ISSN: 0123-3033 – ISSN-e: 2027-8284

INGENIERIA Y COMPETITIVIDAD
REVISTA CIENTÍFICA Y TECNOLÓGICA

Vol. 24 No. 2-2022 - DOI: 10.25100/iyc.v24i2.11762

INGENIERÍA DE SISTEMAS

Un algoritmo de inteligencia adaptable a un marco de ciberseguridad para IIOT

SYSTEMS ENGINEERING

An adaptable Intelligence Algorithm to a Cybersecurity Framework for IIOT

Santiago Ordoñez Tumbo[1], Katerine Márceles Villalba[2] ,SilerAmador Donado[3].

[1,2]Institución Universitaria Colegio Mayor del Cauca, Faculty of Engineering, Computing Engineering Program, I+D in Computing Group, Popayán-Colombia

[3]Universidad del Cauca, Faculty of Electronic Engineering and Telecommunicatios, System Engineering Program, Information Technology Research and Development Group (GTI), Popayán-Colombia

Santiago95@unimayor.edu.co, *samador@unicauca.edu.co, kmarceles@unimayor.edu.co*

Recibido: 22 de noviembre de 2021 – **Aceptado**: 15 de enero de 2022

Abstract

The industrial internet of things (IIoT) has grown in recent years, which makes it possible to publicize recent technological innovations and be able to integrate them with each other, such as smart cities, among other applications such as health, education, transit and others, but at the same time there is a problem that is security, due to the fact that incidents related to IIoT have been registered against data networks, for this reason it is necessary to generate intelligent solutions in cybersecurity, which allow to give a satisfactory solution. The objective of this work was to propose an intelligence technique adaptable to a cybersecurity framework with the ability to solve cybersecurity problems in networks of IIoT devices, for the development of which the research-action methodology (I-A), which consists of merging theory with practice in such a way that the researcher can generate accurate conclusions about the practices carried out. In this sense, with this methodology it is intended to provide solutions to specific problems in a given situation. Based on the above, a systematic literature review of the different artificial intelligence techniques was

Cómo citar:
Ordoñez S, Amador-Donado S, Márceles K. Un algoritmo de inteligencia adaptable a un marco de ciberseguridad para IIOT. *Ingeniería Y Competitividad*, 2022; e22511762. https://doi.org/10.25100/iyc.v24i2.11762

carried out, to finally determine the most appropriate ones and proceed to carry out the respective validations until the appropriate one was selected. Where it was found that there is a great variety of intelligence techniques such as Deep Learning (Deep Learning), who obtained a very high score in the characterization that was carried out due to its great possibilities when integrating the algorithm into the field of cybersecurity, it was identified that they are very poorly characterized; however, in the initial research that was done, the result was how to work with this technology and how to adapt it to cybersecurity. There are different ways to analyze and secure data on the network, one of these is learning techniques, in this research several techniques were identified that with their respective algorithms provided the basis for adaptability with a framework related to IIoT technologies.

Keywords: Cybersecurity, Industrial Internet of Things-IIoT, Artificial Intelligence, Intrusion Detection System, Security Models.

Resumen

El internet industrial de las cosas (IIoT) ha tenido un crecimiento en los últimos años, que permite dar a conocer las recientes innovaciones tecnológicas y poder integrarlas entre sí, como lo son las ciudades inteligentes, entre otras aplicaciones como la salud, educación, tránsito y otras más, pero a su vez se cuenta con una problemática que es la seguridad, debido a que se han registrado incidentes relacionados con IIoT frente a las redes de datos, por ello se hace necesario generar soluciones inteligentes en ciberseguridad, que permitan dar una solución satisfactoria. El objetivo de este trabajo fue proponer una técnica de inteligencia adaptable a un framework de ciberseguridad con la capacidad de solucionar los problemas de ciberseguridad en las redes de los dispositivos IIoT, para el desarrollo de éste se hace uso de la metodología investigación-acción (I-A), la cual consiste en fusionar la teoría con la práctica de tal forma que el investigador pueda generar conclusiones acertadas sobre las prácticas realizadas. En este mismo sentido, con dicha metodología se pretende dar soluciones a problemas concretos en una situación determinada. A partir de lo anterior, se realizó una revisión sistemática de literatura de las diferentes técnicas de inteligencia artificial, para finalmente determinar las más adecuadas y proceder hacer las respectivas validaciones hasta seleccionar la apropiada. Donde se encontró que existen una gran variedad de técnicas de inteligencia como Deep Learning (aprendizaje profundo), quien obtuvo un puntaje muy alto en la caracterización que se realizó por sus grandes posibilidades a la hora de integrar el algoritmo al ámbito de la ciberseguridad, se identificó que se encuentran muy poco caracterizados; sin embargo, en la investigación inicial que se hizo, se obtuvo como resultado el cómo trabajar con esta tecnología y cómo poderla adaptar a la ciberseguridad. Existen diferentes formas de analizar y dar seguridad a los datos en la red, una de esas son las técnicas de aprendizaje, en esta investigación se identificaron varias técnicas que con sus respectivos algoritmos proporcionaron las bases para la adaptabilidad con un framework relacionado con tecnologías IIoT.

***Palabras clave**: Ciberseguridad, Internet industrial de las cosas-IIoT, Inteligencia artificial, algoritmos de ML, Modelos de seguridad*.

1. Introduction

It is well known that network traffic is a matter of study nowadays, because threats are becoming more and more frequent in information systems and data networks, especially those that are exploited through protocols and ports. such as: HTTP or HTTPS (3), this is how the administrators or engineers in their respective organizations are in search of solutions in an efficient and secure way, that guarantee the integrity of the data that circulates in the networks (3).

It is important to mention that currently cybersecurity frameworks are characterized by being static, they are not capable of making decisions or learning from an incident, so this work seeks to propose an intelligence technique adaptable to a cybersecurity framework for IIoT that it is able to prevent and react to any threat without the need to have it registered in its signature bank or intruder detector rules, since threats vary daily, thus leaving systems outdated and vulnerable (4). Due to this, a study was carried out about learning techniques in conjunction with the inclusion of IIoT technologies, in order to integrate into a system that was capable of intelligently to learn under unsupervised algorithms that are immersed in the selected technique and thus demonstrate optimal results.

The development of this article is presented below in the following sessions: the methodology section where some conceptual aspects are addressed, the background and the methods sections are used to solve the problem raised, the final section results and discussion show the analysis of what was obtained and finally the conclusions where the appraisals and contributions of the work carried out are presented.

2. Methodology

Within the development of this work, certain concepts and references that are important were taken into account, and they are listed below:

- Cybersecurity Framework: The cybersecurity framework is a predefined set of policies and procedures by leading cybersecurity organizations (5), cybersecurity frameworks are built and documented to improve cybersecurity strategies in an organization or company.

- IDS: (Intruder Detection System) is a device or application that monitors a network or systems for malicious activity or policy violations (6), the intrusion detection system is constantly analyzing the traffic, it has the ability to identify anomalies or security violations based on patterns and heuristics. Immediately detects an attack, notifies an administrator; likewise, it collects information on each anomaly or attack detected.

- IIoT: With the arrival of the Internet of Things, the industry realized that this technology could be used in its operations, for which the IIoT (Industrial Internet of Things) arose. It refers to the tight integration of computing, networks, and physical objects for industry, in which embedded devices are networked to detect, monitor, and control the physical world to promote business and manufacturing progress (7), IIoT is changing the world of industry in terms of automation in its manufacturing processes, since devices or machines can connect and transfer data between themselves.

Among the most significant references for carrying out the project, the following can be highlighted:

In the first job (8), it combines the management of supervision and artificial intelligence based on ML-Models divided into study of network patterns, together with anomalies-intrusion detection based on IoT systems. Especially with attacks of the DoS (Denial of Service) type using the data mining approach, which is hugely popular in detecting attacks with high performance and low price. In relation to the anomaly-intrusion detection system based on IoT, the scenario has been evaluated in an intelligent environment using SVM (Support Vector Machines).

In the next article (9), the study "Intrusion Detection System using Artificial Intelligence" is described, which is characterized by incorporating an intelligent factor based on neural networks oriented to the detection of the specific problem of port scanning, using the IDS (Intrusion Detection System - SnortTM open source Intrusion Detection System. This article (10), involves the design of a novel intrusion detection system, the use and evaluation of its study model. The new system consists of a collection module, a data management module, a study module, and a response module. For the use of the study module, it involved the implementation of a neural network for intrusion detection.

Each of the aforementioned works contributed to the selection and study of the appropriate intelligence and learning technique capable of analyzing network traffic.

3. Results and Discussion

Regarding the development of the activities, the following results were obtained, which are shown below:

Activity 1. Carry out a review of the deep learning techniques used in the articles found and classified as primary.

It is important to mention that this process was carried out through a systematic review of the literature based on (11), where 201 studies were initially identified in the bibliographic database engines, these from now on are considered as found. Based on the inclusion and exclusion criteria that were determined, it was possible to eliminate redundant studies, until reaching 191 studies that were considered as not repeated. The inclusion criteria that was based on an analysis of the title, abstract and keywords of the articles obtained in the search, where it was taken into account that they integrate blockchain technologies, intrusion detection, framework, deep learning techniques focusing on the field of the IoT(Internet of things); that is, if the article mentions the use of any model, process, framework or methodology for the security of IoT devices through deep learning techniques or methods for the analysis of malicious traffic. The foregoing allowed obtaining 134 studies that were considered relevant, by reading the title, abstract and keywords. The 134 studies were read completely and with the exclusion criteria whose function is to exclude articles that had the following aspects: the study presents a process or methodology for the security of IoT devices, through blockchain techniques or contains deep learning methods for the identification of malicious traffic, but it does not present enough information on its use or application, with this it was possible to obtain 67 primary studies, as can be seen in Table 1.

***Table 1**. Review of bibliographic sources*

Databases	Studies			
	Found	Not repeated	Most relevant	Primary
Google	17	17	16	13
Academic google	89	81	49	12
IEEEXplore	27	26	19	7
ScienceDirect	twenty-one	twenty-one	fifteen	12
EBSCO	10	10	5	3
Microsoft academic	Fifteen	Fifteen	13	9
SpringerLink	22	twenty-one	17	eleven
Total	201	191	134	67

Source: Author's own

These articles provided the basis to characterize and select the learning technique, there were 20 of the 67 articles classified as primary, these are listed in Table 2, where the contribution for which it was taken as a reference for its contribution in this is identified. job.

***Table 2**. List of articles with some intelligence technique*

ARTICLE	INPUT
A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks (12)	Bidirectional Deep Learning Short Term Long Term Memory (BiLSTM)
Blockchain and Random Subspace Learning-Based IDS for SDN-Enabled Industrial IoT Security (13)	Unnamed deep learning-based techniques
Intrusion Detection System for Internet of Things based on Machine Learning (14)	Deep learning was implemented for the implementation of the analysis module
Blockchain-enabled Distributed Security Framework for Next Generation IoT- An Edge-Cloud and Software Defined Network Integrated Approach (15)	Tack Detection Scheme Using a Deep Learning Approach for the Internet of Things
Integrating complex event processing and machine learning An intelligent architecture for detecting IoT security attacks (16)	ML Taxonomy Scheme and Deep Learning for IoT Security.
Advances in Self-learning Intrusion Detection Systems - Systematic Literature Review (17)	Machine learning
BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network (18)	It uses a deep learning algorithm, and sequentially mitigates attacks at the edge of the network.
Sukhpal SinghGill Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges (19)	Intelligence-based deep learning techniques (AI) to maintain QoS (Quality of Service) -supervised learning techniques-unsupervised learning techniques
A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework (20)	Using a particle swarm optimization (PSO) algorithm to automatically adapt deep learning parameters
Detecting Internet of Things attacks using distributed deep learning (21)	A cloud-based distributed deep learning framework for phishing and botnet attack
Enforcing security in Internet of Things frameworks: A Systematic Literature Review (22)	The most promising machine learning (ML) and deep learning (DL) algorithms, their advantages, disadvantages, and applications in IoT security.

Intrusion detection systems in the Internet of things: A comprehensive investigation (23)	Attacks in the social IoT with deep learning
Internet of Things: A survey on machine learning-based intrusion detection approaches (24)	It is recognized as a relevant approach for network intrusion detection in addition to acting as a pattern recognition, image processing and text mining.
IFLBC On the Edge Intelligence Using Federated Learning Blockchain Network (25)	At the forefront of the advent of deep learning is the proliferation of data from various data sources ranging from Internet of Things (IoT) devices to self-driving cars.
Unification of Blockchain and Internet of Things (BIoT) requirements, working model, challenges and future directions (26)	Deep learning (DL), a subset of ML has also been widely deployed to improve IoT security
Research on secure transmission and storage of energyIoT information based on Blockchain (27)	In this mechanism, the dual deep learning model uses two models, namely, disaggregation and aggregation model.
A Deep Learning Framework to Enhance Software Defined Networks Security (28)	This paper revisits network anomaly detection as recent advances in machine learning particularly deep proven success in many areas such as computer vision and speech recognition.
Framework for Detection of Malicious Activities inIoT Networks using Keras Deep Learning Library (29)	IoT Backbone Networks that use the Keras deep learning library.
DL - IDS a deep learning – based intrusion detection framework for securing IoT (30)	It proposes a new deep learning-based intrusion detection system (DL-IDS) to detect security threats in IoT environments.
A Novel Deep Learning Framework for Intrusion Detection System (31)	This document is an attempt to bring a new deep learning framework that can identify both unknown attacks with a maximum accuracy of 82%.

Source: Author's own

Taking into account the different learning techniques identified in the previous table, the most appropriate and used to perform traffic analysis were found and they are the ones that can provide a supervised or unsupervised section, given that in the process of capture, processing and transformation of data it is seen the need to do it this way; likewise, it is articulated to the architecture of the proposed framework, where it allows the use of these types of algorithms. Next, the different learning techniques found for a model of detection, treatment and execution of results to be used in components identified in the currently known tools are listed. (32).

BIDIRECTIONAL(BiLSTM): The bidirectional short-term and long-term memory algorithm presents an extended version of RNs (Neural Networks), which has the inability to learn contextual information for a long time, this mainly caused by the leakage gradient problem. While LSTM employs the idea for related unit gates, which overcomes the problem of gradients and therefore allows information to be preserved for longer periods and thus kept for analysis.

Bidirectional RNs handle forward and backward input sequences using two different hidden layers (33).

SWARM (PSO): Particle Swarm Optimization (PSO) is a population-based EC algorithm, which can be used to solve optimization problems without domain knowledge. The population is made up of a number of particles. Each of them represents a candidate. Find the best solution by updating the velocity and the particle vector according to the equations. In one of the research papers like GetNet an encoding strategy of using a fixed length binary string to represent CNN architectures was proposed (34).

DEEP LEARNING OF MLP: The algorithm of an MLP (multilayer perceptron) can be interpreted as an extension of the regression algorithm where first the input is transformed using a non-linear transformation, with the purpose of projecting the input data to a space that is linearly separable. It is an algorithm that uses many layers to comply with the philosophy of deep learning, one of them and the one that is mentioned the most is the hidden or intermediate one that works as a universal approximation (35).

RESTRICTED BOLTZMANN MACHINES (RBM): It is a neural network that applies to Deep learning a probability distribution on its set of inputs. RBMs have been found applications in (dimensionality reduction, classification, collaborative filtering, feature learning, and mechanical modeling, among others). RBMs are a variant of Boltzmann machines that with the restriction of their neurons forms a bipartite graph, with nodes commonly called visible and hidden respectively. It contains restrictions between algorithms that are used in the subject that interests us, such as deep learning. (36).

MULTILAYER PERCEPTRON (MLP): It is a neural network formed by multiple layers, which makes it a good alternative to solve problems that are not linearly separable, but it can be seen as a limitation when applying Deep learning, for this reason it is called a simple perceptron. In the first case, each output of a neuron in layer "i" is the input of all the neurons of layer "i + 1", while in the second, each neuron of layer "i" is an input of a series of neurons. (region) of layer "i + 1" (37).

From the list of aforementioned techniques, a pre-selection was made, which was generated in relation to a characterization of each technique, in order to select the best at the level of behavior compared to cybersecurity frameworks, according to how it will the algorithm works based on the data collected by IDS technology that will provide the data after analyzing the network traffic, in order to generate the rules intelligently and as accurately as possible (38)For this, it was necessary to follow the guidelines proposed by the algorithms that will be used such as: Scikit-learn, which is one of the best libraries known to program intelligently, due to its large number of algorithms and associated processes, which at the when it is put into operation, it is very easy to use and execute. Kmeans clustering will be the algorithm that will facilitate finding the anomalous information in the dataset. To achieve this, it is necessary to instantiate 4 initial values called “k” values, the columns that will be used in the dataset for the “k” value will be: IP destination, port, time and finally the type of alert. It should be noted that columns of the dataset can be selected randomly, but it is advisable to adapt the algorithm to the project in question, as shown in Table 3.

It can be seen in Table 3, the 4 necessary characteristics that must be taken into account in the selection of the intelligent technique, for the generation of the rule through the intruder detector (39), it is necessary that when classifying and giving some values to the characteristics the scale that was taken was: 5 as the most important, 3 moderately and 1 not important, in this way the comparative table can be read to start in the capturing the characteristics required by the algorithm for automatic rule creation (40).

Next, a review of the possible Deep learning algorithms that meet the requirements identified in table 3 and the framework architecture was carried out, based on the list of articles that were taken as primary, which was extracted from the list of techniques of learning that have already been defined, which can be evidenced that the most appropriate for doing traffic analysis is the deep learning technique.

***Table 3**. Characteristics for rule generation*

Features for generation rule for intelligence	Required for rule creation (yes = 5, no = 1)	Modifiable by algorithm (yes = 5, no = 3)	Can be null (yes = 1, no = 5)	Needed for comparison (yes = 5, no = 1)	Total score
Action (Alert)	Yes	No	No	Yes	18
Protocol	Yes	No	No	Yes	18
Source IP address	Yes	No	No	Yes	18
Source IP port	Yes	No	Yes	No	10
Destination IP address	Yes	No	Yes	No	10
Destination IP port	Yes	No	Yes	No	10
Operation Direction	Yes	No	Yes	No	10
Weather	No	Yes	No	No	12

Source: Author's own

Once all the algorithms obtained from the systematic review of the defined articles had been studied, it began with the comparison of the functioning of each one and thus be able to verify, which is the most optimal, for this a comparison of the algorithms of deep learning found. In addition, a comparison was made taking into account the basic criteria of the operation of deep intelligence or Deep learning (41), with the essential characteristics used and determined in the articles named as primary (see table 4), where it gave as results that the bidirectional deep learning techniques of short and long-term memory (BiLSTM) and Swarm (PSO) with a result of 26 points placing them as the most appropriate to be implemented in the proposed framework, due to the significant fulfillment of the characteristics evaluated as a requirement.

***Table 4.** Algorithms aligned to the deep learning technique*

Deep Learning Technique	Prediction	Precision	Answer	Resource	Weather	Results
Two-way short memory deep learning long-term (BiLSTM)	YES	HIGH	WELL	HIGH	LOW	26
Swarm (PSO)	YES	HIGH	WELL	HALF	LOW	26
MLP Deep Learning	NO	HALF	WELL	LOW	HALF	18

Restricted Boltzmann Machines (RBM)	YES	HIGH	WELL	HALF	HIGH	22
Multilayer Perceptron (MLP)	YES	HALF	WELL	HIGH	HALF	19
YES = 5, NO = 1	HIGH = 5, MEDIUM = 3, LOW = 1	GOOD 5, MEDIUM = 3, BAD = 1	HIGH = 1, MID = 3, LOW = 5	HIGH = 1, MID = 3, LOW = 5		

Source: Author's own

In Table 4, it can be seen that the algorithms were evaluated according to 5 characteristics, which allowed determining the most suitable for the project, giving a justification for why it was selected. To begin with, you have the prediction, which is nothing more than the way the algorithm behaves based on its way of grouping the information, to generate predictions that end up giving detailed information; Regarding precision, the way in which the technique generates the results was evaluated, it is important to note that not all algorithms have a learning preprocessing, some only allow the generation of tables and possible information, for this the precision section will help us; Regarding the response, the speed and precision in which the algorithm responds can be evaluated, but the main characteristic is the information that it can capture and allow us to use; Regarding resources, this item allows determining the dependency of the hardware factor together with its relationship with the time for the execution of the technique.

From the previous classification, it allowed to identify the software and hardware needs that the Deep Learning technique and its algorithm needs for its optimal functioning in the proposed system, in table 5 the 2 selected algorithms are shown in detail together with the software and Suggested hardware for algorithm execution and processing.

***Table 5**. Hardware and Software Requirements*

Deep Learning Algorithm	software	Hardware
Two-way short memory deep learning long-term (BiLSTM)	Programming language with which the algorithm is developed.	Computer
	OS	Suitable IoT device
	Algorithms (bidirectional, Unsupervised).	
	Matlab 2017a, 2017b and 2018a	
	Parallel Computing Toolbox	
	Matlab Deep Learning Toolbox	
	Word processor (Microsoft Word)	
	Github online repositories.	
	CUDA 9.2 driver	
Swarm (PSO)	Altera DSP Builder	Computer
	Github online repositories.	
	Matlab 2017a, 2017b and 2018a	
	Word processor (Microsoft Word)	
	OS	AFPGACycloneII EP2C35

		Development Board

Source: Author's own

After performing a test with both algorithms with an IIoT traffic dataset, it was demonstrated by its effectiveness and efficiency in the identification of anomalies that the deep learning technique with its bidirectional algorithm of short-term, long-term memory (BiLSTM) It is the most suitable for its precision in the answer and the solution to the problem, performance and low cost of resources were definitive aspects to determine it as the most suitable Deep Learning algorithm for this project (42).

4. Conclusions

We live in an environment in which it is necessary to have secure information both on a business and personal level. This is more and more necessary every day, since with the increase in connectivity and the great flow of information there are also great risks generated by computer attacks and fraud attempts in administrative networks, so several must be taken into account aspects of cybersecurity and one of them is the implementation of controls (43). In this same sense, it is important to mention that a latent vulnerability occurs in the transport of data collected by IoT devices, since 98% of the traffic that is generated is not encrypted, which exposes personal and confidential data on the network. Attackers who have successfully overcome the first line of defense (most often through phishing attacks) and have established command and control can eavesdrop on unencrypted network traffic, collect personal or confidential information, and then exploit that data to profit from being on sites like the Dark Web (2020 Unit 42 IoT Threat Report). Under the above, Deep learning is the technique framed in artificial intelligence that is responsible for emulating the neural networks of human beings to feed back and automate predictive analysis, a cybersecurity framework allows the automation of problem solving, in other words deep learning It is used for problems where traditional learning methods do not achieve an appropriate performance, this technology gives the possibility not only to solve the security problem in the network but also to integrate all the necessary elements for its operation in general. (44).

On the other hand, regarding the difficulties that arose during the selection process of the intelligence technique with its algorithm, it was when generating the characterizations, since it was difficult to determine which could be the important characteristics to take into account for detection traffic, but the scientific community helped a lot in making these comparisons, since the documentation is scarce, compared to what is the integration of techniques and devices as it is a technology that is booming as well as the solutions, given by the different organizations that offer ways of how to have a faster connection to the ideas raised in the articles consulted.

5. Acknowledgment

Thanks to the University of Cauca, especially to its GTI research group and to the Computer Science I+D research group of the Colegio Mayor of Cauca University Institution, for the support provided for the development of the project.

6. References

1. Dominguez JEL. Sistema Detector de intrusos ocupando una red Neuronal Artificial. Trabajo de grado de Maestría. Solidaridad México: Universidad Autónoma del Estado de México, Computación; 2015. Report No.: http://hdl.handle.net/20.500.11799/49966.
2. Christian Urcuqui ANJOMG. Machine Learning Classifiers to Detect Malicius Websites. Free Open-Access Proceedings for Computer Science Workshops. 2017; 1950: p. 1-4.
3. Castillo CR. Segu-Info Noticias sobre Seguridad de la Información. [Online].; 2019 [cited 2020 03 03. Available from: https://blog.segu-info.com.ar/2019/09/buscar-la-direccion-lp-real-detras-de.html?m=0.
4. Sifre JP. IDS de red para la detección de ataques sobre SSH y FTP. Trabajo Fin de Master. Alicante, España: Universidad de Alicante, Departamento de Tecnología Informática y Computación; 2020.
5. Angie Valencia PP. Internet Industrial de las Cosas (IIOT): Nueva Forma de Fabricación Inteligente. Popayán: Fundación Universitaria de Popayán , Facultad de Ingeniería; 2021.
6. Miloud Bagaa TTJBBAS. A Machine Learning Security Framework for Iot Systems. IEEE Explore. 2020 May 21;(DOI: 10.1109/ACCESS.2020.2996214): p. 114066 - 114077.
7. Amador Siler AAyBC. Utilizando Inteligencia Artificial para la detección de Escaneos de Puertos. VI Jornada Nacional de Seguridad Informática ACIS 2006. 2006; http://acistente.acis.org.co/typo43/fileadmin/Base_de_Conocimiento/VI_JornadaSeguridad/ArticuloIAPortScan_VIJNSI.pdf: p. 1-12.
8. Chao Liang BSSAMJFDBGN. Intrusion Detection System for Internet of Things based on a Machine Learning approach. 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN). 2019; DOI: 10.1109/ViTECoN.2019.8899448(https://ieeexplore.ieee.org/document/8899448/authors#authors).
9. Mario Piattini Velthuis FPHT. Gestión y desarrollo de proyectos de investigación distribuidos en ingeniería del software por medio de investigación-acción. Revista Facultad de Ingeniería de Universidad de Antioquia. 2013 Sep; ISSN 0120-6230(68): p. 61-74.
10. Osama Alkadi NMBTKKRC. A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks. IEEE Internet of Things Journal. 2020 May 22;(DOI: 10.1109/JIOT.2020.2996590): p. 9463-9472.
11. Abdelouahid Derhab MGAGLMMAFMMFAK. Blockchain and Random Subspace Learning-Based IDS for SDN-Enabled Industrial IoT Security. MDPI - Sensors. 2019; 4(https://doi.org/10.3390/s19143119): p. 1-24.
12. Chao Liang BSSAMJFDBGN. Intrusion Detection System for Internet of Things based on a Machine Learning approach. International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN). 2019 Nov 14;(DOI: 10.1109/ViTECoN.2019.8899448).
13. Darshan Vishwasrao Medhane AKSMSHGMJW. Blockchain-Enabled Distributed Security Framework for Next-Generation IoT: An Edge Cloud and Software-Defined Network-Integrated Approach. IEEE Internet of Things Journal. 2020 Feb 28; 7(DOI: 10.1109/JIOT.2020.2977196): p. 6143 - 6149.
14. José Roldán JBPJMGO. Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks. Science Direct. 2020 Jul 1; 149(https://doi.org/10.1016/j.eswa.2020.113251).
15. Maldonado J. Avances en Sistemas de Deteccion de Intrusos con Auto-aprendizaje - Revisión Sistemática de la Literatura. Sexta Conferencia Nacional de Computación, Informática y Sistemas / CoNCISa 2018 /.

2018 Nov 30;(ISBN: 978-980-7683-04-3): p. 82-87.

16. Shailendra Rathore BWKJHP. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. Journal of Network and Computer Applications. 2019 Oct 1; 143(https://doi.org/10.1016/j.jnca.2019.06.019): p. 167-177.

17. Sukhpal Singh Gill MXSTIS. Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. Science Direct - Internet of Things. 2019 Dec; 8(https://doi.org/10.1016/j.iot.2019.100118).

18. Nickolaos Koroniotis NMES. A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. Future Generation Computer Systems. 2020 Sep 09; 110(https://doi.org/10.1016/j.future.2020.03.042): p. 91-106.

19. Gonzalo De La Torre Parra PRKKRCNB. Detecting Internet of Things attacks using distributed Deep Learning. Journal of Network and Computer Applications. 2020 Aug 1; 163(https://doi.org/10.1016/j.jnca.2020.102662).

20. Mohab Aly FKMHAQSY. Enforcing security in Internet of Things frameworks: A Systematic Literature Review. Science Direct - Internet of Things. 2019 Jul 06;(https://doi.org/10.1016/j.iot.2019.100050).

21. Somayy Hajiheidari KWMBNJN. Intrusion detection systems in the Internet of things: A comprehensive investigation. Science Direct. 2019 Sep 03; 160(https://doi.org/10.1016/j.comnet.2019.05.014): p. 165-191.

22. Kelton A.P. da Costa JPPCOLMVHCdA. Internet of Things: A survey on machine learning-based intrusion detection approaches. Science Direct - Computer Networks. 2019 Mar 14; 151(https://doi.org/10.1016/j.comnet.2019.01.023): p. 147-157.

23. Ronald Doku DBR. IFLBC: On the Edge Intelligence Using Federated Learning Blockchain Network. 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2020 Jun 23;(DOI: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00047): p. 1-6.

24. Bharat Bhushan CSPSAK. Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. Wireless Networks. 2020 Aug 06; 27(https://www.springerprofessional.de/en/unification-of-blockchain-and-internet-of-things-biot-requiremen/18255264): p. 55-90.

25. Hou Rui LHHYZY. Research on secure transmission and storage of energy IoT information based on Blockchain. Peer-to-Peer Networking and Applications. 2020 May 06; 13: p. 1225–1235.

26. Ahmed Dawoud SSCR. A Deep Learning Framework to Enhance Software Defined Networks Security. 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA). 2018 Aug 23;(DOI: 10.1109/WAINA.2018.00172).

27. Abhinaya Nagisetty GPG. Framework for Detection of Malicious Activities in IoT Networks using Keras Deep Learning Library. 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC). 2019 Aug 29;(DOI: 10.1109/ICCMC.2019.8819688).

28. Yazan Otoum DLAN. DL-IDS a deep learning–based intrusion detection framework for securing IoT. Internet Technology Letters. 2019 Nov 29;(https://doi.org/10.1002/ett.3803).

29. Mahwish Amjad HZSZTM. A Novel Deep Learning Framework for Intrusion Detection System. 2019 International Conference on Advances in the Emerging Computing Technologies (AECT). 2020 Sep 10;(DOI: 10.1109/AECT47998.2020.9194224).

30. Claudia Ximena Sanna Morales SALC. modelo de detección de intrusos usando técnicas de Aprendizaje de máquina. Trabajo de grado. Antioquia: Institución Universitaria Tecnológico de Antioquía, Ingeniería en Software; 2018.

31. Jacobson RM. comparativa y estudio de plataformas IoT. Trabajo de grado. Cataluña: Universitat Politécnica de Cataluña, Sistemas; 2017.

32. Joaquín Q. Lima M BBC. Optimización de Enjambre de Partículas aplicada al Problema del Cajero Viajante Bi-objetivo. Revista Iberoamericana de Inteligencia Artificial. 2006; 10(https://www.redalyc.org/pdf/925/92503209.pdf): p. 67-76.

33. Santiago Eguren CACJG. Modelado Probabilistico Basado en Aprendizaje Profundo para la deteccion de anomalias. XXI Workshop de Investigadores en Ciencias de la Computación (WICC 2019, Universidad Nacional de San Juan). Mendoza,Argentina: Universidad Nacional de la Plata, Seguridad Informática; 2019. Report No.: ISBN:978-987-3984-85-3.

34. Ahmed Dawoud SSCR. A Deep Learning Framework to Enhance Software. 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA). 2018 Jul 23;(Doi:10.1109/WAINA.2018.00172).

35. Abhinaya Nagisetty GPG. Framework for Detection of Malicious Activities in IoT Networks using Keras Deep Learning Library. 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC). 2019 Aug 29;(Doi:10.1109/ICCMC.2019.8819688).

36. Waagsnes H. SCADA Intrusion Detection System Test Framework. Master's thesis. Grimstad: University of Agder, Department of Information and Communication Technology; 2017.

37. Anomalías ADuIbe. A-Detector: un IDS basado en anomalías. [Online].; 2018 [cited 2021 mayo 15. Available from: https://www.hackplayers.com/2018/09/a-detector-ids-basado-en-anomalias.html.

38. Reglas SdDdiyS(Cd. Seguridad y redes. [Online].; 2008 [cited 2021 09. Available from: https://seguridadyredes.wordpress.com/2008/01/22/sistemas-de-deteccion-de-intrusos-y-snort-ii-creacion-de-reglas-i/.

39. Jeimy Cano JDMSP. Inteligencia Artificial aplicada al Análisis Forense Digital: Una revisión preliminar. Cibsi 2020. 2020;: p. 1-9.

40. Koroniotis N. A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. Future Generation Computer Systems. 2020 Sep; 110(https://doi.org/10.1016/j.future.2020.03.042): p. 91-106.

41. Martínez JG. Innovación en Ciberseguridad. Estrategia y Tendencias. Revista Economia Industrial. 2018;(https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/JUAN%20GONZ%C3%81LEZ%20MART%C3%8DNEZ.pdf): p. 1-10.

42. Harold Daniel Morán Amórtegui KHM. Análisis comparativo de plataformas Cloud con soporte orientado a servicios de internet de las cosas. Trabajo de grado de Investigación tecnológica. Bogotá : Universidad Católica de Colombia, Facultad de Ingeniería; 2017.