ISSN: 0123-3033 – ISSN-e: 2027-8284

INGENIERIA Y COMPETITIVIDAD
REVISTA CIENTÍFICA Y TECNOLÓGICA

Vol. 24 No. 2-2022 – DOI: 10.25100/iyc.v24i2.11761

SYSTEMS ENGINEERING

Architecture of an intelligent cybersecurity Framework based on Blockchain technology for IIoT

INGENIERÍA DE SISTEMAS

Arquitectura de un Framework de ciberseguridad inteligente basado en tecnología Blockchain para IIoT

Yeisón Isaac Lucio [1§], Siler Amador Donado[2], Katerine Márceles[1]

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

[2]*Universidad del Cauca. Faculty of Electronic Engineering and Telecommunications, System Engineering Program, Information Technology Research and Development Group (GTI), Popayan -Colombia*

yeison.1266@unimayor.edu.co, samador@unicauca.edu.co, kmarceles@unimayor.edu.co

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

Abstract

For organizations today it is very important to have frameworks that can automate certain processes in a certain way that have additional costs for them, and it is that automation takes great importance when the processes are related to cybersecurity, since it is a critical issue that must be updated with the latest technological developments as new vulnerabilities are found over time. That is because, in this work an architecture of a cybersecurity framework based on emerging technologies is proposed that allows to automate the generation of rules and store the information of alerts generated by possible intrusions in a comprehensive way over time, all this making use of IoT devices that are securely connected and authenticated in a Blockchain that stores the entire list of rules and possible alerts generated by certain intrusions. In this way, the rules will be generated automatically by a Deep learning algorithm that is analyzing the traffic that the IoT device emits to the cloud making use of an intrusion detection systemIDS that is monitoring the traffic that passes through a certain network and saves it in a temporary on the device until it is sent to the cloud. Likewise, the architecture also proposes an application layer of which the users who can manage the IoT devices are part, as well as the configurations for their connection with the Blockchain and in the same way they can manage rules and monitoring of the traffic that is being receiving from the devices involved.

Como citar:
Lucio YI, Donado SA, Márceles K. Arquitectura de un Framework de ciberseguridad inteligente basado en tecnología Blockchain para IIoT. *INGENIERÍA Y COMPETITIVIDAD*, In press 2022; e22411761. https://doi.org/10.25100/iyc.v24i2.11761

***Keywords**: Architecture, Blockchain, Deep learning, Frameworks, Internet of Things.*

Resumen

Para las organizaciones hoy en día es muy importante contar con frameworks que puedan automatizar determinados procesos que repercuten en gastos adicionales para estas mismas y es que la automatización toma mucha importancia cuando los procesos están relacionados con la ciberseguridad, dado que es un tema crítico y que debe estar actualizado con las últimas novedades tecnológicas ya que con el pasar del tiempo van encontrando nuevas vulnerabilidades. Por lo anterior, en este trabajo se propone una arquitectura de un framework ciberseguridad basado en tecnologías emergentes que permita automatizar la generación de reglas y almacenar la información de alertas generadas por posibles intrusiones de forma íntegra a través del tiempo, todo esto haciendo uso de dispositivos IoT que se encuentran conectados y autenticados de forma segura en una Blockchain que almacena todo el listado de reglas y las posibles alertas generadas por determinadas intrusiones. De este modo las reglas serán generadas automáticamente por un algoritmo de Deep learning que se encuentra analizando el tráfico que el dispositivo IoT emite hasta la nube haciendo uso de un IDS que está monitoreando el tráfico que pasa por una determina red y lo guarda de forma temporal en el dispositivo hasta que este es enviado hasta la nube. Así mismo, también la arquitectura propone una capa de aplicación de la cual hacen parte los usuarios que podrán administrar los dispositivos IoT, así como también las configuraciones para su conexión con la Blockchain y de igual forma se podrán gestionar reglas y monitoreo del tráfico que se está recibiendo por parte de los dispositivos involucrados.

***Palabras clave**: Arquitectura, Blockchain, Deep Learning, Frameworks, Internet de las cosas.*

1. Introduction

Currently there are different types of Framework that allow organizations to manage certain cybersecurity processes that are of great importance to their environment. Given that day-to-day organizations make use of new emerging technologies such as the IoT (Internet of Things), the need for tools that can help automate all those tasks that are in a way manual and that require a trained staff to be able to execute them, that is because, in recent years frameworks have had great popularity, since they allow users to concentrate on their business logic and not worry about tasks that a well configured tool can do perfectly [(1)]. On the other hand, another latent vulnerability occurs in the transport of the data collected by IoT devices, which 98% of all traffic they generate is not encrypted, which exposes personal and confidential data on the network. Therefore, attackers who have already established command and control through phishing attacks can eavesdrop on unencrypted network traffic, collect personal or confidential information, and then exploit that data for profit from being on sites like the dark web [(2)]. That is why Blockchain technology takes importance in the development of frameworks since it allows to guarantee the immutability of the information, ensuring thatsaid stored information can be integrated. Likewise, Blockchain offers a decentralized architecture, preventing a single entity from having control over certain information. Consequently, this technology is suitable for a cybersecurity framework since it allows the integrity of the information and security in the transmission of data, guaranteeing its immutability; but in addition, it offers advantages such as improved communication between connected devices, since a consensus can be reached on the information that is stored.

The rest of this paper is organized as follows: Conceptualizations is presented in second section, Related works in third section, Methodology in fourth section, Results and Discussion in fifth section. Finally, some concluding remarks are presented in sixth section.

2. Conceptualizations

In order to give clarity in this section, certain concepts that are important to give context to the issue raised are addressed.

1) Blockchain: This technology is created as a support for transactions with bitcoin, in it all the transactions that are packed in blocks are recorded, which the miners are then in charge of verifying [3]. Since its inception and until today, this technology is used mostly in the field of cryptocurrencies, due to the great popularity that bitcoin has had. However, the chain of blocks (Blockchain) allows those assets to operate making use of decentralized accounting books whose main objective is to keep a record of all the transactions that circulate through the entire network. So that this entire ecosystem works, there are different participants such as miners whose role is fundamental in public Blockchains, because they are in charge of collecting all pending transactions and adding them to the network through the generation of a block. The main objective of Blockchain is to guarantee that the information related to the transactions carried out is kept completely immutable over time, managing to guarantee the integrity of the information, but also by removing intermediaries who in centralized systems have a certain control over the information.

2) Cybersecurity: Is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks [4]. Most electronic devices interact with each other, either directly and indirectly through data networks or through storage devices such as: USB sticks that store and transport information from one device to another, cybersecurity is responsible for protect computer networks from malicious attacks, protect applications from threats, in order to maintain the integrity of business or personal data.

3) IIoT: With the arrival of the Internet of Things, the industry realized that this technology could be used in its operations, for which the Industrial Internet of Things (IIoT) emerged. 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 the progress of business and manufacturing [5]. The IIoT is changing the world of the industry in terms of automation in its manufacturing processes since devices or machines can connect and transfer data with each other, the IIoT seeks the interaction of machines, sensors, people and cloud computing, that can communicate and interact in real time to monitor, control manufacturing processes, to improve productivity and performance of machinery within the industry.

4) Threat: A threat is defined as a potential cause of an unwanted incident, which can cause damage to a system or the organization (6). A threat is any action that takes advantage of a vulnerability to undermine the security of an information system. In other words, it could have a potential with a negative effect on some element of the system.

5) Vulnerability: It can be defined as a weakness of an asset or the absence of a control that can be exploited by one or more threats [6]. It is a weakness or failure in an information system that puts data security at risk, allowing an attacker to compromise its integrity, availability or confidentiality, so it is necessary to find and eliminate them as soon as possible.

6) IDS: (Intrusion Detection System) Intrusion Detection System, can be defined as a device or software application that monitors a network or systems for malicious activity or policy violations [7], 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 anomaly or attack; likewise, it collects information on each anomaly or attack detected.

3. Related Works

Next, the related works that are taken as a reference for the development of this research are presented:

1) Securing IoT Devices with Blockchain and Public Key Infrastructure: In this article [8] a PKI (Public Key Infrastructure) environment is established to authenticate IoT devices in a secure way using the Ethereum Blockchain; In addition, a risk analysis is carried out to identify the improvements obtained in terms of security and for this a risk-based audit methodology is established that allows evaluating the prototypes presented to measure the improvements obtained in terms of security. By virtue of the above, it is important to mention that IoT devices present problems in terms of their default configuration, leaving them vulnerable, with this they seek to improve their authentication system through the implementation and deployment of a public key infrastructure distributed under the technology Blockchain.

2) Collaborative IDS based on Blockchain: This article [9] shows the development of a Blockchain from scratch oriented to operate with IDS. In addition, it teaches the technologies used and the structure of the project. In the same way, the link to the source code of the Blockchain network created is shared.

The previous research work highlights the way in which a Blockchain network is developed from scratch, thought and designed to be integrated with the IDS SNORT, for the work that was developed it was important to take into account these types of considerations, since it allows a detailed understanding of the operation of a Blockchain network at the implementation level and how to make an integration between an IDS and a Blockchain.

*3) Development of a traceability system in IoT environments using Hyperledger:*The project [10] addresses the development of a proof of concept (Proof of Concept -PoC-) to implement Hyperledger-Fabric (HF) in IoT. The objective is the collection of events through sensors located on a Raspberry Pi 3 (RPi) and the inclusion of incidents in the HF BC (Blockchain). Likewise, all the information collected can be consumed in real time through a web system. This article has some interesting qualities such as the development of a Blockchain using Hyperledger technology and its integration with IoT, this is of great importance for this project, because this tool allows to build very complete Blockchains that adapt perfectly to the Blockchain that was implemented.

*4) Intrusion detection system for the internet of things based on blockchain and multi-agent systems:*This investigation [11] focuses on the design, implementation and testing of an intrusion detection system that uses a hybrid location strategy based on a multi-agent system, Blockchain and deep learning algorithms. The system consists of the following modules: data collection, data management, analysis and response. It uses an NSL-KDD data set from the National Security Laboratory. This research contributes to the present project the implementation of the intrusion detection system and its integration with deep learning algorithms, since it allows the operation and integration of these two technologies to be understood in a more explicit way, which is of utmost importance. for the development of the proposed framework.

5) A security framework for IoT authentication and authorization based on blockchain technology: On [12] This work makes use of blockchain technology to solve IoT security problems using 5G network. For this, a multilayer network model for IoT based on blockchain is

proposed, this proposal addresses many of the problems associated with the deployment of blockchain technology by dividing the IoT network into a decentralized multilayer system. Genetic algorithms for evolutionary computation and particle swarm optimization are used; likewise, communication and authentication between the nodes of the network is carried out through blockchain, avoiding the existence of a central authority. This is why hyperledger is used to verify the proposed system.

6) Blockchain-enabled Distributed Security Framework for Next Generation IoT- An Edge-Cloud and Software Defined Network Integrated Approach: OnThis document [13] proposes a blockchain-enabled distributed security framework that uses an edge cloud and asoftware-defined network (SDN). Detection of security attacks is achieved at the cloud layer, and consequently, security attacks are reduced at the edge layer of the IoT network. The Software Defined Network (SDN) Enabled Gateway provides dynamic network traffic and flow management, which aids in the recognition of security attacks by determining rogue network traffic flows and decreases security attacks by obstruction of doubtful flows. The results obtained show that, the contribution of this article is focused on its implementation in the cloud, since the authors take advantage of that technology to integrate in such a way that the blockchain network uses the edge of the cloud to function, it is interesting, because this type of novel implementations turn out to be of very useful for the proposed framework.

4. Methodology

In order to establish the different technologies that make up the cybersecurity framework in IIoT, the action research methodology is used [14], which consists of uniting theory with practice in such a way that the researcher can draw correctconclusions about the practices carried out. For this reason, on this occasion the development of this work was carried out from three phases:

Phase 1: Compilation and analysis of studies that propose cybersecurity frameworks related to emerging technologies.

Initially, a systematic review of the literature was carried out on the technologies that are involved in the framework that was built, this review involved searching databases related to computer science that allowed obtaining articles that addressed the issue raised. In total, 201 articles were obtained that were filtered, identifying how many of these articles were repeated and which were considered more relevant according to their title, abstract and keywords. Taking into account this initial filter, the list of articles was reduced to 67, considering as primary articles those that contain information on related technologies that are important for the construction of the framework.

The construction of a framework involves many technologies that must be taken into account for the systematic review, therefore, starting from the list of primary articles, each one was classified taking into account the technology of which we wanted to investigate in detail. Consequently, as can be seen in Table 1, applying the classification by technology, 22 articles were obtained that propose a certain framework and the rest are technologies that are involved in its construction.

Table 1. *Classification by technology of studies*

Technology	Number
IoT	52
IDS	30
Blockchain	33
AI	28
Framework	22
Cloud	12

Since usually not all articles mention a specific tool, framework or platform, the list of articles is reduced, because the objective is to obtain a list of articles that mention a tool to later perform a classification and thus get a top. For example: in the case of Blockchain technology, the list of articles was reduced to 14 as can be seen in Table 2.

Phase 2: Determine and select the technologies to be used for the development of the proposed framework.

Through this phase, a selection was made of the technologies that were used for the construction of the framework and for this the first thing that was done was to create the selection criteria that are very useful when making a selection, since it allows a weighting of certain technology based on the characteristics, which were proposed according to the needs of the implementation; therefore, in Table 2 it is possible to observe the characteristics proposed for the selection of Blockchain technology, as shown, each characteristic can have certain qualitative values, but as it was necessary to obtain a final weighting to have a notion of which is the technology that could best be adapted to the needs raised.

Table 2 *list of articles that deal about blockchain technologies*

	Year of publication	**Title of the article or study**	**Author (s)**	**Blockchain platform**
1	2018	Securing IoT devices with Blockchain and public key infrastructure	(3)	Ethereum
2	2018	Development of a traceability system in IoT environments using Hyperledger	(9)	Hyperledger
3	2019	Secured Framework for IoT Using Blockchain	(15)	Ethereum
4	2020	Research on distributed blockchain-based privacy-preserving and data security framework in IoT	(11)	Hyperledger
5	2020	A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks	(16)	Ethereum
6	2019	A security framework for IoT authentication and authorization based on blockchain technology	(12)	Hyperledger
7	2019	A Blockchain Based Decentralized Authentication Framework for Resource Constrained IOT devices	(17)	Ethereum
8	2019	A Secure Framework for Communication in Internet of Things Application using Hyperledger based Blockchain	(18)	Hyperledger
9	2018	Intrusion Detector for Blockchain based IoT Networks	(19)	Ethereum
10	2019	Blockseciotnet: Blockchain-based decentralized security architecture for IoT network	(20)	Ethereum
11	2020	Utilizing Blockchain for Distributed Machine Learning based Intrusion Detection in Internet of Things	(21)	Ethereum
12	2020	Unification of Blockchain and Internet of Things (biot) requirements, working model, challenges and future directions	(22)	Ethereum, IOTA, Bitcoin, Hyperledger
13	2020	Bacs A blockchain-based access control scheme in distributed internet of things	(23)	Ethereum
14	2020	Towards building a blockchain framework for IoT	(24)	Ethereum, IOTA, Hyperledger

In Table 2, you can see the essentialcharacteristics for the selection of Blockchaintechnology taking into account the needs of the framework, which in this case these requirementsare more focused on a specific Blockchain technology being able to integrate or operate withIoT devices. Therefore, such technology must offer security, confidentiality of transactions; as well as the consumption of resources and thebandwidth is not so high.

Now, in Table 2 only the criteria for the selection of Blockchain technology were considered; therefore, each technology had selection criteria as can be seen in Table 3, the structure of these criteria was the same and what changed were the characteristics that were specified according to the technology and needs.

***Table 3**. selection criteria for blockchain*

Description:	Characteristic	Qualitative value	Quantitative value
Identify the type of Blockchain	Private	Yes	1
		Not	0
Determine if blockchain technology allows the use of smart contracts	Smart contract	Yes	1
		Not	0
It allows to identify if the technology is open source	Open source	Yes	1
		Not	0
Determines if data on the network is kept confidential	Confidential data	Yes	1
		Not	0
Identify if the technology handles authentication and if the integrity of the information can be guaranteed	Authentication and integrity	Yes	1
		Not	0
Determines if the technology handles key management for network access	Key management	Yes	1
		Not	0
It allows to identify if the technology allows to carry out the identification management of the network participants	Identification management	Yes	1
		Not	0
It allows to identify an approximate time of the latency of confirmation of transactions	Transaction confirmation latency	60s <	1
		> 60s && <= 600s	0.5
		> 600s	0

Table 4, shows the criteria that were taken as a reference to make the selection of an IDS, which is necessary for the construction of the proposed framework, so in this case one of the characteristics that were considered were the modes of operation, customization of rules and the consumption of resources that is of vital importance in this case, since said software will be running on an IoT device, so low resource consumption was the main objective when making the selection of the IDS suitable for the framework.

In accordance with the aforementioned, for each technology certain selection criteria were formed that allowed obtaining a top of the technologies that best adapted to the proposed project, which is why each qualitative value that had a certain characteristic must have had a value quantitative since later, when the weighting was carried out, it would be the one that has the most utility.

***Table 4**. selection criteria for ids open source*

Description	Characteristic	Qualitative value	Quantitative value
Supports and performs signature analysis	Signature analysis	Yes	1
		Not	0
Has HIDS mode of operation	HIDS	Yes	1
		Not	0
Has NIDS mode of operation	NIDS	Yes	1
		Not	0
Supports perform anomaly analysis	Anomaly analysis	Yes	1
		Not	0
It has support for linux	Linux support	Yes	1
		Not	0
Allows you to customize the rules (add, modify, delete, etc.)	Rules customization	Yes	1
		Not	0
It allows to launch tasks in several sub processes	Multi thread	Yes	1
		Not	0
Allows you to improve your performance by adding more GPUs	GPU acceleration	Yes	1
		Not	0
Resource consumption level	Resource consumption	High	0
		Medium	0.5
		Low	1

Phase 3: Prepare architecture taking into account the technologies proposed for its construction.

This phase consisted of assembling all the pieces that will make up the framework, that is, taking each of the proposed technologies and carrying out a thorough investigation of the operation of each one of them, but in a more technical way, since this allows to visualize in a way how it would be integrated with the entire ecosystem that the framework will have and thus be able to define

which will be the appropriate place for each of these technologies.

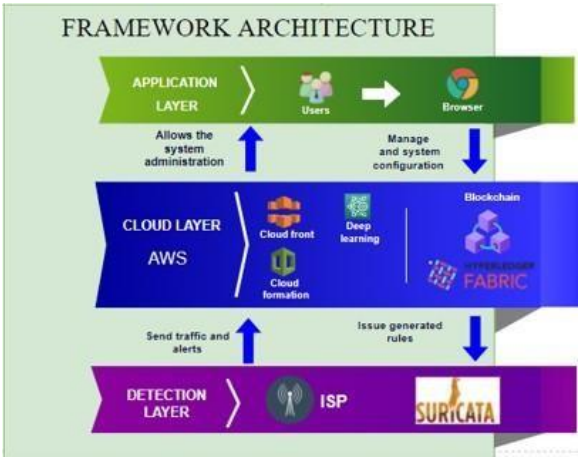

Figure 1. *Framework architecture*

5. Results and Discussion

A. Framework architecture

In Figure 1, you can see the final design of the architecture for the proposed framework, in this case a three-layer architecture was chosen where each layer contains a set of technologies and in turn a certain responsibility.

1) Detection layer: In the detection layer is the IDS that was selected taking into account the criteria mentioned in Table 3, this layer also contains the ISP which is integrated with one of the actors to be highlighted, which is the IDS, who will be census the traffic that is transmitted through said ISP. Therefore, in this layer the traffic will be transmitted to the upper layer, which in this case is the Cloud layer, which is where the heavy work is practically found. This is because this layer is located in the IoT device and to avoid overloading it, this measure is necessary.

2) Cloud layer: This layer contains practically the great part of technologies since the resources in this layer are not limited and therefore it is about obtaining the most benefit, although of course, without overreaching since all the services that are used in this layer have a certain cost that must be assumed, taking into account the above, in this layer a Blockchain is located that is responsible for storing certain information that is necessary to decentralize and maintain in an immutable way over time, on the other hand This layer also contains the Deep learning algorithm that is responsible for analyzing the traffic trying to generate a rule intelligently.

3) Application layer: Finally, this layer refers to the means of access through which users enter and interact with the functionalities offered by the framework, these functionalities are aimed at monitoring malicious network traffic, viewing the list of rules that are stored in the Blockchain , as well as being able to add new ones manually and finally manage the IoT devices.

In this sense, it is important to highlight that each of the layers communicates, in order to transmit certain information that is necessary for the functioning of the framework.

B. Framework functional diagram

To have a clearer idea of how the framework works, it is necessary to understand in a general way what would be the flow that it would have when making use of all the technologies involved, for this in Figure 2, you can see a functional diagram through which it is detailed the general operation, this flow consists of firstly having an IoT device (a Raspberry Pi card) that is monitoring the traffic of a certain network using an IDS, said traffic is temporarily stored in the device and then sent to a database that is hosted in the cloud. This database in turn is the entry point of a Deep learning algorithm (which is also hosted in the cloud).

This brings with it a great advantage since all the devices that are connected to the Blockchain and in turn duly authenticated and identified in it, will

be able to receive this new rule that was automatically generated by the algorithm, that is to say that all the devices will maintain a synchrony in the list of rules that the IDS uses to issue alerts about possible threats.

On the other hand, the Blockchain will also be able to store certain information that is important to maintain immutable traceability over time, such as: the alerts that are generated when a certain IDS rule is activated since some type of intrusion and this is important, since it would give way to subsequently obtaining reports of the number of intrusions detected during a certain period, guaranteeing that the information stored is truthful and that it has not been manipulated.

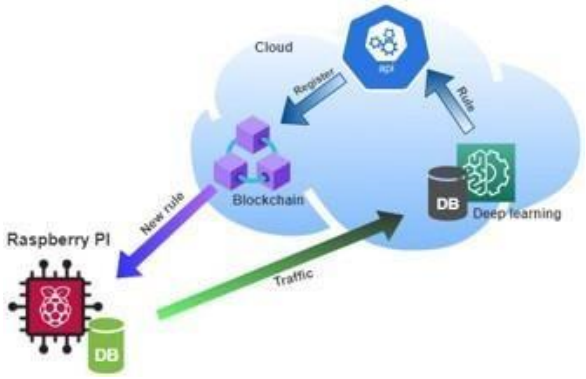

***Figure 2**. Framework functional diagram*

4. Conclusions

In the currently, it is necessary to incorporate technologies that are capable of providing people and organizations with greater security against their confidential data, that is why incorporating technologies such as Blockchain in cybersecurity frameworks for IIoT turns out to be a great alternative since it guarantees the integrity of the information emitted by the devices; in addition, depending on the participation and approach that is given to this technology, it helps to maintain communication between all the nodes of the network, guaranteeing a consensus between them.

One of the main difficulties that can be found when implementing this type of architecture is to choose the Blockchain technology that best suits, since currently there are different types that may seem the most appropriate at first, but when you go to an implementation where it has to be investigated in depth in a technical way, it may turn out that the selected Blockchain ends up not being so appropriate and this can happen due to different factors, perhaps due to integration with other technologies, payment for transactions, confidentiality of information, etc.

For this reason, it is recommended that when selecting a technology a certain top be taken into account, since if the one chosen for having the best score turns out not to be so adequate, you can continue with the second best scored and so on until find the one that best suits the needs of the tool you want to implement.

Another difficulty that exists is the resources of the IoT devices, since these are limited and when working with Blockchain one could think of deploying a certain node in each device, but the reality is that this can overload the device and to avoid that inconvenience it is better to keep the Blockchain in an external place, such as: a cluster distributed in the cloud or it would also be excellent to deploy each node in different clouds, because in the end what is sought with Blockchain is to have a decentralized network, That is why in this case, for the development of the work, it was chosen to maintain the Blockchain in a cluster distributed in the cloud

5. References

(1) Minguez JJ. IDS colaborativo basado en Blockchain. Trbajo de Fin de MásterUniversitario en Seguridad Informática. Logroño: Universidad Internacional de la Rioja, España; 2019.

(2) Palo alto networks. Kublai Khan, Blockchain & The Democratization of Identity. [Online].; 2020 [cited 2021 02 03. Available

from: https://www.sailpoint.com/identity-library/wr-the-democratization-of-identity/.

(3) Balmaseda aranda F. Aseguramiento de dispositivos IoT con blockchain e infraestructura de clave publica. Trabajo de Fin de Master en Seguridad Informática. Logroño: Universidad Internacional de la Rioja, España; 2018.

(4) Kaspersky. ¿Qué es la ciberseguridad? [Online].; 2020 [cited 2021 02 03. Available from: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security.

(5) Navarro BY. Blockchain y sus aplicaciones. [Online].; 2017 [cited 2020 02. Available from: http://jeuazarru.com/wp-content/uploads/2017/11/Blockchain.pdf.

(6) Enrique Javier Santiago JSA. RIESGOS DE CIBERSEGURIDAD EN LAS EMPRESAS. Tecnología y Desarrollo, Revista de ciencia, tecnología y medio ambiente. 2017; 15: p. 3-33.

(7) Sifre JP. IDS de red para detección de ataques sobre SSH y FTP. Máster Universitario en Ciberseguridad - Trabajos Fin de Máster. Alicante: Universidad de Alicante, España; 2020. Report No. http://hdl.handle.net/10045/107579.

(8) Angie Valencia PP. Internet Industrial de las Cosas (IIOT): Nueva Forma de Fabricación. Popayán, Colombia: Fundación Universitaria de Popayán, Facultad de Ingeniería Industrial.

(9) García JI. Desarrollo de un sistema de trazabilidad en entornos IoT mediante Hyperledger. Trabajo fin de master. Madrid:, España; 2018. Report No. http://hdl.handle.net/10486/685363.

(10) Chao Liang BS,SAAKAIMZSKNBI. Intrusion detection system for the internet of things based on blockchain and multi-agent systems. MDPI. 2020 Jul. https://doi.org/10.3390/electronics9071120.

(11) Tian Hongliang XGJWCLHP. Research on distributed blockchain-based privacy-preserving and data security framework in IoT. IET Journals. 2020 Feb. https://doi.org/10.1049/iet-com.2019.0485.

(12) Pajooh HH, Rashid MA. A Security Framework for IoT Authentication and Authorization based on Blockchain Technology. Ieeexplore. 2019 Oct. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00043

(13) Darshan Vishwasrao Medhane AKSMSHJW. Blockchain-enabled Distributed Security Framework for Next Generation IoT: An Edge-Cloud and Software Defined Network Integrated Approach. IeeeXplore. 2020 Feb. https://doi.org/10.1109/JIOT.2020.2977196.

(14) Emilio Berrocal de Luna JEL. El proceso de investigación educativa II: Investigación-acción. Dialnet. 2017; 35-50.

(15) Ali h ANMOHMI. Secured Framework for IoT Using Blockchain. Ieeexplore. 2020 Dec. https://doi.org/10.1109/ICICIS46948.2019.9014853.

(16) Osama Alkadi NMBTKKRC. A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks. Ieeexplore. 2020 May. p. 9463 - 9472.https://doi.org/10.1109/JIOT.2020.2996590.

(17) Soumyashree S. Panda USBKMDJDG. A Blockchain Based Decentralized Authentication. Ieeexplore. 2019 Dec. https://doi.org/10.1109/ICCCNT45670.2019.8944637.

(18) Utkalika Satapathy BKMSSPSSDJ. A Secure Framework for Communication inInternet of Things Application using Hyperledger based Blockchain. Ieeexplore. 2019 Dec.

https://doi.org/10.1109/ICCCNT45670.2019.8944811.

(19) Gunasekaran Raja AGGAG. Intrusion Detector for Blockchain based IoT Networks. Ieeexplore. 2018 Dec. https://doi.org/10.1109/ICoAC44903.2018.8939074.

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

(21) Muhammad Asaad Cheema HKQCCML. Utilizing Blockchain for Distributed Machine Learning based Intrusion Detection in Internet of Things. Ieeexplore. 2020 Sep. https://doi.org/10.1109/DCOSS49796.2020.00074.

(22) Bharat Bhushan CSPSAK. Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. Wireless Networks - Springer Link. 2020; 27: p. 55–90.

(23) Na Shi Liang Tan CYCHJXYLHX.BacS: A blockchain-based access control scheme in distributed. Peer-to-Peer Networking and Applications volume -Springer Link. 2020; 14: p. 2585–2599.

(24) Deepa Pavithran KSJNAKAG. Towards building a blockchain framework for IoT. Cluster Computing -Springer Link. 2020;(23): p. 2089–2103.