UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TRABAJO DE INVESTIGACIÓN

Revisión bibliográfica de técnicas de Deep learning para la detección de ataques distribuidos de denegación de servicios.

PARA OPTAR EL GRADO ACADÉMICO DE BACHILLER EN INGENIERÍA DE SISTEMAS

Autor:
Bances Carlos Indhyra Melissa

Asesor:
Ing. Alberto Enrique Samillan Ayala

Línea de investigación:
Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú
Año 2019

DEDICATORIA

Dedico este proyecto de investigación a Dios, a mis padres.

A Dios porque ha estado conmigo en cada paso que doy, cuidándome y dándome fuerza para seguir adelante.

A mis padres, quien a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento.

AGRADECIMIENTO

Agradezco a Dios por darnos la vida, por guiarnos a lo largo de nuestro camino, por ser el apoyo y fortaleza en aquellos momentos de dificultad.

Gracias a mis padres por ser el principal motor para cumplir mis sueños, por confiar y creer en mí siempre, guiándome con sus consejos.

Agradezco a los docentes de la escuela académico profesional de ingeniería de sistemas de la Universidad Privada Señor de Sipán, por haber compartido sus conocimientos a lo largo de la carrera, de manera especial, al Ing. Alberto Enrique Samillan Ayala asesor del proyecto de investigación quien ha guiado con su paciencia, y su rectitud como docente, y al comité de la comunidad por su valioso aporte para la investigación.

RESUMEN

En los últimos años los ataques distribuidos de denegación de servicios DDoS (por sus siglas en inglés, Distributed Denial of Service) se han convertido en uno de los principales problemas de distintas empresas que poseen servidores a nivel mundial, haciendo colapsar sus sistemas aprovechando las vulnerabilidades. El objetivo de estos ciberdelincuentes es principalmente generar pérdidas cuantiosas de dinero y muchas veces tan solo dañar el prestigio de estas empresas por puro gusto o venganza. Aunque últimamente son más populares los ataques como el 'ransomware' y el 'phishing', los ataques DDoS siguen encabezando las listas entre las más utilizadas por los ciberdelincuentes.

Los ataques DDoS están orientados a dejar sin servicio una página web o una plataforma, generando grandes flujos de información desde diversos puntos de conexión (dispositivos u ordenadores que posean una conexión a internet) hacia un solo destino saturando el número de peticiones al servidor y con ello logrando que la página o servidor deje de funcionar. El desarrollo de técnicas que logren detectar a tiempo estos ataques se ha convertido en un tema de estudio dentro de las diversas investigaciones de muchos autores. Las investigaciones que existen actualmente se centran en analizar el tráfico de red y encontrar características que ayuden a detectar estos ataques a tiempo. Se han desarrollado diversas técnicas para detectar estos ataques, desde la estadística hasta las técnicas más complejas de aprendizaje profundo (Deep learning), con las cuales se ha logrado la obtención de resultados mucho más favorables.

La presente revisión bibliográfica científica tiene como objetivo la recopilación de diferentes técnicas de Deep learning utilizadas para detectar ataques DDoS, estas técnicas están consideradas dentro del aprendizaje automatico. Las investigaciones anteriores no han tomado como referencias técnicas que son utilizadas en otros campos y han logrado muy buenos resultados.

Para ello en la presente investigación se ha llevado a cabo una revisión sistemática de los últimos cinco años, obteniendo investigaciones importantes para la detección de ataques distribuidos de denegación de servicios. En los cuales se han encontrado formas diferentes de detección.

Palabras Clave **–** Ataques DDoS, Aprendizaje automático, Detección de ataques, Aprendizaje profundo.

ABSTRACT

In recent years, distributed attacks of denial of DDoS services (Distributed Denial of Service) have become one of the main problems of different companies that have servers worldwide, causing their systems to collapse taking advantage of vulnerabilities. The aim of these cybercriminals is mainly to generate large losses of money and often only damage the prestige of these companies for pure taste or revenge. Although attacks such as 'ransomware' and 'phishing' are more popular lately, DDoS attacks continue to top the charts among the most used by cybercriminals.

DDoS attacks are aimed at leaving a web page or platform without service, generating large flows of information from various connection points (devices or computers that have an internet connection) to a single destination saturating the number of requests to the server and with This getting the page or server to stop working. The development of techniques that detect these attacks in time has become a subject of study within the various investigations of many authors. The research that currently exists focuses on analyzing network traffic and finding features that help detect these attacks in time. Various techniques have been developed to detect these attacks, from statistics to the most complex deep learning techniques, with which much more favorable results have been obtained.

This scientific literature review aims to compile different Deep learning techniques used to detect DDoS attacks; these techniques are considered in machine learning. Previous research has not taken as technical references that are used in other fields and have achieved very good results.

For this, in the present investigation a systematic review of the last five years has been carried out, obtaining important investigations for the detection of distributed attacks of denial of services. In which different forms of detection have been found.

Keywords – DDoS attacks, Machine learning, Attacks detection, Deep learning.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

I. INTRODUCCIÓN

El estudio de técnicas utilizadas para detectar ataques distribuidos de denegación de servicios se ha estudiado desde hace muchos años, según (Wang & Gombault, 2008) quien utilizo las redes bayesianas y también el algoritmo C4.5 utilizando solo 9 atributos importantes. Sin embargo, los investigadores pensaban que el cerebro humano era más perfecto que la matemática computacional y decidieron utilizar para detectar ataques DDoS una técnica basada en el cerebro humano; las redes neuronales recurrentes (RNN) donde informan que después de haber usado esta técnica se logró mejorar la precisión dando mejores resultados que otros métodos convencionales. (M., Islam, & Sabrina, 2009). Las técnicas basadas en las características del tráfico de red están presentes en (Li, Liu, & Gu, 2010) en el informe titulado "Detection of DDoS attacks based on neural networks" utilizando en combinación las redes neuronales; por ese año no se obtuvieron los resultados esperados pero se demostró que las redes neuronales no solo podían servir para el campo de procesamiento de imágenes como por entonces se pensaba.

La realización del sistema Deep Defense está basada en redes neuronales profundas que consiste en evaluar el tráfico de red entrante en los indicadores de precisión, taza de error, recordar, exactitud, puntuación F1 y AUC; obteniendo resultados significativos reduciendo la taza de error de 7,517% a 2,103% en comparación con otras técnicas convencionales que utilizaban solo aprendizaje automático (Yuan, Li, & Li, 2017).

Otros investigadores (Potluri, Henry, & Diedrich, 2017) utilizaron la combinación de técnicas de Deep learning y técnicas de machine learning para detectar todo tipo de ataques incluidos los ataques DDoS y clasificarlos, las Redes de Creencia Profunda junto con los Autoencoders las utilizaron para extraer las características del tráfico de red y la Regresión Softmax junto con las Maquinas de soporte vectorial(SVM) para poder clasificar los diversos tipos de ataques encontrados; obteniendo la reducción de tiempo de entrenamiento en un 30%.

En otra investigación (Marwane Zekri, 2017) presenta a los ataques DDoS como el causante de daños muy graves a la nube, por lo tanto en este informe implementaron el algoritmo C4.5 junto con la técnica de árbol de decisiones y además se acoplo una tercera técnica basada en la detección de firmas para obtener una mejor precisión en cuanto a la detección de ataques DDoS; se comparó con otras técnicas las cuales son: Naive Bayes y

K-media y se demostró que con el modelo propuesto se obtuvo resultados más precisos llegando a alcanzar el récord de 98,8% en la clasificación correcta y el tiempo de detección llego a los 0.8 segundos.

Sin embargo (Shikhar Seth, 2017) utilizaron técnicas de Deep learning para clasificar correos spam multimodal, es decir utilizando como contenido imágenes y texto; se afirma que las Redes Neuronales Convolucionales poseen un mejor rendimiento en cuanto a clasificación de texto frente a las Redes Neuronales Recurrentes. Se construyeron dos Redes Neuronales Convolucionales: una para la clasificación de imágenes y otra para la clasificación de textos, luego se unieron para convertirse en un solo clasificador y se logró comprobar que el trabajo conjunto de ambas obtiene 98,11% de precisión que supera a otros clasificadores independientes.

En otros campos de estudio las técnicas de Deep learning ha sido utilizadas para el reconocimiento y clasificación de imágenes (Castro, 2017), realizaron una comparación de tres técnicas; una técnica tradicional la cual fue la Imagen de Apilado y dos técnicas de Deep learning las cuales fueron: las Redes Neuronales Convolucionales y los Autoencoders. Se comprobó la efectividad de las técnicas de aprendizaje profundo (Deep learning) ya que superaron a la técnica convencional de imagen de apilado. Pero la técnica que mostró mejor rendimiento fue las Redes Neuronales Convolucionales debido a su capacidad para capturar contexto espacial.

Otras investigaciones (Amjad Alsirhani, 2018) aseguran que los ataques DDoS son una amenaza a la computación en la nube, por lo tanto, se desarrolló un sistema de detección de ataques DDoS utilizando algoritmos de clasificación los cuales son: Naive Bayes, Random Forest y Árbol de Decisión; añadiéndole un enfoque de cálculo paralelo con Apache Spark para lograr acelerar la ejecución de estos algoritmos. Un agregado importante a este trabajo es la creación de un clasificador que utiliza lógica difusa, el cual permite saber cuál de estos algoritmos logra una mejor detección de ataques.

En otro informe (Abigail Koay, 2018) se basa en la entropía, en cómo se puede utilizar para detectar ataques DDoS y como se pueden corregir algunos errores dentro de esta técnica. Se desarrolla el sistema E3ML el cual consiste en una combinación de entropía, Perceptrón multicapa (MLP), Árbol de decisión aleatorio (ADT) y Red Neuronal

Recurrente (RNN). Todas las técnicas son evaluadas respecto a: precisión, puntuación F1 y recordar. El sistema propuesto logra valores altos de precisión en un conjunto de datos donde hay una variedad de ataques DDoS en comparación con otras técnicas. Se ha demostrado que el trabajo en conjunto de técnicas de Machine learning y entropía proporciona mejores resultados ya que obtiene un valor de precisión de 4,74% mas alto que otras técnicas parecidas e incluso un porcentaje mayor en comparación con técnicas diferentes como por ejemplo la técnica de visión por computadora, la cual se basa en la distancia de Barth Mover.

En conclusión, el presente documento ofrece un estudio bibliográfico de las propuestas relacionadas a las técnicas utilizadas en la detección de ataques DDoS.

1.1. Planteamiento del problema de Investigación.

¿Cuál es el estado del conocimiento acerca de las técnicas de Deep learning utilizadas para la detección de ataques distribuidos de denegación de servicios?

1.2. Objetivos

1.2.1. Objetivos generales

Realizar una revisión del material bibliográfico científico sobre las técnicas de Deep learning utilizadas para la detección de ataques distribuidos de denegación de servicios.

1.2.2. Objetivos específicos

a) Elaborar el plan de investigación.
b) Desarrollar el procedimiento de investigación.
c) Crear la documentación de la investigación.

1.3. Marco teórico conceptual

1.3.1. Tipos de ataques informáticos

Cuando se estudia los distintos tipos de ataques informáticos, se puede diferenciar en primer lugar los ataques activos, que producen cambios en la información y en los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema. (Vieites, 2015).

1.3.2. Aspectos de seguridad que compromete un ataque.

Confidencialidad.

El atacante puede robar información personal como contraseñas u otro tipo de datos confidenciales, permitiendo que una persona desconocida tenga acceso a los datos. (Mieres, 2009)

Integridad.

El atacante puede interceptar un mensaje que se envía codificado, a este tipo de ataques se les llama: Bit-Flipping y son considerados ataques contra la integridad de la información. El ataque realiza un mensaje cifrado o una serie de mensajes cifrados. Puede llegar al extremo y convertirse en un ataque de denegación de servicios. (Mieres, 2009)

Disponibilidad.

El atacante utiliza los recursos, como por ejemplo el ancho de banda para inundar con mensajes el sistema de la víctima y lograr la caída de la red, negándole al usuario legitimo el acceso al sistema. Este es un ejemplo de ataque de Denegación de servicios. (Mieres, 2009).

1.3.3. Ataques DDoS

Estos ataques aparecieron por primera vez en el año 1998 y en la actualidad es el ataque más difícil de detectar debido a su naturaleza distribuida. En este tipo de ataque, el atacante utiliza un gran número de computadoras, las cuales reciben el nombre de Zombies, las cuales envían peticiones a un solo destino con el fin de colapsar la red y con ello denegar el acceso a los usuarios legítimos. (Molina, 2015)

1.3.4. Tipos de ataques DDoS

Se pueden dividir en dos categorías dentro del modelo OSI: ataques en la capa de red y ataques en la capa de aplicación. (OpenCloud, 2016).

Ataques en la capa de red.

Este tipo de ataques afectan directamente la capa de red y de transporte del Modelo OSI, enviando muchos más paquetes o más ancho de banda llegando a colapsar el servidor de destino. Estos ataques causan normalmente la interrupción total del servicio y son de diferentes tipos como: desbordamiento por SYN, desbordamiento por DNS, desbordamiento UDP, ataques de amplificación basados en UDP y ping de la muerte. (OpenCloud, 2016).

Ataques en la capa de aplicación.

Estos ataques están orientados a afectar directamente al servidor web, sin efectos negativos en otros puertos y servicios.

Este tipo de ataques consume poco ancho de banda e incluyen lo siguiente: desbordamientos HTTP, ataques lentos y desbordamiento de peticiones DNS. (OpenCloud, 2016).

1.3.5. Redes neuronales convolucionales (CNN)

Una red neuronal convolucional pertenece a las redes de Deep Learning (aprendizaje profundo), que fueron utilizadas a finales de los años 90, pero últimamente se han vuelto muy populares al conseguir resultados impresionantes en el reconocimiento de imágenes, logrando impactar en el área de visión por computador. (Torres, 2018)

Las redes neuronales convolucionales se forman usando tres tipos de capas: convolucionales, pooling y totalmente conectadas. El entrenamiento de CNN consiste en minimizar una función de perdida. (Lacomilla, 2016)

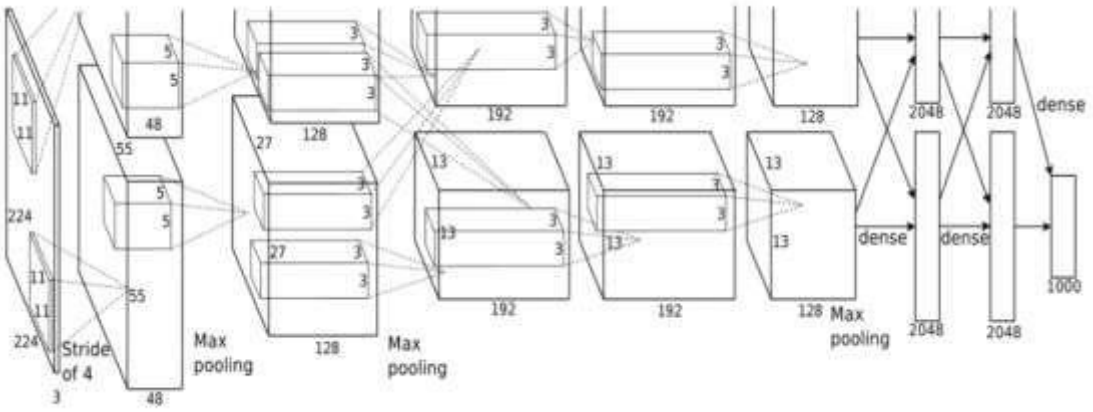

Figura 1: La arquitectura de una red neuronal convolucional ImageNet (Krizhevsky, 2016)

Existen dos arquitecturas básicas de CNN:

- Salida fully connected: las cuales entregan una salida para toda la imagen.

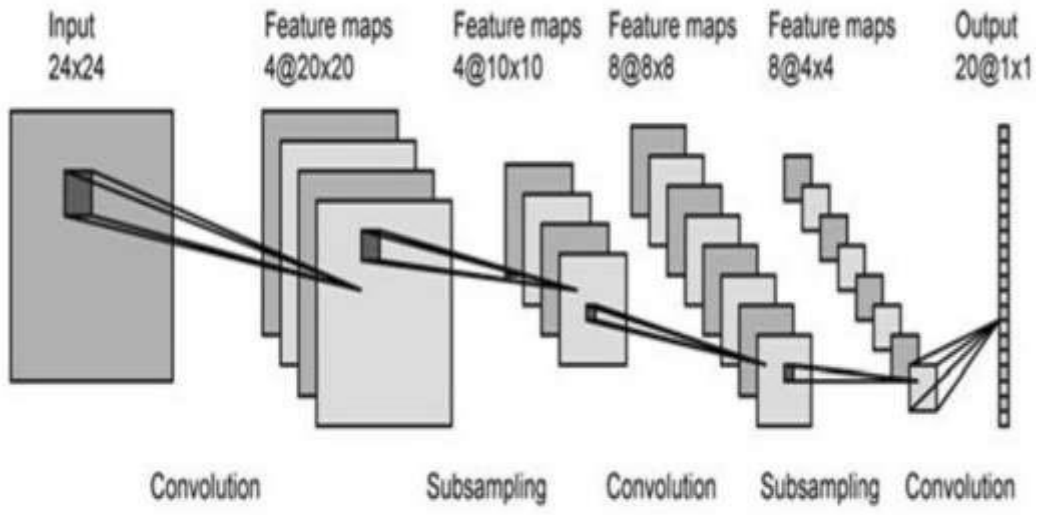

Figura 2: Arquitectura de una CNN de salida fully connected (Lacomilla, 2016)

- Fully convolutional networks: las cuales tienen un encoder y un decoder, comprimen la información y entregan una salida por pixel.

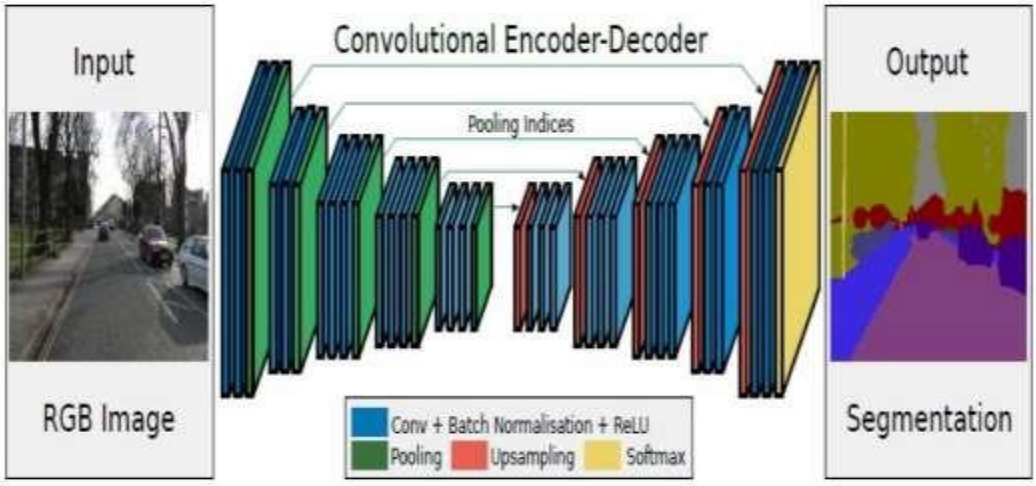

Figura 3: Arquitectura de una CNN de Fully convolutional networks (Lacomilla, 2016)

1.3.6. Redes de creencia profunda (DBN)

Las redes de creencia profunda son consideras arquitecturas de aprendizaje profundo, están compuestas por múltiples capas de variables latentes estocásticas. Estas variables poseen valores binarios y a menudo son denominadas detectores de funciones o unidades ocultas. Las dos capas del nivel superior están conectadas y forman una memoria asociativa.

Estas redes aprenden una capa a la vez y puede ser utilizada en conjunto con otros procedimientos de aprendizaje, para poder afinar los pesos y mejorar el rendimiento de toda la red. (Hinton, 2006)

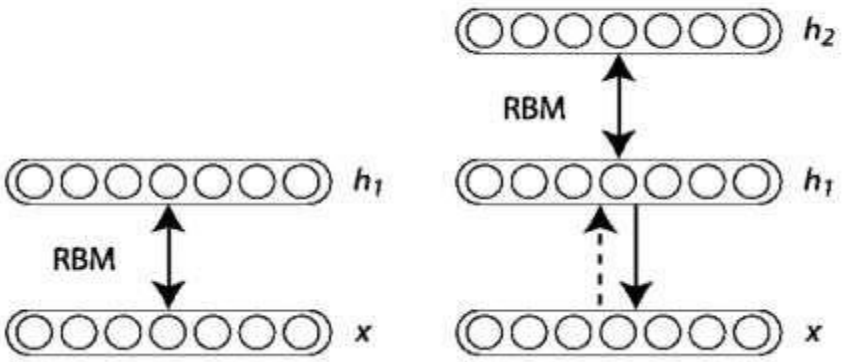

Figura 4: Ejemplo de la arquitectura de una red de creencia profunda (Hinton, 2006)

II. MATERIAL Y METODOS

2.1. Método de la investigación

Para la realización de la revisión bibliográfica científica de este proyecto se tomó como base el método creado por (LAPLANTE, 2017) en su artículo llamado "Review and Analysis of Software Development Team Communication Research", dentro del cual nos ayudara a comprender el desarrollo de un tema específico de forma concisa, válida y justificable. Según lo mencionado anteriormente el siguiente proyecto se centra en la comprensión de técnicas de Deep learning utilizadas para la detección de ataques distribuidos de denegación de servicio, especificando que se ha estudiado un rango de 5 años entre 2013– 2018.

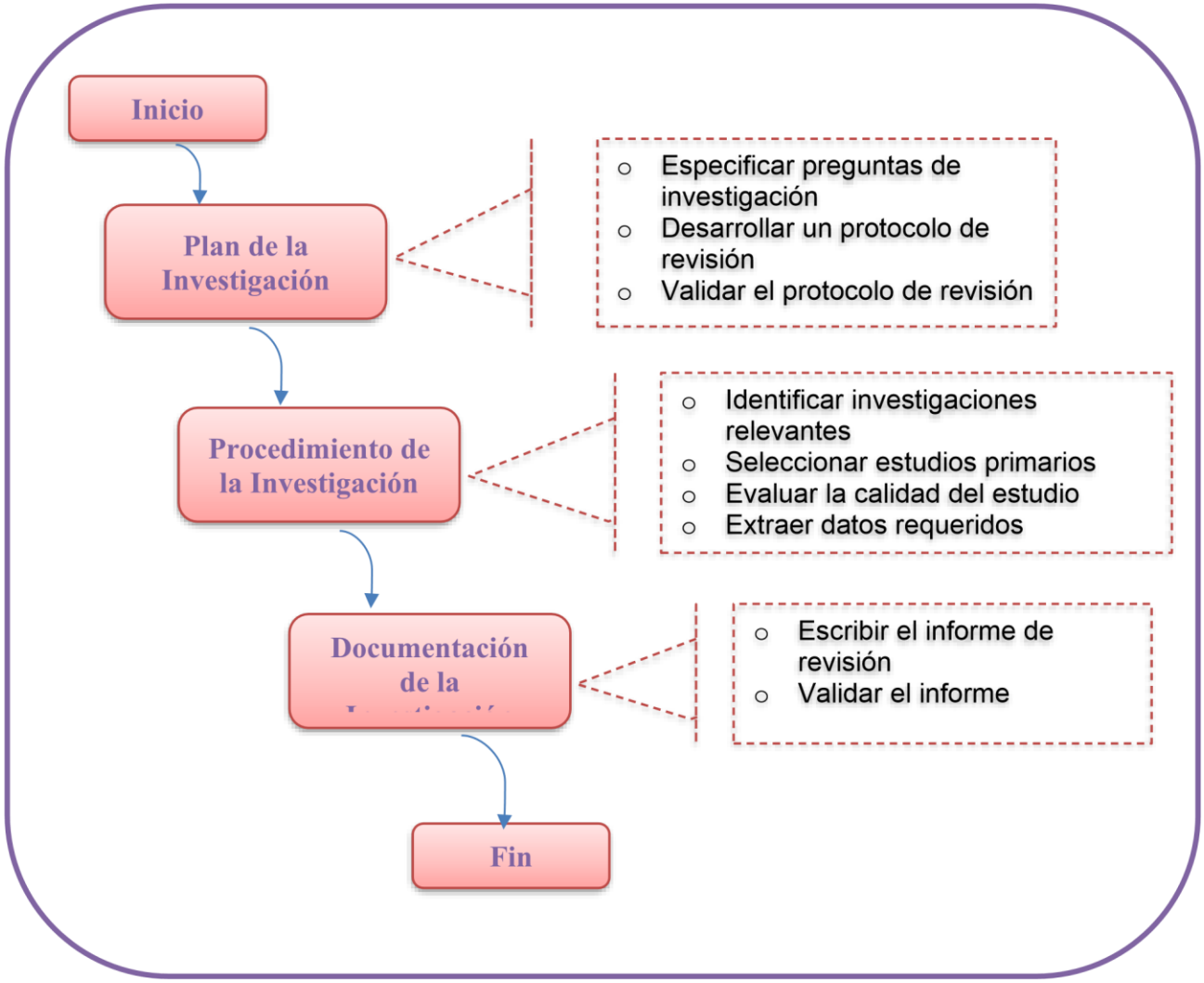

Figura 5: Método de revisión de la literatura científica (LAPLANTE, 2017)

2.2. Plan de la investigación

El objetivo es describir la planificación para realizar el proceso de revisión bibliográfica científica especificando detalladamente los pasos a seguir para garantizar la consistencia y veracidad de la información, en la figura anterior se hace mención, pero se resume en los siguientes 3 pasos:

- Especificar preguntas de investigación que correspondan al estudio.
- Proceso que seguirá a la búsqueda de información
- Condición que se aplique al seleccionar los artículos a incluir en la búsqueda de la información

2.2.1. Interrogantes de la investigación

Las interrogantes de la revisión (IR) son planteadas de acuerdo al estudio de las respuestas y se detallan a continuación:

IR 1: ¿Cuánto material bibliográfico relacionado a las técnicas de detección de ataques distribuidos de denegación de servicios ha sido publicada entre los años 2013 a 2018?

IR 2: ¿Qué tipos de técnicas o algoritmos existen para el proceso de detección de ataques distribuidos de denegación de servicios?

IR 3: ¿Cuantas técnicas de Deep learning encontramos para detectar ataques distribuidos de denegación de servicios?

2.2.2. Protocolos de la revisión

El protocolo de revisión es definido como un conjunto de reglas en las cuales se detalla el proceso de la revisión de la información relacionada acerca de la compresión de las técnicas de Deep learning para la detección de ataques DDoS, de esta manera se logra especificar como se debe realizar la extracción de la información. En este proyecto como primer paso se realizó la clasificación de en qué base de datos se realizará la búsqueda de los artículos científicos relacionados al tema, dicha clasificación se ha realizado mediante la plataforma de SCImago Journal & Country Rank (SJR)

Figura 6: Plataforma web de Scimago Journal & Country Rank(SJR)

Scimago Journal & Country Rank es una plataforma web donde incluye las revistas junto con sus respectivos indicadores a partir de la información que se guarda en la base de datos Scopus. Cabe resaltar que para el filtrado se ajustó las configuraciones respectivas según el estudio del proyecto, en la opción de área se seleccionó Computer Sciencie y en la categoría de temas se seleccionó Artificial Intelligence. Luego de realizar el proceso de filtrado, se seleccionó la base de datos IEEE como base de datos principal, debido a que la mayoría de artículos relacionados con el tema se encuentran allí.

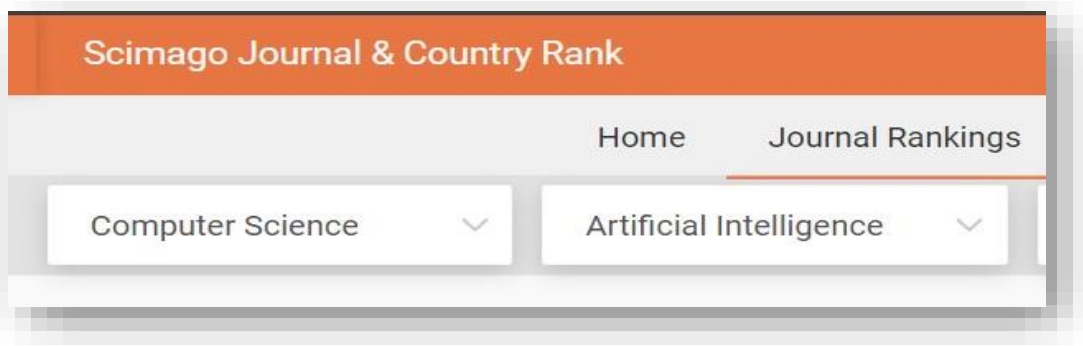

Figura 7: Selección de campos en el ranking Journal

3	IEEE Transactions on Pattern Analysis and Machine Intelligence	journal	3.764 Q1	326	422	577	11838	11286	569	19.42	28.05
4	IEEE Transactions on Neural Networks and Learning Systems	journal	3.658 Q1	180	657	765	24758	9177	755	12.18	37.68
5	International Journal of Computer Vision	journal	3.595 Q1	172	89	278	5311	4345	261	7.56	59.67
6	Cognitive Psychology	journal	3.128 Q1	108	33	104	2278	438	102	4.13	69.03

Figura 8: Selección de base de datos IEEE de la plataforma web SJR.

2.2.3. Validar protocolos de la revisión

Validando el protocolo de revisión, las búsquedas iniciales condujeron a revisiones del protocolo y las preguntas de la investigación; por lo tanto, la validación será discutida más adelante y se utilizará algunas palabras claves incluidos en los artículos.

2.3. Documentación de la investigación

2.3.1. Identificar las investigaciones relevantes

En esta fase después de identificar las propuestas más importantes se responderá las preguntas planteadas en la investigación de la fase 2.1.1. Se formuló una propuesta que se centre en la compresión de las técnicas de detección de ataques DDoS, cabe mencionar que por ser un tema específico se tuvo que generar una regla de búsqueda en donde se utilizó "and" para unir palabras como:" DDoS attacks", "detection techniques" y "machine learning". Utilizando la base de datos de la IEEE se determinó que las revistas serán la fuente principal de esta revisión bibliográfica para garantizar la calidad de este estudio.

Tabla 1: ***Búsqueda de datos y resultados.***

Nº	Base de Datos	Regla de Búsqueda	Resultados
1	IEEE Xplore Digital Library	('DDoS attacks AND detection techniques AND machine learning')	59

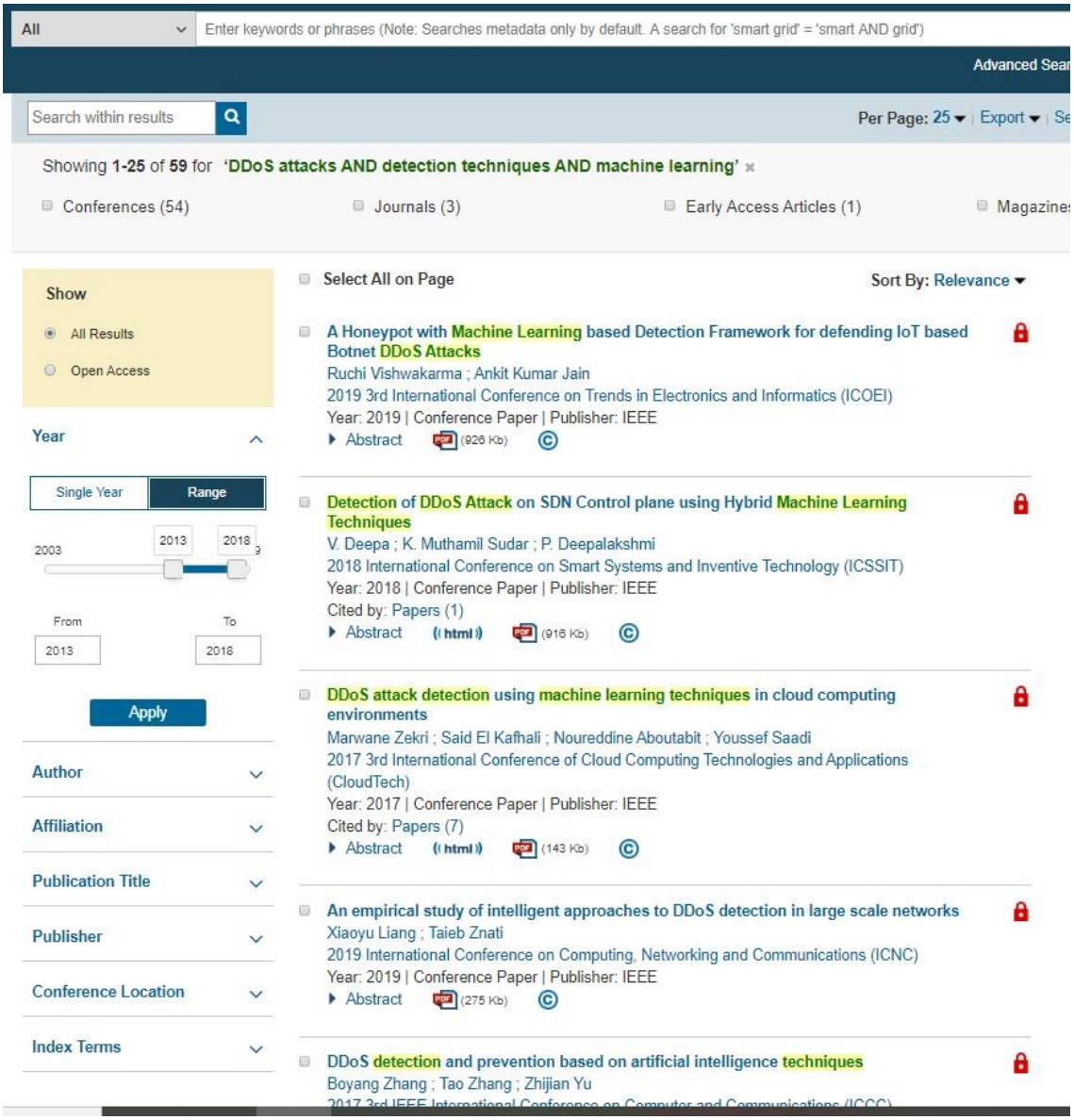

Figura 9: Resultados de la búsqueda en IEEExplore.

2.3.2. Seleccionar los estudios primarios

Para seleccionar los trabajos de la investigación e incluirlos en la revisión bibliográfica, se toma en cuenta los distintos indicadores (palabras claves, revistas, resumen, cantidad de referencias, numero de citas), con la finalidad, que a partir del resultado que genera la búsqueda utilizando la regla propuesta anteriormente para poder describir de manera más equilibrada la revisión. A continuación, se describe las tendencias de los estudios filtrados haciendo énfasis en el año de la publicación, técnicas y los autores de los trabajos de investigación.

Tabla 2: ***Resumen de las propuestas planteadas desde el 2014 - 2018***

Nº	Año	Técnicas	Uso	Eficiencia	Ref.
1	2014	Algoritmo de inspección de recuento y SVM	Detección de ataques DDoS.	98.99%	(Devi, Preetha, Selvaram, & Shalinie, 2014)
2	2014	SVM	Detección de ataques DDoS	98.07%	(Kato & Klyuev, 2014)
3	2014	Algoritmo genético y red neuronal artificial.	Detección de ataques DDoS	90.02%	(Barati, Abdullah, Udzir, Mahmod, & Mustapha, 2014)
4	2014	Árbol de decisión y Naive Bayes	Detectar ataques DDoS	90%	(Balkanli, Alves, & Zincir-Heywood, 2014)
5	2014	Redes neuronales, redes bayesianas, lógica difusa, SVM y Algoritmo genético.	Detección de ataques DDoS en redes SDN.	Mejores resultados	(Ashraf & Latif, 2014)
6	2015	Entropia y Distancia de Hellinger	Detectar ataques DDoS	89.99%	(Tsiatsikas, y otros, 2015)
7	2015	K-Means modificado	Detección de ataques DDoS	98%	(Pramana, Purwant, & Suratman, 2015)
8	2016	Autoencoder	Detección de ataques DDoS	96.99%	(Yadav & Subramanian, 2016)
9	2017	Entropia	Detección de ataques DDoS	87%	(Zubaydi, Anbar, & Wey, 2017)
10	2017	Red Neuronal Convolucional	Clasificación de spam	98.11%	(Shikhar Seth, 2017)
11	2017	Autoencoders y red de creencia profunda	Seguridad en sistemas de control de red.	94.2%	(Potluri, Henry, & Diedrich, 2017)
12	2017	Algoritmo C4.5	Detección de ataques DDoS.	98.8%	(Marwane Zekri, 2017)
13	2017	Red neuronal recurrente	Detección de ataques DDoS	97.99%	(Yuan, Li, & Li, 2017)
14	2018	Red neuronal recurrente y perceptrón multicapa.	Detección de ataques DDoS	94.74%	(Abigail Koay, 2018)
15	2018	Naive Bayes, Random Forest y árbol de decisión	Detección de ataques DDoS	97.4%	(Amjad Alsirhani, 2018)
16	2018	SVM y SOM	Detección de ataques DDoS	96.77%	(Deepa, Sudar, & Deepalakshmi, 2018)

Nº	Año	Técnicas	Uso	Eficiencia	Ref.
17	2018	K-means, LSVM, árbol de decisión, Random forest y red neuronal.	Detección de ataques DDoS	97.6%	(Doshi, Apthorpe, & Feamster, 2018)
18	2018	J48, Random Forest, K-Means y SVM	Detección de ataques DDoS	98.6%	(Rahman, Quraishi, & Lung, 2018)
19	2018	Algoritmo C4.5	Detección de ataques DDoS	99.5%	(Hou, Fu, Cao, & Xu, 2018)
20	2018	SVM y Red neuronal profunda.	Detección de ataques DDoS	92.30%	(V., G., & Hiremath, 2018)
21	2018	Random Forest, K- Means y SVM	Detección de ataques DDoS	95.08%	(Bakker, Ng, & Seah, 2018)

2.3.3. Evaluar la calidad de los estudios

En esta fase para obtener una buena calidad de la investigación se tuvo que abordar con el criterio de inclusión de la revisión integrada. La inclusión de criterios para esta revisión bibliográfica incluyó artículos de revistas que se realizaron investigaciones relacionadas con las técnicas utilizadas en la detección de ataques distribuidos de denegación de servicios. Además de evaluar el enfoque de investigación del documento, se evaluó el impacto global y el valor del H-index de las revistas estos últimos 5 años. El Impacto (impacto #) en la SCImago Journal Rank es representada por el número de citaciones ponderadas en el año seleccionado por los documentos publicados en la revista seleccionada en tres años anteriores y el H-Index la cual cuantifica tanto la productividad científica de la revista como el impacto de la misma. Cabe señalar que los documentos incluidos fueron publicados en revistas de impacto en las que el valor medio es de 2.558 y la media del H-Index es 109.7.

Tabla 3: ***Resumen de impacto de las revistas 2014 – 2018.***

Articulo	Revista	Impact #	H-Index
1	IEEE Transactions on Pattern Analysis and Machine Intelligence	3.764	326
2	IEEE Transactions on Neural Networks and Learning Systems	3.658	180
3	Foundations and Trends in Machine Learning	5.002	25
4	31st International Conference on Machine Learning, ICML 2014	3.849	28
5	International Journal of Computer Vision	3.595	172

6	Cognitive Psychology	3.128	108
7	Journal of Memory and Language	3.007	129
8	IEEE Transactions on Fuzzy Systems	2.794	170
9	Physics of Life Reviews	2.691	52
10	Proceedings - 2016 43rd International Symposium on Computer Architecture, ISCA 2016	2.631	17
11	International Journal of Robotics Research	2.189	142
12	Soft Robotics	2.093	24
13	Neural Networks	1.970	128
14	Journal of the ACM	1.650	117
15	Networks and Spatial Economics	1.626	40
16	Information Sciences	1.620	154
17	Cognitive Science	1.571	98
18	Knowledge-Based Systems	1.460	94
19	Synthesis Lectures on Artificial Intelligence and Machine Learning	1.445	17
20	Journal of Machine Learning Research	1.426	173
#	PROMEDIOS	2.558	109.7

2.3.4. Extraer los datos requeridos

En este paso se dará respuesta a las preguntas de la investigación, donde se extrajeron los siguientes datos de cada estudio:

1. Las palabras clave que se utilizarán en un análisis de contenido para determinar en última instancia las categorías de investigación en comunicación (la taxonomía).
2. Tipo de datos recogidos: cualitativos, cuantitativo, encuesta, revisión de la literatura.
3. Suficiente información para determinar el resultado principal.
4. La información de la revista para permitirnos determinar su valor de impacto y el valor del H-index.

2.3.5. Sintetizar los datos

Para obtener resultados más concretos se debe utilizar y determinar los temas principales de la investigación para poder garantizar los artículos seleccionados, con esto se podrá determinar las categorías de la investigación. Se procedió al análisis del contenido de cada

palabra o conjunto de palabras del cual va más allá del simple conteo de palabras a examinar. Se debe aclarar que para realizar este análisis se basa en la valoración de los términos controlados por INSPEC la cual es una importante base de datos de indexación de literatura científica y técnica, publicada por el Instituto de Ingeniería y Tecnología. En el resultado de la investigación se mostrará el título de la publicación, autor, año de la publicación, palabras clave del autor, términos controlados por IEEE, términos controlados y no controlados por INSPEC, número de citas y referencias de cada publicación.

Tabla 4: ***Valoración de las palabras claves de acuerdo a INSPEC.***

Nº	Título del documento	Autores	Año	Palabras clave del autor	Términos de IEEE	Términos controlados por INSPEC	Términos no controlados por INSPEC	# de citas	# de Ref.
1	An impact analysis: Real time DDoS attack detection and mitigation using machine learning	B.S. Kiruthika Devi; G. Preetha; G. Selvaram; S. Mercy Shalinie	2014	DDoS, IP spoofing, hop count inspection algorithm, support vector machine, rate limiting	IP networs, Computer crime, Filtering, Limiting, Aggregates Measurement, Support vector machines	computer network performance evaluation, computer network security, Internet, IP networks, learning (artificial intelligence), support vector machines	impact analysis, real time DDoS attack detection, real time DDoS attack mitigation, machine learning, distributed denial of service attacks, devastating attack, normal functionality, Internet community, DDoS cyber weapon, hactivitism, personal revenge, antigovernment force, disgruntled employers, cyber espionage, IP spoofing, Internet network, spoofed traffic shares, online monitoring system, OMS, spoofed traffic detection module, interface based rate limiting algorithm, network performance metrics, hop count inspection algorithm, HCF, source IP address, support vector machine, SVM, IBRL algorithm	3	36

2	Large-scale network packet analysis for intelligent DDoS attack detection development	Keisuke Kato; Vitaly Klyuev	2014	network security, bigdata analysis, distributed denial of service attack, machine teaming	Computer crime, IP networks, Support vector machines, Feature extraction, Internet, Training, Kernel	computer network security, data analysis, Internet, learning (artificial intelligence), network servers, radial basis function networks, support vector machines	distributed denial of service attacks, intelligent DDoS attack detection development, large-scale network packet analysis, network security, DDoS attacks, network service, bots, machine learning techniques, Center for Applied Internet Data Analysis, support vector machine, radial basis function kernel	0	26
3	Distributed Denial of Service detection using hybrid machine learning technique	Mehdi Barati; Azizol Abdullah; Nur Izura Udzir; Ramlan Mahmod; Norwati Mustapha	2014	Distributed DoS Attack, Machine Learning, IDS	Computer crime, Artificial neural networks, Genetic algorithms, Feature extraction, Accuracy, Biological cells	computer network security, feature selection, genetic algorithms, learning (artificial intelligence), multilayer perceptrons	deniable false alarm, MLP, multilayer perceptron, Wrapper method, hybrid method, feature selection, ANN, artificial neural network, GA, genetic algorithm, DDoS attack detection system, hybrid machine learning, distributed denial of service detection	6	20

4	Supervised learning to detect DDoS attacks	Eray Balkanli; Jander Alves; A. Nur Zincir-Heywood	2014	Network security, Backscatter detection, Supervised learning, network intrusion detection systems	Backscatter, IP networks, Computer crime, Ports (Computers), Training, Protocols, Decision trees	Bayes methods, computer network security, decision trees, learning (artificial intelligence), pattern classification, public domain software	IP addresses, CART decision tree classifier, Naive Bayes machine learning classifier, Bro opensource system, Corsaro opensource system, backscatter darknet traffic, NIDS, network intrusion detection systems, supervised learning techniques, DDoS attacks	11	33
5	Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniqu e	Javed Ashraf; Seemab Latif	2014	Machine Learning , Software Defined Networking (SDN) , Intrusion Detection , Distributed Denial of Service Attack	Artificial neural networks, Silicon, Bayes methods, Support vector machine classification, Training, Genetics, Classification algorithms	computer network security, learning (artificial intelligence), software defined networking	DDoS attacks, software defined networks, machine learning techniques, SDN, OpenFlow protocol, intrusion attack mitigation, distributed denial of service	29	35

6	Battling against DDoS in SIP: Is Machine Learning - based detection an effective weapon?	Z. Tsiatsikas; A. Fakis; D. Papamartzivanos; D. Geneiatakis; G. Kambourakis; C. Kolias	2015	Session Initiation Protocol, Machine Learning, DDoS, Anomalydetection, Intrusion Detection Systems	Computer crime, Protocols, Computer architecture, Servers, Intrusion detection, Ecosystems	computer network security, Internet telephony, learning (artificial intelligence), signalling protocols	DDoS, machine learning-based detection, network anomalydetection, distributed denial of service detection, SIP-based VoIP ecosystems, session initiation protocol, SIP intrusion detection	0	26
7	DDoS detection using modified K-means clustering with chain initialization over landmark window	Made Indra Wira Pramana; Yudha Purwant; Fiky Yosef Suratman	2015	DDoS, Modified K-Means, Clustering, Chain Initialization, Landmark Window	Clustering algorithms, Data mining, Signal processing algorithms, Computer crime, Algorithm design and analysis, IP networks, Convergence	authorisation, computer network security, pattern clustering	DDoS detection, modified Kmeans clustering, denial-ofservice network attack, user access right, chain initialization over landmark window approach, DARPA 98 dataset	2	10

8	Detection of Application Layer DDoS attack by feature learning using Stacked AutoEncoder	Satyajit Yadav; Selvakumar Subramanian	2016	DDoS, Application Layer DDoS Attack, Deep learning, Feature learning, AutoEncoder, Stacked AutoEncoder	Computer crime, Feature extraction, Machine learning, Web servers, IP networks, Floods, Pattern recognition	computer network security , learning (artificial intelligence) , neural nets	application layer DDoS attack detection, feature learning, Stacked AutoEncoder, application layer distributed denial of service attack, Web security, TCP layer, IP layer, deep learning architecture, very deep neural network	12	14
9	Review on Detection Techniques against DDoS Attacks on a Software-Defined Networking Controller	Haider Dhia Zubaydi; Mohammed Anbar; Chong Yung Wey	2017	Software Defined Networking, SDN, DDoS Attacks, DDoS Detection, SDN Controller	Computer crime, Control systems, Entropy, IP networks, Protocols	centralised control, computer network security, Internet, software defined networking, telecontrol	detection techniques, DDoS attacks, software-defined networking controller, information and communication technologies, Internet, SDN security, remotely controlled networks	1	17

10	Multimodal Spam Classification Using Deep Learning Techniques	Shikhar Seth; Sagar Biswas	2017	E-mail, Spam Classification, Deep Learning, Convolutional Neural Networks, Multimodal	Electronic mail, Postal services, Training, Convolutional neural networks, Computer architecture, Text categorization, Task analysis	convolution, feedforward neural nets, image classification, Internet, learning (artificial intelligence), security of data, text analysis, unsolicited e-mail	Convolutional Neural Networks, hybrid multimodal architectures, text classifiers, multimodal spam classification, deep learning techniques, E-mail system, internet, image classifiers	1	26
11	Evaluation of hybrid deep learning techniques for ensuring security in networked control systems	Sasanka Potluri; Navin Francis Henry; Christian Diedrich	2017	Intrusion Detection System (IDS), Machine Learning, Deep Learning, NSL-KDD, Network Security, Automation	Machine learning, Feature extraction, Intrusion detection, Support vector machines, Automation, Training	Internet, learning (artificial intelligence), networked control systems, security of data	hybrid deep learning techniques, networked control systems, security related problems, automation networks, automation plant, Intrusion Detection System	2	23

12	DDoS attack detection using machine learning techniques in cloud computing environments	Marwane Zekri; Said El Kafhali; Noureddine Aboutabit; Youssef Saadi	2017	Security, Cloud Computing, DDoS attack, Vulnerability, Intrusion Detection, Machine Learning	Computer crime, Cloud computing, Neural networks, Protocols, Computers, Algorithm design and analysis, Machine learning algorithms	cloud computing, computer network security, decision trees, Internet, learning (artificial intelligence)	DDoS attack detection, cloud computing environments, IT technology, on-demand resources, end users, legacy protocols, attacker, cloud performance, innocent compromised computers, DDoS detection system, DDoS threat, signature detection techniques, signatures attacks, DDoS flooding attacks, machine learning techniques, reduced infrastructure cost, Distributed Denial of Service, management organizations, victim cloud infrastructures, decision tree	4	53
13	DeepDefense: Identifying DDoS Attack via Deep Learning	Xiaoyong Yuan; Chuanhuang Li; Xiaolin Li	2017		Computer crime, Feature extraction Machine learning, Learning systems, Recurrent neural networks, Bandwidth	computer network security, feature extraction, Internet, learning (artificial intelligence), recurrent neural nets, statistical analysis	deep defense, deep learning, distributed denial of service attack, DDoS attack, Internet, network traffic, statistical divergence, machine learning, feature extraction, recurrent deep neural network	18	41

14	A new multi classifier system using entropy based features in DDoS attack detection	Abigail Koay; Aaron Chen; Ian Welch; Winston K. G. Seah	2018	DDoS, Entropy, Machine Learning	Computer crime, Entropy, Feature extraction, Machine learning, Media Access Protocol	computer network security, entropy, learning (artificial intelligence), pattern classification, telecommunication traffic	entropy-based features, attack traffic, normal traffic, machine learning classifiers, attack intensities, DDoS attack detection, multiclassifier system, DDoS attacks detection, Multiple entropy-based features	2	29
15	DDoS Attack Detection System: Utilizing Classification Algorithms with Apache Spark	Amjad Alsirhani; Srinivas Sampalli; Peter Bodorik	2018	DDoS Attack, Apache Spark, Apache Hadoop, Classification, DDoS Detection	Computer crime, Classification algorithms, Prediction algorithms, Cloud computing, Fuzzy logic, Sparks, Parallel processing	cloud computing, computer network security, data handling, fuzzy logic, IP networks, parallel processing, pattern classification, telecommunication traffic	classification algorithm, utilized classification algorithms, fuzzy logic system, DDoS attack detection system, configurable computing resources, numerous DDoS attacks, DDoS detection system, MATLAB	2	30

16	Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques	V. Deepa; K. Muthamil Sudar; P. Deepalakshmi	2018	Software Define Network, Machine Learning (ML), Hybrid Machine learning, Distributed Denial of Service (DDoS), Support Vector Machine (SVM), Self Organized Map (SOM)	Computer crime, Support vector machines, Machine learning, Classification algorithms, Software defined networking, Machine learning algorithms	authorisation, computer network security, learning (artificial intelligence), software defined networking	DDoS attack, SDN control plane, network plane, SDN environment, hybrid machine learning model, DDoS attack detection, software defined network, Distributed Denial of Service attack, authorized user, controller protection	0	11
17	Machine Learning DDoS Detection for Consumer Internet of Things Devices	Rohan Doshi; Noah Apthorpe; Nick Feamster	2018	Internet of Things, Anomaly Detection, DDoS, Machine Learning, Feature Engineering	Anomaly detection, Computer crime, Internet of Things, Botnet, Middleboxes, Machine learning	computer network security, Internet, Internet of Things, invasive software, learning (artificial intelligence), neural nets	critical Internet infrastructure, consumer IoT attack traffic, IoT network traffic, machine learning algorithms, neural networks, network middleboxes, DDoS attacks, DDoS detection, Consumer Internet of Things Devices, distributed denial of service attacks, consumer IoT devices	9	24
18	DDoS Attacks	Obaid Rahma	2018	SDN, DDoS, Machine	Control systems, Computer crime,	computer network security, nearest	SDN network, software defined networking, distributed denial-of-	0	12

				Learning, J48,					
	Detection and Mitigation in SDN Using Machine Learning	n; Mohammad Ali Gauhar Quraishi; Chung-Horng Lung		Weka	Machine learning, Floods, Support vector machines, Network topology	neighbour methods, random forests, software defined networking, support vector machines	service attack, support vector machine, DDoS attack detection, machine learning, security threat protection, J48, random forest, knearest neighbors		
19	Machine Learning Based DDoS Detection Through NetFlow Analysis	Jiangpan Hou; Peipei Fu; Zigang Cao; Anlin Xu	2018	DDoS classification, NetFlow, Machine Learning	Computer crime, Feature extraction, Tools, Detectors, Machine learning, Real-time systems, Data mining	computer network security, feature extraction, feature selection, Internet, learning (artificial intelligence), sampling methods, telecommunication traffic	NetFlow feature selection, NetFlow data, research lab network trace, DDoS traffic, realworld NetFlow, DDoS detection, NetFlow analysis, high speed networks, distributed denial of service, machine learning, Internet, traffic sampling data, pattern-based feature extraction, adaptive flow-based feature extraction, random forest, DDoS attack	1	16

20	Detection of DDoS Attacks in Software Defined Network	Karan B. V.; Narayan D. G.; P. S. Hiremath	2018	SDN, DDoS, Snort, Mininet, KDD, SVM, DNN	Computer crime, Support vector machines, Classification algorithms, Machine learning algorithms, Servers, Entropy	computer network security, learning (artificial intelligence), neural nets, pattern classification, software defined networking, support vector machines	cyber-attack, software defined networks, support vector machine classifier, distributed denial of service, SDN environment, anomaly-based attacks, signaturebased attacks, detection system, SDN controller, centralized control plane, emerging networking paradigm, DDoS attacks	0	16
21	Can Machine Learning Techniques Be Effectively Used in Real Networks against DDoS Attacks?	Jarrod N. Bakker; Bryan Ng; Winston K. G. Seah	2018	-	Computer crime, Entropy, Training, Internet of Things, Control systems, Support vector machines, Testing	computer network management, computer network security, learning (artificial intelligence), software defined networking, telecommunication traffic	machine learning techniques, network management, SDN-based traffic classification architecture, legitimate network traffic, software-defined networking, DDoS attack detection, identifyclassify malicious traffic, distributed denial of service attack detection, Internet of Things devices, IoT devices, ML techniques, centralising network information, nmeta2 implementation, nonmalicious traffic classification	2	22

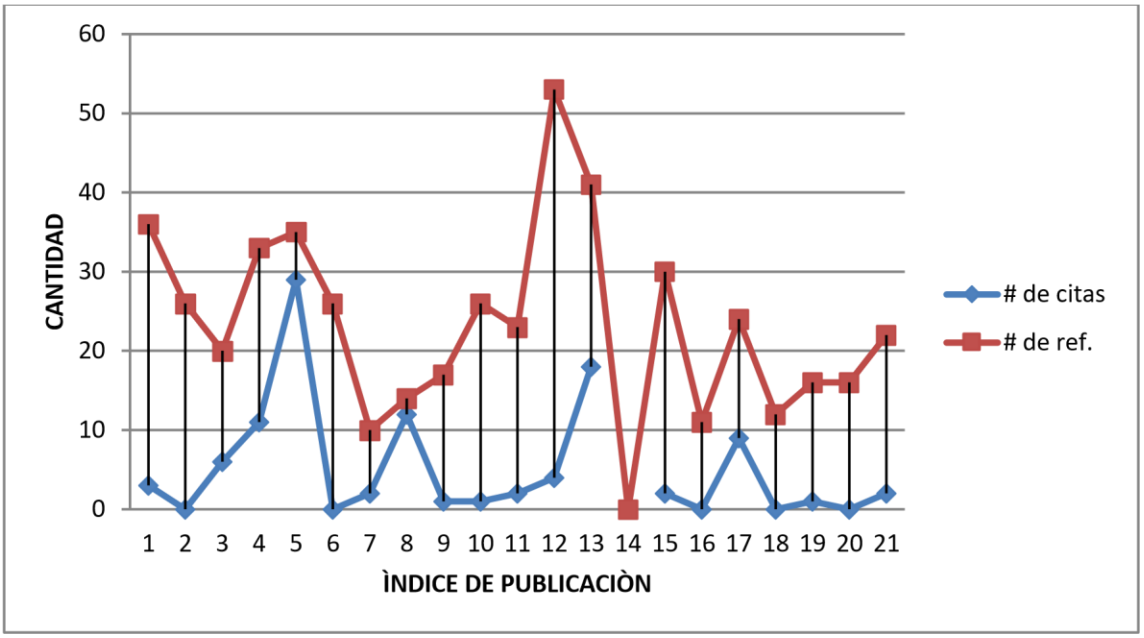

Figura 10: Valoración de los artículos según el número de citas y la cantidad de referencias.

2.4. Documentación de la investigación

En esta fase el objetivo es documentar las respuestas respondiendo las preguntas planteadas previamente y así poder validar el informe.

2.4.1. Validar informe

Los datos y el análisis de esta revisión integradora fueron validados en todo momento por los autores de este trabajo como parte del proceso de revisión.

III. RESULTADOS

En los resultados obtenidos tiene como interpretación basada en la revisión realizada de artículos literarios que se relacionan a técnicas de Deep learning utilizadas para la detección de ataques distribuidos de denegación de servicios, se debe resaltar que para el tema específico no se logró encontrar mucho material, pero si temas relacionados.

Estos artículos se ordenaron de manera ascendente por su año de publicación donde se utilizó una regla de búsqueda. Cabe mencionar que estas investigaciones han ido creciendo cada año, lo que se evidencia más crecimiento es en el año 2014, luego en el 2017 y el año 2018 bajo un poco. Así mismo ha quedado demostrado que el estudio por buscar la mejor técnica de Deep learning en la detección de ataques distribuidos de

denegación de servicios es un tema de investigación constante con un impacto muy importante para los investigadores.

Figura 11: Cantidad de artículos por año aplicando el filtro crudo sobre la regla de búsqueda.

De los 59 artículos sobre las técnicas de aprendizaje automático y Deep learning para la detección de ataques distribuidos de denegación de servicios, se realizó la elección de 21 artículos con la finalidad de analizar que técnicas son las más utilizadas para la detección de ataques DDoS. Por ello el resultado del análisis sirve de forma crítica para la elección de dichos documentos.

3.1. Análisis del resultado

A continuación, se presentará los resultados del análisis respondiendo a las preguntas de investigación antes planteadas, demostrando así que fueron respondidas como parte del proceso de la revisión de la literatura científica.

IR 1: ¿Cuánto material bibliográfico relacionado a la tecnicas utilizadas en la detección de ataques distribuidos de denegación de servicios se encuentra entre los años 2014 a 2018?

La cantidad de material referente a la literatura científica relacionada a las técnicas de utilizadas en la detección de ataques distribuidos de denegación de servicios son ilimitados, sin embargo se tuvo que realizar la propuesta de revisión según un criterio, se

realizó la búsqueda haciendo énfasis en las revistas alojadas en IEEExplore mediante la regla que se generó anteriormente, haciendo el filtrado, se evidenciaron 59 documentos encontrados, de los cuales se seleccionaron 21 en donde muestran las diferentes técnicas que se utilizan para la detección de ataques DDoS.

Tabla 5: ***Resultados más significativos de las técnicas de detección de ataques DDoS.***

Nº	Año	Autores	Titulo	Técnicas	Ref.
1	2014	B.S. Kiruthika Devi; G. Preetha; G. Selvaram; S. Mercy Shalinie	An impact analysis: Real time DDoS attack detection and mitigation using machine learning	Algoritmo de inspección de recuento y SVM	(Devi, Preetha, Selvaram, & Shalinie, 2014)
2	2014	Keisuke Kato; Vitaly Klyuev	Large-scale network packet analysis for intelligent DDoS attack detection development	SVM	(Kato & Klyuev, 2014)
3	2014	Mehdi Barati; Azizol Abdullah; Nur Izura Udzir; Ramlan Mahmod; Norwati Mustapha	Distributed Denial of Service detection using hybrid machine learning technique	Algoritmo genético y red neuronal artificial.	(Barati, Abdullah, Udzir, Mahmod, & Mustapha, 2014)
4	2014	Eray Balkanli; Jander Alves; A. Nur Zincir-Heywood	Supervised learning to detect DDoS attacks	Árbol de decisión y Naive Bayes	(Balkanli, Alves, & Zincir-Heywood, 2014)
5	2014	Javed Ashraf; Seemab Latif	Handling intrusion and DDoS attacks in Software Defined Networks using machine learning technique	Redes neuronales, redes bayesianas, lógica difusa, SVM y Algoritmo genético.	(Ashraf & Latif, 2014)
6	2015	Tsiatsikas; A. Fakis; D. Papamartzivanos; D. Geneiatakis; G. Kambourakis; C. Kolias	Battling against DDoS in SIP: Is Machine Learning-based detection an effective weapon?	Entropía y Distancia de Hellinger	(Tsiatsikas, y otros, 2015)
7	2015	Made Indra Wira Pramana; Yudha Purwant; Fiky Yosef Suratman	DDoS detection using modified K-means clustering with chain initialization over landmark window	K-Means modificado	(Pramana, Purwant, & Suratman, 2015)

Nº	Año	Autores	Titulo	Técnicas	Ref.
8	2016	Satyajit Yadav; Selvakumar Subramanian	Detection of Application Layer DDoS attack by feature learning using Stacked AutoEncoder	Autoencoder	(Yadav & Subramanian, 2016)
9	2017	Haider Dhia Zubaydi; Mohammed Anbar; Chong Yung Wey	Review on Detection Techniques against DDoS Attacks on a Software-Defined Networking Controller	Entropía	(Zubaydi, Anbar, & Wey, 2017)
10	2017	Shikhar Seth; Sagar Biswas	Multimodal Spam Classification Using Deep Learning Techniques	Red Neuronal Convolucional	(Shikhar Seth, 2017)
11	2017	Sasanka Potluri; Navin Francis Henry; Christian Diedrich	Evaluation of hybrid deep learning techniques for ensuring security in networked control systems	Autoencoders y red de creencia profunda	(Potluri, Henry, & Diedrich, 2017)
12	2017	Marwane Zekri; Said El Kafhali; Noureddine Aboutabit; Youssef Saadi	DDoS attack detection using machine learning techniques in cloud computing environments	Algoritmo C4.5	(Marwane Zekri, 2017)
13	2017	Xiaoyong Yuan; Chuanhuang Li; Xiaolin Li	DeepDefense: Identifying DDoS Attack via Deep Learning	Red neuronal recurrente	(Yuan, Li, & Li, 2017)

Nº	Año	Autores	Titulo	Técnicas	Ref.
14	2018	Abigail Koay; Aaron Chen; Ian Welch; Winston K. G. Seah	A new multi classifier system using entropy-based features in DDoS attack detection	Red neuronal recurrente y perceptrón multicapa.	(Abigail Koay, 2018)
15	2018	Amjad Alsirhani; Srinivas Sampalli; Peter Bodorik	DDoS Attack Detection System: Utilizing Classification Algorithms with Apache Spark	Naive Bayes, Random Forest y árbol de decisión	(Amjad Alsirhani, 2018)
16	2018	V. Deepa; K. Muthamil Sudar; P. Deepalakshmi	Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques	SVM y SOM	(Deepa, Sudar, & Deepalakshmi, 2018)
17	2018	Rohan Doshi; Noah Apthorpe; Nick Feamster	Machine Learning DDoS Detection for Consumer Internet of Things Devices	K-means, LSVM, árbol de decisión, Random forest y red neuronal.	(Doshi, Apthorpe, & Feamster, 2018)
18	2018	Obaid Rahman; Mohammad Ali Gauhar Quraishi; Chung-Horng Lung	DDoS Attacks Detection and Mitigation in SDN Using Machine Learning	J48, Random Forest, K- Means y SVM	(Rahman, Quraishi, & Lung, 2018)
19	2018	Jiangpan Hou; Peipei Fu; Zigang Cao; Anlin Xu	Machine Learning Based DDoS Detection Through NetFlow Analysis	Algoritmo C4.5	(Hou, Fu, Cao, & Xu, 2018)

Nº	Año	Autores	Titulo	Técnicas	Ref.
20	2018	Karan B. V.; Narayan D. G.; P. S. Hiremath	Detection of DDoS Attacks in Software Defined Networks	SVM y Red neuronal profunda.	(V., G., & Hiremath, 2018)
21	2018	Jarrod N. Bakker; Bryan Ng; Winston K. G. Seah	Can Machine Learning Techniques Be Effectively Used in Real Networks against DDoS Attacks?	Random Forest, K- Means y SVM	(Bakker, Ng, & Seah, 2018)

Tabla 6: ***Cantidad de las revistas sobre técnicas de detección de ataques DDoS, entre los años 2014 - 2018.***

Año de publicación de los artículos de investigación				
2014	2015	2016	2017	2018
5	2	1	5	8

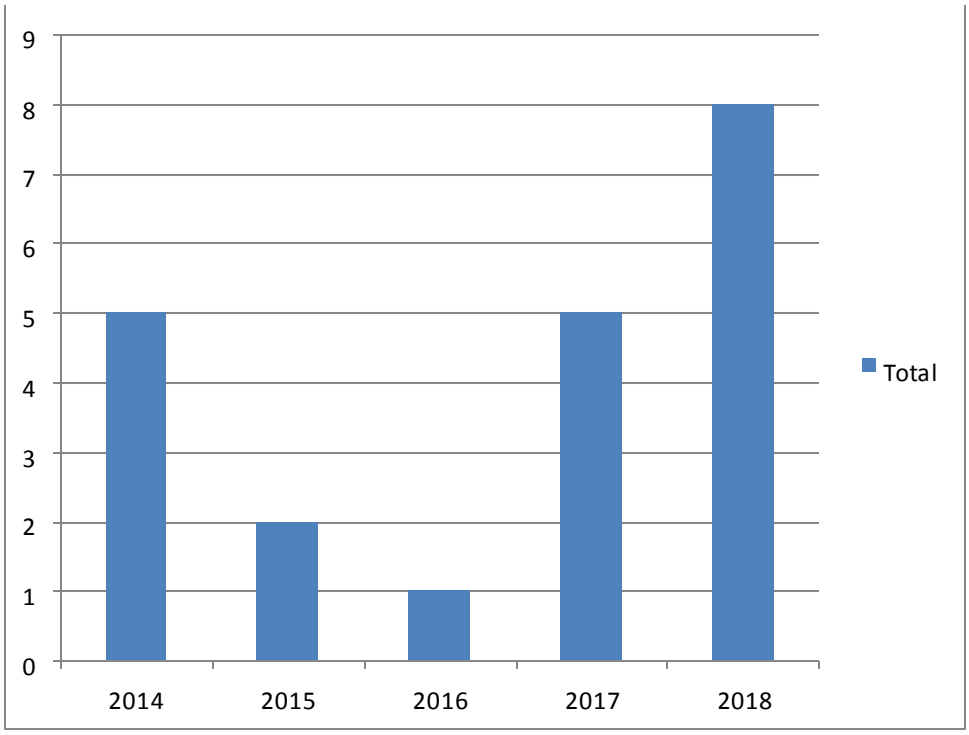

Figura 12: Cantidad de investigaciones publicadas aplicando el filtro final según la revisión.

IR 2: ¿Cuáles son las tecnicas de Deep learning que se usaron para detectar ataques distribuidos de denegación de servicios?

Las revistas bibliográficas científicas muestran información limitada acerca de las tecnicas de Deep learning en el campo de detección de ataques, debido a que estas tecnicas son mayormente utilizadas en otros campos: por ejemplo el de visión por computadora, por lo tanto se tomó en cuenta tecnicas que utilizan aprendizaje automático para esta revisión , después de haber seleccionado las revistas bibliográficas por su mejor rendimiento se hizo un filtro en que fueron utilizadas demostrando un porcentaje de precisión en sus resultados. A continuación, se presenta las distintas técnicas que fueron usadas por los diferentes investigadores.

Tabla 7: Resultado del análisis de la literatura sobre las técnicas de Deep learning en la detección de ataques DDoS.

Nº	Año	Técnicas	Uso	Eficiencia	Ref.
1	2014	Algoritmo de inspección de recuento y SVM	Detección de ataques DDoS.	98.99%	(Devi, Preetha, Selvaram, & Shalinie, 2014)
2	2014	SVM	Detección de ataques DDoS	98.07%	(Kato & Klyuev, 2014)
3	2014	Algoritmo genético y red neuronal artificial.	Detección de ataques DDoS	90.02%	(Barati, Abdullah, Udzir, Mahmod, & Mustapha, 2014)
4	2014	Árbol de decisión y Naive Bayes	Detectar ataques DDoS	90%	(Balkanli, Alves, & Zincir-Heywood, 2014)
5	2014	Redes neuronales, redes bayesianas, lógica difusa, SVM y Algoritmo genético.	Detección de ataques DDoS en redes SDN.	Mejores resultados	(Ashraf & Latif, 2014)
6	2015	Entropia y Distancia de Hellinger	Detectar ataques DDoS	89.99%	(Tsiatsikas, y otros, 2015)
7	2015	K-Means modificado	Detección de ataques DDoS	98%	(Pramana, Purwant, & Suratman, 2015)
8	2016	Autoencoder	Detección de ataques DDoS	96.99%	(Yadav & Subramanian, 2016)
9	2017	Entropia	Detección de ataques DDoS	87%	(Zubaydi, Anbar, & Wey, 2017)
10	2017	Red Neuronal Convolucional	Clasificación de spam	98.11%	(Shikhar Seth, 2017)
11	2017	Autoencoders y red de creencia profunda	Seguridad en sistemas de control de red.	94.2%	(Potluri, Henry, & Diedrich, 2017)
12	2017	Algoritmo C4.5	Detección de ataques DDoS.	98.8%	(Marwane Zekri, 2017)
13	2017	Red neuronal recurrente	Detección de ataques DDoS	97.99%	(Yuan, Li, & Li, 2017)
14	2018	Red neuronal recurrente y perceptrón multicapa.	Detección de ataques DDoS	94.74%	(Abigail Koay, 2018)
15	2018	Naive Bayes, Random Forest y árbol de decisión	Detección de ataques DDoS	97.4%	(Amjad Alsirhani, 2018)
16	2018	SVM y SOM	Detección de ataques DDoS	96.77%	(Deepa, Sudar, & Deepalakshmi, 2018)

Nº	Año	Técnicas	Uso	Eficiencia	Ref.
17	2018	K-means, LSVM, árbol de decisión, Random forest y red neuronal.	Detección de ataques DDoS	97.6%	(Doshi, Apthorpe, & Feamster, 2018)
18	2018	J48, Random Forest, K-Means y SVM	Detección de ataques DDoS	98.6%	(Rahman, Quraishi, & Lung, 2018)
19	2018	Algoritmo C4.5	Detección de ataques DDoS	99.5%	(Hou, Fu, Cao, & Xu, 2018)
20	2018	SVM y Red neuronal profunda.	Detección de ataques DDoS	92.30%	(V., G., & Hiremath, 2018)
21	2018	Random Forest, K- Means y SVM	Detección de ataques DDoS	95.08%	(Bakker, Ng, & Seah, 2018)

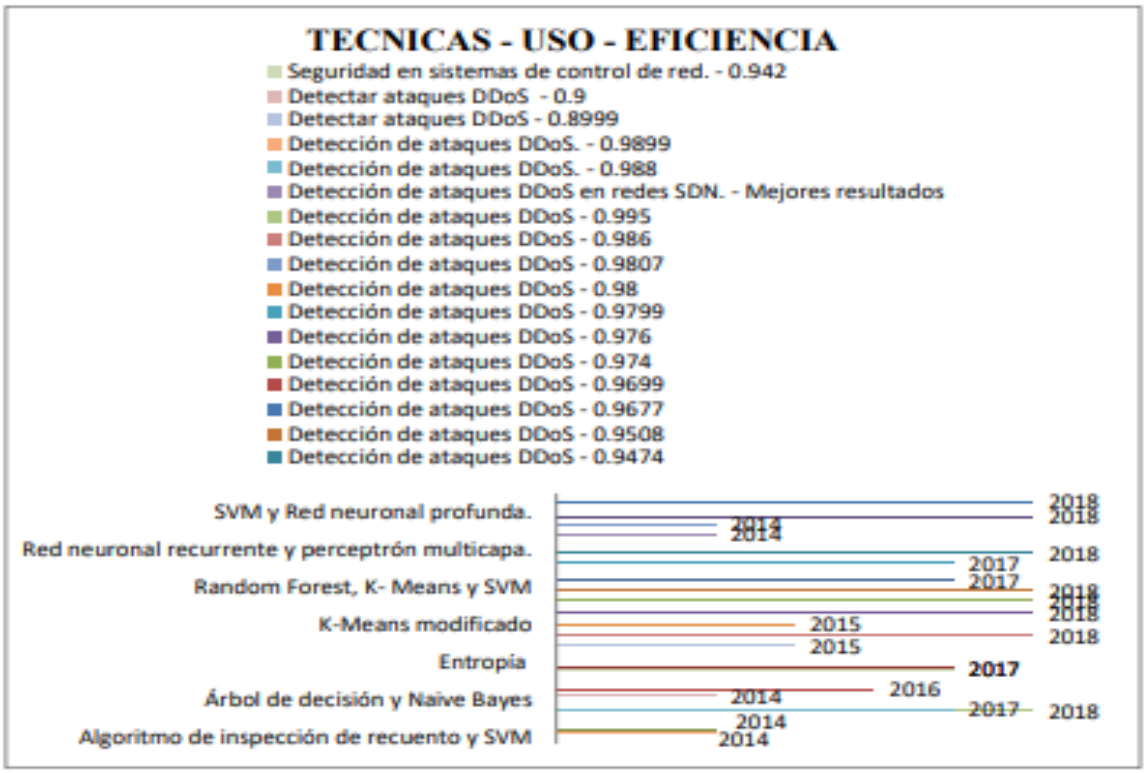

Figura 13: Resultado del análisis de eficiencia de las tecnicas de detección de ataques DDoS.

Figura 13: Resultado del análisis de eficiencia de las tecnicas de detección de ataques DDoS.

IR 3: ¿Cuantas técnicas de Deeplearning encontramos para detectar ataques DDoS? Las tecnicas de Deep learning están dando la hora en diversos campos diferentes como es el de visión por computadora y clasificación de imágenes, pero los investigadores han ido

explorando estas técnicas en la detección de ataque en especial lo DDoS, según las revisiones bibliográficas analizan estas técnicas fusionándolas con tecnicas de aprendizaje automático para obtener mejores resultados. Dentro de la presente investigación se logró encontrar 5 tecnicas que pertenecen a Deep learning.

Tabla 8: ***Resultado del filtro del uso de las técnicas de Deep learning para detectar ataques DDoS.***

Nº	Año	Técnicas	Uso	Eficiencia	Ref.
1	2016	Autoencoders	Detección de ataques DDoS	96.99%	(Yadav & Subramanian, 2016)
2	2017	Red Neuronal Convolucional	Clasificación de spam	98.11%	(Shikhar Seth, 2017)
3	2017	Autoencoders y red de creencia profunda	Seguridad en sistemas de control de red.	94.2%	(Potluri, Henry, & Diedrich, 2017)
4	2018	Red neuronal recurrente y perceptrón multicapa.	Detección de ataques DDoS	94.74%	(Abigail Koay, 2018)
5	2018	Red neuronal profunda.	Detección de ataques DDoS	92.30%	(V., G., & Hiremath, 2018)

Se hizo un filtro más definido para obtener a las técnicas de Deep learning con sus mejores resultados de las revisiones bibliográficas de acuerdo con el año en que se investigaron las técnicas.

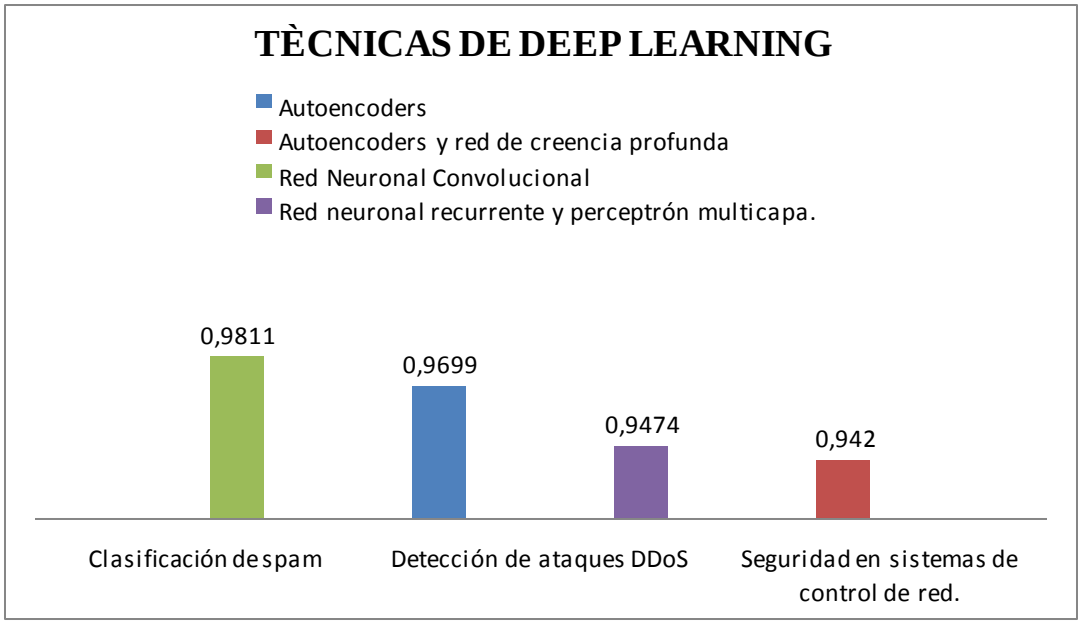

Figura 14: Resultado del análisis de las técnicas de Deep learning.

IV. CONCLUCIONES

Con base en la literatura, esta revisión bibliográfica científica presenta una serie de revisiones de artículos actualizados sobre las técnicas de Deep learning que son utilizadas en la detección de ataques distribuidos de denegación de servicios. Así mismo se detectó la limitada cantidad de tecnicas que existen sobre Deep learning y que son aplicadas en la detección de ataques; mayormente estas tecnicas son utilizadas en otros campos de investigación como clasificación de imágenes o visión por computadora.

La amenaza que trae consigo los ataques DDoS son estudiados desde hace muchos años y con el pasar del tiempo se han buscado nuevas formas o tecnicas que logren contrarrestarlos y obtener resultados mucho más favorables. Las técnicas de Deep learning le ha abierto muchas posibilidades a diversos autores los cuales quieren demostrar que estas tecnicas no solo sirven para clasificar una imagen o reconocer imágenes en movimiento.

Una de las tecnicas vistas en la presente revisión son las Redes neuronales convolucionales, las cuales alcanzan un nivel de precisión muy alto en cuanto a detección de ataques se refiere. Otra de las tecnicas importantes mencionada en esta revisión son las redes de creencia profunda, con las cuales se obtienen resultados muy buenos.

Hay que mencionar que en las revisiones bibliográficas se muestra un gran interés en el campo de inteligencia artificial, específicamente en las redes neuronales.

Por lo tanto, las técnicas más usadas sirven de como referencia a la hora de hacer la revisión científica, con el fin de obtener los mejores resultados en el proceso.

V. REFERENCIAS

Abigail Koay. (2018). A New Multi Classifier System using Entropy-based Features in DDoS Attack Detection. 6.

Amjad Alsirhani, S. S. (2018). DDoS Attack Detection System: Utilizing Classification Algorithms with Apache Spark. 8.

Ashraf, J., & Latif, S. (2014). Handling intrusion and DDoS attacks in Software Defined Networks using machine learning technique.

Bakker, J. N., Ng, B., & Seah, W. K. (2018). Can Machine Learning Techniques Be Effectively Used in Real Networks against DDoS Attacks?

Balkanli, E., Alves, J., & Zincir-Heywood, A. N. (2014). Supervised learning to detect DDoS attacks.

Barati, M., Abdullah, A., Udzir, N. I., Mahmod, R., & Mustapha, N. (2014). Distributed Denial of Service detection using hybrid machine learning technique.

Castro, J. B. (2017). A Comparative Analysis of Deep Learning Techniques for Sub-tropical Crop Types Recognition from Multitemporal Optical/SAR Image Sequences. 8.

Deepa, V., Sudar, K. M., & Deepalakshmi, P. (2018).

Deepa, V., Sudar, K. M., & Deepalakshmi, P. (2018). Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques.

Devi, B. K., Preetha, G., Selvaram, G., & Shalinie, S. M. (2014). An impact analysis: Real time DDoS attack detection and mitigation using machine learning.

Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine Learning DDoS Detection for Consumer Internet of Things Devices.

Hinton, G. &. (2006). Reducir la dimensionalidad de los datos con redes neuronales.

Hou, J., Fu, P., Cao, Z., & Xu, A. (2018). Machine Learning Based DDoS Detection Through NetFlow Analysis.

Kato, K., & Klyuev, V. (2014). Large-scale network packet analysis for intelligent DDoS attack detection development.

Krizhevsky, A. (2016). ImageNet Classification with Deep Convolutional Neural Networks.

Lacomilla, P. (2016). Deep learning: Redes convolucionales. Obtenido de https://ccc.inaoep.mx/~pgomez/deep/presentations/2016Loncomilla.pdf

LAPLANTE, J. F. (2017). Review and Analysis of Software Development Team. 18.

Li, J., Liu, Y., & Gu, L. (2010). Detection of DDoS attacks based on neural networks. 6.

M., A. B., Islam, A. A., & Sabrina, T. (2009). Detection of various denial of service attacks and distributed denial of service using RNN.

Marwane Zekri, D. E. (2017). DDoS attack detection using machine learning techniques in cloud computing environments.

Mieres, J. (2009). Ataques informáticos. http://proton.ucting.udg.mx/tutorial/hackers/hacking.pdf.

Molina, L. F. (2015). Ataques Distribuidos de Denegación de Servicios: modelación y simulación con eventos discretos.

OpenCloud. (2016). Introducción a los ataques DDoS y métodos Anti-DDoS. Obtenido de https://docs.bluehosting.cl/tutoriales/conocimientos-generales/introduccion-a-losataques-ddos-y-metodos-anti-ddos.html

Potluri, S., Henry, N. F., & Diedrich, C. (2017). Evaluation of Hybrid Deep Learning Techniques for Ensuring Security in Networked Control Systems. 8.

Pramana, M. I., Purwant, Y., & Suratman, F. Y. (2015). DDoS detection using modified Kmeans clustering with chain initialization over landmark window.

Rahman, O., Quraishi, M. A., & Lung, C.-H. (2018). DDoS Attacks Detection and Mitigation in SDN Using Machine Learning.

Shikhar Seth, S. B. (2017). Multimodal Spam Classification Using Deep Learning Techniques. 4.

Torres, J. (2018). DEEP LEARNING Introducción práctica con Keras.

Tsiatsikas, Z., Fakis, A., Papamartzivanos, D., Geneiatakis, D., Kambourakis, G., & Kolias, C. (2015). Battling against DDoS in SIP: Is Machine Learning-based detection an effective weapon?

V., K. B., G., N. D., & Hiremath, P. S. (2018).

Vieites, Á. G. (2015). Enciclopedia de la Seguridad Informática. 2ª edición.

Wang , W., & Gombault, S. (2008). Efficient detection of DDoS attacks with important attributes.

Yadav, S., & Subramanian, S. (2016). Detection of Application Layer DDoS attack by feature learning using Stacked AutoEncoder.

Ye , Q., & Doermann, D. (2015). Text Detection and Recognition in Imagery: A Survey, 21.

Yuan, X., Li, C., & Li, X. (2017). DeepDefense: Identifying DDoS Attack via Deep Learning. 8.

Yun Lin, J. W. (2014). Research on Text Classification Based on SVM-KNN. 3.

Zhiquan Wang, Z. Q. (2017). Research on Web Text Classification Algorithm Based on Improved CNN and SVM. 4.

Zubaydi, H. D., Anbar, M., & Wey, C. Y. (2017). Review on Detection Techniques against DDoS Attacks on a Software-Defined Networking Controller.