ISSN 2531-2197

Journal Computer Technology

Volume 7, Issue 18 – January – June – 2023

ECORFAN®

Journal Computer Technology, Volume 7, Issue 18, June - 2023, is a biannual Journal edited by ECORFAN-Spain. Matacerquillas Street 38, CP: 28411. Moralzarzal-Madrid. WEB: http://www.ecorfan.org/spain/rj_tec_informatica.php, revista@ecorfan.org. Editor in Chief: JALIRI-CASTELLON, María Carla Konradis. PhD. ISSN 2531-2197. Responsible for the last update of this issue ECORFAN Computer Unit. Imelda Escamilla Bouchán, PhD. Vladimir Luna Soto, PhD. Updated as of June 30, 2023.

Journal Computer Technology

Definition of Journal

Scientific Objectives

Support the International Scientific Community in its written production of Science, Technology in Innovation in the Area of Engineering and Technology, in subdisciplines Data Management, Establishment of Computer Networks, Design of Database Systems, Software Design, Computer Science, Software, Computer Technology with Services, Business Process Outsourcing, Hardware.

ECORFAN-Mexico, S.C. 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 CONAHCYT-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 - CONAHCYT Research Centers.

Scope, Coverage and Audience

Journal Computer Technology is a Journal edited by ECORFAN-México S.C in its Holding with repository in Spain, is a scientific publication arbitrated and indexed on a quarterly basis. It supports a wide range of content that is evaluated by academic peers by the Double-Blind method, around topics related to the theory and practice of Data Management, Establishment of Computer Networks, Design of Database Systems, Software Design, Computing, Software, Computer Technology with Services, Business Process Outsourcing, Hardware with Diverse Approaches and Perspectives , that contribute to the dissemination of the development of Science Technology and Innovation that allow arguments related to decision-making and influence 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 research and analysis segments outside this field, as long as they meet the requirements of argumentative and scientific rigor, as well as addressing topics of general and current interest of the International Scientific Society.

Editorial Board

Arbitration Committee

Assignment of Rights

The sending of an Article to Journal Computer Technology 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 Spain 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-CONAHCYT- 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 CONAHCYT 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 Data Management, Establishment of Computer Networks, Design of Database Systems, Software Design, Computer Science, Software, Computer Technology with Services, Business Process Outsourcing, Hardware and other topics related to Engineering and Technology.

Presentation of content

In Volume six, issue sixteen, as the first article we present, *Technologies used in museums in Mexico*, by VARGAS-MUÑOZ, Emmanuel & ESCAMILLA-REGIS, Daisy, with secondment at the Tecnológico de Estudios Superiores de Cuautitlán Izcalli, as a second article we present, *Artificial vision techniques at the frontiers of video surveillance*, by PÉREZ-ESCAMILLA, Javier, MENDOZA-GUZMÁN, Lorena, CRUZ-GUERRERO, René and PORRAS-MUÑOZ, Rolando, with an appointment at Tecnológico Nacional de México / ITS del Oriente del Estado de Hidalgo and Tecnológico Nacional de México / ITS del Occidente del Estado de Hidalgo, as a third article we present, *Development of a web application for hotspot token vending machine administration*, by SAMPAYO-RODRÍGUEZ, Carmen Jeannette, GONZÁLEZ-AMBRIZ, Rosalba, LUNA-CARRASCO, Claudia Yadira and LUNA-TREJO, Cupertino, with secondment at Tecnológico Nacional de México - Instituto Tecnológico Superior de Huauchinango, as fourth article we present, *Importance of the analysis of computer attacks on a LAN network applying the predictive-quantitative method*, by SAUCEDO-LEÓN, Daniel, SAMPAYO-RODRÍGUEZ, Carmen Jeannette, GONZÁLEZ-AMBRIZ, Rosalba and MORALES-OLIVARES, Rosibel, with secondment Tecnológico Nacional de México, Instituto Tecnológico Superior de Huauchinango.

Content

Article **Journal Computer Technology**
June 2023, Vol.7 No.18 1-7

Technologies used in museums in Mexico

Tecnologías utilizadas en museos de México

VARGAS-MUÑOZ, Emmanuel†* & ESCAMILLA-REGIS, Daisy

Tecnologico de Estudios Superiores de Cuautitlan Izcalli

ID 1st Autor: *Emmanuel, Vargas-Muñoz* / **ORC ID:** 0000-0002-7038-4308

1st Co-author: *Daisy, Escamilla-Regis* / **ORC ID:** 0000-0003-4062-0514

DOI: 10.35429/JCT.2023.18.7.1.7 Received: January 10, 2023; Accepted June 30, 2023

Abstract

The following article is a product of research on the technologies used in museums, focusing on their historical evolution and their importance in the museum world, allowing us to understand the technological tools used in museums in Mexico. The use of intranets for internal processes will be analyzed, as well as their continuous improvement. The importance of uses of inventory control systems and their development used to control fixed assets, bibliographical heritage, collections, books and audios. Automation in exhibition halls with the use of multimedia. Immersive experiences in thematic exhibitions. As well as the use of digitalization technologies created by universities or private institutions. The importance of all these with a vision in the future is mentioned.

Museums, Platforms, Technology

Resumen

El siguiente artículo es un producto de una investigación sobre las tecnologías utilizadas en museos, centrándonos en la evolución histórica de las mismas y su importancia en el mundo museológico, permitiendo comprender las herramientas tecnológicas ocupadas en museos de México. Se analizará el uso de intranets para procesos internos, así como la mejora continua de los mismos. La importancia de usos de sistemas de control de inventarios y su desarrollo utilizado para control de activos fijos, acervos bibliográficos, colecciones, libros y audios. La automatización en salas de exhibición con uso de multimedia. Experiencias inmersivas en las exposiciones temáticas. Así como uso de tecnologías para la digitalización creadas por universidades o instituciones privadas. Se menciona la importancia de todas estas con una visión en el futuro.

Museos, Plataformas, Tecnología

Citation: VARGAS-MUÑOZ, Emmanuel & ESCAMILLA-REGIS, Daisy. Technologies used in museums in Mexico. Journal Computer Technology. 2023. 7-18:1-7.

* Correspondence to the author (E-mail: 213101033@cuautitlan.tecnm.mx).
† Researcher contributing as first author.

Introduction

According to the International Committee for Museology (ICOM), a museum is a non-profit, permanent institution at the service of society that researches, collects, conserves, interprets and exhibits tangible and intangible heritage. Open to the public, accessible and inclusive, museums foster diversity and sustainability. With the participation of communities, museums operate and communicate ethically and professionally, offering varied experiences for education, enjoyment, reflection and the exchange of knowledge (ICOM, 2010), in addition to this term in the case of Mexico there are many institutions that have created various museums of private collections with different themes, which greatly support the dissemination of their temporary and permanent exhibitions.

In Mexico there are two very important institutions responsible for cultural heritage that are in charge of public museums: the National Institute of Anthropology and History (INAH) and the National Institute of Fine Arts and Literature (INBAL), both governed by the Ministry of Culture, which have a great responsibility as they have the task of generating curatorships for their museums and preserving culture, thus competing with private institutions in attracting visitors.

With the above, we can deduce that there is a great variety of museums with different themes and a wide range of contents aimed at different audiences that visit these spaces, which create competition between these institutions, benefiting their audiences. This allows for the creation of exhibitions and/or quality content, resulting in content such as research articles, books, lectures or colloquiums.

All of the above is of vital importance to be supported with technological tools in order to improve their processes, managing resources in an adequate manner, control systems of their collections, dissemination media such as social networks, radio or television. The importance of exhibitions is to attract their audiences, both specialised and visitors, supported by multimedia materials in order to capture the attention and enjoyment of permanent or temporary exhibitions in museums, generating an image that encourages the viewer to revisit or recommend their visit.

It will address the importance and use of technologies in museums for the benefit of the general public and their vision for the future.

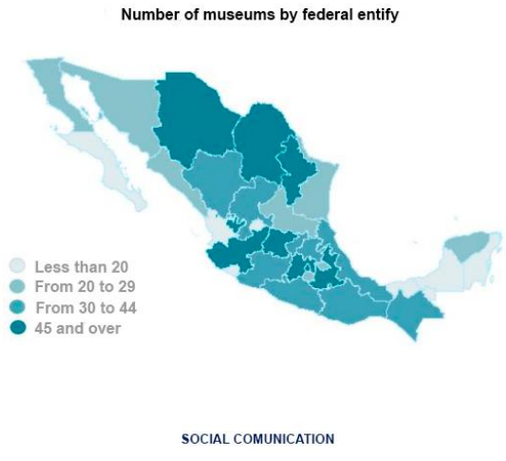
Description of the method

In order to understand the importance of the implementation of technologies in museums in Mexico, these advances were analysed based on the criteria of their popularity in the implementation of these technologies, as well as their impact on visitors.

Thanks to search engines, digital platforms for books and specialised magazines about museums, it was very helpful to learn about the beginnings of technologies implemented in museums, such as the magazine M museos (M Museos de México y del Mundo, 2004), as well as the digital library of UNESCO (UNESCO DOC, 2022) or INAH (Revistas INAH, 2022).

As well as visiting these museums, it was possible to learn more about the implementation of these technologies supporting the veracity of these cultural spaces.

The National Institute of Statistics and Geography (INEGI) reports that there are 849 museums in Mexico up to the year 2022, segmenting the areas of the national territory where the greatest number of museums exist. Analysing where the greatest number of cultural centres are located, which allowed us to analyse where technological advances have been implemented, mainly in the central zone where there is a greater concentration of these spaces.



Graphic 1 Number of museums by state
Source: (INEGI)

The qualitative methodology is adapted to this type of research as the information obtained allows us to learn more about experiences in the implementation of different technologies in different museums.

Internal process management platforms (intranet)

Since the use of the Internet as an essential element in our lives, many platforms have been created for control in different organisations. In 1995, Dr. Steven L. Tellen first used the term intranet, which functioned as a series of pages that could be consulted by a group of people. In the case of museums, they began to generate platforms that would allow them to control their internal processes.

In 1998 the Museo Nacional del Virreinato (MNV) was the first to create an intranet, in conjunction with IBM, INAH and the museum's IT staff created this platform, SIM Sistema de Información de Museos, later renamed SIGE (Sistema de Información, Gestión y Evaluación), which allowed them to view museum information, It allowed them to see information about the museum, temporary and permanent exhibitions and its organisational structure as well as its projects where the areas documented their processes, to have communication through a network of internal messages called agreements, as well as a section called opinions that allowed the staff to answer questions or congratulations from the public, as well as general inicators.

This intranet was one of the most complete in its time, allowing the evolution of the way of managing the resources of a museum in an integral way, thanks to the vision of Miguel Fernandez Felix, former director of this museum, who revolutionised the way of seeing a museum worldwide. (M Museos de México y del Mundo, 2004)

Graphic 2 SIGE
Source: (Museo Nacional del Virreinato)

Kiosks

Since the creation of the touch screen in 1971 by Dr. Sam Hurst, many interactive materials ranging from video games to interactive kiosks have been implemented in many places. In the case of museums they were and will be very useful for the visiting public to interact with an interface that will provide them with information.

This technology is implemented in most museums in Mexico because of its ease of installation and accessibility for the development of interfaces. To mention a few: Museo Nacional de Antropología, Museo Nacional del Virreinato, MIDE, MUNAL, Universum among many others. Its application in the case of virtualisation of books, zoom in maps and images.

Pintura en Internet (Rodriguez, 2005) was an exhibition that was based on a platform that allowed the consultation of more than 913 paintings of the MNV supported with kiosks that could be consulted in an interactive way, allowing to see in detail each piece with the help of a zoom and games allowing that all type of public could visit the exhibition in person or from their computer, impacting the way of seeing a pioneer museum in the creation of virtual exhibitions.

Interactive Screens and Touch Wall in the Museum of Memory, the implementation of this technology based on a wall with screens controlled by touch screens is an innovative application showing on these screens information such as cultural diversity, the power of the media, to mention a few topics, with which we can see the good use of this technology (Sordo Madaleno, et al., 2011).

ISSN 2531-2197

Bank digital collections

The importance of being able to digitise the pieces is of vital importance for their consultation and background of their conservation within museums, there are several platforms that allow the consultation of this material online in conjunction with different repositories.

Canon, together with the National Museum of Anthropology, has had a project since 2010 to digitise collections in a high-resolution format, with the aim of promoting archaeological research by means of a photographic record, embedding this information in a large database for consultation (Canon, 2010).

An image bank is the Mediateca INAH, a digital repository that can be accessed from its website to different collections of all museums and archaeological sites, as well as reference materials such as photographic collections, audios and videos that help visitors learn about everything the institute offers in order to learn about Mexico's cultural heritage.

The Mexican platform created by the Ministry of Culture in 2017 is made up of different digital banks of different organisations, institutions and museums belonging to the Ministry, linked by different databases that are updated automatically, which allows for a robust system in terms of the variety of content that can be consulted, as it contains all the digitised collections, being a project that promotes the accessibility of digital content for the general population. (Secretaria de Cultura - Mexico, 2017).

Videomapping

Videomapping is a visual technique that consists of projecting images with the support of lights, cinema projectors, video projectors on surfaces that with effects can create visual experiences for the viewer. For the implementation it is important to have many factors such as space, light, perspective as with it the projection will be positioned to square the reference points to improve a suitable vanishing point, sound is a plus that allows to involve the viewer in the projection in the case of video. (Maniello, 2015).

Architectural videomapping, which is currently used for the illumination of facades and of course the projection of videos, in the case of museums is used for historical recreations or with the idea of being able to bring the public closer.

There are many museums that have used the projection on facades, one of them is the palace of fine arts that in 2016 and 2017 during the festival of lights allowed to enhance the building as well as the series of projections and textures allowed the general public to contemplate the beauty of the building.

Another museum was the National Museum of Art, which projected digital and visual art called Mappa Mundi on its façade. This videomapping was on the occasion of Mondiacult, Unesco's international conference on cultural policies that paid homage to Mexican culture with projections and a show with free access. This shows the importance of the use of this technology for the dissemination of the museum (Puntodincontro, 2022).

Robotics

This technology is used in different fields, in the case of industry or for the automation of manufacturing processes, to mention a few. In the case of the Museo del Virreinato in San Luis Potosi that implemented is the case of Royito a humanoid robot has an appearance very similar to a human being, characterised as a friar, is owned by the company Intelirobot S.C., temporarily was used to give guided tours as part of the international day of museums in 2018, which allowed children to interact with this character. (Bajo, El;, 2019).

Virtual Tours

With the COVID 19 pandemic, many museums closed their doors, so an alternative was sought to show their spaces, achieving this with virtual tours that allowed them to simulate a real space as if they were in that space. In the case of some museums, they used 365° technologies and Google Street View, the latter being the most realistic as they used photographs of this space. Technologies such as people art factory (peopleartfactory, 2019) were used to simulate spaces that are created in a virtual way to mount exhibitions without having a room.

ISSN 2531-2197

I will mention some museums that implemented this type of virtual tours; Bellas Artes, Museo de Arte Moderno, Museo Nacional de San Carlos, Museo Nacional del Virreinato, Museo de Arte Indígena Contemporáneo, Antiguo Colegio de San Ildefonso, Dolores Olmedo, MUNAL - Museo Nacional de Arte, Templo Mayor, El Tajín, Museo del Pueblo Maya (Yucatán), Museo de las Culturas del Norte (Paquimé), Monte Albán, Teotihuacán, Castillo de Chapultepec, Museo Cuauhnáhuac (Palacio de Cortés) Museo Frida Kahlo (Casa Azul) to name a few. (36 virtual museum tours, 2022).

Streaming

During the covid-19 pandemic, museums suspended activities, affecting already scheduled activities such as academic activities like colloquiums and artistic activities like concerts or plays, so online transmission or streaming was used, helping to continue with different activities remotely. YouTube was one of the most widely used tools during this period, as it was able to broadcast all kinds of events and was a valuable tool, as it allowed to reach many more people in many parts of the world, not only in Mexico.

In the case of museums belonging to the Ministry of Culture, a website called "Contigo a la Distancia" was created to promote digital culture and free access, with tours of museums and archaeological sites, films, books, concerts, conferences, documentaries, plays, audios, applications and much more. With this, the use of digital tools was promoted for the development of many activities in pandemic, using technology to bring the public closer to the museums (Contigo en la distancia, 2019).

Summary of results

This research work studied the different museums that use technology, and an exhaustive investigation was carried out in different media such as books, catalogues, research magazines and magazines specialising in museums, as well as the existing collection of the National Institute of Anthropology and History, the Media Library and the Mexican Platform. It can be concluded that the importance of technology in these museums is of vital importance, as it allows them to function well and attract visitors to these museums.

The use of technology and the advances made in recent years confirm the importance of the implementation of these technologies in order to control the collections, as well as the implementation of these technologies for dissemination purposes, attracting more visitors to these museums.

Without forgetting customer satisfaction as a business model, it can be observed that the vast majority of museums that have implemented technology and have evolved within this museographic environment have been able to have a more functional and advanced structure compared to other museums that have not dared to implement it.

Conclusions

The results of this research allow us to understand the importance of implementing technology in museums for the dissemination and preservation of cultural goods in Mexico. This is reflected in the quality of temporary or permanent exhibitions, as they help the evolution of internal museum processes. As well as the products that derive from them, such as papers, colloquiums, digital platforms that allow the good development and control of the pieces that are analysed for research purposes, with which the collections are exhibited in the exhibition rooms or published on digital platforms. Interactivity is essential as the visiting public can learn more about the piece and generate experiences that encourage them to return or recommend the cultural space.

Looking to the future, museums can implement many technologies such as multimedia, virtual reality, augmented reality, photogrammetry, architectural reconstructions, simulated spaces and holograms, which will allow visitors to have an experience that they can enjoy during a visit to a museum.

Recommendations

Museums that are implementing new technologies should rely on the experiences of other museums so that they can analyse the pros and cons, determine the alternatives in their implementation and analyse the resources that can be used in development and implementation.

ISSN 2531-2197

Furthermore, it is essential to have a development team or an IT area, and it is important that this team will be able to generate new content and technologies, as they will know the needs and scope of the museum.

Conclusions

It is necessary to invest and implement new technologies for the research and dissemination of culture in Mexico, especially in exhibitions where visitors can have better experiences when visiting a museum and have a pleasant experience, as well as being accessible to all citizens.

References

36 recorridos virtuales por museos . (2022). 36 recorridos virtuales por museos . Obtenido de Canva: Canva.com

Agustí Canals, I. H. (2020). Plataformas digitales: fundamentos y una propuesta de clasificación. Catalunya, España: Oikonomics.

Bajo, El;. (15 de mayo de 2019). Conoce a Royito, el robot guía que estará en el Museo del Virreinato. Obtenido de aorquesta.mx: https://laorquesta.mx/conoce-a-royito-el-robot-guia-que-estara-en-el-museo-del-virreinato/

BRENNEN, J. S. (2016). The International Encyclopedia of Communication Theory and Philosophy. Estados Unidos: Wiley Blackwell.

Cabrera, E. M. (2001). estratégia y organización en la vinculación univeridad-empresa. ALTEC.
Campos, R. M. (2005). Diseño de páginas web y diseño gráfico. España: Ideaspropias Editorial, S.L.

Canon. (2010). El Museo Nacional de Antropología en el Siglo XXI. Obtenido de CANON: https://www.canon.com.mx/registrofotografico-mna-canon/

Contigo en la distancia. (2019). Contigo en la distancia. Obtenido de Contigo en la distancia: https://contigoenladistancia.cultura.gob.mx/

Corcoles Tendero, J. E. (2015). Diseño de interfaces web. España: RA-MA Editorial.

Few, S. (2007). Pervasive Hurdles to Effective Dashboard Design. Newsletter: Visual Business Intelligence.

HubSpot. (2020). Experiencia de usuario. Estados Unidos: Portal Web.

ICOM International Committee for Museology (ICOFOM). (2010). Conceptos claves de museología. Paris : ICOM.

M Museos de México y del Mundo. (2004). El sistema de información y gestión (SIM) del Museo Nacional del Virreinato. Gestión, público y nuevas tecnologías en un museo mexicano. M Museos de México y del Mundo, 89.

Maniello, D. (2015). Augmented Reality in public spaces. Basic Techniques for video mapping. Le Penseur.

Marqués, M. (2009). Bases de datos. España: Castelló de la Plana.

peopleartfactory. (2019). New digital experiences for art. Obtenido de peopleartfactory: https://peopleartfactory.com/

Puntodincontro. (26 de septiembre de 2022). Mappa Mundi: in Messico videomapping italiano sulla facciata del MUNAL. Obtenido de https://puntodincontro.mx/es/2022/09/26/mappa-mundi-en-mexico-videomapping-italiano-en-la-fachada-del-munal/

Raya Cabrera, J. L. (2015). Sistemas informáticos. Madrid, España: RA-MA Editorial.

Regino, O. (2015). Lógica de programación orientada a objetos. Bogotá, Colombia: Ecoe.

Revistas INAH. (2022). Revistas INAH.

Rodriguez, A. M. (11 de 12 de 2005). En Internet, colección pictórica del Museo Nacional del Virreinato - La Jornada. La jornada.

Secretaria de Cultura - México. (2017). Mexicana. Obtenido de Mexicana: https://mexicana.cultura.gob.mx/es/repositorio/home

Sordo Madaleno, J., Leatherbarrow, D., Adria, M., Arditti, A., Arditti, J., & Ollae-Laprune, P. (2011). mty. Obtenido de Memoria y tolerancia: https://www.myt.org.mx/sala-tolerancia

UNESCO DOC. (2022). Bliblioteca Digital UNESCO. Obtenido de https://unesdoc.unesco.org/inicio.

Article **Journal Computer Technology**
June 2023, Vol.7 No.18 8-22

Artificial vision techniques at the frontiers of video surveillance

Técnicas de visión artificial en fronteras de la video vigilancia

PÉREZ-ESCAMILLA, Javier´*†, MENDOZA-GUZMÁN, Lorena, CRUZ-GUERRERO, René and PORRAS-MUÑOZ, Rolando

Tecnológico Nacional de México / ITS del Oriente del Estado de Hidalgo. Carretera Apan-Tepeapulco Km 3.5, Colonia Las Peñitas, C.P. 43900, Apan Hidalgo, México.
´ Tecnológico Nacional de México / ITS del Occidente del Estado de Hidalgo. Paseo del Agrarismo 2000, Carretera Mixquiahuala - Tula, Km. 2.5. Mixquiahuala de Juárez, Hidalgo, C.P.42700.

ID 1st Author: *Javier, Pérez-Escamilla* / **ORC ID:** 0009-0008-4090-2259, **CVU CONAHCYT ID:** 939609

ID 1st Co-author: *Lorena, Mendoza-Guzmán* / **ORC ID:** 0009-0005-7802-6352, **CVU CONAHCYT ID:** 1289555

ID 2nd Co-author: *René, Cruz-Guerrero* / **ORC ID:** 0000-0003-1276-2419, **CVU CONAHCYT ID:** 551299

ID 3rd Co-author: *Rolando, Porras-Muñoz* / **ORC ID:** 0009-0006-1065-9695, **CVU CONAHCYT ID:** 1289586

DOI: 10.35429/JCT.2023.18.7.8.22 Received: January 15, 2023; Accepted June 30, 2023

Abstract

The present work addresses the task of identifying a predatory behavior of robbery of homes or businesses. The proposed objective is the detection of blunt elements used in the commission of the crime, limiting the context to barrettes, covered faces, people and gates (doors or windows). The proposal addresses the task of object identification applying Single Shot Detectors (SSD). Due to its versatility and the physical resources applied, the structure of SSD ResNet50 V1 FPN 640x640 has been chosen from the TensorFlow Model Zoo to train and validate the classification. This has been built in five classes, for the training and validation set, an average of 50 annotations per class have been processed. Additionally, a support function was worked on in the detection of human activity. The evaluated model obtained a mA of 69% in the detection of objects and in the identification of criminal behavior it showed a performance of 69%.

Predatory behaviour, Attention mechanisms, Deep learning

Resumen

La investigación, aborda la tarea de la identificación de una conducta predatoria de robo a casa habitación o negocio. El objetivo planteado es la detección de elementos contundentes usados en la comisión del delito, limitando el contexto a barretas, rostros cubiertos, personas y cancelería (puerta o ventana). La propuesta, aborda la tarea de identificación de objetos aplicando Single Shot Detectors (SSD). Por la versatilidad y los recursos físicos aplicados se ha optado por la estructura de SSD ResNet50 V1 FPN 640x640, del Zoológico de modelos de TensorFlow para entrenar y validar la clasificación. Éste se ha construido en cinco clases, para el conjunto de entrenamiento y validación se han procesado en promedio 50 anotaciones por clase. Adicionalmente, se trabajó una función de apoyo en la detección de la actividad humana. El modelo evaluado obtuvo una mAP de 69% de precisión en la detección de objetos y en la identificación de la conducta delictiva mostró un desempeño del 69%.

Conducta predatoria, Mecanismos de atención, Aprendizaje profundo

Citation: PÉREZ-ESCAMILLA, Javier, MENDOZA-GUZMÁN, Lorena, CRUZ-GUERRERO, René and PORRAS-MUÑOZ, Rolando. Artificial vision techniques at the frontiers of video surveillance. Journal Computer Technology. 2023. 7-18:8-22.

* Correspondence to Author (E-mail: javierperez@itsoeh.edu.mx)
† Researcher contributing as first author.

Introduction

Artificial intelligence (AI) has developed human capabilities. "Enhanced artificial intelligence" is the new frontier in the implementation of smart devices, which in turn opens up new possibilities for solving problems associated with security and video surveillance [1]. Various artificial intelligence techniques have resurfaced with great interest, one example being Deep Neural Networks (DNN), which perform well for identifying faces, vehicles, weapons, and other objects associated with a security system [2]. The preparation of the inputs, as well as their pre-processing, represent the challenge of correct selection for the good performance of a machine learning model [3].

Object detection has gained emphasis in AI topics, where neural networks have made the greatest contribution [4]. In this case, the process requires collecting diversity in the training data, assuming a relative position of the object, scanning the input or scene, performing a classification to determine the class of the object, and obtaining the relative position of the object [5]. Various techniques are applied to the position of the object, taking into account the characteristics of the model, e.g, [6].

Computer vision (CV) is presented as a mature and extensive element, easy to integrate into projects where image processing is required. CV is the part of AI behind the comprehension and manipulation of videos and images [7]. Multiple computer vision tools are incorporated as a solution system for a specific problem [8]. The integration of this into technology is all the rage, through face recognition for the security of cell phones, banking transactions, and autonomous, land and air vehicles, just to name a few examples. Object detection is no exception.

Object localization differs from classification, while the task of classifying is to determine a label for an object, localizing allows finding the position of the object within an image. Multiple objects can be located, for this action, the location algorithms specialize in making cuts to the image to determine areas of interest or regions of interest (ROI). In general, DNN models have been shown to perform better [9].

The model used in this research focuses on the detection of movements similar to criminal behavior, limiting the context to people who violate a door or window with a blunt object such as a crowbar and whose faces are covered. So then, we know the elements that make up the scene to recognize human action. The descriptions and references given in [10] have been used to describe the behavior. Using a labeling tool, annotations have been made for each image that correspond to the proposed classes.

Previous works

Hu et al. (2015), ask the question Why do Convolutional Neural Networks (CNN) work so well? They propose a set of deep neural network architectures, oriented to face recognition, using a set of labeled photos called LFW or Labeled Face in the Wild. It builds models based on the deep neural network AlexNet [11], where it applies combinations of three convolution layers, a dense layer and an output dimensionality reduction function (softmax). Something that stands out is that it makes 30 cuts to the LFW instances for training and concludes that the differentiation between the different models is supported by the scale and the regions of the input to be reviewed [12].

Nam et al. (2018) proposed a scale-invariant pyramid model, considering that a better input can improve the performance of a CNN. They study the characteristics of different architectures, such as DeepFace, DeepID, FaceNet, and the VGG. They develop a set of patterns, under the assumption that some features are not evaluated by the convolutional network, limiting its performance. In addition, they consider that in video surveillance, the entrance has variations in pose, lighting, expression, and image quality. They use a public pool called LFW and a database called CCTV. The implementation of mechanisms that use characteristics not considered before, improves the performance of the RED vs. a CNN VGG, having better results when the input is 200x200 pixels [13].

ISSN 2531-2197

Wong et al. (2017), proposed an object tracking system based on the premise of simple labeling, placing classification in a second stage. Thus, it streamlines the crawl process and shows that it improves crawl performance when combined with the algorithm's object state information. They face the challenge of detection and classification from an online video by applying the multiple object tracking algorithm, MOT for its acronym in English Multiple Object Tracking. The proposed model is based on: identifying objects through SEF algorithms, (Shape Estimating Finder); track features with a combination of CACTuS, for Competitive Attentional Correlation Tracker using Shape, and FL, for Feature Learning. In a second stage, it applies the classification of the objects, so it concludes its work with great precision [14].

Padmaja, Myneni and Patro, (2020) raised the possible applications of the recognition of multiple activities and multiple objects, MAMO, Multi Activity-multi object recognition. They recognize the challenges in public areas such as hospitals and universities, early warning, tracking, and intelligent video surveillance, as well as the integration of existing components and algorithms such as YOLO and alike. They describe the different components and collections of images for training, as well as the use of metrics based on classification. It highlights algorithms like DeepLandmark and the effects of stock rankings. In addition, it provides a comparison of the methods and goals to be achieved in new developments [15].

Lu et al. (2017), addressed the object position prediction task. They design a system of LSTM, Long Short Term Memory. They propose a tensor based on the position of the detection and a characteristic matrix of the object. They solve the regression and association error computation problems in the trace. It contributes substantially by reversing the direction of reproduction of a video. The model is based on a recurrent network with a normalization layer, where using SSD it identifies and tracks the element, using object detection, object classification, and object position for feature matrix extraction. They conclude with good precision in the approximation of the trajectory of the object [16].

Sai, Sasikala (2019) implemented an application for object detection and counting using CV and SSD tools based on Fast R-CNN, from the Fast Regional Convolutional Neural Network. They focus their efforts on input pre-processing, with 70 instances of the “gun” and “knife” classes. By making adjustments to the model, they limit the number of bounding boxes. They conclude with a great ability to identify and count multiple objects [17].

Materials and methods

In the development, various concepts and techniques of computer science are applied, here, the most relevant are mentioned to provide a general context of the work.

Machine learning (ML)

Machine learning (ML) is the science and art where it is possible for the machine to simulate the learning process. Through a study of the problem, the associated data is modeled, supported by mathematical and/or statistical tools. Then, it is required to program an algorithm that helps the trial-and-error process, so the task will be automated. As a result, the proposed model is capable of adapting to changes. For problems that have a solution, a set of adaptations or rules may be required, and the performance may change depending on the algorithms applied. An additional advantage is that for complex, solvable problems, ML techniques will be able to find a solution. Lastly, for problems that fluctuate, ML algorithms can be adapted. Sometimes ML systems can provide relevant information on the problem at hand. ML can be divided into 2 categories of algorithms: supervised ones, such as linear regression and classification; unsupervised ones such as clustering, association rules, visualization and dimensionality reduction [18].

Deep Neural Networks

Marvin Minzky coined the term Perceptrons, which describes the behavior of a neuron and defines it as an inference engine that identifies the characteristics of an object, in order to classify it within a defined hierarchy [19].

ISSN 2531-2197

Artificial Neural Networks (ANN). They respond to an imitation of human parallel processing capacity, considering the fundamental difference that machines are sequential, these networks acquire knowledge based on experience, are adaptable, fault tolerant, and have nonlinear behavior [20].

In the context of ML, deep learning is about the variants and ways of connecting the ANNs; it takes as its inspiration the structures and connections of the human brain, thus elements called neurons perform specific tasks with the data. Here, the connections are dozens of networks and millions of neurons. The importance of knowing the types of layers and operations of a neural network enables researchers to propose models for specific tasks, so we can list the components in a deep network [21]:

1) Convolutional layer

This layer operates on the model input, performing the calculation of convolution operations. A convolution is an array sweep operation by a filter or kernel, resulting in a new array.

$$y_{rc}^{l} = \sum_{i=1}^{Fr} \sum_{j=1}^{Fc} y_{(r+1-1)(c+j-1)}^{l-1} w_{ij}^{l} + b^{l} \quad (1)$$

The output y_{rc}^{l} de $\{r, c\}$, is a function of Fr, Fc, which is the number of columns and rows in the pass filter. w_{ij}^{l} is the value of the filter at position {i,j}. $y_{(r+1-1)(c+j-1)}^{l-1}$ represents the value of the input to this layer at position {r+i-1,c+j-1}. b^{l} is bias value.

2) Dense layer

This layer represents classical neurons in perceptrons. Its main function is linear regression or classification.

3) Activation function

Activation functions bring the non-linearity of the functions and add multi-layer activations at the output of the network. Softmax and RELU are of interest.

$$Softmax = f_j(z_i) = \frac{e^{z_i}}{\sum_j e^{z_j}} \quad (2)$$

$$RELU = f(x) = max(0 + z_i) \quad (3)$$

4) Pooling layer

This layer is used to reduce the output volume of the convolutional layers. It allows the perceptron to increase the field of perception of the network, thus adding viable features to improve the classification capacity of the model.

$$h_{xy}^{l} = max_{i=0..s, j=0...s} h^{l-1}(x+i)(y+j) \quad (4)$$

5) Dropout layer

It is the layer that allows you to avoid overtraining. It eliminates the contributions of some neurons next to the input and output connections, based on a random probability.

6) Batch Normalization

This layer increases the stability of the training by normalizing the outputs of the previous activation layers. It applies the operations by subtracting the provided mean and dividing it by the standard deviation.

$$y = \frac{\lambda}{\sqrt{Var[x]+\epsilon}} x + (\beta - \frac{\lambda E[x]}{\sqrt{Var[x]+\epsilon}}) \quad (5)$$

Where, multiple mini batches β, sized m with mean and variance are processed and averaged among them in order to obtain the general mean and variance. The network is assumed to have a set of trainable parameters that is the input to the execution algorithm $\Theta = \{x^{(k)}\}\ _{k=1}^{K}$. So, by batch, the parameters of the activation functions are updated$\Theta \cup \{\gamma^{(k)}, \beta^{(k)}\}_{k=1}^{K}$.

7) Epoch

An epoch is a training cycle of the neural network where all the model operations are performed. The "weights" of the activation functions that offer the greatest gain to the model are stored here.

Object detectors

CV allows addressing unsupervised learning problems, this recent approach is becoming known as unsupervised visual learning. Here, elements of the real world with dimensions of space and time become relevant.

ISSN 2531-2197

Objects are local outliers in the global scene, small in size and with a different appearance and motion than their larger background. It is then when the pixels and frames become relevant, but they have a difference in dimensionality. Algorithms such as VisionPCA [22] converge on quickly identifying the differentiation between the background and the objects in the frame. Thus, one can choose with high precision (not necessarily high recall) data samples that belong to a single object or category. Multiple techniques are viable, such as graphs, segmentation, and deep learning [23].

Object detectors apply a set of techniques that take advantage of the capabilities of DNNs, where convolutional operations are capable of mapping object classes. The use of bounding boxes (BB) is incorporated, by means of a hypothesis of the position of the object, a box of its location is drawn. In contrast, SSDs are a set of techniques and tools that may be larger than deep networks, but they do all the tasks in one fell swoop. In Figure 1 we show examples of R-CNN, for Regional CNN, and YOLO, for You Only Look Once [24]. A comparison chart is illustrated in Figure 1.

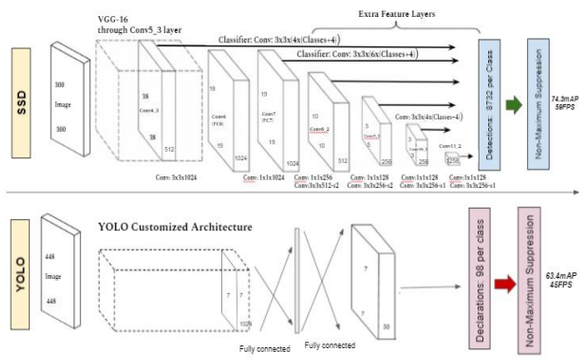


Figure 1 Comparison of activation diagrams. While SSD applies convolution operations seeking to perform object detection using "Multi-scale feature maps for detection" and then applies a classification process, YOLO, on the other hand, uses autoencoders.

In an input where multiple classes are available, the strategy of sub-mapping the input is advantageous, so that there is no longer just one ROI but several samples to verify. This sweep process is done using a regression strategy.

Fast R-CNN

An improvement in the processing of SSDs implies that, by having multiple object instances in one input, classification can be done with limited physical resources. We show an abstraction of the model in Figure 2. For the Fast R-CNN model, shared compute and memory resources are used. So, then it improves detection applying a sub-sampling of the h x w input by a network of H x W samples. Each input is reduced with max-pooling. In the model, the input is processed using convolution and activation functions with softmax. BB are worked on with regression. A loss function is applied in the context, previously, annotations of the ROIs have been made for the classification. A re-example thread is executed in the background, where Stochastic Gradient Descent (SGC) is used as the optimization function [25].

1) Classification function:

$$L(p,u,t^u,v) = L_{cls}(p,u) + [u \geq 1]L_{loc}(t^u,v) \quad (6)$$

The location and classification are associated for each ROI, where $L_{cls}(p,u) = logp_u$ is the logarithmic loss for the true class u.

2) Loss function:

$$L_{cls}(t^u,v) = \sum_{i\in\{x,y,w,h\}} smooth_{L1}(t_i^u - v_i) \quad (7)$$

Where:

$$smooth_{L1}(x) = \{0.5x^2 if|x| < 1|x| - 0.5\ otherwise \quad (8)$$

The calculation of the partial derivative of loss for each example (ROI).

$$\frac{dL}{dx_i} = \sum_r \sum_j [i = i^*(r,j)]\frac{dL}{dy_{rj}} \quad (9)$$

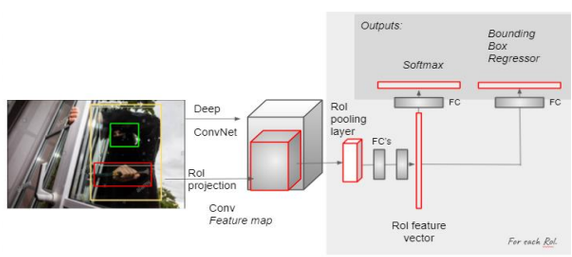


Figure 2 Fast R-CNN activation diagram. A set of mapping functions, a re-instance of the input, and activation functions for classification and regression for localization are denoted.

ISSN 2531-2197

RetinaNet

RetinaNet is a neural network model for object detection, where the use of the identity function becomes relevant. This function permeates the idea that a small neural network performs well and that it should be much easier to learn the "activation weights". So, it is a matter of passing the input directly to the output of the intermediate layers. The network adds the input to the output; this is called the residual block. This process consists of two paths: the first is a series of regular neuronal layers, or main branch; the second is a direct path from input to output, or shortcut branch. Batch normalization and RELU are operations applied to the main branch. [26] In Figure 3, the architecture is illustrated.

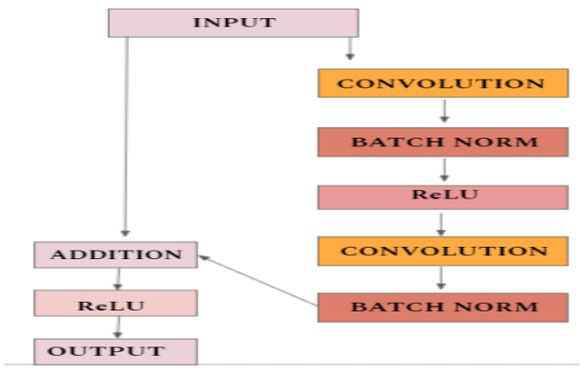


Figure 3 Residual network block. In the main branch, it consists of a convolution layer, normalization, linear rectification, convolution and normalization layer. In the secondary branch, the entry is added directly to the main branch. Finally, a linear rectification is performed and the output of the block is computed.

Metrics

The metrics of an ML model are basically calculated based on correctly classified instances, TP or True Positives, and FP or False Positives; and not correctly classified, TN or True Negatives, and FN or false negatives. The associated functions are: Accuracy, which measures the correctness of the model; Recall, which measures the model's ability to discriminate between classes; and Precision, which measures the model's ability to correctly recognize new instances between classes [27].

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (10)$$

$$Recall = \frac{TP}{TP+FN} \quad (11)$$

$$Precision = \frac{TP}{TP+FP} \quad (12)$$

In the case of object detectors, the Mean Average Precision metric, mAP, is regularly included. The mAP value is useful for assessing location and segmentation model performances as well as classification. With this metric, the classification and localization of the model are assessed. For this, we need to know the annotation of the location and class called fundamental truth or Ground Truth. This is how a BB and a class label are denoted. Since we are checking a delimiter, the box, a metric is required that indicates exactly how the model has created that delimiter of the object. Here, the calculation of intersection over union (IoU) is the relation between the delimiter given by the model of the intersection with Ground Truth, on the union and the Ground Truth [28].

$$IoU = \frac{A \cap B}{A \cup B} \quad (13)$$

$$mAP = \frac{1}{n}\sum_{K=1}^{k=n} AP_k \quad (14)$$

Where n = number of class and $AP_k = Average\ Precision\ of\ class\ K$.

LabelImg

In the annotation corresponding to the Ground Truth values, the LabelImg tool is used. It was built by Massachusetts Institute of Technology (MIT), using the Python language and a plugin called 'Qt' for graphical controls. In it, annotations can be made in XML format, for YOLO format and for the set of visual objects called PASCAL Dataset. It saves the positions of the BB and the class to which each object in an image corresponds to. [29].

For the labeling of the classes, those used in the COCO (Common Context) set are taken as a reference, where the elements represented are found in their natural environment. Differences in labeling vary between different data sets; for example, in VOC, Visual Object Class, similarly, they mainly store the location and class of the object, either by segmentation or location of bounding boxes [30].

ISSN 2531-2197

Transfer Learning

Given the large amount of time required to train a neural network, the task of implementing solutions to specific problems is addressed by a knowledge transfer technique, Transfer Learning (TL). Here the benchmark in performance and relevance of the application domain plays an important role. A review of the models helps to determine those susceptible to apply and compare [31].

Color spaces and moments

In the intensity change analysis of pixels in an image, it allows to obtain crucial information about the objects in an image. In this case, the HSV color spaces, Hue Saturation and Value, highlight characteristics that are not denoted with the naked eye, converting an RBG color space to a more enriched one. This is how new associated colors appear, such as yellow, magenta, and cyan. This technique can help tracking objects based on pixel intensity. [32].

Deep learning in images is based on the composition of multiple nonlinear transformations. Data is processed into abstract semantic representations formed on the network (end-to-end paradigm). These representations have great flexibility and adaptation, where the quality of the representation is affected by the integrity of the training data; the robustness is affected by the computational cost; the robustness of the geometric transformation is limited; therefore, it requires the augmentation of data; geometric invariance is affected by time/space complexity. In a pre-convolutional neural network, aspects of frequency transformation, Texture, dimensionality, Moments and Moment invariants, discriminability, and robustness are considered [33].

Methodology to develop

The waterfall methodology has the characteristic of delivering the product until the end of the development cycle, where a set of deliverables is generated in a limited space of time and where it can be iterated [34].

The application development cycle consists of six steps to achieve implementation. The complete cycle is illustrated in Figure 4. The first stage consists of searching for images associated with the problem. The second stage consists of tagging the objects that have been found in the application. The third stage consists of generating the training and test sets. The training stage consists of carrying out a set of adjustments to the model so that it can adjust the activation weights of the functions. The metrics preparation stage consists of activating the TensorBoard features so that it shows the performance graphs. The last stage consists of testing the model against a validation set.

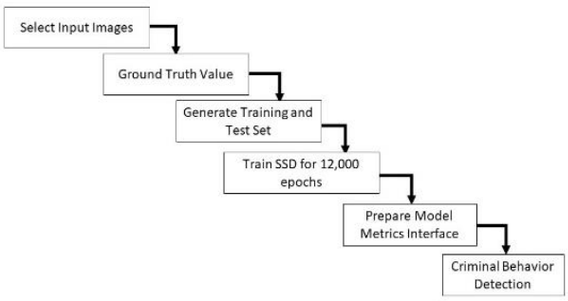


Figure 4 *Stages of work.* The parts of the process are illustrated. The last task verifies the functionality of the model,

1) Image selection

56 images were selected from the internet, they were sought to be in JPG format, 24 bits of color depth and 94 dpi of horizontal and vertical resolution. In addition, they will have some of the elements used in the breakage of the door scene. The images are in their natural state, that is, in the real context in which they occur. Note: All those images are used for academic and research purposes.

2) Ground Truth Value

Using the LabelImg tool, 56 XML (Extensive Markup Language) encoded files of bounding box truth value annotations were obtained. This work was done manually and sought to obtain an average of 56 annotations per class.

ISSN 2531-2197

3) Training and testing set

The training set and the test set were separated into 42 and 14 images, respectively. Compiled files called Tf Records are created, which are used with the ML software TensorFlow and Keras.

4) Train SSD at 12,000 epochs

Using Transfer Learning and the DNN model called ResNet 50 V1 FPN 640x640 SSD, the adaptation for the purpose of the project is made. The process begins by declaring the number of classes, the location of the training and test sets, the number of epochs, and the weights of the COCO dataset saved. The latter is a pre-trained model that is used to transfer the activation weights of the model. In this case, it was compiled using a computer with a Nvidia 730 video card, Ryzen 5 CPU, 16GB RAM, 128GB SSD.

5) Prepare model metrics interface

Tensor Board includes a set of visual tools for reviewing model metrics. In this case, a local service is enabled with output to port 6006. Thus, it is possible to access the graphs of the object detection metrics in Figure 5, where the output of the model is illustrated.

Figure 5 Tensorboard. The partial training results are shown in training and validation metrics, in this case at 8000 epochs.

6) Prepare model metrics interface

For behavior detection, a helper function is used. The validation of the condition that activates the scene is based on an If-Then-Else criterion to determine if the classes are present in the image. The bounding box labels displayed in the output are referenced.

Results and discussion

The shortage of images of criminal behavior to be treated limit their quality. In many cases, they are of low resolution and relatively small size. For the purpose of this research, a minimum standard of 96 dots per inch horizontally and vertically, 24 bits depth and in JPG format, from the English Joint Photographic Experts Group, were processed.

The dimensions of the scenes are varied, ranging from 148 x 341 and up to 808 x 818 in height and width, with a maximum width of 1200 pixels. Given the variety of sizes, the model performs a scaling to a fixed size of 640 x 640 pixels, in addition to using image enlargement, and horizontal rotation.

Figure 6 *Training Set*. The images with the required classes are highlighted. If there is difficulty finding the required number of images, the context of use is limited.

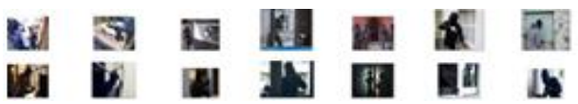


Figure 7 *Test set.* The number of images is reduced, but the annotations are approximately 14 per class.

Figures 6 and 7 show the proposed training and test sets. The images were obtained from the web, and their purpose is educational. The selection is due to the fact that objects are present in human action. The crowbar is the critical element to identify human activity, but the context of its use is also diverse, what is relevant is the human action that takes place, as shown in Figure 8.

ISSN 2531-2197

Figure 8 Image of the training set. In the illustration, there are the objects to be detected: the crowbar, covered face, person and the door. The action is to open a door with a crowbar.

Using LabelImg, annotations were made on the images. The system for labeling in the test set is illustrated in Figure 9. Figure 10 shows the labeling of an image for the training set.

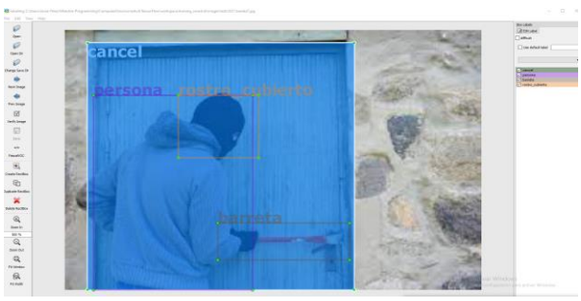


Figure 9 Use of LabelImg. In the test set. Object annotations were performed on the test set. In this image of the test set, the objects are clearly observed, however, the gate is partially obstructed by the person.

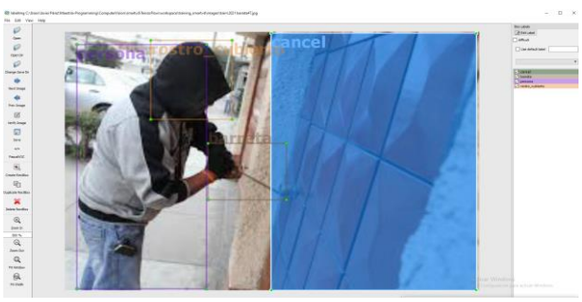


Figure 10 Use of LabelImg in the training set. Annotations of objects were performed on the training set. In this case, the objects are present, although the door is inclined and is different from a glass door.

Using Transfer Learning, through Tensor Flow, a training process for the SSD was set up. Here, the annotations of the images of the training and test sets were transformed into Tfrecord format, which is the labeling format required by the model. The following hyper parameters for the training were configured: 12,000 steps, the number of classes and the evaluation metrics, highlighting that the evaluation and tuning metrics found in the COCO dataset were used. The steps are illustrated in Figure 11.

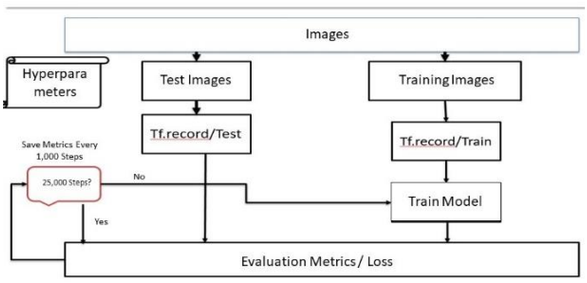


Figure 11 SSD training. The steps for the training design are shown, the hyper parameters are the fine-tuning of the model. Every 1000 steps, the metrics or checkpoint is saved.

Once the model has carried out partial training, the results shown in Tensor Board have been reviewed, in Figure 12 and Figure 13 we show the partial results in 12,000 processed epochs. It can be seen that the error in the classification and the total error tend to decrease with the passage of time.

Figure 12 *Loss function vs Classification.* This tends to decrease. In an optimal model, the curves tend to remain at a value between 0.5 on the Y axis. Some of the objects are not classified correctly, or in their case, they may be one on top of the other.

ISSN 2531-2197

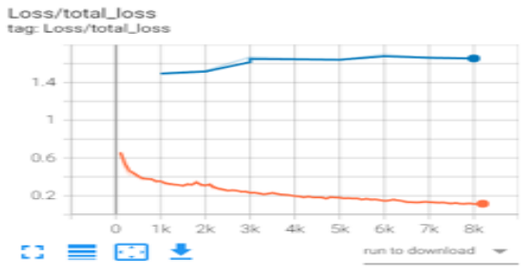


Figure 13 *Loss function vs total loss.* The process is more stable, but it does not tend to improve the curve tendency. An optimal model is close to 1 (orange line).

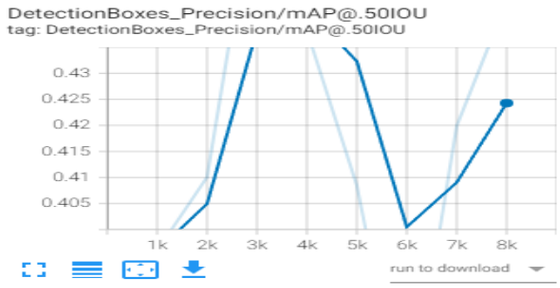


Figure 14 Precision graph at 8,000 epochs. The overall performance of location accuracy is shown. Here we demonstrate that occlusion and model confusion affect the precision of the bounding box

Figure 14 shows the IoU metrics, where the trend is low in the early stages of training. Although it shows instability, it is possible to adjust the IoU value, but the system may identify ROI as slightly different from the true value. Example in Figure 15.

Figure 15 Evaluation, at 6,000 steps. It is possible to observe the output expected by the process, in this case the detection of criminal behavior objects.

Figure 15 illustrates on the left side the figure used in the evaluation and on the right side the truth value annotations, in this case at 6,000 epochs, it is found in the Cancel object, covered face, person, but not the crowbar.

Figure 16 Image normalized in the process. The Tensor Board displays the normalized image. Denoted here is the color space of the blue area, which is a crowbar. However, the gate or other desired object is not denoted.

Figure 16 and Figure 17 illustrate the normalization stage of a training image, here the possibility of using HSV and moments in a manual identification is denoted.

Figure 17 Image normalized in the process. Tensor Board displays the normalized image. Here, the yellow and black color space is denoted, and the desired object (bar) is not distinguishable in color.

Figure 18 shows a normalized image of the training set. Here, the HSV is clearly highlighted, but the shape of the object is not completely clear, the door is transparent, increasing the difficulty.

Figure 18 Normalized training image. Color space denotes the crowbar in red pixels. The person is in a dark color space, but the door is not clearly visible.

ISSN 2531-2197

Figure 19 Image of the training set. Here, we illustrate the normalized image on the left and the raw image on the right. In this case, the normalization does not help in the detection of the object; the model must look for another activation function.

Figure 19 illustrates the complexity of detection. Hand tools can help achieve identification.

Figure 20 illustrates the detection of the crowbar, thus, the identification of the elements of the context has been achieved. For the detection of criminal behavior, it is verified if the 4 objects are present in the scene, taking as reference the labels of the BB.

Figure 20 Image in the validation, the detection of the crowbar is achieved at 9,000 times.

Financing

This work was financed by the Tecnológico Nacional de México (TECNM) and the state of Hidalgo through the software engineering and distributed systems research line of the ITS del Occidente del Estado de Hidalgo and the ITS del Oriente del Estado de Hidalgo.

Conclusions

The proposal meets the proposed objective by using border vision techniques in the video surveillance branch, where the identification of criminal behavior is done with an object detection model and a support function for the recognition of criminal behavior. The quality of the sets affects the final performance, where the quality and quantity of the inputs have an impact on the model, as mentioned in [33].

Using the strategy used in [11] the quality of the geometric transformations is compromised, but the advantage is that the scene contains the objects in their real environment.

Using the techniques used in [13] greatly improves the result, as long as the objects in the scene are not in occlusion. The moments of the scene help to determine some objects, but as long as they are clearly identifiable, regularly those that stand out in color.

The investigation takes the lessons regarding image transformation and uses a regression model for the bounding box. It addresses the tasks of security, video surveillance, and detection of multiple activities with different tools than those proposed in [14], [15], since RetinaNet and a manual tool for behavior identification are used. A solution similar to [17] is implemented, but focused on the identification of an action in human activity.

In this research, what was proposed by [16], where the consistent positioning of objects in a sequence of scenes is discussed, was not implemented. It is addressed in a later work.

The model was designed for an image resolution of 640 x 640 pixels, a lower resolution was found to significantly affect the accuracy metric.

Acknowledgments

We thank the Master's program in Computer Systems of the ITS del Oriente del Estado de Hidalgo (ITESA) and the educational program of Engineering in Computer Systems of the ITS del Occidente del Estado de Hidalgo. Also, Eduardo Daniel Montufar Romero for the revision on the English language revisions of this work.

ISSN 2531-2197

References

[1] Shinde, P. P., & Shah, S. (2018, August). A review of machine learning and deep learning applications. In *2018 Fourth international conference on computing communication control and automation (ICCUBEA)* (pp. 1-6). IEEE. Recover in july, 18, 2023, of IEEE Xplore: https://ieeexplore.ieee.org/document/8697857. DOI:10.1109/ICCUBEA.2018.8697857.

[2] Stubbs, J. J., Birch, G. C., Woo, B. L., & Kouhestani, C. G. (2017, October). Physical security assessment with convolutional neural network transfer learning. In *2017 International Carnahan Conference on Security Technology (ICCST)* (pp. 1-6). IEEE. Recover in july, 18, 2023, of IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/8167800.DOI:10.1109/CCST.2017.8167800.

[3] Shanmugamani, R. (2018). *Deep Learning for Computer Vision: Expert techniques to train advanced neural networks using TensorFlow and Keras*. Packt Publishing Ltd.

[4] Papageorgiou, C. P., Oren, M., & Poggio, T. (1998, January). A general framework for object detection. *In Sixth International Conference on Computer Vision (IEEE Cat. No. 98CH36271)* (pp. 555-562). IEEE. Recover in july, 18, 2023, of IEEE Explore: https://ieeexplore.ieee.org/abstract/document/710772.DOI:10.1109/ICCV.1998.710772.

[5] Borji, A., Cheng, M. M., Hou, Q., Jiang, H., & Li, J. (2019). Salient object detection: A survey. *Computational visual media*, *5*(2), 117-150. Recover en july fr, 18, 2023, of Springer link: https://link.springer.com/article/10.1007/s41095-019-0149-9. DOI:https://doi.org/10.1007/s41095-019-0149-9.

[6] He, Y., Zhu, C., Wang, J., Savvides, M., & Zhang, X. (2019). Bounding box regression with uncertainty for accurate object detection. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 2888-2897). Recover in july, 18, 2023, of ARXEIV: https://arxiv.org/pdf/1809.08545.pdf. DOI: https://doi.org/10.48550/arXiv.1809.08545.

[7] Szeliski, R. (2010). *Computer vision: algorithms and applications.* Springer Science & Business Media.

[8] Jähne, B., & Haußecker, H. (2000). *Computer vision and applications*. Academic Press.

[9] Bai, X., Huang, M., Prasad, N. R., & Mihovska, A. D. (2019, November). A survey of image-based indoor localization using deep learning. In *2019 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC)* (pp. 1-6). IEEE. Recover in july, 18, 2023, of IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/9096144.DOI:10.1109/WPMC48795.2019.9096144.

[10] Penanchino A. Cómo prevenir delitos, como reconocer actitudes sospechosas. Foro de Seguridad. Recover in july, 18, 2023, of Foro de seguridad latinoamericano: https://www.forodeseguridad.com/artic/prevenc/3099.htm.

[11] Ahonen T., Hadid A., and Pietikainen. M. Face recognition with local binary patterns. In Computer vision-eccv 2004, (pp 469–481). Springer, 2004 J. Recover in july 18, 2023, of Springer Link: https://link.springer.com/chapter/10.1007/978-3-540-24670-1_36. DOI: https://doi.org/10.1007/978-3-540-24670-1_36.

ISSN 2531-2197

[12] HU, G., Yang, Y., Yi, D., Kittler, J., Christmas, W., Li, S., & Hospedales, T. (2015). When Face Recognition Meets With Deep Learning: An Evaluation of Convolutional Neural Networks for Face Recognition. *Proceedings of the IEEE international conference on computer vision workshops*, pp. 142-150. Recover in july 18, 2023, of ARXIV: https://arxiv.org/pdf/1504.02351.pdf. DOI: https://doi.org/10.48550/arXiv.1504.02351

[13] Nam, G. P., Choi, H., Cho, J., & Kim, I. J. (2018). PSI-CNN: A pyramid-based scale-invariant CNN architecture for face recognition robust to various image resolutions. *Applied sciences*, *8*(9), 1561. Recover in july18, 2023, of MDIP: https://www.mdpi.com/2076-3417/8/9/1561. DOI:https://doi.org/10.3390/app8091561.

[14] WONG, S., Stamatescu, V., Gatt, A., Kearney, D., Lee, I., & McDonnell, M. (2017). Track everything: Limiting prior knowledge in online multi-object recognition. IEEE Transactions on Image Processing, 26(10), pp. 4669-4683. Recover in july 19,2023, of IEEE Explore: https://ieeexplore.ieee.org/abstract/document/7907205: DOI:10.1109/TIP.2017.2696744

[15] Padmaja, B., Myneni, M. B., & Patro, E. K. (2020). A comparison on visual prediction models for MAMO (multi activity-multi object) recognition using deep learning. *Journal of Big Data*, *7*(1), 1-15. Recover in july 19, 2023, of Springer Open: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-020-00296-8DOI:https://doi.org/10.1186/s40537-020-00296-8.

[16] Lu, Y., Lu, C., & Tang, C. K. (2017). Online video object detection using association LSTM. In Proceedings of the *IEEE International Conference on Computer Vision*. (pp. 2344-2352). Recover in july 19, 2023, of IEEE Xplore: https://ieeexplore.ieee.org/document/8237519. DOI:10.1109/ICCV.2017.257.

[17] Sai, B. K., & Sasikala, T. (2019). Object detection and count of objects in image using tensor flow object detection API. In 2019 I*nternational Conference on Smart Systems and Inventive Technology* (ICSSIT) (pp. 542-546). IEEE. Recover on july 19, 2023, of IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/8987942.DOI:10.1109/ICSSIT46314.2019.8987942.

[18] Géron, A. (2019). *Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow: Concepts, tools, and techniques to build intelligent systems.* O'Reilly Media Inc.

[19] Gallant, S. I. (1990). Perceptron-based learning algorithms. *IEEE Transactions on neural networks*, *1*(2), pp. 179-191. Recover on july 19, 2023, of IEEE Xplore: https://ieeexplore.ieee.org/document/80230 DOI: 10.1109/72.80230.

[20] Villanueva Limón, F. J. (2017). *Algoritmo de protección con reconocimiento de patrones usando una red neuronal para líneas de transmisión*. [Master's Thesis]. Instituto Politécnico Nacional. Recover in july 19, 2023 of Repositorio Dspace: https://tesis.ipn.mx/bitstream/handle/123456789/22770/tesis_FJVL.pdf?sequence=1&isAllowed=y

[21] Alla, S., & Adari, S. K. (2019). *Beginning anomaly detection using Python-based deep learning.* New Jersey: Apress.

[22] Stretcu O, Leordeanu M (2015, September) Multiple frames matching for object discovery in video. In: *BMVC* (Vol 1m No. 2. p. 3). Recovery in july 19, 2023, of https://meilongzhang.github.io/assets/pdf/videoPCA/bmvc_videopca.pdf.

[23] Forsyth, D., & Ponce, J. (2011). *Computer vision: A modern approach* (p. 792). Prentice hall.

ISSN 2531-2197

[24] Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C. Y., & Berg, A. C. (2016). Ssd: Single shot multibox detector. In *Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11–14, 2016, Proceedings, Part I 14* (pp. 21-37). Springer International Publishing. Recover in july 19, 2023, of Springer Link: https://link.springer.com/chapter/10.1007/978-3-319-46448-0_2 DOI: https://doi.org/10.1007/978-3-319-46448-0_2.

[25] Girshick, R. (2015). Fast r-cnn. In Proceedings of the *IEEE international conference on computer vision* (pp. 1440-1448). Recover in july 19, 2023, of IEEE Xplore: https://ieeexplore.ieee.org/document/7410526. DOI: 10.1109/ICCV.2015.169.

[26] Li, J., Li, C., Fei, S., Ma, C., Chen, W., Ding, F.,& Xiao, Z. (2021). Wheat ear recognition based on RetinaNet and transfer learning. *Sensors*, *21*(14), 4845. Recover in july 20, 2023, of MDPI: https://www.mdpi.com/1424-8220/21/14/4845. DOI: https://doi.org/10.3390/s21144845.

[27] Vujović, Ž. (2021). Classification model evaluation metrics. *International Journal of Advanced Computer Science and Applications*, *12*(6), 599-606. Recover in july 19, 2023, of Research Gate: https://www.researchgate.net/profile/Zeljko-Vujovic/publication/352902406_Classification_Model_Evaluation_Metrics/links/60dede1592851ca9449f17bb/Classification-Model-Evaluation-Metrics.pdf. DOI: 10.14569/IJACSA.2021.0120670.

[28] Tarang S. (2018) Medición de modelos de detección objetos - mAP - ¿Qué es la precisión media? on Towars data Science. Recover in july 19, 2023, of Towards Data Science: https://towardsdatascience.com/what-is-map-understanding-the-statistic-of-choice-for-comparing-object-detection-models-1ea4f67a9dbd.

[29] Python Software Fundation (2021) LabelImg on Python Package Index Recover in july 19, 2023, of Python: https://pypi.org/project/labelImg/1.4.0/

[30] Lin, T. Y., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D.,… & Zitnick, C. L. (2014). Microsoft coco: Common objects in context. In *Computer Vision–ECCV 2014: 13th European Conference, Zurich, Switzerland, September 6-12, 2014, Proceedings, Part V 13* (pp. 740-755). Springer, Cham. Recover in july 19, 2023, of Springer Link: https://link.springer.com/chapter/10.1007/978-3-319-10602-1_48. DOI: https://doi.org/10.1007/978-3-319-10602-1_48.

[31] Zhuang, F., Qi, Z., Duan, K., Xi, D., Zhu, Y., Zhu, H., ... & He, Q. (2020). A comprehensive survey on transfer learning. *Proceedings of the IEEE*, *109*(1), 43-76. Recover in july 19,2023, of IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/9134370. DOI: 10.1109/JPROC.2020.3004555.

[32] T. Carron and P. Lambert (1994, Noviembre), Color edge detector using jointly hue, saturation and intensity. In *Proceedings of 1st International Conference on Image Processing* (Vol. 3, pp. 977-981). IEEE. Recover in july 19, 2023, of IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/413699 DOI: 10.1109/ICIP.1994.413699.

[33] Qi, S., Zhang, Y., Wang, C., Zhou, J., & Cao, X. (2021). A survey of orthogonal moments for image representation: theory, implementation, and evaluation. A*CM Computing Surveys (CSUR)*, *55*(1), 1-35. Recover in july 20, 2023, of ACM Digital Library: https://dl.acm.org/doi/abs/10.1145/3479428 DOI:https://doi.org/10.1145/3479428.

ISSN 2531-2197

[34] Fagarasan, C., Popa, O., Pisla, A., & Cristea, C. (2021, August). Agile, waterfall and iterative approach in information technology projects. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1169, No. 1, p. 012025). IOP Publishing. Recover in july 20, 2023, of IOP Science: https://iopscience.iop.org/article/10.1088/1757-899X/1169/1/012025/meta. DOI 10.1088/1757-899X/1169/1/012025.

ISSN 2531-2197

Article **Journal Computer Technology**
June 2023, Vol.7 No.18 23-31

Development of a web application for hotspot token vending machine administration

Desarrollo de aplicación web de administración para máquina expendedora de fichas hotspot

SAMPAYO-RODRÍGUEZ, Carmen Jeannette†*, GONZÁLEZ-AMBRIZ, Rosalba, LUNA-CARRASCO, Claudia Yadira and LUNA-TREJO, Cupertino

Tecnológico Nacional de México - Instituto Tecnológico Superior de Huauchinango, Maestría en Tecnologías de la Información, Ingeniería en Sistemas Computacionales, México.

ID 1st Author: *Carmen Jeannette, Sampayo-Rodriguez* / **ORC ID:** 0000-0001-8844-6055, **CVU CONAHCYT ID:** 951529

ID 1st Co-author: *Rosalba, González-Ambriz* / **ORC ID:** 0000-0001-5400-9754, **CVU CONAHCYT ID:** 368433

ID 2nd Co-author: *Claudia Yadira, Luna-Carrasco* / **ORC ID:** 0000-0002-4092-9987, **CVU CONAHCYT ID:** 368419

ID 3rd Co-author: *Cupertino, Luna-Trejo* / **ORC ID:** 0000-0001-5898-8486, **CVU CONAHCYT ID:** 904398

DOI: 10.35429/JCT.2022.18.8.22.30 Received: January 25, 2023; Accepted June 30, 2023

Abstract

This article describes the features of a web application to manage the availability and acquisition of wireless internet access credentials of vending machine, it followed the OOHMD agile software development methodology, for the implementation we used the client-server architecture, the JavaScript programming language, the JavaScript runtime environment of Node. js JavaScript runtime environment, Express web development framework for Node.js, Sequelize ORM, MySQL relational database management system, Passport authentication middleware, EJS open source template engine, Bootstrap CSS framework, JSON data interchange format and Visual Studio Code IDE. As a contribution, there is a web application that allows the synchronization of available tokens and the sale of a wireless internet access credential vending machine, which connects through the internet. The methodology used allowed to have an adequate development process to obtain a quality product that resulted in a web application that efficiently provides the available access credentials and manages the access credentials acquired from the vending machine.

Methodology, Application, Development, Synchronization, Credentials

Resumen

El presente artículo describe las característica de una aplicación web para administrar la disponibilidad y adquisición de credenciales de acceso a internet inalámbrico de máquina expendedora, se siguió la metodología ágil de desarrollo de software OOHMD, para la implementación se empleó la arquitectura cliente-servidor, el lenguaje de programación de JavaScript, el entorno de ejecución de JavaScript de Node.js, el framework de desarrollo web para Node.js de Express, el ORM de Sequelize, el sistema de gestión de base de datos relacional de MySQL, el middleware de autenticación de Passport, el motor de plantillas de código abierto de EJS, el framework de Bootstrap CSS, el formato de intercambio de datos JSON y el IDE de Visual Estudio Code. Como contribución se cuenta con una aplicación web que permite la sincronización de fichas disponibles y la venta de una máquina expendedora de credenciales de acceso a internet inalámbrico, que se conecta a través de internet. La metodología empleada permitió tener un proceso de desarrollo adecuado para obtener un producto de calidad que dio como resultado una aplicación web que brinda de manera eficiente las credenciales de acceso disponibles y administra las credenciales de acceso adquiridas de la máquina expendedora.

Metodología, Aplicación, Desarrollo, Sincronización, Credenciales

Citation: SAMPAYO-RODRÍGUEZ, Carmen Jeannette, GONZÁLEZ-AMBRIZ, Rosalba, LUNA-CARRASCO, Claudia Yadira and LUNA-TREJO, Cupertino. Development of a web application for hotspot token vending machine administration. Journal Computer Technology. 2023. 7-18:23-31.

* Correspondence to the author (E-mail: carmen.sr@huauchinango.tecnm.mx).
† Researcher contributing as first author.

Introduction

Object-Oriented Hypermedia Design and Hypermedia (OOHDM) is a model focused on the development of hypermedia applications, proposed by Daniel Schwabe and Gustavo Rossi with the objective of simplifying and facilitating the design of hypermedia applications, its stages are: information gathering and conceptual design, navigation design, abstract interface design and implementation. Web applications are tools that allow performing operations from a computer through the internet and according to them for the development of web applications, the most used methodology is the agile methodology and they observed that OOHDM meets the most optimal method (Ríos, Ordóñez, Segarra, & Zerda, 2017).

JavaScript is an interpreted programming language used primarily to create interactive web applications. It runs on the client side (web browser) and allows user interaction, manipulation of the DOM (Document Object Model) and the creation of animations and visual effects on the web page. It is also used on the server side (Node.js) to create web applications and APIs (Mozilla, s.f.)

Node.js is a JavaScript runtime environment based on Google Chrome's V8 JavaScript engine. It was created by Ryan Dahl in 2009 and allows developers to use JavaScript both client-side and server-side. Node.js is an open source server-side programming platform that uses a non-blocking, event-driven input/output model to provide fast, scalable performance (Kinsta, 2021).

Express is a web development framework for Node.js that allows you to create web applications and APIs quickly and easily. It was created in 2010 by TJ Holowaychuk and is currently one of the most popular and widely used frameworks in Node.js. Express provides a number of features and tools for developing web applications, such as routing, middleware, integration with other Node.js modules, error handling and RESTful API creation. In addition, it is highly customizable and allows developers to define their own application architecture. (Express, n.d.; Startechup, 2021).

Sequelize is a Node.js ORM (Object-Relational Mapping) that allows developers to interact with relational databases using JavaScript objects. Sequelize is compatible with different relational databases, such as PostgreSQL, MySQL, SQLite, among others (Sequelize, n.d.).

MySQL is an open source relational database management system (RDBMS) widely used in web applications. It was originally created by Michael Widenius and David Axmark in 1995, and has since been acquired by several companies. MySQL is compatible with multiple programming languages, such as PHP, Python, Java, Node.js, among others, and is used in a wide variety of applications, from small web applications to large enterprise systems. (MySQL, n.d.; IONOS, 2022).

Passport is an authentication middleware for Node.js that is used to authenticate requests in web applications. It provides a set of authentication strategies that allow developers to authenticate requests using different services, from local authentication to services such as Google, Facebook, Twitter, among others (Passport, n.d.).

EJS (Embedded JavaScript) is an open source template engine for JavaScript that runs on the server. It allows developers to create dynamic web pages by generating HTML through templates containing JavaScript code and HTML markup. (EJS, n.d.)

Bootstrap CSS is a popular framework, which includes a set of predefined styles, classes and components of HTML, CSS and JavaScript to help developers create web pages quickly and efficiently. It was originally created by Twitter and is now maintained by the open source community. It offers a wide variety of features, such as a responsive grid system, typography, forms, buttons, navigation, modals, alerts and much more. (RockContent, 2021).

JSON is the acronym for "JavaScript Object Notation". It is a lightweight data interchange format that is easy for humans and machines to read and write. It is mainly used to transfer structured data over the web (MDN Web Docs, n.d.).

ISSN 2531-2197

Visual Studio Code is an open source integrated development environment (IDE) developed by Microsoft that is used to write, debug and enhance software code. It is also highly customizable and supports a wide range of extensions and plug-ins that can help improve developer productivity. It supports several programming languages and is widely used by software developers and programmers around the world (Microsoft Corporation, 2021).

The article describes the methodology for the development of a web application that allows the administration, availability and token sales (credentials, username and password) of a token vending machine to connect to a wireless internet access point (hotspot) of a wireless internet service provider (wisp) that sells access credentials on a prepaid basis.

The importance of this web application is that it facilitates the management of available credentials and sales control for the vending machine from any location where internet access is available and eliminates the need to go on site to add more available credentials to the machine.

Although there are several solutions that could be carried out to have the web application and one of them prior to this article, the administration of credentials from google services using a google datasheet was presented. However, there was a need for a customized web application with a friendly and easy to use interface.

And as mentioned by Pandurman (2023) data from different sensor devices can be accepted directly and through network connections, which will be used in real time for user interfaces, text files and access to other systems through Representational State Transfer Application Programming Interface (REST API) services.

A solution was sought for the web application to manage the credentials and perform the cuts of tokens sold from various vending machines using a REST API.

The problem that is mainly addressed is that the vending machines will be placed in rural communities that are difficult to access or are located far from the city, and if the access credentials, which were originally sold in paper cards, had to be printed and taken to the locality when they ran out, it is now possible through the web application to load them and have them available when required, making it easier to determine the amount of credentials sold and the cash amount to be held at the time of withdrawal. In addition, it reduces the use of paper printing and allows local people to acquire them in self-service format at any time, 24 hours a day.
In the first section of the article you will find descriptions of the terms used as the methodology employed and the technology used for the development of the application, a brief description of the problem and objective, followed by the description of the activities carried out by stages of the methodology that was worked, results where the pages of the application are shown and the functionality for vending machine management is described, the acknowledgements to our funding source, the conclusions and finally the references or sources of consultation used.

Methodology to be developed

The methodology used for the development of the web application was the OOHDM.

The artifacts generated by each stage are presented below:

Stage 1. Requirements gathering and conceptual design

The functional requirements of the application were as follows:

RF01: The application should allow registering a system administrator and request username and password to log in.

RF02: The application should show general information on available tokens sold, total tokens held and show the profile of the most sold tokens, statistics by profile of available tokens, sold tokens and total tokens held.

RF03: The application must allow adding new cards under the command format: name=AA00001 password=276 limit-uptime=02:00:00 profile= "PLAN_TEST".

ISSN 2531-2197

RF04: The application must allow to perform search filters by cards and profiles.

RF05: The application must have a sales section and show the amount of total sales and by dispatching machines per profile.

RF06: The application must allow the following configurations: change the system user, change the password, add new profiles, edit existing profiles, activate or deactivate and delete them, add new vending machines, edit existing ones, deactivate or activate and delete them, delete the history of tokens sold by different search filters.

RF07: La aplicación debe permitir el cierre de sesión.

Figure 1 shows the use case diagram of the web application.

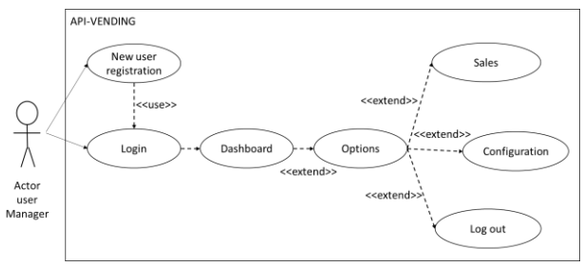


Figure 1 Diagram of use cases
Source: Own elaboration

Stage 2 Navigation design

Figure 2 shows the navigability map of the application.

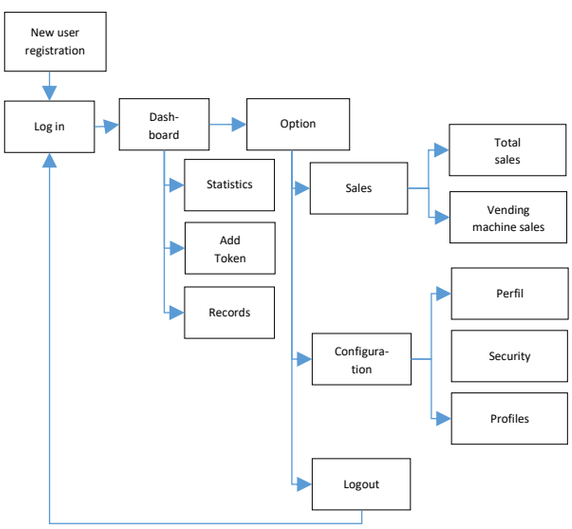
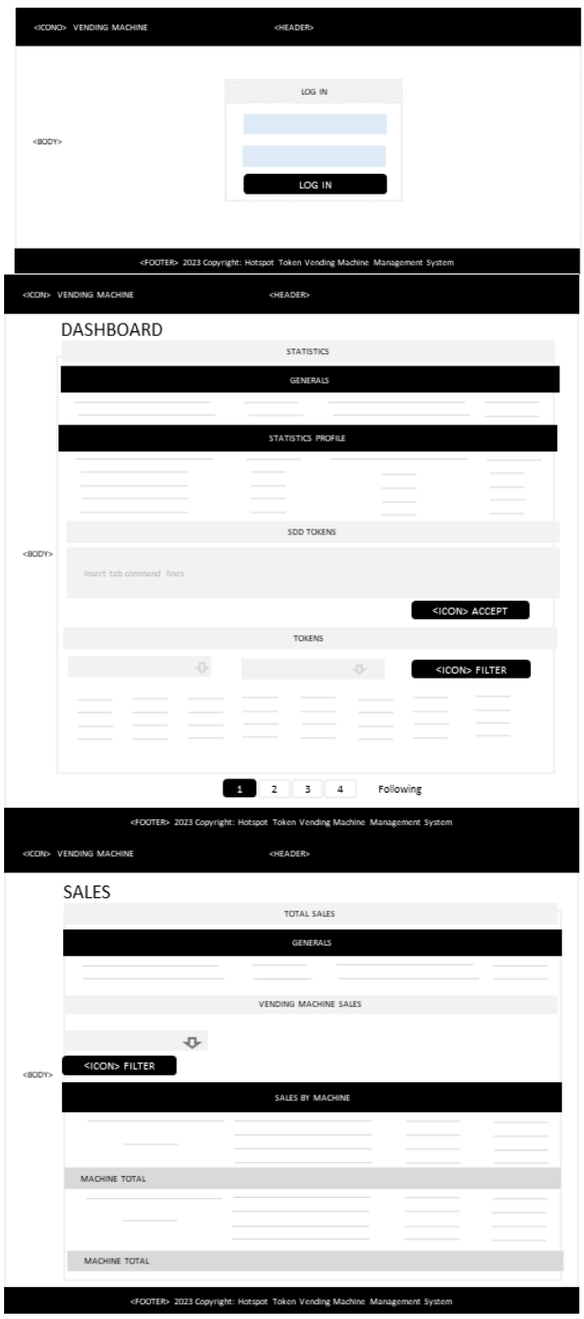


Figure 2 Navigability map
Source: Own elaboration

Stage 3 Abstract interface design

The Abstract Data View (ADV) model was used to design the abstract interface.



ISSN 2531-2197

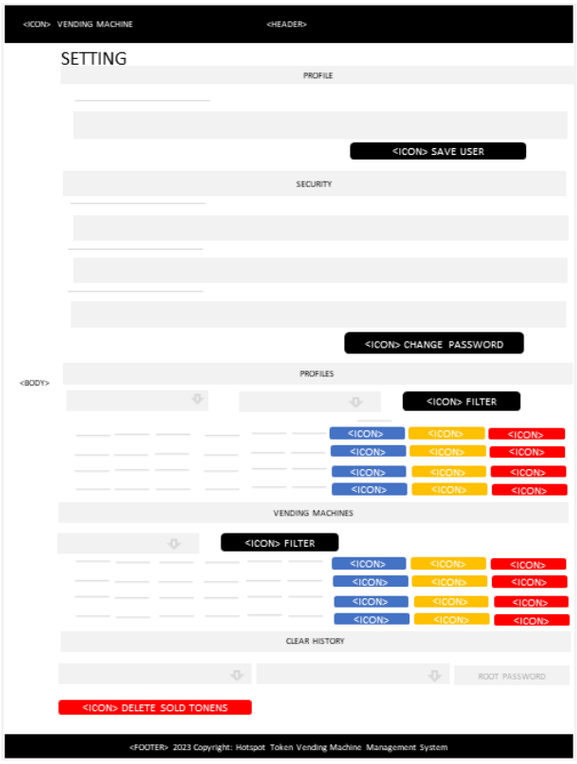


Figure 3 Abstract views
Source: Own elaboration

Stage 4. Implementation

The hotspot token vending machine web application follows a client-server architecture. The server side has been developed using the JavaScript programming language, through the Node.js runtime environment and the Express framework. In addition, the application has a connection to a MySQL database, accessed through the Sequelize ORM, which facilitates interaction with the stored data.

For user authentication, the system uses the Passport authentication middleware, which allows easy administration of system users and their sessions. As for the graphical interfaces of the application, they are generated by the server using the EJS template engine and sent to the user's web browser.

From the client side, there are two possible ways to interact with the system. The first is through a web browser, accessing the HTTP address where the system is hosted. In this way, the user can make requests to the server using the HTTP protocol and obtain the views and data generated by the system, allowing him to manage the tokens, the vending machines and the sales made.

The second way to interact with the system is through a vending machine. In order to carry out queries and sales of the tokens stored in the system, it is necessary to properly configure the machine. The interaction is done through the JSON format, by sending requests to the server and receiving responses.

Figure 4 shows the client-server architecture used for the application.

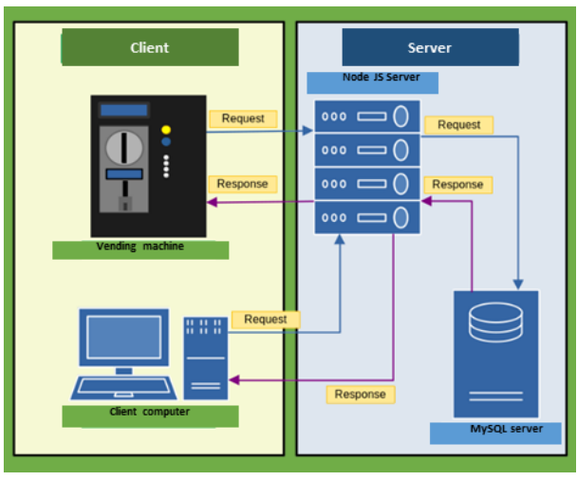


Figure 4 Client-server architecture. ***Own elaboration.***

Figure 5 shows the relational diagram of the classes, attributes and operations of the application.

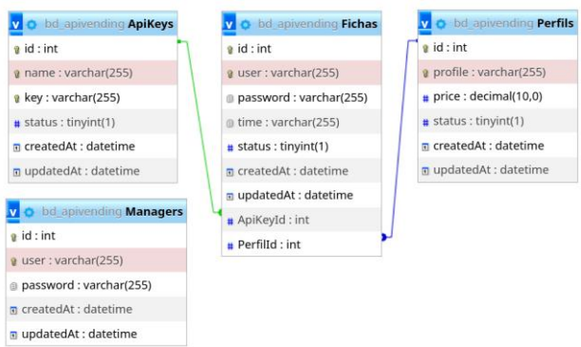


Figure 5 Relational diagram. *Own elaboration.*

Table 1 shows the routes of the web application.

Route	HTTP Method	Request	Response	Description
/	GET		HTML	System login page
/signin	GET		Redirect /	System login page
/signin	POST	user, password	HTML	System Login
/signup	GET		HTML	System registration page
/signup	POST	user, password, passwordConfirm	HTML	System registration
/logout	GET		Redirect /	Logout
/change-user	POST	user	Redirect /config	Change user name
/change-password	POST	password, newPassword, newPasswordConfirm	Redirect /config	Change user password
/config	GET		HTML	Configuration page
/dashboard?status=&profile=&vending=&page=	GET		HTML	Administration page
/addProfile	POST	profile, price	Redirect /config	Add new profile
/change-profile-status/id	GET		Redirect /config	Change profile status
/edit-profile/id	GET		HTML	Edit profile page
/edit-profile/id	POST	profile, price, status	Redirect /config	Edit a profile
/delete-profile/id	GET		Redirect /config	Delete a profile
/addKey	POST	name	Redirect /config	Add new vending machine
/change-key-status/id	GET		Redirect /config	Change vending machine status
/edit-vending/id	GET		HTML	Edit vending machine pagevending
/edit-vending/id	POST	name, key, status	Redirect /config	Edit a vending machine
/delete-vending/id	GET		Redirect /config	Delete vending machine
/fichas	POST	fichas	Redirect /dashboard	Add tokens
/clearHistory	POST	range	Redirect /config	Delete cards
/vending	POST	JSON { "key":"" }	JSON { "estatus": "Correcto", "result": [{ "perfil": "", "precio": 0, "disponibles": 0 }] }	Available profiles
/vending/price	POST	JSON { "key":"" }	JSON { "estatus": "Correcto", "result": { "user": "", "password": "", "precio": 0 } }	Sold hotspot profile

Table 1 Routes of the application
Source: Own elaboration

Results

Figure 6 shows the first login page to the application, where you must register a new user who will be the system administrator, enter name and password and password confirmation, then you can log in.

Figure 6 New user registration page
Source: Own elaboration

Figure 7 shows the login page.

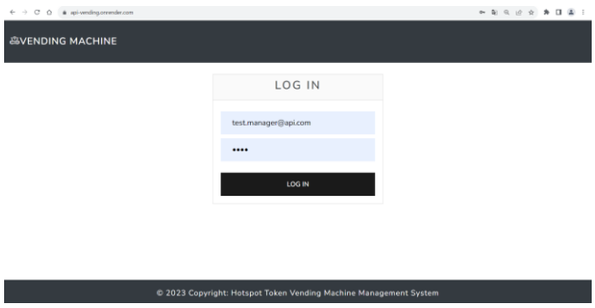


Figure 7 Login page
Source: Own elaboration

When logging in with the registered user and password you will enter the application and see the main page divided into 3 sections: statistics, add cards and cards, as shown in Figure 8.

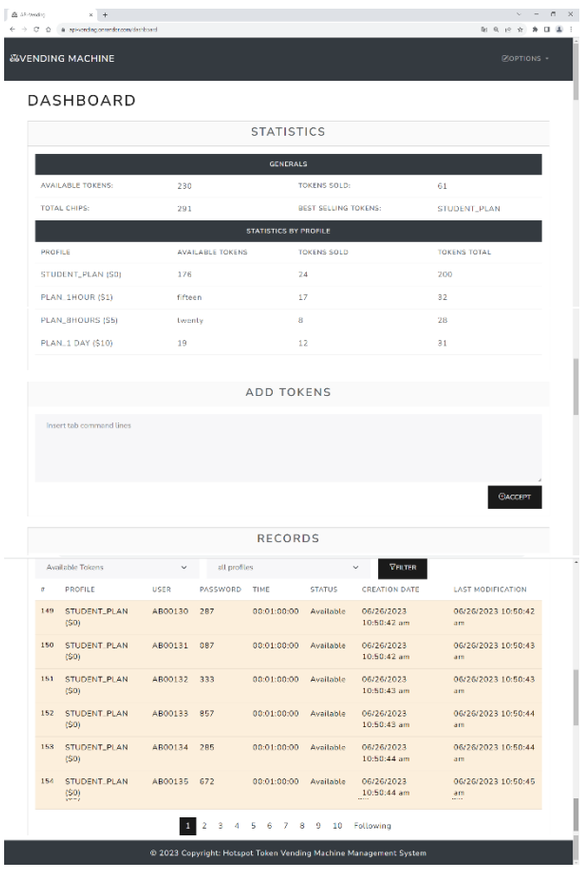


Figure 8 Dashboard page
Source: Own elaboration

1. Statistics: this section displays general statistics showing information on available, sold, total and most sold tokens; and statistics by profile showing available, sold and total tokens.

2. Add tokens: in this section the commands are entered with the mandatory data structure: name=AA00001 password=276 limit-uptime=02:00:00 profile= "PLAN_TEST", shown in Figure 9.

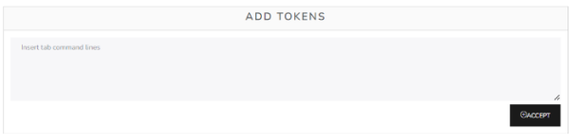


Figure 9 Add tab section of the statistics page
Source: Own elaboration

3. Cards: this section displays cards by applying any of the search filters: by available cards, sold cards and all cards of all profiles or by any other profile that is registered.

On the upper right side is the "Options" drop-down menu that allows you to go to the sales, configuration or logout page. As shown in Figure 10.

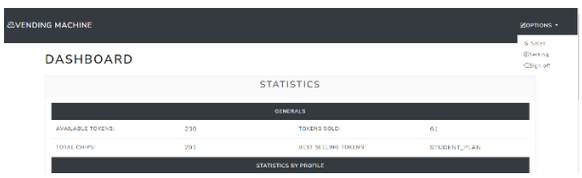


Figure 10 Options menu
Source: Own elaboration

Sales: this option shows the information on sales made and is divided into two sections: total sales and sales of the vending machine. As shown in Figure 11.

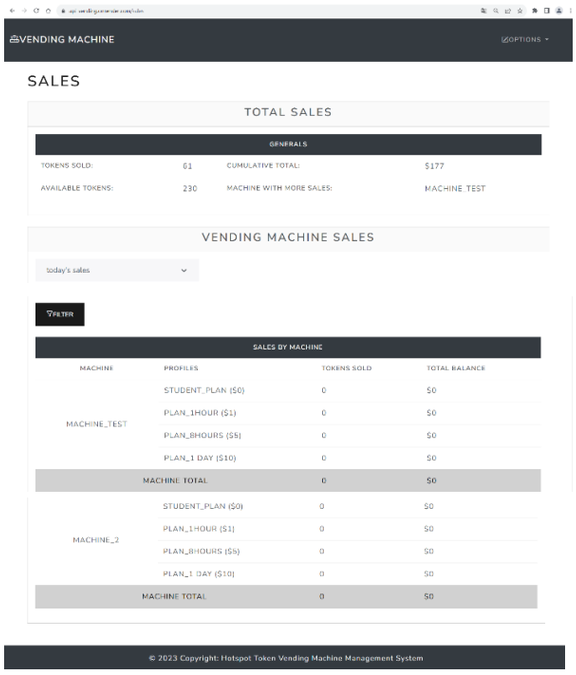


Figure 11 Sales page
Source: Own elaboration

The sales section shows general information on: tokens sold, tokens available, total accumulated amount and top selling machine.

The vending machine sales section displays machine information, profiles, tokens sold and accumulated balance by the selected sales search filters: today, yesterday, week, last week, month, last month, by custom date range and all sales.

2. Configuration: this option allows making the general configurations of the application for its operation and is divided into three sections: profile, security and profiles, vending machine and clear history. As shown in Figure 12.

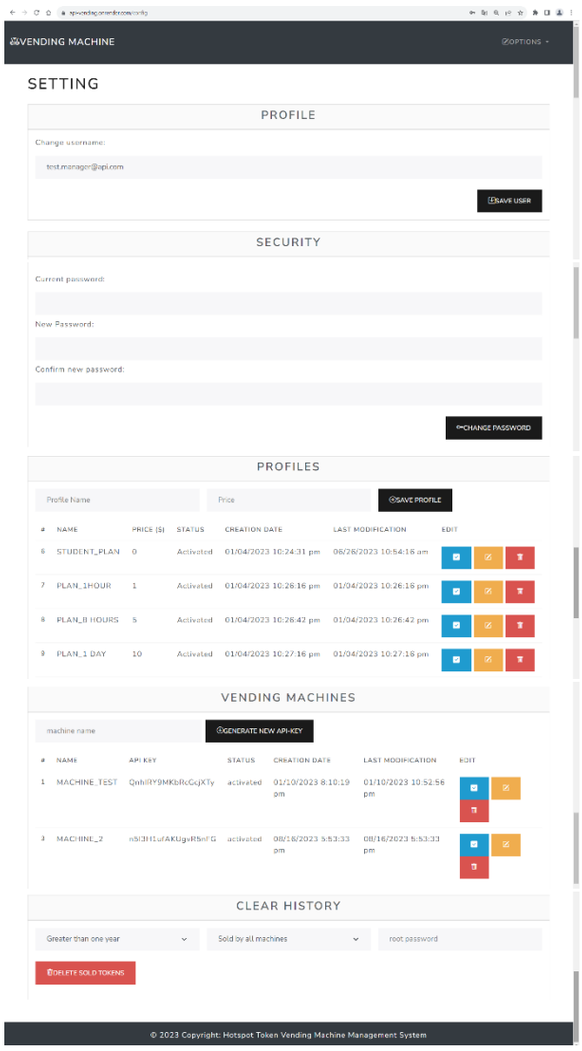


Figure 12 Configuration page
Source: Own elaboration

- Profile: this section allows you to change the name of the web application user.

- Security: this section allows you to change the password to enter the system.

- Profiles: this section allows to create and save the profiles of the cards: name, price, status, creation date, last modification. Once the profiles have been created, they can be edited: activate or deactivate the profile, edit the selected profile and delete the selected profile.

- Vending machine: this section allows to name the machine and generate a new api-key. Once created, it shows the machine information: name, api-key, status, creation date, last modification and the edit buttons to activate or deactivate the machine, edit and delete.

- Clear history: this section allows deleting sold cards by date: older than one year, six, three or one month, all sold, all cards - reset of sold for all machines or a specific registered machine. Such deletion of the history is with the confirmation of the password of the root administrator of the application.

- Logout: this option closes the web application by returning to the web application authentication page.

Acknowledgment

We thank the Tecnológico Nacional de México/Instituto Tecnológico Superior de Huachinango (TECNM/ITSH), the Master in Information Technologies, the Computer Systems Engineering program and the "Intelligent Computing" academic group with code ITESHUAU-CA-3 for the support provided.

Financing

This article has been funded by TECNM/ITSH [SPeI-SR-014 -2023].

Conclusions

The methodology used allowed to have an adequate development process to obtain a quality product that resulted in a web application that efficiently provides the available access credentials and manage the access credentials purchased from the vending machine.

There is a web application hosted on a free onreder.com server, which allows to manage the availability and sale of wireless internet access credentials of a vending machine.

The application works adequately, however one of the improvements that can be made is to upload it to a paid server to make the connection between the vending machine and the application more efficient in order to reduce the communication time with the server.

ISSN 2531-2197

References

EJS. (s.f.). *Embedded JavaScript templating.* https://ejs.co/

Express. (s.f.). *Fast, unopinionated, minimalist web framework for Node.js.* https://expressjs.com/

IONOS. (28 de noviembre de 2022). *¿Qué es MySQL?*. https://www.ionos.es/digitalguide/servidores/know-how/que-es-mysql/

Kinsta. (13 de mayo de 2021). *¿Qué es Node.js?*. https://kinsta.com/es/base-de-conocimiento/que-es-node-js/

MDN Web Docs. (s.f.). *JSON*. https://developer.mozilla.org/es/docs/Learn/JavaScript/Objects/JSON

Microsoft Corporation. (2021). *Visual Studio Code.* [Computer software]. https://code.visualstudio.com/

Mozilla. (s.f.). *JavaScript. Mozilla Developer Network.* https://developer.mozilla.org/es/docs/Web/JavaScript

MySQL. (s.f.). *MySQL: MySQL Community Server.* https://www.mysql.com/

Passport. (s.f.). *Simple, unobtrusive authentication for Node.js.* http://www.passportjs.org/

Panduman, YYF, Funabiki, N., Ito, S., Husna, R., Kuribayashi, M., Okayasu, M., ... &Sukaridhoto, S. (2023). Un Edge DeviceFramework en la Plataforma de Servidor de Aplicaciones IoT de SEMAR. Información, 14 (6), 312.

Ríos, J. R. M., Ordóñez, M. P. Z., Segarra, M. J. C., & Zerda, F. G. G. (2017). Estado del arte: Metodologías de desarrollo en aplicaciones web. *3c Tecnología: glosas de innovación aplicadas a la pyme*, 6(3), 54-71. https://dialnet.unirioja.es/servlet/articulo?codigo=6143045

RockContent. (22 septiembre de 2021). *¿Qué es Bootstrap?* https://rockcontent.com/es/blog/bootstrap/

Sequelize. (s.f.). *A promise-based ORM for Node.js.* https://sequelize.org/

Startechup. (15 de enero de 2021). *Express.js: qué es, para qué se usa y cuándo y dónde utilizarlo en el desarrollo de aplicaciones empresariales.* https://www.startechup.com/es/blog/express-js-what-it-is-used-for-and-when-where-to-use-it-for-your-enterprise-app-development/.

ISSN 2531-2197

Article **Journal Computer Technology**
June 2023, Vol.7 No.18 32-39

Importance of the analysis of computer attacks on a LAN network applying the predictive-quantitative method

Importancia del análisis de los ataques informáticos sobre una red LAN aplicando el método predictivo-cuantitativo

SAUCEDO-LEÓN, Daniel†, SAMPAYO-RODRÍGUEZ, Carmen Jeannette*, GONZÁLEZ-AMBRIZ, Rosalba and MORALES-OLIVARES, Rosibel

Tecnológico Nacional de México, Instituto Tecnológico Superior de Huauchinango, Ingeniería en Sistemas Computacionales, México.

ID 1st Author: *Daniel, Saucedo-León* / **ORC ID:** 0000-0003-2302-7233, **CVU CONAHCYT ID:** 1264052

ID 1st Co-author: *Carmen Jeannette, Sampayo-Rodriguez* / **ORC ID:** 0000-0001-8844-6055, **CVU CONAHCYT ID:** 951529

ID 2nd Co-author: *Rosalba, González-Ambriz* / **ORC ID:** 0000-0001-5400-9754, **CVU CONAHCYT ID:** 368433

ID 3rd Co-author: *Rosibel, Morales-Olivares* / **ORC ID:** 0009-0008-7151-5761, **CVU CONAHCYT ID:** 1296958

DOI: 10.35429/JCT.2023.18.7.32.39 Received: January 25, 2023; Accepted June 30, 2023

Abstract

In a global scenario, the amount of equipment exposed, the defense tools installed, the user culture and the subculture of information theft and damage to assets, it is necessary to create predictive stochastic models that can create a quantitative simulation about of a possible attack, and where appropriate the spread of it in an environment.

Security, Models, Predictive

Resumen

En un escenario mundial, la cantidad de equipos expuesta, las herramientas de defensa instaladas, la cultura del usuario y la subcultura de robo de información y daño en activos, se hace necesario la creación de modelos estocásticos predictivos que puedan crear una simulación cuantitativa acerca de un posible ataque, y en su caso la propagación del mismo en un entorno.

Seguridad, Modelos, Predictivos

Citation: SAUCEDO-LEÓN, Daniel, SAMPAYO-RODRÍGUEZ, Carmen Jeannette, GONZÁLEZ-AMBRIZ, Rosalba and MORALES-OLIVARES, Rosibel. Importance of the analysis of computer attacks on a LAN network applying the predictive-quantitative method. Journal Computer Technology. 2023. 7-18:32-39.

* Correspondence to the author (E-mail: carmen.sr@huauchinang.tecnm.mx).
† Researcher contributing as first author.

Introduction

With the continuous expansion of global network communications, the combination of traditional industries and the Internet is becoming more and more extensive. Network attacks are becoming more and more frequent, resulting in more and more threats and network losses.

Network security situational analysis (NSA) technology [I] incorporates data from intrusion detection system (IDS), firewall, virus detection system (VDS) and other network security protection devices. Essentially, it is an overall reflection of network security status and trends and can further serve as important evidence for early warning, network hardening and attack responses.

DBAG situation awareness or situational awareness [II] (SA) is a mental representation and understanding of objects, events, people, system states, interactions, environmental conditions, and any other factors in a specific situation that may affect the performance of complex or dynamic human tasks.

CVSS. The vulnerability measurement and scoring system, which allows to translate an arithmetic score into a qualitative representation of attack risk (low, medium, high and critical) [III]. This model, together with what is used in statistics and econometrics, in particular in time series, an autoregressive integrated moving average model or ARIMA methodology (autoregressive integrated moving average) is a statistical model that uses variations and regressions of statistical data in order to find patterns for a prediction into the future. It is a dynamic time series model, i.e. future estimates are explained by past data and not by independent variables. It was developed in the late 1960s. Box and Jenkins (1976) systematized it [IV] to achieve predictive models based on historical variables.

SNORT IDS. [V] It is an intrusion detection system, which for this research will be used in its intrusion prevention mode.

Micro Focus ArcSight is a cyber security product, first launched in 2000, that provides big data security intelligence and analytics software for security information and event management and log management.

MULVAL. It is a network security analyzer based on logical concepts, developed by Kansas State University. https://github.com/risksense/mulval.

The situation prediction technology includes two steps:

1. The first is the recognition of the situation. It refers to understanding the factors of the overall situation in the current network. The factors include the information of the network environment, attack strategies and defense strategies. The object is the current security state.

2. The second is situation prediction. Based on the previous step, it analyzed the regularity of the security situation and predicted the future trend in advance.

The exponential smoothing method is a way of forecasting the demand for a product over a given period. It estimates that demand will be equal to, for example, the average of historical consumption for a given period, giving greater weighting to values closer in time. It is optimal for random demand patterns where it is relevant to eliminate the impact of historical irregular elements by focusing on recent or targeted demand periods. [VI]

The 3 methods of predicting the network security situation by category are:

1. Methods based on time-space sequence (STS). The assumption of this method is that the change of the safety situation is regular and periodic. Suitable for short-term forecasting, time prediction is the next phase, and the value is fuzzy. [VII]

2. Methods based on graph theory (GRT). The GRT method uses vulnerability information in the network environment to generate the state transition diagram. In addition, it is designed from the intruder's perspective. The future situation is predicted based on the current network situation. [VIII]

3. Method based on game theory (GAT). Game theory is the study of mathematical models of conflict and cooperation between intelligent rational prediction of decisions. [IX][X]

ISSN: 2531-2197

Other necessary studies are required to solve the following problems:

1. General situational factors. STS and GRT methods primarily analyze attacker and environment information while ignoring defense information.

2. Accurate and complete prediction of the situation. Current research focuses on discovering the attack target, recognizing the attack path and predicting the probability of success.

In this document, a quantitative network situation prediction method that unifies the dynamic Bayesian attack graph (DBAG) is demonstrated.

The contributions of this document are as follows:

4. 1.- More complete prognostic information is obtained. The highlight is that not only can we predict common behaviors such as attack focus, attack path and probability of exploitation. In addition, the specific time to compromise the network can be calculated.

5. 2.- We design the risk quantification method for the security situation based on attack prediction. We provide a complete solution for the administrator to understand the security situation by quantitative value. One innovation is that we combine the common vulnerability scoring system (CVSS) [XI] with the information of predicted attack behaviors to quantify the possible risk from two angles of host and network.

Methodology to be developed

1. Network security situation prediction model. Predictions depend on the assessment of the adversary's attack capability, the effects of the defender's strategy, and information from the dynamically changing environment. Consequently, any change in the network security situation will lead to more or less changes.

Framework for quantifying the security situation based on attack predictions. The core idea is through collecting various information from running states of network devices to be aware of the "current situation" of the network, including network topology and connectivity, attack capability, observed attack events and defense strategies. Then, the above sample data is encoded into the DBAG to predict the possible attack.

Based on the attack prediction results and CVSS, we can further quantify the "future state" through security risk metrics. The feature of the framework is that the "future situation" can be adjusted in real time along with the "current situation" flexibly at any time. [XII]

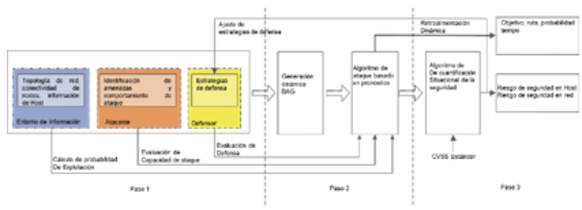


Figure 1 Predictive network security framework
Source: [XIII]

According to the framework, the specific steps are summarized as follows:

Step 1 Compilation of network security status factors.

Step 2 Network attack behavior prediction.

Step 3 Prediction of the network security situation.

2. Attack prediction algorithm

In this section, we first evaluated the attack capability of the adversary, then we calculated the vulnerability and the probability of exploitation of such vulnerability, as well as the expected time cost of future attacks, finally we calculated the prediction algorithm based on the DBAG and the complexity of the algorithm.

Attack Capability Metric. Assume that the attacker's ASLK attack capability is equal to the highest ever exploited ACPX of ASLK can be formulated as follows:

$$\mathrm{ASLK} = \max\big(\mathrm{ACPX}\ (\mathrm{Vuln})\big) \qquad (1)$$

ISSN: 2531-2197

Vulnerability exploitability probability metric. The relative vulnerability exploitability probability under different ACPX and ASLK is shown in Table 1.

ACPX	p(ACPX,ASLK) ASLK=LOW	ASLK=MEDIUM	ASLK=HIGH
Low	0.56	0.69	0.89
Medium	0.3	0.51	0.75
High	0.1	0.3	0.4

Table 1 Assessment of the probability of vulnerability exploitability
Source: Information processed with data obtained from the measurement of a network of 300 computers, between March 10 and March 23, 2023.

The probability of exploitability at the age or exposure time of the vulnerability (v), is as follows:

$$p(v) = \frac{p(ACPX,ASLK)}{F(t)} \quad (2)$$

Expected Attack Time-Cost Metric. The expected exploitation time with an unknown vulnerability cost V denoted as $ASLTexpcted$ is as follows:

$$ASLT_{Esperado} = \frac{ASLT_{prior}}{p(v)} \quad (3)$$

DBAG-based attack prediction algorithm. In this subsection, we encode the above information into the DBAG. In addition, by calculating the state transition equilibrium, the possible follow-up attack information can be predicted according to the equilibrium state.

Performance análisis of algorithms.

The complexity is:

$$O(nk) \quad (4)$$

The complexity of the space is:

$$O(4n2 + 2n) \quad (5)$$

3. Method of quantification of the security situation.

The impact metric of a vulnerability v is as follows:

$$Impact(V) = 10 \times (1 - (1 - C) \times (1 - I) \times (1 - A)) \quad (6)$$

Where C, I and A are the confidentiality, integrity and availability impact sub-scores respectively, and the score is obtained by querying the U.S. government's National Vulnerability Database (NVD) (NIST, 2023). [XIV]. The quantification of the security situation can be measured by the different types of attack and the severity of the threat.

Algorithm for quantifying the security situation. Input. Input matrices (SP, AT, DT, QD), vectors (T, P) and information (x, y, V, Weight). Output. Output $NSAr$ ($hostx$) and $NSAr$ ($network$).

Results

For method verification, SNORT IDS is used to collect the raw alert data during the test. Subsequently, two prediction experiments are conducted to verify the validity and rationality of our methods. Finally, the advantages of our methods are compared and discussed.

Network environment information. Small-scale experiment, the network is built and its topology is shown in Figure 2.

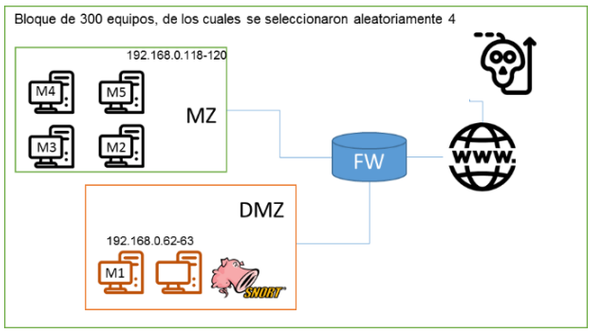


Figure 2 Test or experimental network topology determined for the research.
Source: Own elaboration

The network includes the firewall, intrusion detection system, five victim hosts and one attack host through the firewall with preset policies, the network is divided into two subnets.

Host M1 and IDS are deployed in the DMZ zone, and victim hosts M2, M3, M4 and M5 are deployed in the trusted zone. In addition, external hosts are prohibited from accessing hosts in the trusted zone and the adversary (connected to the Internet) can only communicate with host M1 (in the DMZ zone) via HTTP protocol (port 80).

ISSN: 2531-2197

Through scanning and querying network vulnerabilities on NVD public sites, we can obtain detailed information about vulnerabilities as shown in Figure 3 and Table 2.

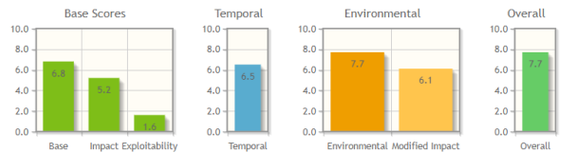


Figure 3 Predictive Network Security Framework
Source: Own elaboration

Whose attack vector is: CVSS v3.1 Vector AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:H/E:H /RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC: H/MPR:L/MUI:R/MS:C/MC:H/MI:H/MA:H

Host	Service	Impact	CVE Code
M1	Apache	2.9	CVE-2020-1954
M2	DNS	6.4	CVE-2008-4126
	Linux cfingerd	10	CVE-1999-0243
M3	Windows Network File System	10	CVE-2020-17051
M4	DNS	10	CVE-2020-1350
M5	MYSQL	2.9	CVE-2014-0420

Table 2 Vulnerability information
Source: Own elaboration

Six vulnerabilities are discovered in the five internal hosts, each of the six vulnerabilities is unique, publicly known and denoted by a CVE identifier.

According to the network topological structure and vulnerability information, the MULVAL tool is employed to generate the network attack graph as shown in Figure 4.

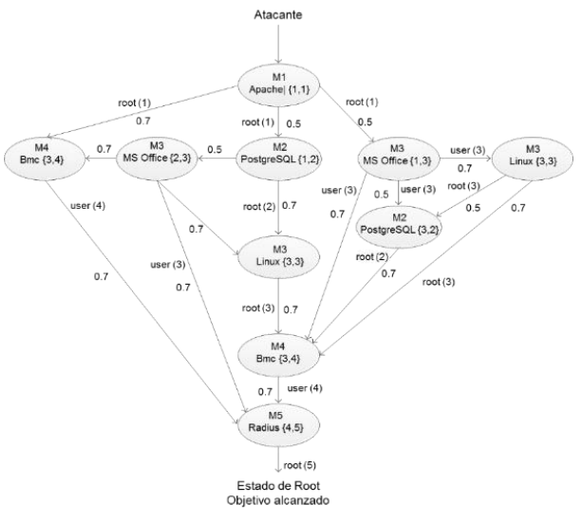


Figure 4 Experimental network attack graph
Source: Own elaboration

The granularity of the generated attack graph is the polynomial level, meanwhile, the generated graph is a directed acyclic graph.

Data collection test. To obtain from the real world experimental data, two skillful users of our network attack and defense scenario were selected and simulated, playing the roles of adversary and defender, respectively, and performing the experiment on the test network.

Experiment 1. In the first experiment, the raw alert sample data was selected from 9:00 am -11:00 am and analyzed through the ArCSight attack detection tool, finding the Exploit Vulnerability Probability Assessments and Expected Attack Time Cost shown in Table 3.

CVE #	Probability of success	Attack expectation in time/cost (h)
CVE-2020-1954	0.7230	0.2746
CVE-2008-4126	0.5163	0.3845
CVE-1999-0243	0.3097	0.6409
CVE-2020-17051	0.7222	0.2749
CVE-2020-1350	0.7215	0.2751
CVE-2014-0420	0.7229	0.274 6

Table 3 Experiment 1
Source: Own elaboration

The attacker has executed vulnerability exploitation on hosts M1 and M2 at 9:18 a.m. and 9:42 a.m. To forecast the subsequent attack behavior and security situation, the predictive algorithm and threat quantification method implemented together, the following steps were carried out and shown in Figure 5:

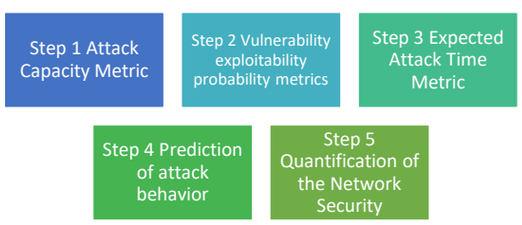


Figure 5 Steps of the predictive algorithm and quantitative threat method
Source: Own elaboration

ISSN: 2531-2197

Transition	CVE#	Probability	Time/Cost Expectation
S1→S2	CVE-2020-1954	0.7230	0.2746
S2→S3	CVE-2008-4126	0.5163	0.3845
S2→S4	CVE-2020-17051	0.7222	0.2749
S2→S6	CVE-2020-1350	0.7215	0.2751
S3→S4	CVE-2020-17051	0.7222	0.2749
S3→S5	CVE-1999-0243	0.3097	0.6409
S3→S6	CVE-2020-1350	0.7215	0.2751
S4→S3	CVE-2008-4126	0.5163	0.3845
S4→S5	CVE-1999-0243	0.3097	0.6409
S4→S6	CVE-2020-1350	0.7215	0.2751
S4→S7	CVE 2014-1878	0.7229	0.2746
S5→S3	CVE-2008-4126	0.5163	0.3845
S5→S6	CVE-2020-1350	0.7215	0.2751
S6→S7	CVE 2014-1878	0.7229	0.2746

Table 4 Description of attack behavior
Source: Own elaboration

According to Table 4, there are 14 different types of transition states/behaviors in the target network based on the primary attack sequence extracted from the observed sample alert.

All 9 possible attack paths from $S1$ to $S7$ are depicted in Table 5.

Number	Attack Route
Ruta 1	S1→S2→S6→S7
Ruta 2	S1→S2→S3→S4→S7
Ruta 3	S1→S2→S3→S6→S7
Ruta 4	S1→S2→S3→S4→S5→S6→S7
Ruta 5	S1→S2→S3→S5→S6→S7
Ruta 6	S1→S2→S4→S6→S7
Ruta 7	S1→S2→S4→S3→S6→S7
Ruta 8	S1→S2→S4→S5→S3→S6→S7
Ruta 9	S1→S2→S4→S4→S6→S7

Table 5 Possible attack routes
Source: Own elaboration

Quantification of the security situation occurs in two situations described below:

1. Host security status. We use the security situation quantification algorithm to calculate The security situation of hosts and network as detailed in Table 6.

Iterations	M1	M2	M3	M4	M5	Web
0	2.26	3.97	0	0	0	1.02
1	2.26	3.97	6.44	4.47	0	3.20
2	2.26	3.97	6.75	5.32	0.63	3.62
3	2.26	3.97	6.75	6.04	1.76	4.11
4	2.26	3.97	6.75	6.70	2.12	4.35
5	2.26	3.97	6.75	6.70	2.44	4.44

Table 6 Security predictions
Source: Own elaboration

Based on the predictions of attack behaviors obtained in step 4, the security situation of the host network is visualized illustrated in Figure 6, in which the horizontal axis is the cycle and the vertical axis is the NSA value [XV]. The higher value indicates the higher risk level at that time.

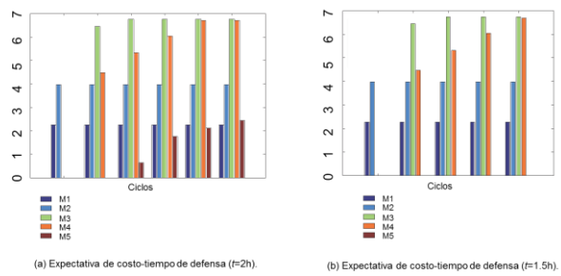


Figure 6 Host security status
Source: Own elaboration

By using the quantification of the host security situation, the administrator can recognize the threat of hosts, severity and further control the security risk of critical assets in a timely manner.

2. Network security situation. Considering two cases in Figure 7, the cost of defense time $t = 2$ and $t = 1.5$. the changes in the network security situation are illustrated in Figure 5, where the horizontal axis indicates the completion time of each attack step and the vertical axis indicates the security with its risk value, the higher value means the higher network risk, combined with Figure 5, we can obtain the following:

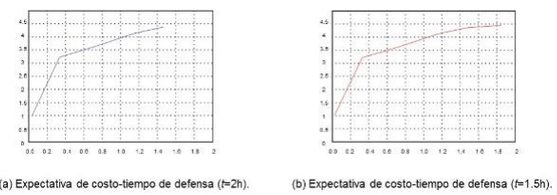


Figure 7 Network security status
Source: Own elaboration

- **Similarities**. In the initial phase, the entire network was at a "low" risk level, but, with the deepening of the attack phase, the attacker gradually realized the purpose of the invasion and the corresponding security risk and deficiencies were also increasing. Then the risk level was transformed to "medium", which is verified as true by the applied examinations and tests.

- **Differences.** Two cases are taken into account as follows; for the case t = 2, the attack ends in almost 1.8 h. During this period, the risk continues to increase. The results confirm that the change in the network situation may reflect the actual attacks of the method used.

For the case t = 1.5, along with the vulnerability applied by the defender, the attacker cannot continue to invade the host M5, so the invasion ends in almost 1.4 h, which indicates that the total network risk can be effectively reduced by strengthening the defense strategies.

Also, the results show that the predictions can be updated according to the defense strategies adaptively.

Acknowledgements

To the Tecnológico Nacional de México/Instituto Tecnológico Superior de Huauchinango.

Financing

Funding: This work was funded by Tecnológico Nacional de México/Instituto Tecnológico Superior de Huauchinango.

Conclusions

To optimize the prediction of the current network situation with this predictive method, two fundamental contributions are achieved in this paper.

1. The general factors of the network situation, such as attacker, defender and environment are taken into account to reflect dynamically and in real time the attack-defense confrontation feature.

2. The security situation is displayed from two levels (host and network) based on comprehensive attack prediction information.

Specifically, a prediction method of network security situation using the Bayesian attack graph presented in this paper through assessing the adversary's attack capability and combining the already detected alert events, it is possible to analyze the subsequent attack behaviors.

Based on that, the underlying security risk of the host and network are quantitatively calculated with the CVSS and asset information. The results show that this method is feasible, flexible and of low computational complexity in contrast to other similar studies.

This solution can achieve the purposes of an accurate attack, achieving intent recognition, route detection and probability of success through predictive action. In addition, the time cost of each step in the iterations makes it possible to calculate attack scenarios.

By quantifying the attack threat, the IT system administrator can assess the severity of the critical threat to assets and further infer and control the security situation in a timely manner. As we all know, the attack threat is always hidden within a network. Once an exploit occurs, the latent risk will be brought to the table, causing a series of security issues.

In the future of further research, an effective security strengthening strategy could be implemented based on the predictions of the security situation of each network, moreover, considering that all routes can be used to penetrate the system and to violate critical assets, the cost and benefit are different for each case and thus what is associated with the selected route. Therefore, to achieve security improvement on a cost-benefit basis in a budget constrained scenario is the key point in this research.

References

[I]. Security Information and Event Management tool. (s/f). Microfocus.com. Recuperado el 30 de enero, 2023, de https://www.microfocus.com/en-us/cyberres/secops/arcsight-esm.

ISSN: 2531-2197

[II]. Allsopp, W. (2017). Advanced penetration testing: Hacking the world's most secure networks. John Wiley & Sons. Recuperado el …(agregar fecha de consulta) de https://ns2.elhacker.net/descargas/manuales/Hacking%20y%20Seguridad%20informatica/advancedpenetrationtesting.pdf

[III]. Schiffman, "Sistema de puntuación de vulnerabilidad común (CVSS) ". Recuperado el … de https://www.first.org/cvss/

[IV]. Box, G. E. P and Jenkins, G.M., (1976). "Time series analysis: "Forecasting and control," Holden-Day, San Francisco. Recuperado el …

[V]. Snort - network intrusion detection & prevention system. (n.d.). Snort.org. Recuperado el 11 de febrero, 2023, de https://www.snort.org/

[VI]. Métodos y fórmulas para la Suavización exponencial simple. (n.d.). Recuperado el 12 de febrero, 2023, de https://support.minitab.com/es-mx/minitab/20/help-and-how-to/statistical-modeling/time-series/how-to/single-exponential-smoothing/methods-and-formulas/methods-and-formulas/

[VII]. Box, G. E. P and Jenkins, G.M., (1976). "Time series analysis: „Forecasting and control," Holden-Day, San Francisco. Es la misma que la IV

[VIII]. Métodos basados en grafos. Recuperado el 14 de marzo, 2023, de http://pdg.cnb.uam.es/pazos/cursos/bionet_UAM/Grafos_CAguirre.pdf

[IX]. Taha, H. A. (2010). Investigación de Operaciones: Una Introducción (9a ed.). Pearson. Recuperado … de https://frh.cvg.utn.edu.ar/pluginfile.php/54151/mod_resource/content/1/Introducci%C3%B3n%20a%20la%20Investigaci%C3%B3n%20de%20Operaciones%20%289na%20ed%29%20-%20Hillier%20%20Lieberman.pdf

[X]. Fernandez, et al., (2020). CADENAS DE MARKOV - Métodos cuantitativos para la toma de decisiones III (1ª ed.). Universidad Politécnica de Cataluña. Recuperado el … de https://upcommons.upc.edu/bitstream/handle/2117/96718/9788498806113.pdf?sequence=1

[XI]. Diogenes, Y., & Ozkaya, E. (2023). Cybersecurity - attack and defense strategies: Infrastructure security with Red Team and Blue Team tactics. Packt Publishing. Recuperado de …

[XII]. Allsopp, W. (2017). Advanced penetration testing: Hacking the world's most secure networks. John Wiley & Sons. Es la misma que la II

[XIII]. Villamizar, C. (2020, October 22). ¿Qué es NIST Cibersecurity Framework? GlobalSuite Solutions. Recuperado el … de https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/

[XIV]. NVD - home. (s/f). Nist.gov. Recuperado el 05 de enero, 2023, de https://nvd.nist.gov/

[XV]. Allsopp, W. (2017). Advanced penetration testing: Hacking the world's most secure networks. John Wiley & Sons. Es la misma que la II Y XII

ISSN: 2531-2197

[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-CONAHCYT) (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

Abstract (In Spanish, 150-200 words)

Objectives
Methodology
Contribution

Keywords (In English)

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

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 Computer Technology. 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

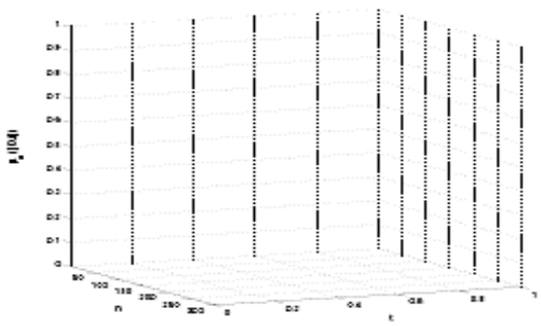
[Title No.12 in Times New Roman, single spaced and bold]

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.

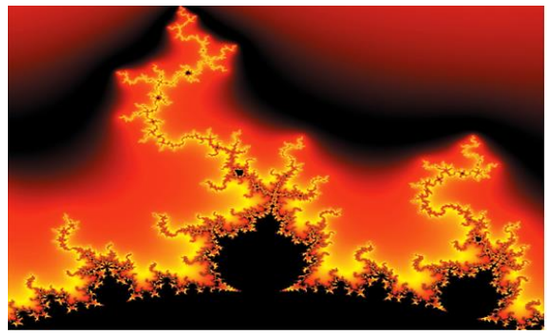


Figure 1 Title and *Source (in italics)*

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:

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

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 2531-2197

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.

- Authentic Signature in blue colour of the Conflict of Interest Format of Author and Co-authors.

ISSN 2531-2197

Reservation to Editorial Policy

Journal Computer Technology 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 Computer Technology 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 Spain 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 Spain for its Journal Computer Technology, 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 Co-authors	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)
EBSCO (Research Database - EBSCO Industries)
RESEARCH GATE (Germany)
GOOGLE SCHOLAR (Citation indices-Google)
REDIB (Ibero-American Network of Innovation and Scientific Knowledge- CSIC)
MENDELEY (Bibliographic References Manager)
HISPANA (Information and Bibliographic Orientation-Spain)

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

38 Matacerquillas, CP-28411. Moralzarzal –Madrid-España. Phones: +52 1 55 6159 2296, +52 1 55 1260 0355, +52 1 55 6034 9181; Email: contact@ecorfan.org www.ecorfan.org

Journal Computer Technology

2531 2197
ISSN 2531 - 2197

www.ecorfan.org