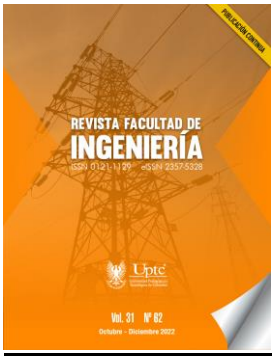
Revista Facultad de Ingeniería
ISSN: 0121-1129
ISSN: 2357-5328
Universidad Pedagógica y Tecnológica de Colombia

Llanten-Lucio, Yeison-Isaac; Amador-Donado, Siler; Márceles-Villalba, Katerine
Validation of Cybersecurity Framework for Threat Mitigation
Revista Facultad de Ingeniería, vol. 31, no. 62, e200, 2022, October-December
Universidad Pedagógica y Tecnológica de Colombia

DOI: https://doi.org/10.19053/01211129.v31.n62.2022.14840

Available in: https://www.redalyc.org/articulo.oa?id=413974254001

Revista Facultad de Ingeniería
Journal Homepage:
https://revistas.uptc.edu.co/index.php/ingenieria



Validation of Cybersecurity Framework for Threat Mitigation

Yeison-Isaac Llanten-Lucio[1]
Siler Amador-Donado[2]
Katerine Márceles-Villalba[3]

Received: June 18, 2022 **Accepted:** September 22, 2022 **Published:** October 02, 2022

Citation: Y.-I. Llanten-Lucio, S. Amador-Donado, K. Márceles-Villalba, "Validation of Cybersecurity Framework for Threat Mitigation", *Revista Facultad de Ingeniería*, vol. 31 (62), e14840, 2022. https://doi.org/10.19053/01211129.v31.n62.2022.14840

Abstract

Currently on the Internet there are many threats that threaten the security of the information of users who daily access this network using different devices that connect from their homes or organizations that in many cases do not have security controls enough and end up exposing themselves to all those threats that grow over time. That is why this article aims to propose the validation of a cybersecurity framework that allows mitigating and reducing risks to increase security levels

[1] Institución Universitaria Colegio Mayor del Cauca (Popayán-Cauca, Colombia). yeison.1266@unimayor.edu.co. ORCID: 0000-0003-1021-2392
[2] M. Sc. Universidad del Cauca (Popayán-Cauca, Colombia). samador@unicauca.edu.co. ORCID: 0000-0002-4571-8273
[3] M. Sc. Institución Universitaria Colegio Mayor del Cauca (Popayán-Cauca, Colombia). kmarceles@unimayor.edu.co. ORCID: 0000-0002-4571-0714

through the implementation of controls for homes and organizations using emerging technologies such as: IoT, Blockchain and Deep Learning. The foregoing was carried out with the methodological approach of action research starting from the improvement of the process in search of transformation, thus obtaining as results the integration of the aforementioned methodologies for the detection of possible malicious hosts within an internal network through an intelligent analysis of the traffic that passes through the same network in order to intelligently generate rules in intrusion detection systems (IDS) in an automated way and that these rules can in turn be distributed through a secure channel using the Blockchain technology, to finally guarantee the integrity of said rules and that also allows maintaining the immutability and synchronization of the same information with all the devices connected to the framework.

Keywords: blockchain; cybersecurity; framework; risks; threats; validation.

Validación de framework de ciberseguridad para la mitigación de amenazas

Resumen

Actualmente en internet se encuentran muchas amenazas que atentan a la seguridad de la información de los usuarios que diariamente acceden a esta red haciendo uso de diferentes dispositivos que se conectan desde sus hogares u organizaciones que en gran cantidad de casos no cuentan con los controles de seguridad suficientes y terminan exponiéndose a todas esas amenazas que crecen con el pasar del tiempo. Es por ello que en este artículo tiene como objetivo proponer la validación de un framework de ciberseguridad que permita mitigar y disminuir los riesgos para aumentar los niveles de seguridad a través de la implementación de controles para los hogares y organizaciones haciendo uso de tecnologías emergentes como: IoT, Blockchain y Deep Learning. Lo anterior, se llevó a cabo con el enfoque metodológico de investigación acción partiendo desde el mejoramiento de proceso en busca de transformación, obteniendo de esa manera como resultados la integración de las metodologías antes mencionadas para detección de posibles host maliciosos dentro de una red interna mediante un análisis inteligente del tráfico que transita por la misma red con el fin de generar de manera inteligente

reglas en sistemas de detectores de intrusos (IDS) de forma automatizada y que a su vez estas reglas se puedan distribuirse por un canal seguro haciendo uso de la tecnología Blockchain, para finalmente garantizar la integridad de dichas reglas y que además permita mantener la inmutabilidad y la sincronización de la misma información con todos los dispositivos conectados al framework.

Palabras clave: amenazas; blockchain; ciberseguridad; framework; riesgos; validación.

Validação da estrutura de segurança cibernética para mitigação de ameaças

Resumo

Atualmente na Internet existem muitas ameaças que ameaçam a segurança das informações dos usuários que diariamente acessam essa rede utilizando diferentes dispositivos que se conectam de suas residências ou organizações que em muitos casos não possuem controles de segurança. aquelas ameaças que crescem ao longo do tempo. É por isso que este artigo tem como objetivo propor a validação de um framework de cibersegurança que permita mitigar e reduzir riscos para aumentar os níveis de segurança por meio da implementação de controles para residências e organizações usando tecnologias emergentes como: IoT, Blockchain e Deep Learning. O exposto foi realizado com a abordagem metodológica da pesquisa-ação a partir do aprimoramento do processo em busca de transformação, obtendo como resultado a integração das metodologias mencionadas para a detecção de possíveis hosts maliciosos dentro de uma rede interna por meio de uma análise inteligente de o tráfego que passa pela mesma rede para gerar de forma inteligente regras em sistemas de detecção de intrusão (IDS) de forma automatizada e que essas regras possam por sua vez ser distribuídas através de um canal seguro usando a tecnologia Blockchain, para finalmente garantir a integridade do referido regras e que também permite manter a imutabilidade e sincronização da mesma informação com todos os dispositivos conectados ao framework.

Palavras-chave: ameaças; blockchain; cíber segurança; estrutura; riscos; validação.

I. INTRODUCTION

Cybersecurity is gaining strength today, with the passage of time the number of devices connected to the Internet increases and therefore more and more people have devices to access the Internet from their homes or work. According to [1] it is expected that by the year 2023 there will be more than 29.3 billion devices connected to the internet and although this is great news it also poses a great risk for people, given that when a device connects to the internet it is exposed to a large number of cybersecurity threats, such as: denial of service attacks, brute force attacks, all kinds of malware (botnets, ransomware, Trojans, among others). In turn, these threats mean that people may lose sensitive information or, in extreme cases, lose control over their device, and despite the fact that there are currently intrusion detection systems (IDS) that seek to mitigate these threats, they are limited. Due to the difficulty in defining rules for all attack patterns, in addition to the fact that these types of systems are designed for administrators with knowledge of networks and cybersecurity. That is why the developed framework aims to increase these levels of cybersecurity by detecting possible malicious hosts within a given network by analyzing the traffic and intelligently building rules from it, but also distributing these rules to all the devices that are connected. In that order of ideas, to achieve all of the above operations, use was made of emerging technologies such as blockchain, IoT and Deep Learning, which made it possible to grant all the advantages they offer and provided important characteristics to cybersecurity.

Taking into account the above, for the development of the framework the research-action methodology was used, which allowed an identification of the needs in order to define a development plan to be carried out, in turn this methodology also allowed a reflection about the results that were obtained in order to determine if the result was the expected one or if a new iteration was required. Below are some conceptualizations related to the research in order to have a better understanding of the topic addressed: Cybersecurity is the action of defending computer equipment, mobile devices, electronic systems, networks and data against malicious attacks that affect integrity, availability and confidentiality [2]. Blockchain technology appears as a means for cryptocurrency transactions. Blockchain is a record of all transactions

that are condensed into blocks, which are then validated by miners. On the other hand, a virtual currency that is not properly issued by a financial or government entity, it is difficult to guarantee the integrity and fidelity to carry out a transaction. The cybersecurity framework (Cybersecurity Framework) refers to a defined set of policies and procedures issued by the main cybersecurity organizations [3], cybersecurity frameworks are built and documented to improve cybersecurity strategies in an organization or company. An Intrusion Detection System (IDS) can be defined as a device or software application that monitors a network or systems for malicious activity or policy violations [4], the intrusion detection system is constantly analyzing traffic, it has the ability to identify anomalies or violations based on patterns and heuristics. At present, artificial intelligence has taken a great boom, it is being applied in many fields of computing, one of its fundamental components is Deep Learning. Deep Learning can be defined as a class of Machine Learning algorithms [4]. With the arrival of the internet of things, the industry realized that this technology could be used in its operations, for which the IIoT emerged, which refers to the close integration of computing, networks and physical objects for the industry, in which devices Embedded devices are networked to sense, monitor, and control the physical world to advance business and manufacturing [5]. According to [6] lambda is an AWS service that is responsible for executing code without provisioning or managing servers. Lambda powers the code in a highly available compute infrastructure and is responsible for performing all compute resource management tasks, including server and operating system maintenance, capacity provisioning and autoscaling, and monitoring. Hyperledger-Fabric is an open source platform that allows you to configure custom Blockchain networks and that can be used in many ways, in [7] it is defined as an organization-level distributed accounting platform that offers modularity and versatility for a wide set of industry use cases. Amazon SQS (Servicio Cola de mensajes) is a service that provides benefits to distributed systems by allowing microservices to be decoupled and scaled[8]. Amazon amplify is an AWS service that enables developers to quickly and easily build infrastructure, with the flexibility to take advantage of the breadth of AWS services as use cases change by leaps and bounds[9].

In the same order of ideas, it is important to highlight the investigations that were taken as references for the development of this work, among them are the following: In this study [10], the authors first introduce the three-tier architecture of IoT and discuss the corresponding security issues of each layer, then discuss the compatibility between IoT and Blockchain. Second, they propose a new IoT Blockchain-based distributed security architecture, which relies on perception layer gateway nodes to protect data storage and exchange and uses middleware servers to analyze and process data for the present work.

This research [11], involves the design of a novel intrusion detection system and the implementation and evaluation of its analysis model. This article provides the fundamental bases for the implementation of a neural network; likewise, it provides concepts that must be taken into account when building a neural network. On the other hand, it is also very helpful that this article is focused on instruction detection together with IoT, since they are technologies that the proposed framework intends to integrate.

In this article [12], a new framework model and a hybrid algorithm are proposed to solve the problem of how to select an effective Machine Learning algorithm when there are several Machine Learning algorithms for cyber-attack detection for IoT security systems. The learning algorithm is selected for the identification of malicious traffic and anomalies and the broader ML (Machine Learning) algorithm performance evaluation metrics are also selected.

In this paper [13], In particular, spectral partitioning is proposed to divide the IoT network into autonomous systems (AS) that allow traffic monitoring for intrusion detection (ID) by selected AS border area nodes in a distributed manner. The contribution to this project is the specification of vulnerabilities presented and the use of Blockchain in IoT technologies, the way of training the Machine Learning algorithm can also be taken into account.

This document has three notable contributions [14]. First, a secure, efficient, reliable and sustainable algorithm powered by Blockchain is proposed. Second, an analytical hierarchy process (AHP)-based intelligent decision-making approach to secure, concurrent, interoperable, sustainable, and trustworthy blockchain. This article

proposes an AHP based solution to help industry experts and how to select the most relevant and critical parameters like (online reliability with packet loss rate), (convergence in mapping with delay) and (interoperability in association with performance) to improve product performance. In the industry.

However, it is necessary to highlight that each of the related works contributed in terms of the construction and validation of the framework since the aspects that contributed to its structuring were taken up, which can be evidenced during the methodological development.

II. METHODOLOGY

As mentioned above, in this work the action-research methodology is used, therefore, for the development of this methodology, a separation was made by phases for the development of the project, in each of these phases the selected methodology, as can be seen below, four phases were obtained which together make up the entire project carried out:

A. Phase 1: Framework Architecture

It includes the planning and design of the architecture of the framework, therefore, in this phase all the platforms and tools that are intended to be used in the development are involved and that is why before preferring a certain platform or tool, a review was carried out systematic analysis that included the analysis of 201 articles collected in different academic databases that allowed choosing the technologies and tools that best suited the needs of the framework.

Taking into account the above, the defined architecture is shown, which consists of three layers specified below.

- **Application layer:** This layer comprises all the user interaction with the framework and the means by which users can interact, which in this case is through the browser that allows access to a graphical interface to administer and manage the framework configuration.

- **Cloud layer AWS (cloud storage layer with AWS):** In this layer all the information processing is carried out, all the traffic is stored and all the source code of the framework is housed.
- **Detection layer:** In this layer are the nodes that are in charge of capturing all the traffic using tools such as meerkat and then sending the captured traffic to the cloud layer where the collected data is expected to be processed. In turn, the nodes are recording rules stored in the Blockchain that are previously generated and registered by an intelligent algorithm that is in charge of generating said rules based on the traffic that was previously issued.

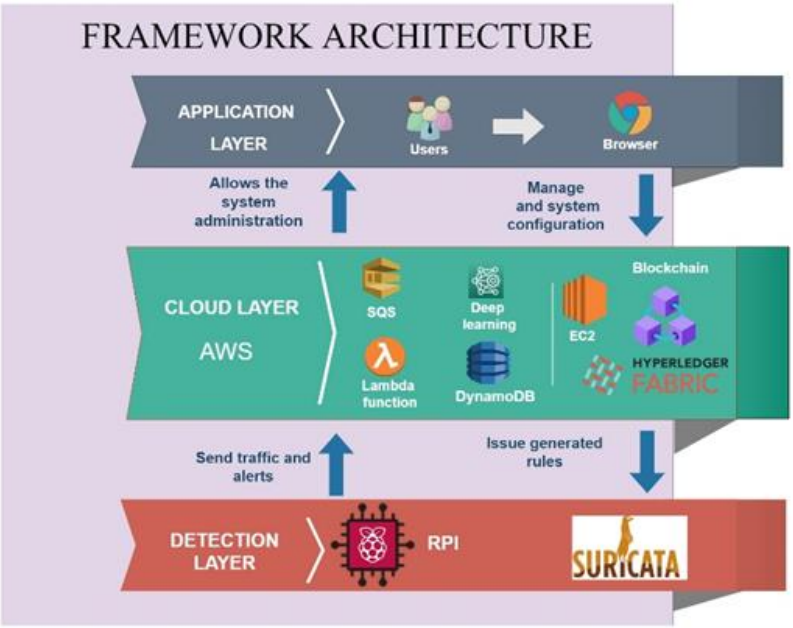


Fig. 1. Framework architecture

In the architecture, the tools and platforms that were used can be observed graphically, as well as the interaction between the layers that make it up. However, to have greater clarity on how all the integrated parts of the framework are working, the functional diagram in Figure 2 was defined. This diagram shows how all these parts interact, starting from the IoT device, which is in charge of collecting all the data. traffic and send it to the cloud where there is a lambda in charge of debugging

the traffic so that later messages are put in an SQS from which an EC2 instance will be capturing the messages, which is where the Deep Learning algorithm is located.

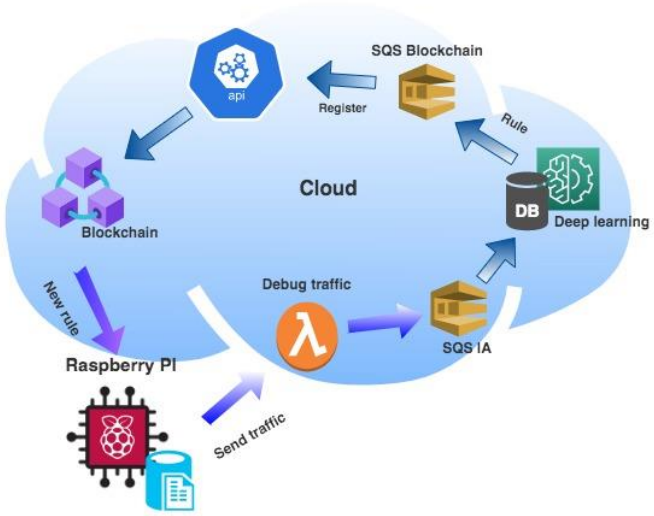


Fig. 2. Functional diagram

It is this algorithm that analyzes traffic for anomalies to intelligently generate rules that will later be used by the IDS configured on IoT devices, but before the device can use the rules generated by the algorithm. Then continuing with the functional diagram after the rules are generated by the algorithm they are sent to another SQS from which an API will be reading that is responsible for registering each of the rules in the Blockchain so that later the registered rule is distributed to all devices that are connected to the framework. Finally, the rule will be synchronized with the rules that the IoT device has so that the IDS takes them into account when analyzing but before the device can use the rules generated by the algorithm. Then continuing with the functional diagram after the rules are generated by the algorithm they are sent to another SQS from which an API will be reading that is responsible for registering each of the rules in the Blockchain so that later the registered rule is distributed to all devices that are connected to the framework. Finally, the rule will be synchronized with the rules that the IoT device has so that the IDS takes them into account when analyzing but before the device can use the rules generated by the algorithm. Then continuing with the functional diagram after the rules are generated by the algorithm

they are sent to another SQS from which an API will be reading that is responsible for registering each of the rules in the Blockchain so that later the registered rule is distributed to all devices that are connected to the framework. Finally, the rule will be synchronized with the rules that the IoT device has so that the IDS takes them into account when analyzing then continuing with the functional diagram after the rules are generated by the algorithm they are sent to another SQS from which an API will be reading that is responsible for registering each of the rules in the Blockchain so that later the registered rule is distributed to all devices that are connected to the framework. Finally, the rule will be synchronized with the rules that the IoT device has so that the IDS takes them into account when analyzing Then continuing with the functional diagram after the rules are generated by the algorithm they are sent to another SQS from which an API will be reading that is responsible for registering each of the rules in the Blockchain so that later the registered rule is distributed to all devices that are connected to the framework. Finally, the rule will be synchronized with the rules that the IoT device has so that the IDS takes them into account when analyzing traffic and thus be able to trigger alerts based on the new rule. Figure 3 shows the flowchart of the framework in which some sections that could not be perceived in the functional diagram can be analyzed in detail, as is the case of the web client that is in the application layer and what happens when traffic is not considered a threat.

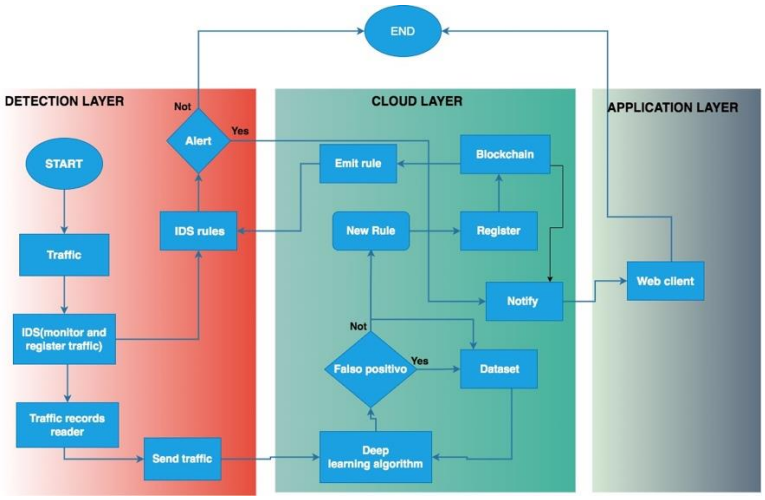


Fig. 3. Flowchart

According to the above, it can be seen that the architecture is not enough to have the full context of the framework's operation and that is why the other diagrams allow greater clarity of how all the selected platforms and tools are orchestrated.

B. Phase 2: Deployment of the Selected Blockchain Technology Adapted to the Business Model

In this phase, the deployment of the Blockchain network configured in accordance with the business model of the framework is carried out, this business model is made up of organizations that make up a consortium and that agree to share information among all the participants of said consortium, therefore, the participation of new members must be approved by all the members that make up said consortium. In this way, it is understood that the Blockchain network is a network based on privileges where anyone who does not have the necessary permissions will not be able to enter. Having the above clear, figure 4 shows the architecture of the Blockchain network defined for this framework and that according to Hyperledger-Fabric is made up of organizations and each organization has different components that are described below:

- **Organization (ORG):** Organizations are a fundamental part of a Hyperledger network, they are practically the participants in the network and it is considered that there is decentralization in a network as long as it is made up of several organizations[15].
- **Peers (P):** The peers or nodes are the anchor points for the applications that want to interact with the Blockchain network. These peers contain the smart contracts and ledgers used to encapsulate shared processes and shared information on a network, respectively[15].
- **Certification Authority (CA):** Since there can be many participants in a Blockchain network, they must be fully identified to have confidence in the transactions that can be carried out[15].
- **Ledger(L):** In Hyperledger, the concept of a ledger is used in which factual information about the state of the entire Blockchain is stored[15].

- **Orders (O):** The computers are configured nodes that are in charge of receiving batches of transactions that are ordered and packaged in blocks[15].
- **Application Client (A):** As its name indicates, this component refers to the applications that connect through a peer to the Blockchain network to send transactions and in turn consult information that is stored in the Blockchain.
- **Channels (C):** In Hyperledger, a channel is a communication mechanism that is used to communicate between the members of the consortium.
- **Smart Contracts (S):** Smart contracts define executable logic that generates new facts that are added to the ledger, thus a smart contract defines the rules between different organizations in executable code [15].

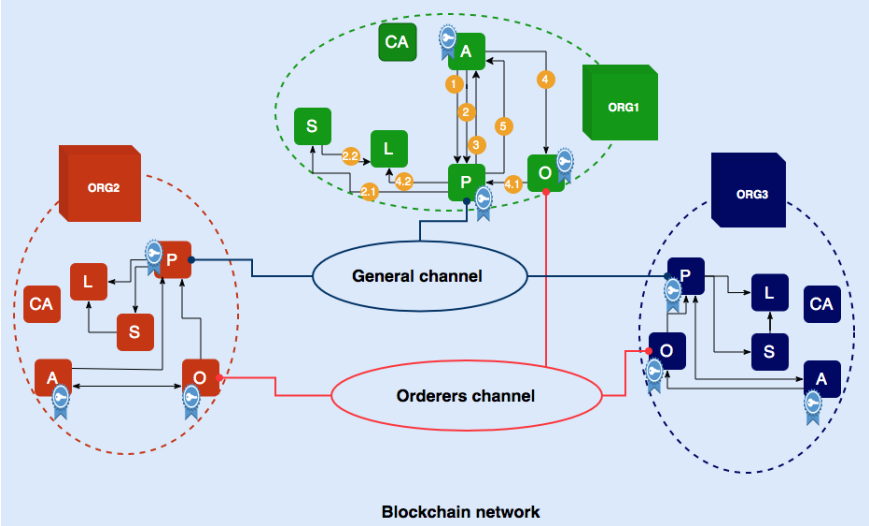


Fig. 4. Blockchain architecture

Now, having each component in figure 4 clear, it can be seen that this architecture is made up of three organizations and each organization is made up of other components that are connected and in turn all the organizations are communicating through a general channel, the which communicates to each peer of a certain organization and channel for the ordering nodes. In addition, it should also be noted that the components denoted as **P, O** and **A** have certificates that identify them as a component authorized to interact on the network. On the other hand, it can also be noted that these components communicate to validate transactions and thus be able

to store the asset, which in this case are the IDS rules. This communication is more noticeable in organization one (ORG1), for greater clarity each numbering is described below.

1. Initial connection with the peer.
2. It invokes the smart contract with a purpose.

2.1. The peer invokes the smart contract.

2.2. Through the smart contract, a query, update or insertion request is made.

3. The client is answered, if it is only a request for consultation, the process ends.
4. The application makes a request for the transaction to be ordered.

4.1. Transactions are sent in a block to the peer.

4.2. The peer updates the Ledger with the block of transactions.

5. An update event is responded back to the client.

Continuing with the architecture of the Blockchain network defined in figure 4, its implementation is carried out, for which different tools are used such as: peer, fabric-ca, configtxgen, configtxlator, etc. These tools are nothing more than binaries that are provided by Hyperledger-Fabric and that, after being installed on a machine, work from the command console, but given that there can be many commands that must be executed, it is preferred to handle yaml files in which you can better specify the required configuration[16]. Containers are light and lightweight so they don't consume many resources of the machine on which they are running. Therefore, for all container management, the Docker tool is used, which allows easy manipulation of containers, as well as many images defined by the community. Taking into account the above, Hyperledger already has some defined images with the necessary tools to configure a Blockchain network. Finally, as indicated above, one of the advantages of using containers is that deployment is facilitated since the containers always run identically in other environments, therefore, for the deployment of this network in the cloud, use was made of the EC2 service provided by AWS to create an instance and thus be able to deploy this Blockchain network in the cloud so that it can be used by the other components of the framework.

C. Phase 3: Construction of a Web Client to Manage the Nodes of Your Network and its Configuration

This phase consisted of implementing a web client that would allow the users and administrators of the organizations to interact with the framework so that the administrators could manage companies, rules, alerts, devices and could access a dashboard to observe important information. on the collected traffic. Taking into account the above, to build a web client it is necessary to have a backend that consumes the information that in this case is stored in DynamoDB and as can be seen in figure 5, the Backend was implemented using lambda functions under an environment execution as NodeJS.

On the other hand, there is the web client which was implemented using the vue.js framework and the AWS CloudFront service to reduce the load time of the web client for users when accessed from a certain location. Then, as you can see, the web client accesses certain Backend services that in turn consume a database that is where the configuration of the devices and the traffic they capture are stored.

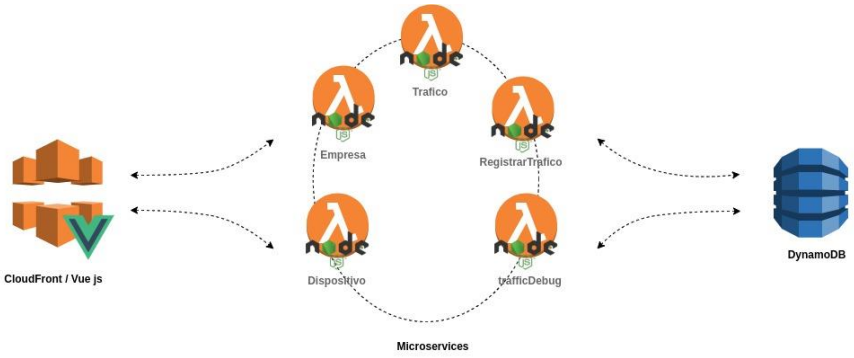


Fig. 5. Web client architecture

As mentioned above, the Backend of the framework is made up of services that have a certain responsibility, therefore, each of the services is described below.

- **Enterprise or Organization:** This service is in charge of managing the organizations.

- **Traffic:** This service is responsible for obtaining the traffic stored in the database, allowing filters to be carried out based on certain criteria.
- **Register traffic:** It is intended to record all the traffic that is emitted from IoT devices.
- **Device**: Allows the management of IoT devices using the IoT core service provided by AWS.
- **Traffic Debug:** It purges the incoming traffic from the devices to send it to the algorithm in an orderly way and thus prevent the algorithm from performing this task.

Subsequently, the definition of the components that make up the framework proceeded with the implementation and for this the AWS Amplify framework was used, which allowed the infrastructure to be defined quickly, making it possible to focus more on the business logic and not to worry a bit about this section, since if it had not had this tool it would have delayed development.

According to the above, the web client was implemented and two user profiles were defined, the first is the administrator user who is in charge of managing the companies and rules that the framework has. When an organization is created, a normal user is created who will be able to access a dashboard view as shown in figure 6, this dashboard shows information about the traffic collected by the devices, such as the packets captured and the alerts issued for the same.

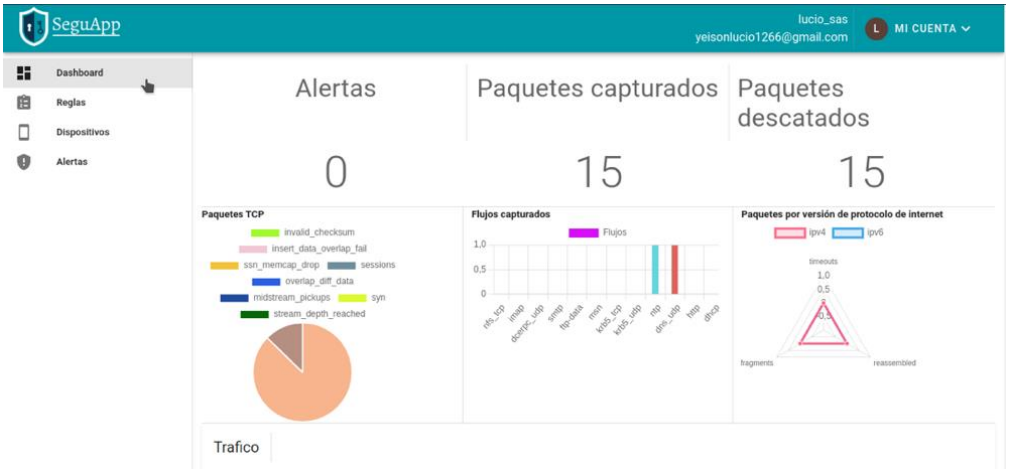


Fig. 6. Dashboard for normal user profile

The normal user also has access to the list of rules that the framework contains, but the difference is that this profile will only be able to view said list, unlike the administrator user who will be able to make changes to the rules and add others manually. Now, this user is the one who will be able to add devices that will be in charge of capturing the traffic in the internal networks where they connect, having said that for the devices, a configuration related mainly to the certificates that allow connecting to both the Blockchain network and the to the AWS IoT Core service.

As mentioned above, the user profile can only view the rules contained in the framework, as shown in figure 7, the rules can be generated automatically by the algorithm, but they can also be entered manually by an administrator user. . It should be noted that these rules obtained directly from the Blockchain network and in case of registering a manual rule, it will be registered in the Blockchain network in the same way, it is for this reason that in figure 9 the type of generation can be perceived.

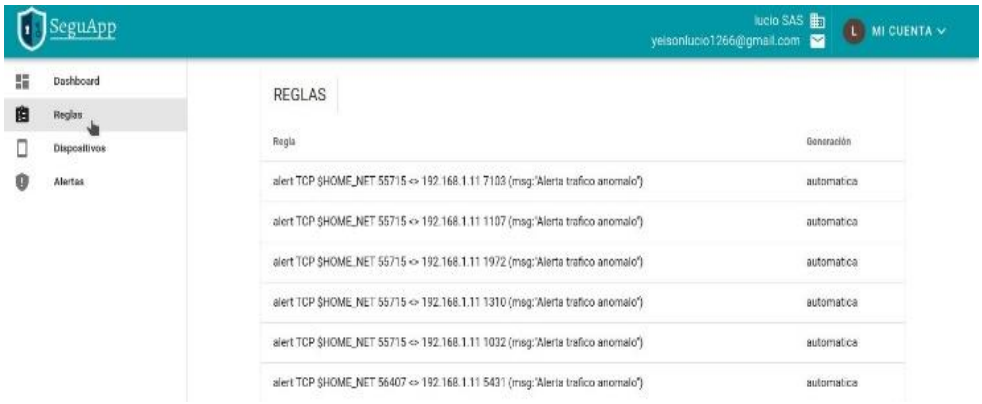


Fig. 7. List of rules for the user profile

D. Phase 4: Evaluation of the Functioning of the Proposed Framework Against Cyberattacks on Internal Networks

This phase includes the evaluation of the proposed framework where three scenarios were set that test the functioning of the framework against the following three types of attacks.

1. **DDOS**: According to [17] this type of attack consists of interrupting the normal traffic of a server or service by making a large number of requests in a short time, making that server or service stop working.

2. **ARP poisoning**: [18] Indicates that a type of attack that allows infiltrating a network to sniff the packets that pass through the network allowing the attacker to obtain sensitive information from the victim.
3. **Backdoor**: In [19] it is mentioned that it is a type of malware that is used to gain unauthorized access, mainly cybercriminals spread malware through unsecured entry points (backdoors) and makes its way to sensitive data.

For each of the attacks, an environment was structured where the framework was tested against each of the attacks. This environment is implemented in a virtualized private network where there is an attacking machine and a victim machine. Likewise, there is also a raspberry pi that connects to the network to be able to capture the network flow and be able to send it to the framework for analysis. Taking the above into account, Figure 8 shows the network architecture where the attack scenarios were set up.

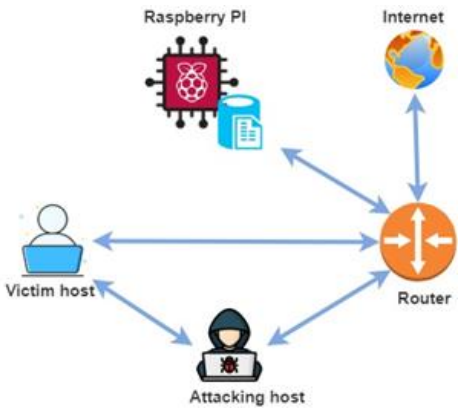


Fig. 8. Network architecture for framework evaluation

Each of the attacks was executed in a controlled way in the proposed environment to determine if the framework works against the attacks carried out, that is why Table 1 shows the result for each of the attacks, this table contains the following columns described below:

- **Attack:** It is the name of the attack.
- **Process:** Result of the execution of the attack.
- **Detected:** This column refers to the result of whether the framework detected the attack.

- **Execution time:** Time it took to execute the attack.

Table 1. Attacks carried out for framework evaluation.

Attack	Process	Detected	Execution time
DDOS	Successful	Yes	3 minutes
ARP poisoning	Successful	Yes	8 minutes
back door	Successful	Yes	5 minutes

III. Results and Discussions

Taking into account phase 1, an architecture was defined and implemented that integrates the tools and platforms that were selected from a systematic review in the main academic databases. Phase 2 allowed to form an architecture for the Blockchain network, which after being defined and analyzed was built using the Hyperledger-Fabric platform using all its advantages and characteristics regarding information security for the needs of the framework. they are of the utmost importance. In phase 3, a web client was built that allows users to make use of the framework, in this way users will be able to access different sections and view the analyzed traffic, see the generated rules, connect new devices and review the alerts that were created. for each device. Finally, in phase 4 an evaluation of the operation was carried out, the main idea of this evaluation was to be able to compare if the framework really managed to identify certain attacks and in turn validate the operation of the integration of all the technologies used. Therefore, for this evaluation, 3 types of attacks were proposed that were replicated in a controlled environment and that the framework successfully identified.

IV. Conclusions

The use of AWS was of the utmost importance for the development of this framework, by virtue of the fact that multiple services were integrated that contribute in large part to the operation of the framework and although the use of these services must be paid according to the consumption for the use. of applications that are in a development phase and that are relatively small do not imply a great expense and this is due to two important factors, the first is that when you create an account for the first time you have a free tier with the duration of a year, which is very beneficial

for experimentation. The other factor is that some of the services have a free layer up to a certain limit and small applications usually do not consume as much and even more when they are in the development phase.

Since this project uses IoT, one of the biggest drawbacks when working with IoT devices are the hardware resources and in the development of this framework this limitation was very important, because the traffic that is captured must be stored in the Raspberry Pi. 3 using the Raspbian operating system. Since this resource is limited, this traffic had to be stored temporarily while it was sent to the cloud and later deleted to free up said space and not saturate the device. On the other hand, the resources consumed by the tools used must also be taken into account, in this case suricata was used, which is a software that usually runs on systems where there are no hardware limitations so that it can be make the most of it. However,

the initial configuration of a Blockchain network was not at all simple and, being a relatively new technology, there is not enough documentation, however, for the development of this framework, Hyperledger-Fabric was used, which facilitates the configuration in a certain way of an initial network. Another point to consider is the deployment, since the nodes of the network must be deployed in separate infrastructure since in this way availability is guaranteed in case some of the peers for some reason cannot work and in addition to that, referring to the infrastructure, it must be taken into account that the Hardware resources are always high, so when deployment is required, an infrastructure robust enough to support the execution of a node must be acquired. In this specific case, an AWS instance was used to launch all the components that make up the network using docker, in other words, each component was deployed in a container within the same instance. In this same sense, it was important to validate the framework with regard to the integration of each of its components through the configuration of three proposed scenarios, where it was possible to successfully demonstrate its operation through the recognition of attacks denial of services, ARP poisoning and backdoor, being detected and automatically generating the respective rule.

AUTHORS' CONTRIBUTION

Yeison-Isaac Llanten-Lucio: Investigation, Methodology, Writing-review and editing.

Siler Amador-Donado: Investigation, Methodology, Writing-review and editing.

Katerine Márceles-Villalba: Investigation, Methodology, Writing-review and editing.

ACKNOWLEDGMENT

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

REFERENCES

[1] D. Corral Henández, "5G, una carrera por la hegemonía y el futuro con muchos beneficios," *Documento Marco del Instituto Español de estudios estratégicos*, pp. 734–759, 2020.

[2] J. M. Aguilar Antonio, "La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas," *Revista de Estudios en Seguridad Internacional*, vol. 6, no. 2, pp. 17–43, 2020. https://doi.org/10.18847/1.12.2

[3] S. Amador Donado, Y. I. Llante Lucio, K. Márceles Villlalba, "Arquitectura de un Framework de ciberseguridad inteligente basado en tecnología Blockchain para IoT," *Revista Ingeniería y Competitividad*, vol. 24, no. 2, pp. 1–13, 2022. https://doi.org/10.25100/iyc.v24i2.11761

[4] J. Pérez Sifre, "IDS de red para la detección de ataques sobre SSH y FTP," Masther Thesis, Universidad de Alicante, Spain, 2020.

[5] A. Valencia, P. Portilla, "Internet Industrial de las Cosas (IIOT): Nueva Forma de Fabricación Inteligente," Grade Thesis, Fundación Universitaria de Popayán, Colombia, 2019.

[6] N. Duminil, *AWS Lambda - Développez des micro-services en Java sur la plateforme serverless d'Amazon*, 2016. https://static.fnac-static.com/multimedia/editorial/pdf/9782409028359.pdf

[7] Hyperledger, *Hyperledger Fabric*, 2022. https://www.hyperledger.org/wp-content/uploads/2020/03/hyperledger_fabric_whitepaper.pdf

[8] J. P. Buddha, R. Beesetty, *The Definitive Guide to AWS Application Integration*, Berkeley, CA: Apress, 2019. https://doi.org/10.1007/978-1-4842-5401-1

[9] K. Raj Neupane, "Serverless full-stack web application development guidelines with AWS Amplify framework," Grade Thesis, Haaga-Helia University of Applied Sciences, Finlande, 2022.

[10] H. Tian, X. Ge, J. Wang, C. Li, H. Pan, "Research on distributed blockchain-based privacy-preserving and data security framework in IoT," *IET Communications*, vol. 14, no. 13, pp. 2038–2047, 2020. https://doi.org/10.1049/iet-com.2019.0485

[11] C. Liang *et al*., "Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems," *Electronics*, vol. 9, no. 7, e1120, 2020. https://doi.org/10.3390/electronics9071120

[12] M. Shafiq, Z. Tian, Y. Sun, X. Du, M. Guizani, "Selection of effective Machine Learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433-442, 2020.

[13] M. A. Cheema, H. K. Qureshi, C. Chrysostomou, M. Lestas, "Utilizing Blockchain for Distributed Machine Learning based Intrusion Detection in Internet of Things," in *16th International Conference on Distributed Computing in Sensor Systems*, 2020.

[14] H. Sodhro, S. Pirbhulal, M. Muzammal, L. Zongwei, "Towards Blockchain-Enabled Security Technique for Industrial Internet of Things Based Decentralized Applications," *Journal of Grid Computing*, vol. 18, pp. 615-628, 2020.

[15] Y. L. Lucio, K. M. Villalba, S. A. Donado, "Adaptive Blockchain Technology for a Cybersecurity Framework in IIoT," *IEEE Revista Iberoamericana de Tecnologias del Aprendizaje*, e1, 2022. https://doi.org/10.1109/rita.2022.3166857

[16] J. P. Lazarte Mendez, "Contendores Docker como estrategia de virtualización," Grade Thesis, Universidad Mayor de San Simón, Bolivia, 2019.

[17] J. Bautista Rosell, "Ataques DDoS con IoT, Análisis y Prevención de Riesgos," Grade Thesis, Universidad Carlos III de Madrid, Spain, 2019.

[18] M. A. Yandún Velasteguí, J. V. Hidalgo Guijarro, "Ejemplos prácticos en el laboratorio de cyberseguridad – UPEC,", *SATHIRI*, vol. 15, no. 2, pp. 273–289, 2020. https://doi.org/10.32645/13906925.1002

[19] Y. Liu, X. Ma, J. Bailey, F. Lu, "Reflection Backdoor: A Natural Backdoor Attack on Deep Neural Networks," *Lecture Notes in Computer Science*, vol. 12355, pp. 182–199. https://doi.org/10.1007/978-3-030-58607-2_11