werner Eisenbarth, Christine Lehane, A. J. W. W. (2019). Exploring the use of smartphones and tablets among people with visualimpairments: Are mainstream devices replacing the use of traditional visual aids? AssistiveTechnology, 1–13. https://doi.org/10.1080/10400435.2019.1682084

Zambrano, D. M., Daza Álava, Y. D., Pinargote Zambrano, J. D., & Lituma Ramirez, E. D. (2019). Prototipo para orientación de personas con discapacidad Visual mediante una aplicación para móvil. Revista Científica, 2(35), 247–257. https://doi.org/10.14483/23448350.14523.

ISSN 2410-3993

Article **Journal of Technology and Innovation**
December 2020 Vol.7 No.21 32-37

# Comparative analysis of methods to determine deflection in steel beams: theoretical analysis, finite element and experimental

# Análisis comparativo de métodos para determinar la deflexión en vigas de acero: análisis teórico, elemento finito y experimental

ALOR-SAVEDRA, Gabriela†, ALAFFITA-HERNÁNDEZ, Francisco Alejandro, ESCOBEDO-TRUJILLO, Beatris Adriana* and SILVA-ÁGUILAR, Oscar Fernando

*Universidad Veracruzana, Faculty of Engineering, Coatzacoalcos campus, Mexico.*
*Universidad Veracruzana, Research Center on Energy and Sustainable Resources. Mexico.*

ID 1st Author: *Gabriela, Alor-Saavedra*

ID 1st Co-author: *Francisco Alejandro, Alaffita-Hernández* / **ORC ID:** 0000-0002-9462-0160, **Researcher ID Thomson:** 57103583500

ID 2nd Co-author: *Beatris Adriana, Escobedo-Trujillo* / **ORC ID:** 0000-0002-8937-3019, **Scopus ID:** 54417142300, **CVU CONACYT ID:** 173174

ID 3rd Co-author: *Oscar Fernando, Silva-Aguilar* / **ORC ID:** 0000-0002-5109-3193, **CVU CONACYT ID:** 338659

**DOI:** 10.35429/JTI.2020.21.7.32.37 Received July 30, 2020; Accepted December 30, 2020

**Abstract**

This work makes a comparative study of two methods to determine deflection in steel beams: (a) Theoretical and (b) Finite element. For method (a) the solution of the differential equation associated with the modeling of the deflection of a beam is found, while for method (b) a simulation is made in Solidworks. Both methods are compared with experimental data in order to analyze which of the methods presents less uncertainty and show the usefulness of the theoretical part in the modeling of physical systems.

**Steel beams, Deflection, Punctual load**

**Resumen**

El trabajo hace un estudio comparativo de dos métodos para determinar la deflexión en vigas de acero: (a) Teórico y (b) Elemento finito. Para el método (a) se encuentra la solución de la ecuación diferencial asociada al modelado de la deflexión de una viga, mientras que, para el método (b) se hace una simulación en Solidworks. Ambos métodos son comparados con datos experimentales con la finalidad de analizar cuál de los métodos presenta menor incertidumbre y mostrar la utilidad de la parte teórica en el modelado de sistemas físicos.

**Vigas de acero, Deflexión, Carga puntual**

**Citation:** ALOR-SAVEDRA, Gabriela, ALAFFITA-HERNÁNDEZ, Francisco Alejandro, ESCOBEDO-TRUJILLO, Beatris Adriana and SILVA-ÁGUILAR, Oscar Fernando. Comparative analysis of methods to determine deflection in steel beams: theoretical analysis, finite element and experimental. Journal of Technology and Innovation. 2020. 7-21:32-37.

* Correspondence to Author (E-Mail: bescobedo@uv.mx)
† Researcher contributing as first author.

## Introduction

Currently, for the design of some structural element, tools are used to simulate the deflection of a beam subjected to various loads, this detailed analysis is to more accurately visualize the response of the element under the loads to which it will be subjected during its life useful or some natural phenomenon. Detailed analysis of the deflection of a beam can be accomplished in two different ways: using software, both of which reduce the time for calculating the deflections. These programs, in general, work with the finite element method and in addition to the deflections they can provide other data. The second way is to do the analysis by means of mathematical formulas, mostly with differential equations, that is, look for what effect the element will have and find the formula that models this phenomenon.

In (Huo, 2017) they analyze steel beams, which, when subjected to a load in a laboratory test, the beam becomes deformed. 6 tests are carried out on 6 different profiles, once the results are displayed they propose another 4 profiles. The two types of profiles are cold rolled and hot rolled. The ABAQUS® program was also used to make the comparison with the test data. The experimental and simulated results are almost the same. In the work of (J. T. Katsikadelis, 2003) et al. A deflection analysis is made by means of Euler-Bernoulli equations contemplating a variable stiffness that undergoes large displacements under general boundary conditions that may be non-linear. As the properties of the beam's cross-section vary along its axis, the coefficients of the differential equations that govern the beam are variable as well. On the other hand, like (JT Katsikadelis, 2003), (Peijun Wang, 2016) et al., Suggest that the finite element method is very effective for the behaviors that beams may have when subjected to loads of mock tests. There are several works that do the deflection analysis of beams, we recommend the reader to review the references of the articles cited in this work.

In this work we will analyze the deflection of a steel beam per finite element in Solidworks®, as well as, using the differential equation of the elastic. We compare the deflection results by the aforementioned methods with the experimental data obtained from the test carried out in the authors' work (Huo, 2017).

## Deflection by laboratory test

The first data that are considered for the comparison of the deflection are those presented in (Huo, 2017). These data are obtained through the test described below:

Six impact tests were carried out on different type "I" profiles of cold rolled steel, welded at the ends to place the supports. The test was carried out with the machine shown in Figure 1 where a force was applied by means of the load control to the hammer with a weight of 980 kg and a maximum fall height of 16 m, the hammer falls to a certain height and impacts the midsection of each steel beam. A system was used to acquire the data which were captured by means of sensors distributed along the web of the beam.

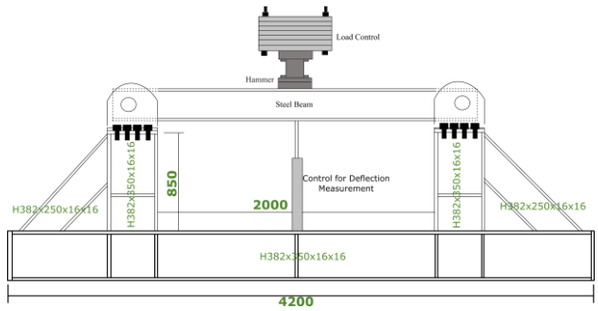



**Figure 1** General view of the impact test

The area where the hammer will be impacted was reinforced with plates so that when the load was applied, the profile would not suffer a greater torsion. Since the test not only seeks to obtain the deflection that exists in the beam but also other phenomena, the applied loads are different. Once the tests were carried out, and taking into account the results of the six previous tests, they carried out four more tests, but on type “I” profiles of hot rolled steel.

This test was conducted at the Center for Integrated Protection of Engineering Structures Research (CIPRES) at Hunan University in Changsha, People's Republic of China.

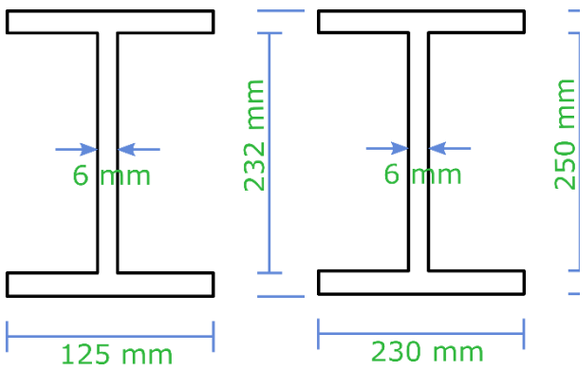
The data found in Table 1 are some of the data presented in (Huo, 2017), they are not all since only those shown in the table are used.

ISSN 2410-3993

| Profiles | Measurements (mm) | $F_{umax}$ kN | $F_{ue}$ kN | $F_{uc}$ kN | $F_p$ kN |
|---|---|---|---|---|---|
| Cold rolled | | | | | |
| HW11-58 | H266x182x6x8 | 822 | 382 | 290 | 230 |
| Hot rolled | | | | | |
| HR7-46 | H250x125x6x9 | 790 | 260 | 176 | 136 |

**Table 1** Steel Profile Details and Specifications

Table 1 shows the forces captured by the sensors. The forcé *Fumax* is the maximum impact force taken by the sensors, Fue is the average impact force of all the forces captured during the time of the test, Fuc is the static concentrated force and Fp is the plastic capacity of the beam. To calculate the deflection of the beam, both with Solidworks® and with a differential equation, the load Fue will be used, for the 2 beams HW11-58 and HR7-46.




*a) Profile HR7-46* *b) Profile HW11-.58*

**Figure 2** Profile measurements

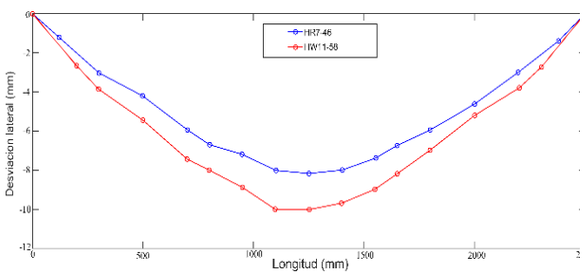



**Figure 3** Impact test overview

The results of Figure 3 are the deflections of the two profiles under the loads by the average impact forces (*Fue*).

## Deflection by finite element method in Solidworks

The beam shown in (Huo, 2017) is drawn in the same way, with the same dimensions and the same material, see Figure 4 and proceed to do the hammer test. Unlike the data obtained by the hammer test in Huo, 2017, only two different profiles are used in Solidworks®.

A simulation of the two profiles is performed with the force It was given in Table 1. Once the required simulations are performed, the information is processed in Matlab®.

Figure 4 presents the beam with all the elements that are needed, the fasteners, loads and meshing.

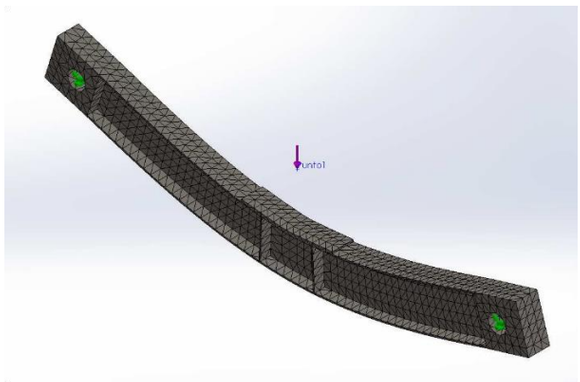


**Figure 4** Beam model in Solidworks®

## Deflection by analytical method (Elastic method or double integration)

For the elastic equation, it is a homogeneous material beam and has a uniform cross section throughout the length of the beam. At the center of the cross section, an imaginary line called the neutral axis or axis of symmetry is drawn. If force is applied in the plane perpendicular to the neutral axis, this axis presents a distortion, this distortion of the neutral axis is known as deflection or elastic curve, see Figure 5.

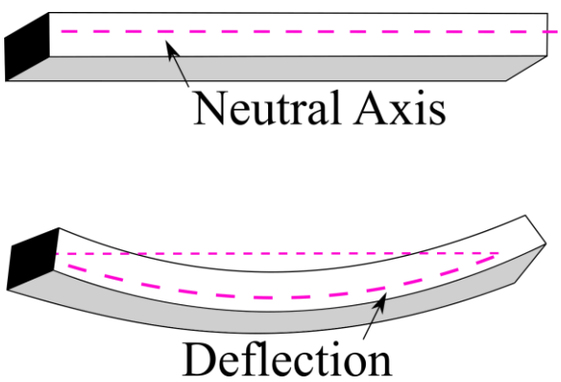



**Figure 5** Representation of the elastic curve of a beam

In the elastic theory it is shown that the bending moment (Mx) at a point along the length of the beam (x) is related to the load to which the beam may be subjected by the following equation (Denis G. Zill, 2013):

ISSN 2410-3993

$$\frac{d^2y}{dx^2} = -\frac{M}{EI} \quad (1)$$

Equation (1) is an ordinary, linear, second-order differential equation, and governs the evolution of the elastic curve, which describes the deflections that a beam experiences when subjected to transverse loads.

The multiplication of EI represents the stiffness of the beam. The modulus of elasticity is taken from the data provided by Solidworks® when selecting the material of the beam. The moments of inertia (I) are as follows:

- $3.892x10^{-5}$ $m^4$ for profile HR7-46
- $5.628x10^{-5}$ $m^4$ for profile HW11-58

The M in equation (1) represents the bending moment.

The load P applied to the beam is in the center of the beam span. The supports have vertical reactions P / 2, the normal forces cancel out since it is assumed that the beam is not subjected to a horizontal force. Taking the reactions in the supports, the bending moment is calculated. There are two bending moments (2) - (3), one before the middle of the beam (SECTION I), and the other is considered after the middle and as far as it ends (SECTION II). These moments are those that are substituted in equation (1), each one in its respective section.

$$M_{x1} = \frac{P}{2}x \quad 0 \le x \le \frac{L}{2} \quad (2)$$

$$M_{x1} = \frac{P}{2}x - P\left(x - \frac{L}{2}\right) \quad 0 \le x \le \frac{L}{2} \quad (3)$$

Then the deflections for the sections are as follows:

SECTION I

$$y = \frac{1}{EI}\left(-\frac{Px^3}{12} + \frac{PL^2}{16}x\right) \quad (4)$$

SECTION II

$$y = \frac{1}{EI}\left(-\frac{Px^3}{12} - \frac{PLx^2}{4} + \frac{3PL^2}{16}x + \frac{PL^3}{48}\right) \quad (5)$$

To find the maximum deflection in the beam, we substitute x = L / 2 in equations (4) and (5) and we have the following result for both sections:

$$y_{max} = \frac{PL^3}{48EI}$$

**Results**

Deflection in hot rolled steel profile (HR7-46) Table 1 shows the force Fue that was applied to the beam, and Figure 6 shows the Solidworks simulation with its respective load. The colors shown represent the deflections, as it is moving, blue represents the 0 displacement and red the maximum displacement.

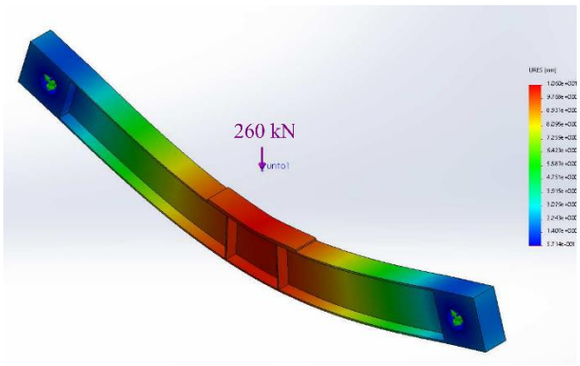



**Figure 6** Deflection of a hot rolled steel beam subjected to a load of 260 kN

Table 2 shows the deflections that exist along the beam, with the experimental data given in (Huo, 2017) and Solidworks, as well as a column that contains the quadratic error at each node.

| Length. | Exp. | Solidworks® | Quadratic Error |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 12 | -0.120 | -0.137 | 0.000289 |
| 30 | -0.302 | -0.358 | 0.003136 |
| 50 | -0.419 | -0.582 | 0.026569 |
| 70 | -0.594 | -0.781 | 0.034969 |
| 80 | -0.670 | -0.861 | 0.036481 |
| 95 | -0.719 | -0.951 | 0.053824 |
| 110 | -0.802 | -1.013 | 0.044521 |
| 125 | -0.817 | -1.034 | 0.047089 |
| 140 | -0.808 | -1.013 | 0.042025 |
| 155 | -0.737 | -0.951 | 0.045796 |
| 165 | -0.674 | -0.895 | 0.048841 |
| 180 | -0.594 | -0.780 | 0.034596 |
| 200 | -0.461 | -0.586 | 0.015625 |
| 220 | -0.299 | -0.362 | 0.003969 |
| 240 | -0.138 | -0.138 | 0 |
| 250 | 0 | 0 | 0 |

**Table 2** Profile HR7-46. Deflection along the hot rolled steel beam with a load of 260 kN

ISSN 2410-3993

*Deflection in cold rolled steel profile (HW11-58)*

As for the beam with hot rolled profile, the force Was applied to the beam with a cold rolled steel profile and the simulation was carried out in Solidworks®, see Figure 7. Table 3 contains all the deflections, with their respective values. As can be seen, the quadratic error between the experimental data given in (Huo, 2017) and those obtained in the simulation is small, this indicates that the simulation in Solidworks gives a good approximation of the deflection in steel beams.

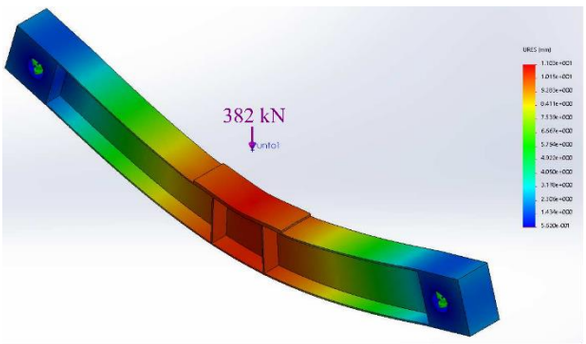



**Figure 7** Deflection of a cold rolled steel beam under different loads

| Length. | Exp. | Solidworks® | Quadratic Error |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 20 | -0.265 | -0.237 | 0.000784 |
| 30 | -0.385 | -0.361 | 0.000576 |
| 50 | -0.543 | -0.597 | 0.002916 |
| 70 | -0.743 | -0.795 | 0.002704 |
| 80 | -0.800 | -0.876 | 0.005776 |
| 95 | -0.888 | -0.973 | 0.007225 |
| 110 | -1.000 | -1.04 | 0.0016 |
| 125 | -1.001 | -1.103 | 0.010404 |
| 140 | -1.000 | -0.976 | 0.000576 |
| 155 | -0.888 | -0.976 | 0.007744 |
| 165 | -0.800 | -0.920 | 0.0144 |
| 180 | -0.743 | -0.794 | 0.002601 |
| 200 | -0.543 | -0.589 | 0.002116 |
| 220 | -0.685 | -0.363 | 0.103684 |
| 240 | -0.265 | -0.233 | 0.001024 |
| 250 | 0 | 0 | 0 |

**Table 3** Profile HR11-58. Deflection along the cold rolled steel beam with a load of 382 kN

**Deflection by analytical method**

Tables 4 and 5 present the deflections that exist in the beam by experimental means and by means of an analytical method or differential equations, as well as a column of mean square errors at each node, for profiles HR7-46 and HR11-58., respectively. Similarly, in the Solidworks simulation it is found that the quadratic error between the experimental data given in (Huo, 2017) and those obtained with the solution of the differential equation (1) is small, this indicates that the solutions (4) - (5) also give a good approximation of deflection in steel beams.

| Length. | Exp. | Analítico | Quadratic Error |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 12 | -0.120 | -0.147 | 0.000729 |
| 30 | -0.302 | -0.365 | 0.003969 |
| 50 | -0.419 | -0.588 | 0.028561 |
| 70 | -0.594 | -0.778 | 0.033856 |
| 80 | -0.670 | -0.859 | 0.035721 |
| 95 | -0.719 | -0.952 | 0.054289 |
| 110 | -0.802 | -1.009 | 0.042849 |
| 125 | -0.817 | -1.05 | 0.054289 |
| 140 | -0.808 | -1.014 | 0.042436 |
| 155 | -0.737 | -0.953 | 0.046656 |
| 165 | -0.674 | -0.893 | 0.047961 |
| 180 | -0.594 | -0.778 | 0.033856 |
| 200 | -0.461 | -0.588 | 0.016129 |
| 220 | -0.299 | -0.365 | 0.004356 |
| 240 | -0.138 | -0.148 | 1E-04 |
| 250 | 0 | 0 | 0 |

**Table 4** Profile HR7-46. Deflection along the hot rolled steel beam with a load of 260 kN.

| Length. | Exp. | Analítico | Quadratic Error |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 20 | -0.265 | -0.2628 | 4.84E-06 |
| 30 | -0.385 | -0.39 | 0.000025 |
| 50 | -0.543 | -0.627 | 0.007056 |
| 70 | -0.743 | -0.830 | 0.007569 |
| 80 | -0.800 | -0.945 | 0.021025 |
| 95 | -0.888 | -1.011 | 0.015129 |
| 110 | -1.000 | -1.082 | 0.006724 |
| 125 | -1.001 | -1.18 | 0.032041 |
| 140 | -1.000 | -1.085 | 0.007225 |
| 155 | -0.888 | -1.017 | 0.016641 |
| 165 | -0.800 | -0.953 | 0.023409 |
| 180 | -0.743 | -0.839 | 0.009216 |
| 200 | -0.543 | -0.616 | 0.005329 |
| 220 | -0.685 | -0.377 | 0.094864 |
| 240 | -0.265 | -0.249 | 0.000256 |
| 250 | 0 | 0 | 0 |

**Table 5** Profile HR11-58. Deflection along the cold rolled steel beam with a load of 382 kN.

ISSN 2410-3993

## Conclusions

As can be seen in Table 6, the mean square errors are small, even the difference between the two methods is not really significant, which is a very good indication that the analytical methods do not lose their validity. It is important to highlight the fact that using Solidworks increases precision, which is the most suitable for very large projects.

| Profile | Solidworks | Analytical method |
|---|---|---|
| HR7-46 | 0.02574882 | 0.026221 |
| HR11-58 | 0.00965471 | 0.01450081 |

**Table 6** Mean square error for both profiles HR7-46 and HR11-58 for the two methods analyzed

## References

Jinqing Zhang; Jingsi Huo. (2017). *Dynamic behaviour and catenary action of axially-restrained steel beam under impact loading*. Structure, 11:84–96.

G. C. Tsiatas J. T. Katsikadelis. (2003*) Large deflection analysis of beams with variable stiffness*. Acta Mechanica, 164:1–13.

Mei Liu Peijun Wang, Changbin Liu. (2016). *Large deflection behavior of restrained corrugate web steel beams in a fire. Journal of Constructional Steel Research*, 126:92–106.

Warren S. Wright Denis G. Zill. (2013). *Ecuaciones diferenciales, con problemas con valores de frontera*. CENGACE Learning.

ISSN 2410-3993

# [Title in Times New Roman and Bold No. 14 in English and Spanish]

Surname (IN UPPERCASE), Name 1st Author†*, Surname (IN UPPERCASE), Name 1st Coauthor, Surname (IN UPPERCASE), Name 2nd Coauthor and Surname (IN UPPERCASE), Name 3rd Coauthor

*Institutional Affiliation of Author including Dependency (No.10 Times New Roman and Italic)*

*International Identification of Science - Technology and Innovation*

ID 1st Author: (ORC ID - Researcher ID Thomson, arXiv Author ID - PubMed Author ID - Open ID) and CVU 1st author: (Scholar-PNPC or SNI-CONACYT) (No.10 Times New Roman)

ID 1st Coauthor: (ORC ID - Researcher ID Thomson, arXiv Author ID - PubMed Author ID - Open ID) and CVU 1st coauthor: (Scholar or SNI) (No.10 Times New Roman)

ID 2nd Coauthor: (ORC ID - Researcher ID Thomson, arXiv Author ID - PubMed Author ID - Open ID) and CVU 2nd coauthor: (Scholar or SNI) (No.10 Times New Roman)

ID 3rd Coauthor: (ORC ID - Researcher ID Thomson, arXiv Author ID - PubMed Author ID - Open ID) and CVU 3rd coauthor: (Scholar or SNI) (No.10 Times New Roman)

(Report Submission Date: Month, Day, and Year); Accepted (Insert date of Acceptance: Use Only ECORFAN)

**Abstract (In English, 150-200 words)**

Objectives
Methodology
Contribution

**Keywords (In English)**

Indicate 3 keywords in Times New Roman and Bold No. 10

**Abstract (In Spanish, 150-200 words)**

Objectives
Methodology
Contribution

**Keywords (In Spanish)**

Indicate 3 keywords in Times New Roman and Bold No. 10

**Citation:** Surname (IN UPPERCASE), Name 1st Author, Surname (IN UPPERCASE), Name 1st Coauthor, Surname (IN UPPERCASE), Name 2nd Coauthor and Surname (IN UPPERCASE), Name 3rd Coauthor. Paper Title. Journal of Technology and Innovation. Year 1-1: 1-11 [Times New Roman No.10]

* Correspondence to Author (example@example.org)
† Researcher contributing as first author.

## Introduction

Text in Times New Roman No.12, single space.

General explanation of the subject and explain why it is important.

What is your added value with respect to other techniques?

Clearly focus each of its features

Clearly explain the problem to be solved and the central hypothesis.

Explanation of sections Article.

## Development of headings and subheadings of the article with subsequent numbers

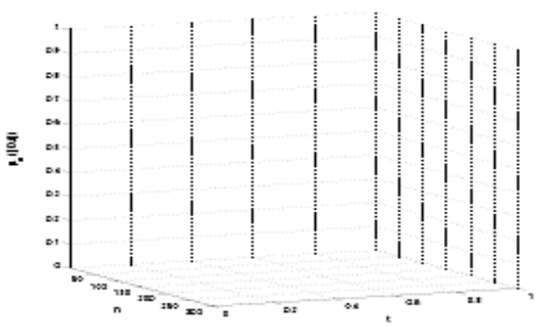
[Title No.12 in Times New Roman, single spaced and bold]

Products in development No.12 Times New Roman, single spaced.

## Including graphs, figures and tables-Editable

In the article content any graphic, table and figure should be editable formats that can change size, type and number of letter, for the purposes of edition, these must be high quality, not pixelated and should be noticeable even reducing image scale.

[Indicating the title at the bottom with No.10 and Times New Roman Bold]



**Graphic 1** Title and *Source (in italics)*

Should not be images-everything must be editable.

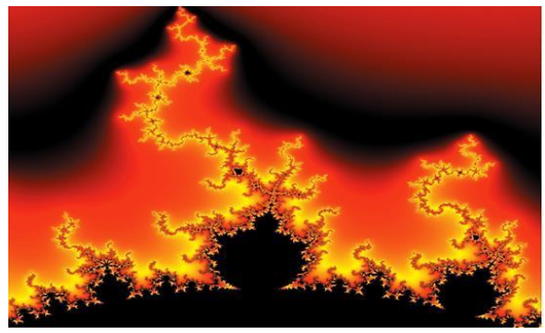


**Figure 1** Title and *Source (in italics)*

Should not be images-everything must be editable.

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

**Table 1** Title and *Source (in italics)*

Should not be images-everything must be editable.

Each article shall present separately in **3 folders**: a) Figures, b) Charts and c) Tables in .JPG format, indicating the number and sequential Bold Title.

**For the use of equations, noted as follows:**

$$Y_{ij} = \alpha + \sum^{h=1} \beta_h X_{hij} + u_j + e_{ij} \quad (1)$$

Must be editable and number aligned on the right side.

## Methodology

Develop give the meaning of the variables in linear writing and important is the comparison of the used criteria.

## Results

The results shall be by section of the article.

## Annexes

Tables and adequate sources

## Thanks

Indicate if they were financed by any institution, University or company.

## Conclusions

Explain clearly the results and possibilities of improvement.

ISSN 2410-3993

**References**

Use APA system. Should not be numbered, nor with bullets, however if necessary numbering will be because reference or mention is made somewhere in the Article.

Use Roman Alphabet, all references you have used must be in the Roman Alphabet, even if you have quoted an Article, book in any of the official languages of the United Nations (English, French, German, Chinese, Russian, Portuguese, Italian, Spanish, Arabic), you must write the reference in Roman script and not in any of the official languages.

**Technical Specifications**

Each article must submit your dates into a Word document (.docx):

Journal Name
Article title
Abstract
Keywords
Article sections, for example:

*1. Introduction*
*2. Description of the method*
*3. Analysis from the regression demand curve*
*4. Results*
*5. Thanks*
*6. Conclusions*
*7. References*

Author Name (s)
Email Correspondence to Author
References

**Intellectual Property Requirements for editing:**

-Authentic Signature in Color of Originality Format Author and Coauthors

-Authentic Signature in Color of the Acceptance Format of Author and Coauthors

ISSN 2410-3993

**Reservation to Editorial Policy**

Journal of Technology and Innovation reserves the right to make editorial changes required to adapt the Articles to the Editorial Policy of the Journal. Once the Article is accepted in its final version, the Journal will send the author the proofs for review. ECORFAN® will only accept the correction of errata and errors or omissions arising from the editing process of the Journal, reserving in full the copyrights and content dissemination. No deletions, substitutions or additions that alter the formation of the Article will be accepted.

**Code of Ethics - Good Practices and Declaration of Solution to Editorial Conflicts**

**Declaration of Originality and unpublished character of the Article, of Authors, on the obtaining of data and interpretation of results, Acknowledgments, Conflict of interests, Assignment of rights and Distribution**

The ECORFAN-Mexico, S.C Management claims to Authors of Articles that its content must be original, unpublished and of Scientific, Technological and Innovation content to be submitted for evaluation.

The Authors signing the Article must be the same that have contributed to its conception, realization and development, as well as obtaining the data, interpreting the results, drafting and reviewing it. The Corresponding Author of the proposed Article will request the form that follows.

Article title:

– The sending of an Article to Journal of Technology and Innovation emanates the commitment of the author not to submit it simultaneously to the consideration of other series publications for it must complement the Format of Originality for its Article, unless it is rejected by the Arbitration Committee, it may be withdrawn.

– -None of the data presented in this article has been plagiarized or invented. The original data are clearly distinguished from those already published. And it is known of the test in PLAGSCAN if a level of plagiarism is detected Positive will not proceed to arbitrate.

– References are cited on which the information contained in the Article is based, as well as theories and data from other previously published Articles.

– The authors sign the Format of Authorization for their Article to be disseminated by means that ECORFAN-Mexico, S.C. In its Holding Bolivia considers pertinent for disclosure and diffusion of its Article its Rights of Work.

– Consent has been obtained from those who have contributed unpublished data obtained through verbal or written communication, and such communication and Authorship are adequately identified.

– The Author and Co-Authors who sign this work have participated in its planning, design and execution, as well as in the interpretation of the results. They also critically reviewed the paper, approved its final version and agreed with its publication.

– No signature responsible for the work has been omitted and the criteria of Scientific Authorization are satisfied.

– The results of this Article have been interpreted objectively. Any results contrary to the point of view of those who sign are exposed and discussed in the Article.

**Copyright and Access**

The publication of this Article supposes the transfer of the copyright to ECORFAN-Mexico, SC in its Holding Bolivia for it Journal of Technology and Innovation, which reserves the right to distribute on the Web the published version of the Article and the making available of the Article in This format supposes for its Authors the fulfilment of what is established in the Law of Science and Technology of the United Mexican States, regarding the obligation to allow access to the results of Scientific Research.

Article Title:

| Name and Surnames of the Contact Author and the Coauthors | Signature |
|---|---|
| 1. | |
| 2. | |
| 3. | |
| 4. | |

**Principles of Ethics and Declaration of Solution to Editorial Conflicts**

**Editor Responsibilities**

The Publisher undertakes to guarantee the confidentiality of the evaluation process, it may not disclose to the Arbitrators the identity of the Authors, nor may it reveal the identity of the Arbitrators at any time.

The Editor assumes the responsibility to properly inform the Author of the stage of the editorial process in which the text is sent, as well as the resolutions of Double-Blind Review.

The Editor should evaluate manuscripts and their intellectual content without distinction of race, gender, sexual orientation, religious beliefs, ethnicity, nationality, or the political philosophy of the Authors.

The Editor and his editing team of ECORFAN® Holdings will not disclose any information about Articles submitted to anyone other than the corresponding Author.

The Editor should make fair and impartial decisions and ensure a fair Double-Blind Review.

**Responsibilities of the Editorial Board**

The description of the peer review processes is made known by the Editorial Board in order that the Authors know what the evaluation criteria are and will always be willing to justify any controversy in the evaluation process. In case of Plagiarism Detection to the Article the Committee notifies the Authors for Violation to the Right of Scientific, Technological and Innovation Authorization.

**Responsibilities of the Arbitration Committee**

The Arbitrators undertake to notify about any unethical conduct by the Authors and to indicate all the information that may be reason to reject the publication of the Articles. In addition, they must undertake to keep confidential information related to the Articles they evaluate.

Any manuscript received for your arbitration must be treated as confidential, should not be displayed or discussed with other experts, except with the permission of the Editor.

The Arbitrators must be conducted objectively, any personal criticism of the Author is inappropriate.

The Arbitrators must express their points of view with clarity and with valid arguments that contribute to the Scientific, Technological and Innovation of the Author.

The Arbitrators should not evaluate manuscripts in which they have conflicts of interest and have been notified to the Editor before submitting the Article for Double-Blind Review.

**Responsibilities of the Authors**

Authors must guarantee that their articles are the product of their original work and that the data has been obtained ethically.

Authors must ensure that they have not been previously published or that they are not considered in another serial publication.

Authors must strictly follow the rules for the publication of Defined Articles by the Editorial Board.

The authors have requested that the text in all its forms be an unethical editorial behavior and is unacceptable, consequently, any manuscript that incurs in plagiarism is eliminated and not considered for publication.

Authors should cite publications that have been influential in the nature of the Article submitted to arbitration.

**Information services**

**Indexation - Bases and Repositories**

LATINDEX (Scientific Journals of Latin America, Spain and Portugal)
RESEARCH GATE (Germany)
GOOGLE SCHOLAR (Citation indices-Google)
REDIB (Ibero-American Network of Innovation and Scientific Knowledge- CSIC)
MENDELEY (Bibliographic References Manager)

**Publishing Services**

Citation and Index Identification H
Management of Originality Format and Authorization
Testing Article with PLAGSCAN
Article Evaluation
Certificate of Double-Blind Review
Article Edition
Web layout
Indexing and Repository
ArticleTranslation
Article Publication
Certificate of Article
Service Billing

**Editorial Policy and Management**

21 Santa Lucía, CP-5220. Libertadores -Sucre–Bolivia. Phones: +52 1 55 6159 2296, +52 1 55 1260 0355, +52 1 55 6034 9181; Email: contact@ecorfan.org www.ecorfan.org

# Journal of Technology and Innovation



2410 3993
ISSN 2410 - 3993

www.ecorfan.org