FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TRABAJO DE INVESTIGACIÓN

Detección de Ataques Distribuidos de Denegación de Servicios en Servidores web utilizando algoritmos de Machine Learning

PARA OPTAR EL GRADO ACADÉMICO DE BACHILLER EN INGENIERÍA DE SISTEMAS

Autor(es)

Huaman Guerrero Lili Yanina

https://orcid.org/0009-0007-7047-848X

Montalvan Ramos Jesus Alexander

https://orcid.org/0009-0004-3805-6525

Asesor

Dr. Forero Vargas Manuel Guillermo

https://orcid.org/0000-0001-9972-8621

Línea de investigación

Tecnología e innovación en desarrollo de la construcción y la industria en un contexto de sostenibilidad

SubLínea de investigación

Innovación y tecnificación en ciencia de los materiales, diseño e infraestructura

Pimentel – Perú

2024

Huaman Guerrero / Montalvan Ra

Detección de Ataques Distribuidos de Denegación de Servicios en Servidores web utilizando algoritmos

Universidad Señor de Sipan

Detalles del documento

Identificador de la entrega
trn:oid:::26396:409313171

Fecha de entrega
25 nov 2024, 9:09 a.m. GMT-5

Fecha de descarga
25 nov 2024, 9:10 a.m. GMT-5

Nombre de archivo
tesis -turnitin.docx

Tamaño de archivo
1.7 MB

32 Páginas

6,822 Palabras

37,678 Caracteres

17% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto mencionado
- Coincidencias menores (menos de 8 palabras)

Fuentes principales

13% Fuentes de Internet
6% Publicaciones
10% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

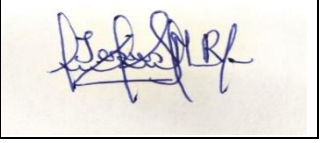
DECLARACIÓN JURADA DE ORIGINALIDAD

Quien(es) suscribe(n) la **DECLARACIÓN JURADA**, somos Lili Yanina Huaman Guerrero, Jesús Alexander Montalvan Ramos del Programa de Estudios de Ingeniería de Sistemas de la Universidad Señor de Sipán, declaro (amos) bajo juramento que soy (somos) autor(es) del trabajo titulado:

DETECCIÓN DE ATAQUES DISTRIBUIDOS DE DENEGACIÓN DE SERVICIOS EN SERVIDORES WEB UTILIZANDO ALGORITMOS DE MACHINE LEARNING

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán (CIEI USS) conforme a los principios y lineamientos detallados en dicho documento, en relación a las citas y referencias bibliográficas, respetando al derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y auténtico

En virtud de lo antes mencionado, firman:

Huaman Guerrero Lili Yanina	DNI: 71862573	
Montalvan Ramos Jesus Alexander	DNI: 77238711	

Pimentel, 13 de septiembre de 2024

Dedicatoria

A Dios por regalarnos el privilegio de la vida, a mi familia por ser ese pilar de soporte y apoyo para poder lograr mis objetivos.

Huaman Guerrero Lili Yanina.

A Dios por haberme permitido llegar a este momento, por darme la salud para alcanzar mis metas.

Montalvan Ramos Jesus Alexander.

Agradecimientos

Agradezco profundamente a Dios por permitirme alcanzar una meta que muchas personas sueñan y anhelan.

A mis padres, por su esfuerzo incansable para formar en mí una persona de bien, y a todos aquellos que me brindaron su apoyo para hacer de este logro una realidad.

A mis profesores, por su constante dedicación en inculcar valores en mí.

INDICE

INDICE DE TABLA

INDICE DE FIGURAS

Resumen

Los ataques DDoS, representan una amenaza significativa en el campo de la ciberseguridad, debido a su capacidad para interrumpir servicios legítimos y causar daños financieros y reputacionales. Estos ataques se efectúan al comprometer múltiples dispositivos que envían tráfico masivo para saturar los sistemas. A pesar de los avances en las tecnologías de protección y en las técnicas de mitigación, estos ataques siguen evolucionando y presentan desafíos constantes para la seguridad.

Las técnicas de machine learning, como XGBoost , AdaBoost y perceptrón multicapa, se emplean se utilizan para mitigar y detener estos ataques. El perceptrón multicapa ha mostrado una alta precisión, alcanzando el 91,2%, mientras que otros modelos también ofrecen buenos resultados, pero con algunas limitaciones. La implementación de filtros adaptativos y estrategias de defensa en capas ha sido efectiva para reducir el tráfico de ataque y limitar el daño colateral.

Eventos recientes, como el ataque DDoS a CloudFlare en 2023, que superó los 71 millones de solicitudes por segundo, demuestran la creciente sofisticación de estos ataques. A pesar de las medidas adoptadas, incluyendo modelos matemáticos y técnicas de aprendizaje automático para detectar ataques con alta precisión, la amenaza sigue siendo un desafío. Para enfrentar y mitigar los ataques DDoS de manera efectiva, es crucial combinar técnicas avanzadas de aprendizaje automático con estrategias de defensa en capas.

Palabras Clave: DDoS, Servidores web, Machine learning, Mitigación

Abstract

DDoS attacks represent a significant threat in the field of cybersecurity due to their ability to disrupt legitimate services and cause financial and reputational damage. These attacks are executed by compromising multiple devices that generate massive traffic to overwhelm systems. Despite advancements in protective technologies and mitigation techniques, these attacks continue to evolve and present ongoing security challenges.

Machine learning techniques, such as XGBoost, AdaBoost, and multilayer perceptrons, are employed to mitigate and prevent these attacks. The multilayer perceptron has demonstrated high accuracy, achieving 91.2%, while other models also provide good results but with some limitations. The implementation of adaptive filters and layered defense strategies has proven effective in reducing attack traffic and limiting collateral damage.

Recent events, such as the 2023 DDoS attack on Cloudflare, which exceeded 71 million requests per second, highlight the increasing sophistication of these attacks. Despite adopted measures, including mathematical models and machine learning techniques for precise attack detection, the threat remains a challenge. To effectively address and mitigate DDoS attacks, it is crucial to combine advanced machine learning techniques with layered defense strategies

Keywords: DDoS, Web servers, Machine learning, Mitigation

I. INTRODUCCIÓN

1.1. Realidad Problemática

Los ataques distribuidos de denegación de servicio (DDoS) representan una de las mayores preocupaciones para los especialistas en seguridad informática, debido a su alta frecuencia y a su capacidad para interrumpir el acceso legítimo a los servicios. Estos ataques logran su efectividad mediante la explotación de vulnerabilidades en un gran número de equipos, que son comprometidos y configurados para formar un "ejército" que ejecuta los ataques de manera coordinada y masiva.

Al desarrollar defensas contra ataques predefinidos y predecibles es unos de los objetivos deseables por parte de la comunidad dedicada a la prevención y detección de intrusiones, dada la vulnerabilidad inherente de los sistemas centralizados de control. Con el avance en la inteligencia de los conmutadores y su separación, los atacantes han aumentado su interés en saturar tanto los datos como el plano de control, utilizando para ello ataques DDoS [1]. Unos de los aspectos claves a considerar al usar una nube o un servidor web es la seguridad, la accesibilidad, la disponibilidad y la integración, ya que debido a cualquier ataque al servidor alojado en la nube pueden causar tiempo de inactividad, lo que puede provocar daños financieros y de reputación [2]

A pesar de los avances en técnicas de aprendizaje automático, se han identificado limitaciones significativas en la literatura existente. Estas limitaciones incluyen el manejo inadecuado de datos faltantes y valores atípicos, la selección arbitraria de hiperparámetros, y la falta de una evaluación exhaustiva del tiempo de respuesta y el rendimiento de los modelos. La magnitud y sofisticación de estos ataques se evidencian en incidentes como el ataque DDoS a CloudFlare en 2023, que superó los 71 millones de solicitudes por segundo, así como en el impacto sobre la empresa desarrolladora de ChatGPT. Estos eventos destacan la creciente complejidad y el desafío que representan los ataques DDoS en el panorama actual de la ciberseguridad [3]

En este contexto, los ataques DDoS representan una amenaza considerable para los servidores web, especialmente para los servidores de nombres raíz DNS, debido a su vulnerabilidad a direcciones IP fijas y tráfico UDP falsificado. Un estudio reciente desarrolló una estrategia de defensa en capas que emplea una biblioteca de filtros adaptativos, optimizados para distintos tipos de ataques. Esta estrategia ha demostrado ser altamente efectiva, logrando reducir el tráfico de ataque a un

rango manejable y mantener el daño colateral por debajo del 2%, incluso en pruebas con ataques reales [4].

Para el desarrollo de la industria de diversos dominios es crucial la utilización de machine learning ya que puede allanar el camino hacia nuevas direcciones de investigación y ayudar la detención de los ataques DDoS en los servidores web ya que está generando nuevos desafíos y problemas para la comunidad. Según un informe público de los servicios web de Amazon, el mayor ataque DDoS masivo registrado hasta el momento tuvo lugar en febrero de 2020. Para realizar esta tarea, los atacantes cibernéticos utilizan servidores web CLDAP pirateados, esto dificulta la prevención de ataques, la detección y mitigación de DDoS. [5]

Los autores [2], en la investigación, “A Review on Defense Mechanisms Against Distributed Denial of Service (DDoS) Attacks on Cloud Computing”, el 2021; Indicaron que, en los últimos años se han dirigido principalmente a la infraestructura de la nube. La investigación mostró que algunos ataques DDoS no se pueden prevenir, detectar o mitigar, en la cual estos son los que comienzan con una dirección IP legítima o cuya firma no se almacena en la base de datos de firmas de la instalación. Es por ello que, propusieron un mecanismo de detección basado en Fuzzy diseñado para detectar ataques DDoS en servidores web al filtrar los paquetes entrantes antes de llegar a la nube. Además, analizaron el comportamiento dinámico del paquete y mediante el mismo se procesó un informe de los hallazgos del problema al administrador del servidor web. Así mismo este modelo de prueba se basó en el modelo combinado de IRC, AH e Internet para detectar botnet y darknet desde la dirección IP en el servidor. También ayudó a detectar el 86 % de la fuente de ataque e hizo que el sistema se bloquee en esa ruta de origen para optimizar la eficiencia de la detección del ataque.

Otros autores [6], en la investigación, “DDOS Attack Identification using Machine Learning Techniques”, realizado en 2021; argumentaron que, la mayoría de ataques están diseñados para cerrar un servidor y también pueden cerrar temporalmente los servicios más importantes que debe proporcionar. Por lo cual, plantearon el uso de técnicas de aprendizaje automatico como AdaBoost y XGBoost a tales problemas de clasificación, indicaron que los bosques aleatorios también ayudan con una clasificación muy precisa a este tipo de problemas, en la cual las redes neuronales, como los modelos de perceptrón multicapa, también se utilizaron para este problema de clasificación. Al final, AdaBoost una precisión del 87,5 %, Random Forest alcanzó el 89,65 %, y el perceptrón multicapa logró un 91,2 % en

comparación con bases de datos de firmas anteriores. Aunque XGBoost, Random Forest y AdaBoost demostraron buenos resultados, el perceptrón multicapa no fue tan efectivo.

Sin embargo [7], indicaron que los ataques DDoS representan uno de los problemas de seguridad más difíciles de identificar, mitigar y rastrear en la actualidad. Aunque la aplicación de estrictos estándares de seguridad, como firewalls y soluciones específicas del proveedor, puede ayudar, los atacantes a menudo infectan sistemas confiables mediante troyanos y software malicioso. Por ello, propusieron dos modelos para la identificación de ataques DDoS: un modelo matemático y un modelo de aprendizaje automático. El modelo matemático examina la relación entre el tiempo de llegada de las solicitudes y el rendimiento del sistema. Entre los modelos de aprendizaje automático propuestos fueron la regresión logística y Naive Bayes. Los resultados indicaron que el modelo matemático logró una precisión de 99,75 %, mientras que la regresión logística presentó una precisión en el rango de 99 % y el 100 %, y Naive Bayes logró una precisión entre el 98 % y el 99 %. La regresión logística demostró un rendimiento superior en comparación con Naive Bayes.

[8] abordaron la amenaza persistente de los ataques DDoS, que continúan poniendo en riesgo servidores y dispositivos de red. Por ello, propusieron cuatro técnicas para mejorar la detección de paquetes maliciosos: basadas en estadísticas, conocimientos, informática de software y machine learning utilizando n-gramas. Los resultados mostraron que las técnicas 2-Gram y 3-Gram fueron las más efectivas, alcanzando una precisión de detección del 99,98 %, superior al 98,7 % obtenido en investigaciones anteriores.

Según lo planteado en la investigación [9] titulada “A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks” (2022), realizada en Pakistán, la detección de intrusos es un problema complejo de clasificación que requiere una implementación precisa de algoritmos. Por ello, propusieron mejorar la precisión de los modelos mediante la aplicación de técnicas de organización del tráfico y estrategias de preprocesamiento, logrando una mejora de hasta el 45 %. Además, se observó que los métodos actuales, basados en esteganografía de imágenes y técnicas de *machine learning*, demostraron que el modelo XGBoost es particularmente eficaz para la detección de ataques DDoS. Los modelos supervisados superaron a las técnicas no supervisadas en rendimiento. Sin embargo, la eficacia de estos modelos está condicionada por la calidad del conjunto

de datos utilizado durante las fases de entrenamiento y prueba. El estudio subrayó la importancia de proporcionar soluciones de detección más accesibles y rápidas que los métodos de aprendizaje profundo, y la necesidad de avanzar del aprendizaje no supervisado hacia el aprendizaje supervisado, tanto para conjuntos de datos etiquetados como no etiquetados.

En otros estudios [10], indicaron que los ataques DDoS siguen representando un desafío significativo para los proveedores de servicios de Internet. Estos ataques suelen estar dirigidos a servidores web de organizaciones importantes como bancos, corporaciones, medios de comunicación y entidades gubernamentales. Aunque estos ataques rara vez resultan en el robo o pérdida de información crítica, pueden causar daños considerables a la reputación de las víctimas y generar costos elevados en términos de tiempo y recursos para manejar las consecuencias. Para abordar este problema, los estudios analizaron mecanismos de defensa contra ataques DDoS, clasificándolos en dos grupos principales: según el nivel de actividad y según la ubicación. La primera categoría se divide en mecanismos preventivos y reactivos, mientras que la segunda categoría se basa en la ubicación, diferenciando entre la red de la víctima y la red intermedia. Los resultados mostraron una tasa de correlación del 84,22 %, indicando una alta precisión en la detección de ataques. Sin embargo, el 15,78 % de los mecanismos revisados presentaron errores en la precisión detectada. Estos hallazgos proporcionan a los investigadores una comprensión más detallada de los mecanismos de defensa contra DDoS y sugieren áreas de mejora para aumentar la precisión y eficacia de estos sistemas en el futuro.

La presente investigación es esencial y oportuna debido al creciente número y sofisticación de los ataques distribuidos de denegación de servicio (DDoS), los cuales representan una amenaza significativa para la estabilidad y seguridad de los servidores web. Este estudio no solo ofrece una visión clara sobre qué algoritmos y modelos han demostrado mejor rendimiento en la detección de DDoS, sino que también establece una base sólida para futuras investigaciones y desarrollos en esta área crítica.

1.2. Formulación del Problema

¿Cómo identificar en forma eficiente los ataques distribuidos de denegación de servicio usando algoritmos de machine learning?

1.3. Hipótesis

Mediante el uso de algoritmos de machine learning se identificará con eficiencia los ataques distribuidos de denegación de servicios en servidores web.

1.4. Objetivos

1.4.1. Objetivos Generales

Realizar un análisis sobre la detección de ataques distribuidos de denegación de servicio en servidores web, aplicando algoritmos de machine learning.

1.4.2. Objetivo Específicos

a) Caracterizar las técnicas de clasificación de tráfico web en ataques DDoS
b) Evaluar los algoritmos de machine learning más efectivos para la detección de ataques DDoS.
c) Revisar los modelos propuestos para la detección de ataques DDoS

1.5. Teorías relacionadas al tema

1.5.1. Ataques DDoS

Son ataques que provienen de diferentes fuentes combinados en un solo flujo en el punto final, donde varios atacantes realizan el envío de solicitudes. Estos ataques suelen llevarse a cabo mediante bots, que habitualmente consisten de computadoras infectadas y es controlada de forma remota por los atacantes. Cuando el ataque tiene éxito, y el servidor o los servidores quedan inoperativos, los sitios web afectados no volverán a funcionar correctamente hasta que se detenga el ataque o se bloqueen las conexiones maliciosas [11].

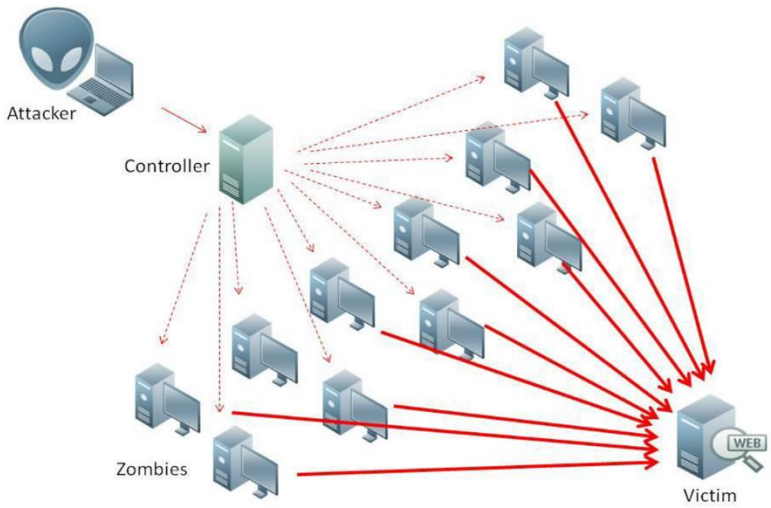


Figura 1: Ataque DDoS a servidores web. Fuente:[12]

¿Cómo funcionan los ataques DDoS?

A diferencia de otros tipos de ciberataques, los ataques DDoS no se basan en explotar vulnerabilidades particulares en los sistemas informáticos. En cambio, emplean protocolos de red estándar, como el Protocolo de Transferencia de Hipertexto (HTTP) y el Protocolo de Control de Transmisión (TCP), para inundar endpoints, aplicaciones y otros activos con un volumen de tráfico superior a su capacidad de procesamiento. Los servidores web, enrutadores y otras infraestructuras de red tienen una capacidad finita para manejar solicitudes y mantener conexiones simultáneas. Al saturar el ancho de banda disponible de estos recursos, los ataques DDoS bloquean su capacidad para responder a solicitudes y paquetes de conexión legítimos [13].

Tipos de Ataques DDoS

Según el autor [14] ,existen diversos tipos de ataques DDoS, cada uno con métodos específicos para saturar y afectar los sistemas y servicios en línea. A continuación se presentan algunos de los más comunes:

Ataques de inundación de tráfico:

- **Inundación SYN:** Este ataque explota el protocolo TCP al enviar una gran cantidad de solicitudes sincronizadas al servidor sin completar el proceso de conexión, lo que agota los recursos del servidor y lo deja fuera de servicio.
- **Inundación UDP:** Consiste en inundar al servidor objetivo con un alto volumen de paquetes basados en el Protocolo de Datagrama de Usuario. Debido a que UDP carece de mecanismos de control de congestión, el servidor puede quedar sobrecargado.
- **Inundación ICMP:** Consiste en enviar paquetes fraudulentos basados en el Protocolo de mensajes de control de Internet, que suelen utilizarse para pings o trazas de red. La sobrecarga de estos paquetes puede saturar los recursos del servidor.

Ataques de agotamiento de recursos:

- **Agotamiento de ancho de banda:** Se refiere a la situación en la que la cantidad de datos que se pueden transmitir a través de una red se utiliza por completo, lo que provoca una disminución en el rendimiento y lentitud en la transmisión de información.

- ❖ **Agotamiento de recursos del servidor:** Esto ocurre cuando un servidor se queda sin los recursos necesarios para manejar todas las solicitudes que recibe, como el almacenamiento, la memoria RAM y el ancho de banda. Lo que puede ralentizar o inutilizar el servidor

Ataques de capa de aplicación:

- **Inundación HTTP/HTTPS:** Se enfoca en consumir los recursos de un servidor web mediante el envío masivo de peticiones HTTP o HTTPS. Esto abruma al servidor con un alto volumen de solicitudes, lo que puede causar que el servicio web se vuelva lento o incluso se caiga.
- **Amplificación DNS:** Se aprovechan configuraciones incorrectas en servidores, para enviar respuestas exageradas a la víctima. El atacante envía consultas pequeñas ya que responden con datos mucho mayores. Este tipo de ataque puede generar una sobrecarga considerable en el sistema.

1.5.2. Efectos de los ataques DDoS.

Según el autor [15], indica que, existen variedades de efectos, pero dependiendo de la naturaleza del ataque, que son las siguientes:

a) Tiempo de inactividad del sitio web: Esto significa que no podrá acceder a ningún negocio que gane a través de su sitio web, hasta que el sitio web vuelva a estar en funcionamiento, lo cual afectaría su reputación como propietario del sitio.

b) Problemas con el servidor y el alojamiento: Si el sitio web experimenta regularmente ataques que no toma medidas para mitigar, esto podría generar conflictos con su proveedor de alojamiento. Pero un buen host le brindará las herramientas adecuadas para defender el contra ataques DDoS.

c) Debilidad del Sitio Web: Un ataque DDoS puede aumentar la vulnerabilidad de un sitio al concentrar todos los esfuerzos en restaurar su funcionamiento, lo que puede desviar la atención de los sistemas de seguridad y hacer que estos resulten ineficaces durante el ataque.

d) Pérdida de tiempo y recursos: Arreglar un sitio web afectado por DDoS lleva tiempo, eso puede ocasionar pérdida de tiempo y ganancias en la

cual puede ocasionar que la empresa u organización pierda reputación y su nivel de competencia.

1.5.3. Impactos de los ataques DDoS

Los casos de ataques DDos a empresas de medios o grupos de derechos humanos son motivo de preocupación, pero hay varios aspectos a considerar: en primer lugar, dada las circunstancias en las que se producen estos ataques, cuando más prolongado sea el impacto de un ataque DDoS menos daño técnico puede tener y mayor será el impacto emocional.

Sin embargo, al monitorear activamente su trabajo, la organización o movimiento atacado puede censurarse a sí mismo en el futuro, lo que se denomina efecto escalofriante. A nivel técnico muchos grupos no tienen las mismas capacidades técnicas y recursos que los atacantes.

En caso de un ataque DDoS deben abordarse inmediatamente técnicas en los cuales son los siguientes:

- Cambiar el proveedor de alojamiento web.
- Pida ayuda a un experto en seguridad digital.
- Realice cambios en su comportamiento organizacional.
- Comprenda lo que sucede dentro de su organización y desarrolle funciones para mitigar futuros ataques.

Un ataque distribuido de denegación en el servidor web de una organización con personal mínimos y recursos limitados no es lo que necesitan además de los muchos problemas que pueden enfrentar [16].

1.5.4 Clasificación de ataque DDos.

Los ataques distribuidos de denegación de servicio (DDoS) se pueden clasificar en diferentes categorías basadas en el nivel del protocolo que atacan y el impacto que tienen sobre los recursos del servidor. A continuación, se presentan las principales clasificaciones de estos ataques:

A. Ataques DDoS en la Capa de Transporte

Estos ataques utilizan protocolos de transporte como TCP y UDP para llevar a cabo la denegación de servicio. Los tipos comunes de ataques en esta categoría incluyen:

- **Inundación SYN:** Los ataques de inundación SYN son realizados típicamente por botnets que consumen los recursos del servidor al explotar el proceso de enlace de tres vías del protocolo TCP. Este ataque se lleva a cabo enviando una gran cantidad de paquetes SYN al servidor objetivo a alta velocidad. Los atacantes nunca completan el proceso de enlace de tres vías, lo que provoca que el servidor se vea abrumado, resultando en fallos, reinicios o una degradación general del rendimiento de la red.
- **Inundación UDP:** En un ataque de inundación UDP, un host remoto envía numerosos paquetes UDP a puertos aleatorios en la máquina de destino a una velocidad extremadamente alta. Este tipo de ataque agota el ancho de banda de la red disponible, causando bloqueos y una notable reducción en el rendimiento del sistema.

B. Ataques por Capa de Aplicación

Los ataques de esta categoría están enfocados en los recursos específicos de las aplicaciones que se ejecutan en un servidor.

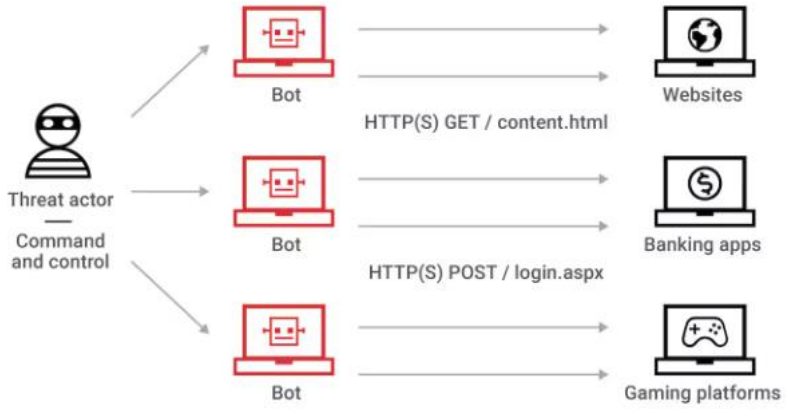


Figura 2: Ataques por Capa de Aplicación. Fuente: [17]

Se dividen en dos subcategorías principales:

- **Ataques de Gran Volumen a la Capa de Aplicación:** Estos ataques son similares a los ataques DDoS tradicionales en cuanto a que involucran grandes volúmenes de tráfico, como solicitudes HTTP GET y POST, dirigidas a la víctima. Sin embargo, a diferencia de otros ataques, estos están específicamente diseñados para consumir

los recursos de la aplicación y pueden requerir menos tráfico malicioso para causar un impacto significativo.

- **Ataques de Bajo Volumen a la Capa de Aplicación**: Estos ataques se caracterizan por la pequeña cantidad de tráfico necesaria para comprometer a la víctima. Se pueden clasificar en tres tipos:
  - Ataques de baja velocidad que envían tráfico en pulsos periódicos de corta duración.
  - Ataques de baja velocidad que explotan los parámetros de sincronización del lado del servidor enviando o recibiendo tráfico más lento de lo esperado.
  - Ataques de un solo disparo que dañan a las víctimas en una sola solicitud [18].

C. Clasificación de Ataques según Capas del Modelo OSI

Adicionalmente, es útil agrupar los ataques DDoS en función de las capas del modelo OSI que afectan, lo que permite una comprensión más detallada de su impacto:

#	Capa	Aplicación	Descripción	Ejemplo de vector
7	Aplicación	Datos	Procesamiento de red para la aplicación	Inundaciones HTTP, inundaciones de consultas DNS
6	Presentación	Datos	Representación de datos y cifrado	Abuso de SSL
5	*Sesión*	*Datos*	*Comunicación entre hosts*	*N/D*
4	Transporte	Segmentos	Conexiones integrales y confiabilidad	Inundaciones SYN
3	Red	Paquetes	Determinación de la ruta y direccionamiento lógico	Ataques de reflexión UDP
2	*Enlace de datos*	*Marcos*	*Direccionamiento físico*	*N/D*
1	*Físico*	*Bits*	*Medios, señal y transmisión binaria*	*N/D*

Figura 3: Modelo OSI (Interconexión de Sistemas Abiertos). Fuente: [19]

- **Ataques a la capa de infraestructura**

Los ataques dirigidos a las capas 3 y 4 del modelo OSI son conocidos como ataques a la infraestructura, y suelen ser los más frecuentes en el ámbito de los ataques DDoS. Entre estos se encuentran vectores como las inundaciones SYN y los ataques con paquetes de datagramas de usuario (UDP). Este tipo de ataques generalmente se caracterizan por su alto volumen, con el objetivo de saturar la capacidad de red o del servidor de la aplicación

- **Ataques a la capa de aplicación**

Los ataques que se dirigen a las capas 6 y 7 se conocen como ataques a la capa de aplicación. Aunque menos comunes, estos ataques son más sofisticados y específicos. A diferencia de los ataques a la infraestructura, suelen tener un volumen menor, pero se dirigen a componentes críticos y costosos de las aplicaciones, impidiendo el acceso de usuarios legítimos. [19].

1.5.5. Arquitecturas de Ataques DDoS

A continuación, se presentan diversas arquitecturas utilizadas en ataques distribuidos de denegación de servicio (DDoS), cada una con características y mecanismos específicos: [20]

A. Arquitectura Centralizada de Ataques DDoS

Una arquitectura de ataque DDoS centralizada incluye cuatro componentes principales: el atacante, el servidor objetivo, la botnet y el sistema de Comando y Control (C&C). En esta configuración, el atacante utiliza el sistema C&C para controlar y coordinar la botnet en tiempo real, como se muestra en la Figura 4. En este modelo, los zombis, que son las máquinas controladas por la botnet, no se comunican directamente entre sí.

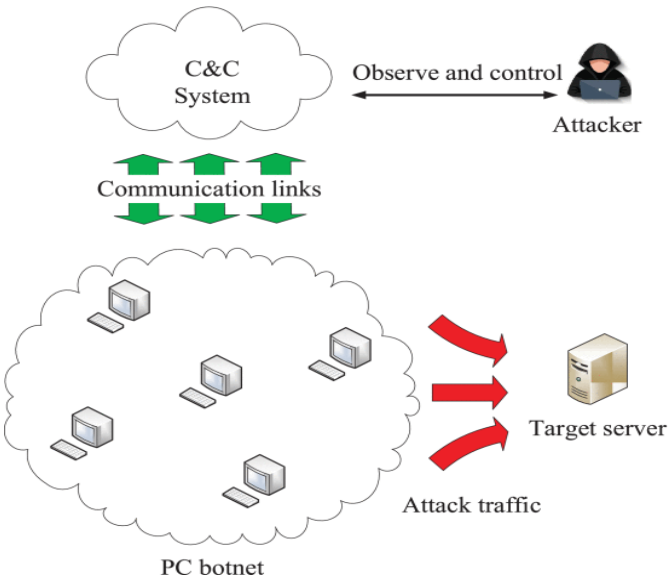


Figura 4: Diagrama de la arquitectura de ataque DDoS centralizado.
Fuente:[20]

Esta arquitectura presenta varias ventajas. Primero, la botnet es difícil de detectar ya que no hay comunicación directa entre los zombis que pueda ser monitoreada. Segundo, la gestión en tiempo real permite al atacante adaptar su estrategia de ataque de manera flexible y dinámica.

B. Arquitectura Descentralizada de Ataques DDoS

Para aumentar la resistencia y robustez de la botnet, se han desarrollado arquitecturas de ataque DDoS descentralizadas. Una configuración típica de esta arquitectura consta de tres elementos: el atacante DDoS, el servidor objetivo y la botnet, como se ilustra en la Figura 5. En esta arquitectura, todas las máquinas de la botnet forman una red de comunicación peer-to-peer (P2P). El atacante gestiona indirectamente la botnet a través de esta red P2P, emitiendo consultas o instrucciones de ataque a una máquina específica que luego se propagan a las demás máquinas dentro de la red.

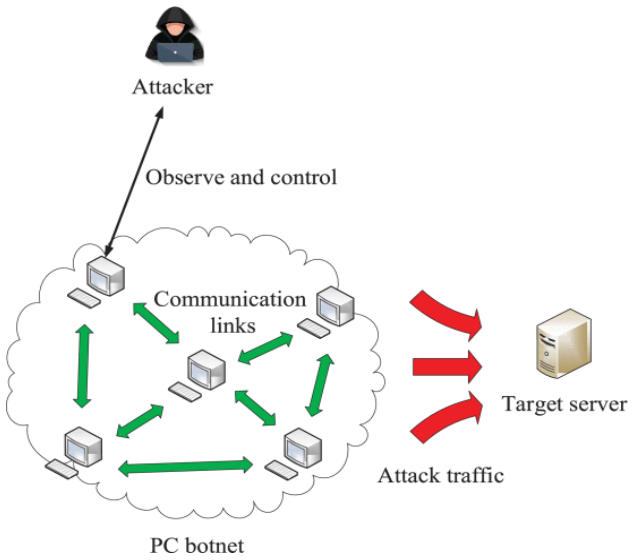


Figura 5: Diagrama de la arquitectura de un ataque DDoS descentralizado. Fuente:[20]

C. Nueva Arquitectura de Ataque DDoS

Para diseñar una arquitectura de ataque DDoS eficiente y de bajo costo, se deben considerar simultáneamente tres propiedades: bajo costo de administración, indetectabilidad y alta robustez. En respuesta a estas necesidades, se propone una nueva arquitectura de ataque DDoS que se detalla a continuación.

Esta nueva arquitectura también consta de tres componentes: el atacante DDoS, el servidor objetivo y la botnet, como se muestra en la Figura 6. En esta configuración, el atacante no gestiona activamente la botnet. En lugar de eso, el atacante crea un malware bots con un módulo de ataque predefinido que implementa una estrategia de ataque específica. Una vez desplegado, el malware sigue esta estrategia de manera autónoma, lo que simplifica la administración del ataque y reduce el costo asociado.

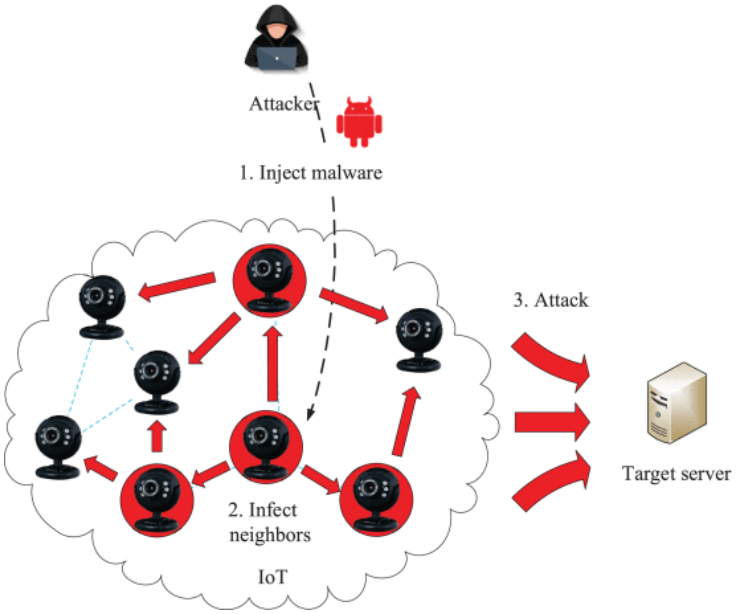


Figura 6: Diagrama de la nueva arquitectura de ataque DDoS. Fuente:[20]

1.5.6. Etapas de Mitigación de DDoS en servidores Web

- Detección: La identificación temprana de ataques DDoS se logra mediante herramientas de análisis de comportamiento de usuarios y entidades (UEBA), que aplican algoritmos de aprendizaje automático para detectar irregularidades en el tráfico de red y servidores.
- Respuesta: Una vez detectada una amenaza DDoS, es fundamental actuar rápidamente para mitigar el ataque. Esto generalmente se realiza desviando o absorbiendo el tráfico malicioso dirigido al servidor o a otro objetivo específico. Una técnica común es el enrutamiento DNS, ya que este mecanismo está siempre activo y es efectivo para manejar ataques tanto a nivel de aplicación como de red.

- ❖ Filtrado: El filtrado del tráfico permite distinguir entre tráfico legítimo y malicioso. Esto se realiza bloqueando el tráfico malicioso mientras se asegura que los usuarios legítimos no experimenten interrupciones.
- ❖ Análisis: Para mejorar la defensa contra futuros ataques DDoS, es esencial analizar el ataque y la respuesta de seguridad implementada. Este análisis se realiza recopilando datos sobre el ataque, incluidos los registros del sistema.

1.5.7. Machine Learning

Es una rama de la inteligencia artificial, permite a los algoritmos identificar patrones recurrentes en conjuntos de datos. Estos datos pueden incluir palabras, números, estadísticas, imágenes, entre otros. Los algoritmos de aprendizaje automático tienen la capacidad de aprender y realizar tareas de manera autónoma [21]

Tipos de Algoritmos

Red neuronal:

El modelo red neuronal artificial, consta de cuatro componentes principales: Primero, un conjunto de sinapsis o conexiones que regulan la actividad neuronal. Segundo, un sumador que integra todas las entradas del núcleo con sus respectivas sinapsis. Tercero, funciones de activación no lineales que limitan la amplitud de la salida de la red neuronal. Finalmente, un umbral externo que determina cuándo se activa una neurona [22].

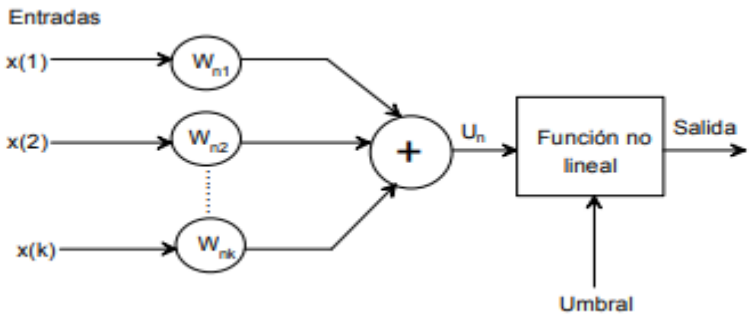


Figura 7: Esquema de un modelo neuronal. Fuente: [22]

Random forest

El RF es un método de ensamblaje compuesto por una colección de árboles de decisión. Son clasificadores que utilizan un enfoque de divide y vencerás.

Los datos se dividen en cada nodo y la selección se realiza en las hojas. RF emplea técnicas de bagging y aleatoriedad para combinar las predicciones de los árboles de decisión y reducir el sesgo general de un único árbol [23].

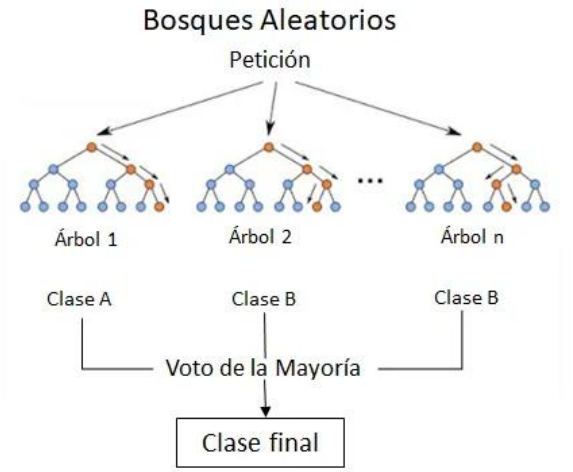


Figura 8: Esquema de Random forest. Fuente: [24]

K Vecinos Más Cercanos

El KNN es un algoritmo de aprendizaje supervisado, que se utiliza en los conflictos de regresión y clasificación. El algoritmo selecciona un punto de datos y encuentra los k vecinos más cercanos. La nueva entrada se clasifica según la clase mayoritaria de los vecinos. Generalmente, valores pequeños de k conducen a un modelo subajustado, mientras que valores altos aumentan el sesgo y el tiempo de computación. Es crucial elegir el valor óptimo de k para obtener el mejor rendimiento del clasificador [23]

LightGBM

LGBM, desarrollado por Microsoft, es un tipo de árbol de decisión impulsado por gradient boosting. Los árboles de decisión en general identifican divisiones que generan el mayor cambio en la entropía o la mayor ganancia de información antes y después de cada división. Se utiliza un algoritmo basado en histogramas o preordenado para calcular la mejor división, lo que puede ser muy lento con conjuntos de datos grande s [23].

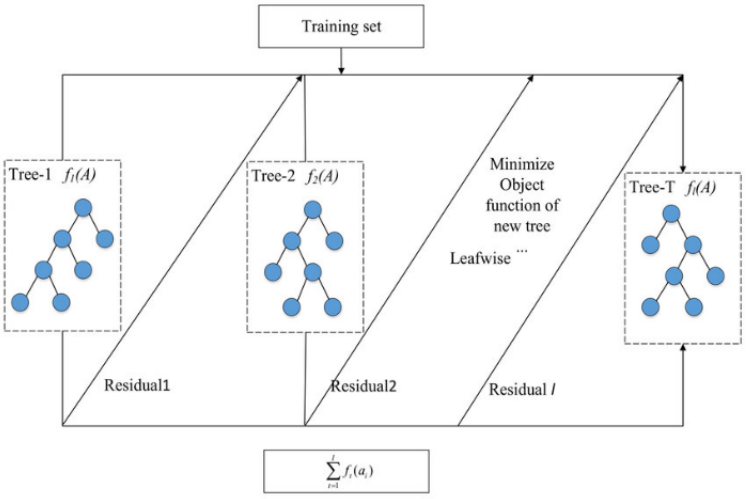


Figura 9: Modelo LightGBM. Fuente: [25]

XGBoost

XGB es un algoritmo de árboles de decisión impulsados por gradient boosting que incorpora el marco del Gradient Boosting Machine (GBM), XGB optimiza el marco de GBM abordando datos faltantes con conciencia de esparsidad, previniendo el sobreajuste con LASSO y mejoras algorítmicas, y encontrando divisiones óptim.as de los árboles con el algoritmo Weighted Quantile Sketch [23]

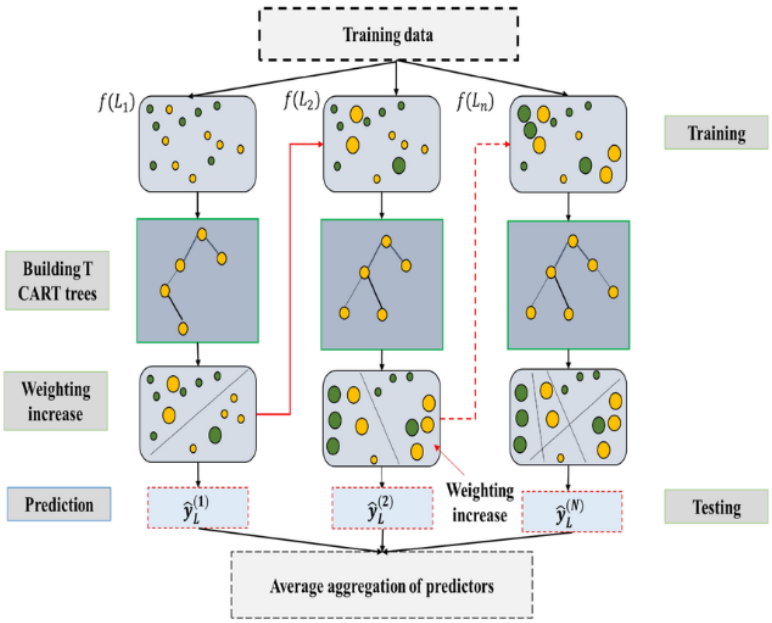


Figura 10: Esquema del modelo XGBoost. Fuente: [26]

II. METODO DE INVESTIGACION

Para esta investigación, se realizó una búsqueda exhaustiva utilizando operadores booleanos para recopilar información crítica y relevante sobre la detección de ataques DDoS mediante algoritmos de machine learning. Se emplearon operadores booleanos para filtrar y seleccionar artículos relevantes de fuentes confiables como Scopus, SciencieDirect, IEEE Xplore y EBSCO, con un enfoque en la literatura publicada en los últimos 5 años, entre los años 2020 al 2024.

2.1. Cadena de Búsqueda:

Para identificar artículos relevantes sobre la detección de ataques DDoS mediante algoritmos de machine learning, se diseñaron cadenas de búsqueda que integran términos clave. Las cadenas de búsqueda utilizadas fueron:

- En Scopus:
  - ✓ ddos AND attack AND machine AND learning
  - ✓ ddos AND attack AND servers AND web
  - ✓ detection AND ddos AND machine OR server AND web
  - ✓ detection OR attack AND ddos AND machine AND learning

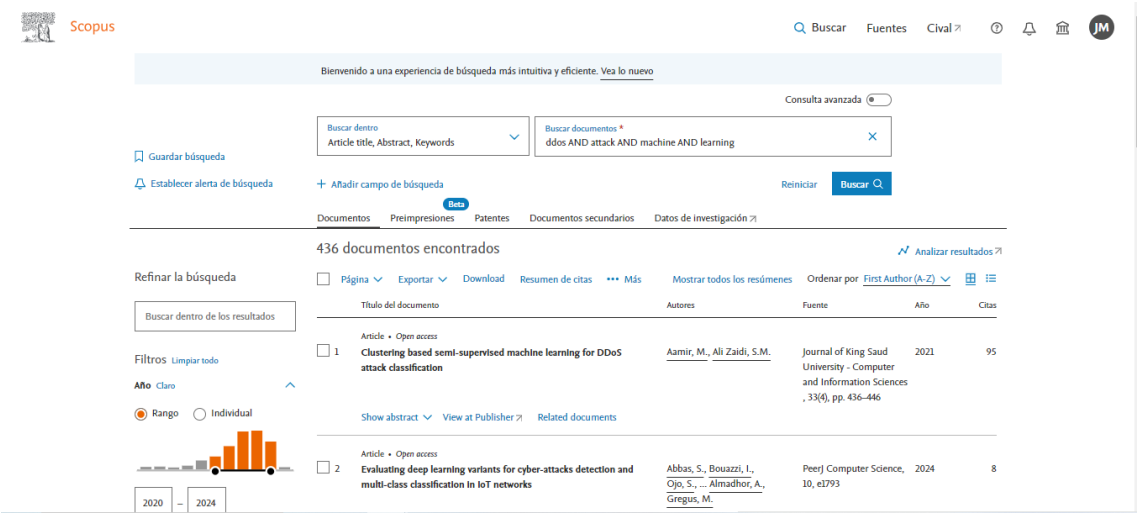


Figura 11: Búsqueda de artículos entre los años 2020 al 2024 de la base de datos Scopus. Fuente: Elaboración Propia

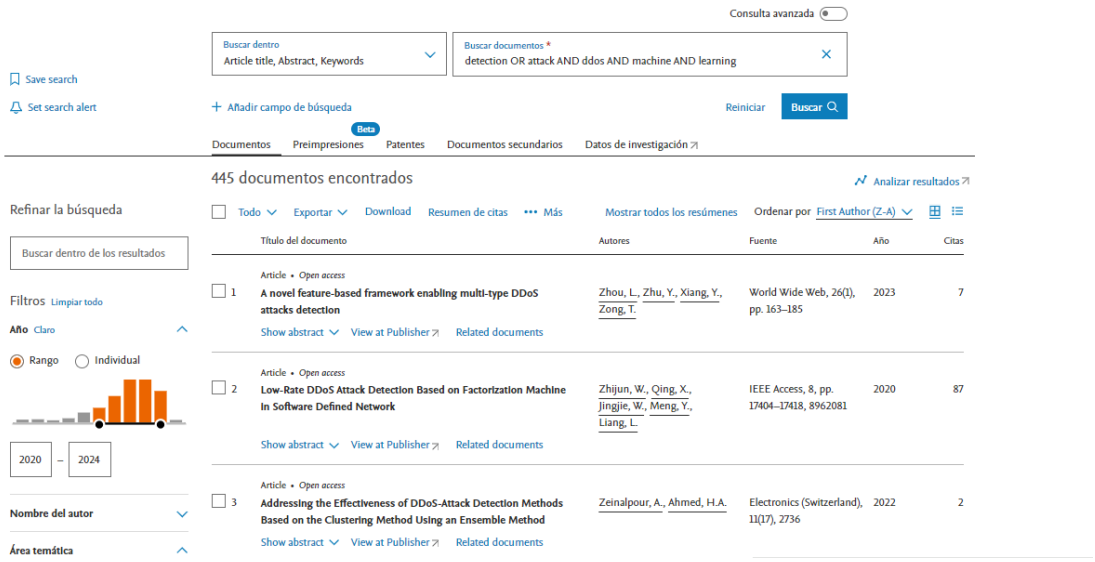


Figura 12: Utilización de cadena enfocada a la búsqueda en artículos de la base de datos Scopus. Fuente: Elaboración Propia

- SciencieDirect:
  - ✓ DDoS attacks" OR "Detection" AND "Machine Learning" ddos AND Machine Learning Techniques AND Detection Methods
  - ✓ "Denial of Service" AND "Machine Learning") AND ("Detection" OR "Prevention") AND ("Web Servers" OR "Network Security")
  - ✓ DDoS Detection AND Machine Learning AND Classification Algorithms

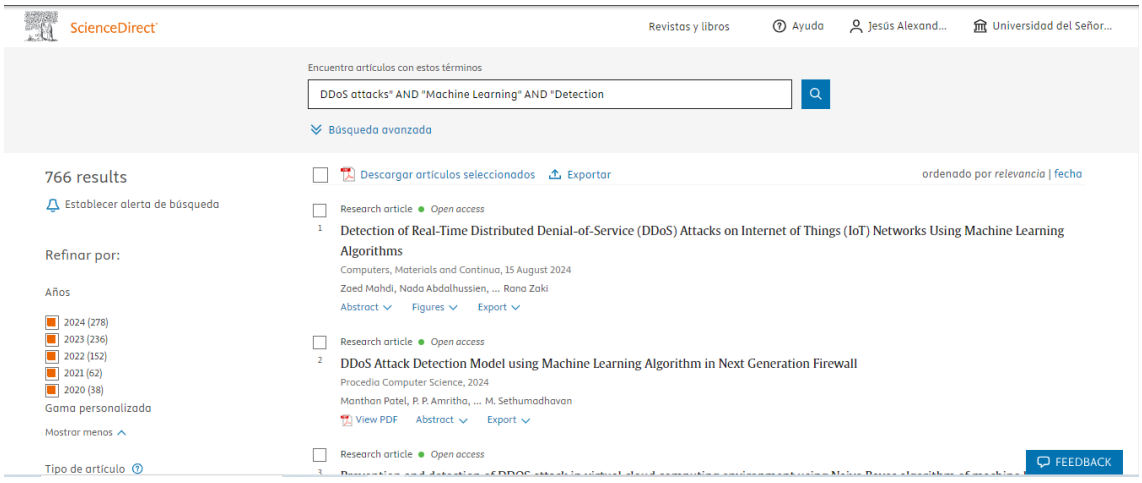


Figura 13: Búsqueda de artículos entre los años 2020 al 2024 de la base de datos SciencieDirect. Fuente: Elaboración Propia

Figura 14: Utilización de cadena enfocada a la búsqueda en artículos de la base de datos SciencieDirect. Fuente: Elaboración Propia

- IEEE Xplore
  - ✓ "DDoS" AND "Machine Learning"
  - ✓ Distributed Denial-of-Service Attack
  - ✓ DDoS Attack Detection by Using Machine

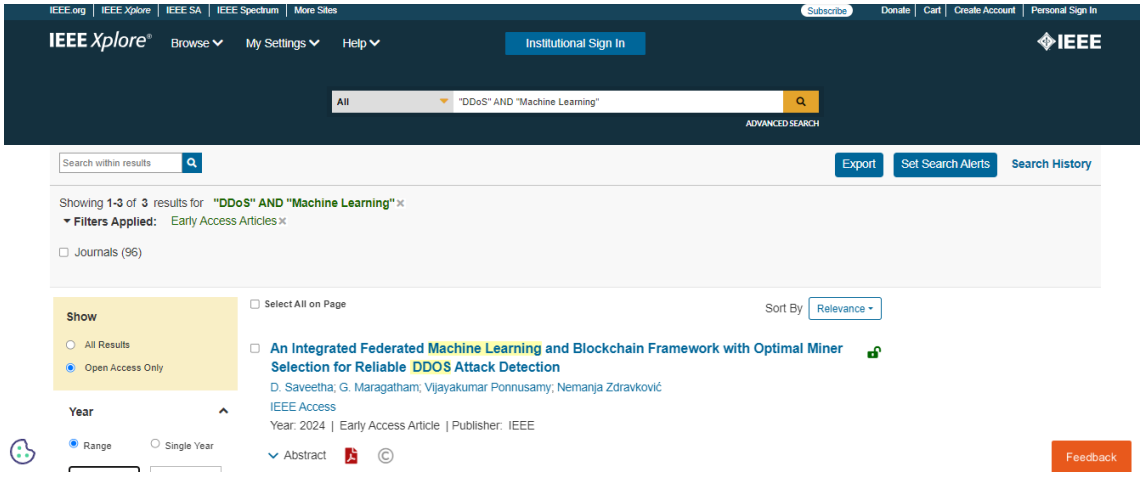


Figura 15: Búsqueda de artículos, utilizando cadena de búsqueda entre los años 2020 al 2024 de la base de datos IEEE Xplore. Fuente: Elaboración Propia

- EBSCO
  - ✓ "Distributed Denial of Service" AND "Machine Learning Algorithms" AND "Detection Strategies"
  - ✓ Machine Learning AND DDoS Attacks AND Intrusion Detection Systems
  - ✓ DDoS Attack Detection AND ML Techniques

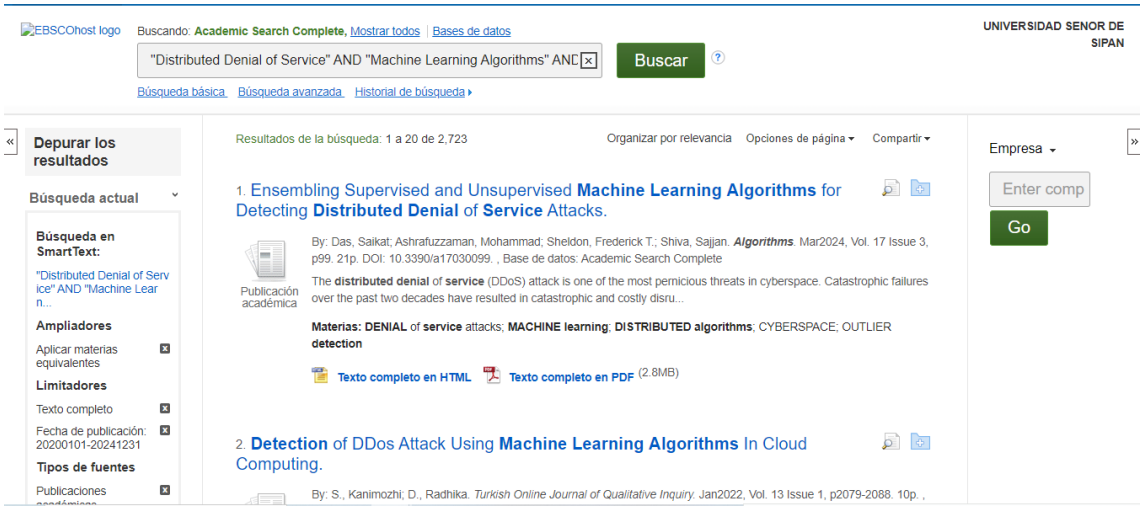


Figura 16: Búsqueda de artículos, utilizando criterios de búsqueda entre los años 2020 al 2024 de la base de datos EBESCO. Fuente: Elaboración Propia

2.3. Interrogantes de la Investigación

El estudio plantea responder a las siguientes interrogantes:

PRE1. ¿Cuánto material bibliográfico relacionado con los ataques distribuidos de denegación de servicio (DDoS) se ha publicado entre el año 2020 y 2024?

PRE2. ¿Qué técnicas se utilizaron para evaluar los algoritmos de aprendizaje automático más efectivos para la detección de ataques DDoS?

PRE3. ¿Qué modelos se analizó para los modelos propuestos para la detección de ataques DDoS?

2.3. Criterios de selección

- Criterio de Inclusión:

- Artículos en español o inglés.
- Artículos de revisión científicas, investigación y académicas.
- Artículos que necesariamente se refiere al tema abordado.
- Se priorizaron estudios con acceso completo al contenido para un análisis detallado.
- Fecha de artículos a revisar (2020-2024).

- Criterio de Exclusión:

- Artículos en idiomas diferentes a español o inglés.
- Artículos que no se encuentran en revistas científicas.
- Artículos sin acceso.
- Fecha de artículos a revisar por fuera del rango especificado.

2.4. Evaluar la calidad de los estudios

En esta etapa, la calidad de la investigación se abordó aplicando criterios de inclusión específicos como parte de la revisión integral de la literatura. Se seleccionaron exclusivamente artículos publicados en revistas científicas que abordaran la detección de ataques DDoS en servidores web utilizando algoritmos de aprendizaje automático.

Además de evaluar el enfoque de investigación de los documentos, se examinó el impacto general y el valor del H-index de las revistas en las que estos artículos fueron publicados.

La tabla 1. presenta el SCImago Journal Rank (impacto #) y el H-index de cada revista que publicó los documentos incluidos en este estudio. La mayoría de los documentos analizados provienen de revistas de alto impacto, con un valor medio de impacto de 1.763 y una media del H-index de 137.8.

Tabla 1: Clasificación de Revistas por Impacto y H-Index (2023)

Artículo	Revista	Impact #	H-Index
1	IEEE Access	0,960	242
2	Journal of King Saud University Computer and Information Science	1.198	60
3	IEEE Transactions on Information Forensics and Security	2.890	167
4	Journal of Network and Systems Management	1.043	40
5	Future Generation Computer Systems	1.946	164
6	Expert Systems with Applications	1.875	271

7	Computer Networks	1.520	155
8	Journal of Network and Computer Applications	2.417	141
9	Digital Communications and Networks	1.941	44
10	Computers and Electrical Engineering	1.041	94
#	Promedio	1.763	137.8

Fuente: Elaboración propia

2.5. Validación del Protocolo de revisión

La validación se ha llevado a cabo mediante un análisis detallado de las palabras clave y los criterios de inclusión utilizados en los artículos revisados. Este análisis asegura que el protocolo esté alineado con los objetivos de investigación y que las respuestas a las preguntas planteadas sean precisas y pertinentes.

III. RESULTADO

Los resultados obtenidos se basan en la revisión bibliográfica de los artículos relacionados a los ataques DDoS en servidores web, aplicando algoritmos de machine learning. Esta sección presenta la respuesta del análisis que responde a las preguntas de investigación planteadas anteriormente [2.3].

PRE1. ¿Cuántos material bibliográfico relacionado con los ataques distribuidos de denegación de servicio (DDoS) se ha publicado entre el año 2020 y 2024?

Para responder a esta pregunta, se realizó una valoración del material bibliográfico publicado sobre la detección de ataques DDoS en servidores web durante el período de 2020 a 2024. Se aplicó un filtro para identificar y seleccionar artículos relevantes de revistas reconocidas, con especial énfasis en las publicaciones en IEEE Access debido a su alta relevancia en el campo.

La Tabla 2 muestra la cantidad de publicaciones sobre ataques DDoS en cada año dentro del período de estudio. Los datos revelan una tendencia creciente en la producción científica en este campo, con un notable aumento en los últimos años.

Tabla 2: Resultado de la búsqueda de material bibliográficos

Año	**Cantidad**
2020	37
2021	72
2022	122
2023	127
2024	87

Fuente: Elaboración Propia

Además, la Tabla 3 presenta un resumen de los 20 documentos más relevantes encontrados en esta búsqueda integradora. Estos documentos abordan una variedad de enfoques y técnicas para la detección de ataques DDoS, incluyendo modelos de machine learning y algoritmos avanzados.

Tabla 3: Documentos sobre Detección de Ataques DDoS (2020-2024)

Nº	Año	Título del documento	Autores	Revista	Pais	Ref.
1	2020	Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of ddos attacks in cloud	Bhardwaj, Aanshi; Mangat, Veenu; Vig, Renu	IEEE Access	India	[27]
2	2020	Distributed Denial-of-Service Prediction on IoT Framework by Learning Techniques	Dwivedi, Shubhra; Tripathi, Sarsij Vardhan, Manu;	Open Computer Science	India	[28]
3	2020	An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks	Sahoo, K.S.; Tripathy, B.K.; Naik, K.; Khari, M.; Burgos, D.	IEEE Access	India	[29]
4	2020	A review on honeypot-based botnet detection models for smart factory	Seungjin, L.; Abdullah, A.; Jhanjhi, N.Z.	International Journal of Advanced Computer Science and Applications	Malasia	[30]
5	2021	Combining Deep Learning Models for Enhancing the Detection of Botnet Attacks in Multiple Sensors Internet of Things Networks	Hezam, A.A.; Mostafa, S.A.; Alanda, A.; Baharum, Z Salikon, M.Z.	International Journal on Informatics Visualization	Malasia	[31]
6	2021	Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms	Azmi, M.A.H.; Foozy, C.F.M.; Hamid, I.R.A.; Sukri, K.A.M.; Amnur, H.	International Journal on Informatics Visualization	Malasia	[32]

7	2021	Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning	Sangodoyin, A.O.; Akinsolu, M.O.; Pillai, P.; Grout, V.	IEEE Access	Reino Unido	[33]
8	2021	SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning	Yungaicelan Naula, Noe Marcelo; Vargas Rosales, Cesar; Perez-Diaz, Jesus Arturo	IEEE Access	México	[34]
9	2022	SD-Honeypot Integration for Mitigating DDoS Attack Using Machine Learning Approaches	Sumadi, F.D.S; Widagdo, A.R.; Reza, A.F.; Syaifuddin	International Journal on Informatics Visualization	Indonesia	[35]
10	2022	A DDoS attack detection and countermeasure scheme based on DWT and auto-encoder neural network for SDN	Ramin Fadaei Fouladi; Orhan Ermişb , Emin Anarim	Computer Networks	Turquía	[36]
11	2022	An efficient SVM based DEHO classifier to detect DDoS attack in cloud computing environment	Gowthul Alam MM; Jerald Nirmal Kumar S.; Uma Mageswari R; Michael Raj TF	Computer Networks	India	[37]

12	2022	A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks	Ismail; Mohmand, M.I.; Hussain, H.; Rahman, I.U; Haleem, M.	IEEE Access	Pakistán	[38]
13	2023	Optimized Artificial Intelligence Model for DDoS Detection in SDN Environment	Al-Dunainawi, Yousif; Al-Kaseem, Bilal R.; Al-Raweshidy, Hamed S.	IEEE Access	Irak	[39]
14	2023	SDNTruth: Innovative DDoS Detection Scheme for Software-Defined Networks (SDN)	Linhares, Tiago; Patel, Ahmed.; Barros, Fernandez, Marcial; Ana Luiza.	Journal of Network and Systems Management	Brasil	[40]
15	2023	Enhancing DDoS Attack Detection Using Snake Optimizer With Ensemble Learning on Internet of Things Environment	Aljebreen, Mohammed; Mengash, Hanan Abdullah; Arasi, Munya A.; Aljameel, Sumayh S.; Salama, Ahmed S.; Hamza, Manar Ahmed	IEEE Access	Arabia Saudita	[41]
16	2023	Enhancing the Efficiency of Gaussian Naïve Bayes Machine Learning Classifier in the Detection of DDOS in Cloud Computing	Naiem, Sarah; Khedr, Ayman E.; Idrees, Amira M.; Marie, Mohamed I.	IEEE Access	Egipto	[42]

17	2024	FTG-Net-E: A hierarchical ensemble graph neural network for DDoS attack detection	Abu Bakar, R.; De Marinis, L.; Cugini, F.; Paolucci, F.	Computer Networks	Italia	[43]
18	2024	Enhanced detection of low-rate DDoS attack patterns using machine learning models	Bocu, Razvan; Iavich, Maksim	Journal of Network and Computer Applications	Georgia	[44]
19	2024	Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model	Alashhab, A.A.; Zahid, M.S.; Isyaku, B.; Abdullah, T.A.A.; Maiwada, U.D.	IEEE Access	Malasia	[45]
20	2024	Rule-Based with Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems (CPPS)	Hussain, Ayaz.; Marin Tordera, Eva; Masip-Bruin, Xavi; Leligou, Helen C.	IEEE Access	España	[46]

Fuente: Elaboración Propia.

PRE2. ¿Qué técnicas se utilizaron para evaluar Los algoritmos de aprendizaje automático más efectivos para la detección de ataques DDoS?

Para abordar esta pregunta, se llevó a cabo un análisis detallado de las técnicas de aprendizaje automático empleadas en la detección de ataques DDoS en servidores web. A continuación, se presenta una tabla que resume las técnicas de machine learning utilizadas en los estudios revisados entre 2020 y 2024.

Tabla 4: Técnicas de Aprendizaje Automático utilizadas por el autor (2020-2024)

Año	Autores	Técnicas
2020	Sahoo, Kshira Sagar;Tripathy, Bata Krishna; Ramasubbareddy, Somula; Naik, Kshirasagar; Khari, Manju; ; Burgos, Daniel, Balusamy, Balamurugan;	Máquinas de Soporte Vectorial (SVM), Análisis de Componentes Principales Kernel (KPCA), Algoritmos Genéticos (GA), XGBoost, Autoencoder Escaso (SAE), Máquinas de Boltzmann Restringidas (RBM), Redes Neuronales Profundas.
2020	Shubhra Dwivedi, Manu Vardhan and Sarsij Tripathi	Árboles de Decisión, Perceptrón Multicapa, Naive Bayes, Máquinas de Vectores de Soporte, C4.5, Análisis de Componentes Principales, Lógica Difusa, Redes Bayesianas
2020	Seungjin, Lee; Abdullah, Azween; Jhanjhi N.Z.	Detección de anomalías, Clasificación binaria, Detección de comandos y control (C&C), Análisis de datos de honeypots.
2020	Le D.T.; Dao M.H.; Nguyen Q.L.T.	Autoencoders Apilado y Redes Neuronales Profundas
2021	Azmi, Muhammad Aqil Haqeemi; Foozy, Cik Feresa Mohd; Sukri, Khairul Amin Mohamad; Abdullah, Nurul	Redes Neuronales Artificiales (ANN), Naïve Bayes y Árbol de Decisión

	Azma; Hamid, Isredza Rahmi A.; Amnur, Hidra	
2022	Ramin Fadaei Fouladi; Orhan Ermişb , Emin Anarim	Red neuronal Artificial y Las Redes neuronales convolucionales
2022	Ismail; Mohmand, Muhammad Ismail; Hussain, Hameed; Khan, Ayaz Ali; Ullah, Ubaid; Zakarya, Muhammad; Ahmed, Aftab; Raza, Mushtaq; Rahman, Izaz Ur; Haleem, Muhammad	Random Forest y XGBoost
2023	Naiem, Sarah; Khedr, Ayman E.; Idrees, Amira M.; Marie, Mohamed I.	Random Forest, Support Vector Machine, Decision Trees, regresión lineal y logística, y Gaussian Naïve Bayes
2023	Linhares, Tiago; Patel, Ahmed.; Barros, Ana Luiza.; Fernandez, Marcial	logistic regression, random forest, support vector machine y k-nearest neighbor (KNN)
2024	Ramadass, Parthasarathy; shree Sekar, Raja; Srinivasan, Saravanan; Kumar Mathivanan, Sandeep; Dev Shivahare, Basu; Mallik, Saurav; Ahmad, Naim; Ghribi, Wade;	Redes neuronales convolucionales cuánticas (QCNN), Optimización mejorada de la hiena manchada (EHSO)

2024	Becerra-Suarez, Fray L.; Fernández-Roman, Ismael; Forero, Manuel G.	Random Forest (RF), Decision Trees (DT), Redes Neuronales Artificiales (ANN), Redes Neuronales Profundas (DNN), Redes Neuronales Convolucionales (CNN), Modelos basados en LSTM (Long Short-Term Memory), Modelos híbridos combinando GRU (Gated Recurrent Unit) y LSTM, Autocodificadores (Autoencoders), Modelos optimizados con Harris Hawks y redes neuronales LSTM.

Fuente: Elaboración Propia

PRE3. ¿Qué modelos se analizó para los modelos propuestos para la detección de ataques DDoS?

La revisión de la literatura ha identificado diversos modelos y técnicas de aprendizaje automático aplicados a la detección de ataques DDoS, cada uno con distintos niveles de eficacia. Aunque algunas técnicas avanzadas, como las Redes Neuronales Convolucionales (CNN) y las Redes Neuronales Convolucionales Cuánticas (QCNN), se utilizan predominantemente en otros campos, su aplicación en la detección de ataques DDoS está en aumento. A continuación, se presentan los modelos más destacados junto con sus porcentajes de eficacia, basados en el análisis de los artículos revisados:

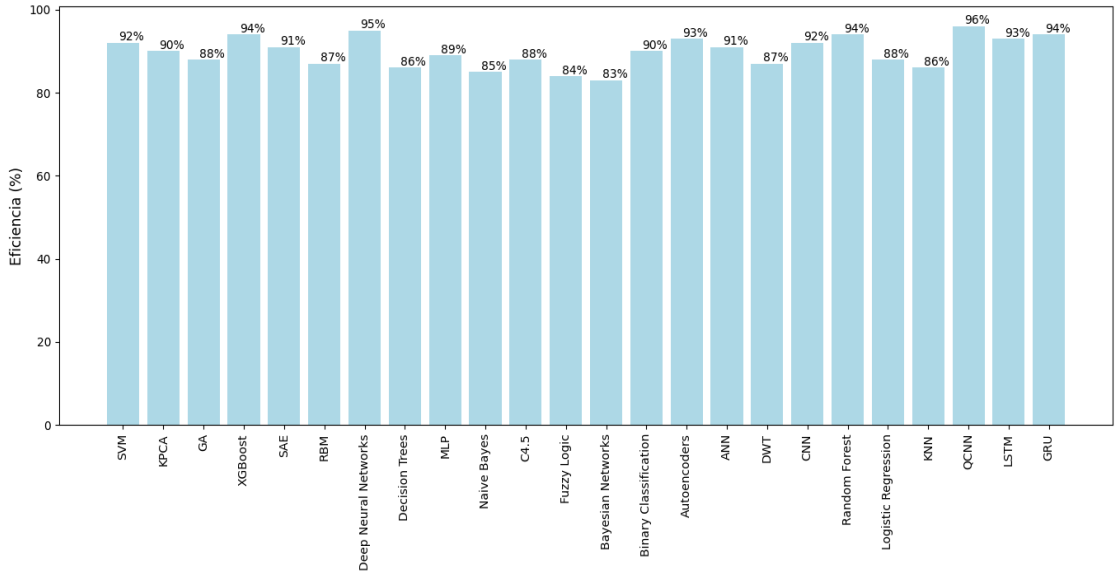


Figura 17: Análisis de Eficiencia de los algoritmos machine learning. Fuente: Elaboración Propia

VI. DISCUSIÓN Y CONCLUSIONES

➢ Discusión

Esta investigación revela que los ataques distribuidos de denegación de servicio (DDoS) continúan siendo una amenaza significativa para la seguridad informática debido a su alta frecuencia y capacidad para interrumpir el acceso legítimo a los servicios. Los avances en la inteligencia de los conmutadores y la separación de datos y control han incrementado el interés de los atacantes en saturar estos sistemas mediante ataques DDoS. La creciente sofisticación de estos ataques refleja la necesidad urgente de desarrollar y mejorar mecanismos de detección y mitigación eficaces.

Un estudio [2], destaca que los ataques DDoS se han dirigido principalmente a la infraestructura en la nube en los últimos años. Este cambio en el objetivo subraya la necesidad de adaptar las técnicas de defensa a los nuevos entornos de ataque. En este contexto, los modelos de aprendizaje automático han demostrado ser herramientas valiosas para la detección de ataques DDoS. La investigación indicó que la regresión logística y el Naive Bayes, dos modelos de machine learning evaluados, mostraron una alta precisión en la identificación de estos ataques. En particular, la regresión logística sobresalió con una precisión de entre el 99 % y el 100 %, superando ligeramente a Naive Bayes, que logró una precisión entre el 98 % y el 99 %.

➢ Conclusión

1. Se determinó las caracterizar y técnicas de clasificación de tráfico web en ataques DDoS, Unos de los aspectos claves a considerar al usar una nube o un servidor web es la seguridad, la accesibilidad, la disponibilidad y la integración, ya que debido a cualquier ataque al servidor alojado en la nube pueden causar tiempo de inactividad, lo que puede provocar daños financieros y de reputación.

2. Se estableció que al evaluar los algoritmos de machine learning más efectivos para la detección de ataques DDoS. En esta investigación mostró que algunos algoritmos fueron eficientes para prevenir, detectar o mitigar. Es por ello que, propusieron un mecanismo de detección basado en Fuzzy diseñado para detectar ataques DDoS en servidores web al filtrar los paquetes entrantes antes de llegar a la nube.

3. Se concluyó que al Revisar los modelos propuestos para la detección de ataques DDoS, dentro de la investigación se llegó a entender que este modelo de prueba se basó en el modelo combinado de IRC, AH e Internet para detectar botnet y darknet desde la dirección IP en el servidor. También ayudó a detectar el 86 % de la fuente de ataque e hizo que el sistema se bloquee en esa ruta de origen para optimizar la eficiencia de la detección del ataque.

V. REFERENCIAS

[1] P. Ramadass *et al.*, «BSDN-HMTD: A blockchain supported SDN framework for detecting DDoS attacks using deep learning method», *Egypt. Inform. J.*, vol. 27, 2024, doi: 10.1016/j.eij.2024.100515.

[2] D. Radain, S. Almalki, H. Alsaadi, y S. Salama, «A Review on Defense Mechanisms Against Distributed Denial of Service (DDoS) Attacks on Cloud Computing», en *2021 International Conference of Women in Data Science at Taif University (WiDSTaif)*, mar. 2021, pp. 1-6. doi: 10.1109/WiDSTaif52235.2021.9430220.

[3] F. L. Becerra-Suarez, I. Fernández-Roman, y M. G. Forero, «Improvement of Distributed Denial of Service Attack Detection through Machine Learning and Data Processing», *Mathematics*, vol. 12, n.º 9, 2024, doi: 10.3390/math12091294.

[4] A. S. M. Rizvi, J. Mirkovic, J. Heidemann, W. Hardaker, y R. Story, «Defending Root DNS Servers against DDoS Using Layered Defenses (Extended)», *Ad Hoc Netw.*, vol. 151, 2023, doi: 10.1016/j.adhoc.2023.103259.

[5] S. Sambangi, L. Gondi, y S. Aljawarneh, «A Feature Similarity Machine Learning Model for DDoS Attack Detection in Modern Network Environments for Industry 4.0», *Comput. Electr. Eng.*, vol. 100, 2022, doi: 10.1016/j.compeleceng.2022.107955.

[6] S. Peneti, «DDOS Attack Identification using Machine Learning Techniques», presentado en 2021 International Conference on Computer Communication and Informatics, ICCCI 2021, 2021. doi: 10.1109/ICCCI50826.2021.9402441.

[7] K. Kumari y M. Mrunalini, «Detecting Denial of Service attacks using machine learning algorithms», *J. Big Data*, vol. 9, n.º 1, 2022, doi: 10.1186/s40537-022-00616-0.

[8] A. Maslan, K. M. Mohamad, y C. F. M. Foozy, «Enhancement detection distributed denial of service attacks using hybrid n-gram techniques», *Telkomnika*

Telecommun. Comput. Electron. Control, vol. 20, n.º 1, pp. 61-69, 2022, doi: 10.12928/TELKOMNIKA.v20i1.18103.

[9] M. I. Mohmand *et al.*, «A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks», *IEEE Access*, vol. 10, pp. 21443-21454, 2022, doi: 10.1109/ACCESS.2022.3152577.

[10] A. Ghaben, M. Anbar, I. H. Hasbullah, y S. Karuppayah, «Mathematical Approach as Qualitative Metrics of Distributed Denial of Service Attack Detection Mechanisms», *IEEE Access*, vol. 9, pp. 123012-123028, 2021, doi: 10.1109/ACCESS.2021.3110586.

[11] «What is a DDoS Attack? DDoS Meaning, Definition & Types | Fortinet». Accedido: 12 de septiembre de 2024. [En línea]. Disponible en: https://www.fortinet.com/resources/cyberglossary/ddos-attack

[12] Y. Fernández, «Qué es un ataque DDoS y cómo puede afectarte», Xataka. Accedido: 12 de septiembre de 2024. [En línea]. Disponible en: https://www.xataka.com/basics/que-es-un-ataque-ddos-y-como-puede-afectarte

[13] «¿Qué es un ataque DDoS? | IBM». Accedido: 12 de septiembre de 2024. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/ddos

[14] «Ataques DDoS: Qué son, evolución y cómo prevenirlos y mitigarlos», Computing. Accedido: 12 de septiembre de 2024. [En línea]. Disponible en: https://www.computing.es/informes/ataques-ddos-que-son-su-evolucion-y-como-prevenirlos-y-mitigarlos/

[15] R. McCollin, «Explicación de los Ataques DDoS: Causas, Efectos. ¿Cómo Proteger su Sitio Web?», Kinsta®. Accedido: 12 de septiembre de 2024. [En línea]. Disponible en: https://kinsta.com/es/blog/que-es-un-ataque-de-ddos/

[16] «OrgSec-Case-study-DDoS-attacks-June-2020.pdf». Accedido: 12 de septiembre de 2024. [En línea]. Disponible en: https://www.theengineroom.org/wp-content/uploads/2020/08/OrgSec-Case-study-DDoS-attacks-June-2020.pdf

[17] «¿Qué es un ataque DDoS a la capa de aplicaciones?», Akamai. Accedido: 12 de septiembre de 2024. [En línea]. Disponible en: https://www.akamai.com/es/glossary/what-is-application-layer-ddos-attack

[18] N. M. Yungaicela-Naula, C. Vargas-Rosales, y J. A. Perez-Diaz, «SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning», *IEEE Access*, vol. 9, pp. 108495-108512, 2021, doi: 10.1109/ACCESS.2021.3101650.

[19] «Qué es un ataque DDOS y cómo proteger su sitio contra uno», Amazon Web Services, Inc. Accedido: 12 de septiembre de 2024. [En línea]. Disponible en: https://aws.amazon.com/es/shield/ddos-attack-protection/

[20] K. Huang, L. -X. Yang, X. Yang, Y. Xiang, y Y. Y. Tang, «A Low-Cost Distributed Denial-of-Service Attack Architecture», *IEEE Access*, vol. 8, pp. 42111-42119, 2020, doi: 10.1109/ACCESS.2020.2977112.

[21] Daniel, «Machine Learning: definición, funcionamiento, usos», Formación en ciencia de datos | DataScientest.com. Accedido: 12 de septiembre de 2024. [En línea]. Disponible en: https://datascientest.com/es/machine-learning-definicion-funcionamiento-usos

[22] Y. Muñoz-Castaño *et al.*, «Desarrollo de una aplicación para la predicción de ingredientes y recetas de cocina por medio de TensorFlow y máquinas de soporte vectorial», *Rev. Ing. Univ. Medellín*, vol. 19, n.º 37, pp. 195-215, dic. 2020, doi: 10.22395/rium.v19n37a10.

[23] J. Halladay *et al.*, «Detection and Characterization of DDoS Attacks Using Time-Based Features», *IEEE Access*, vol. 10, pp. 49794-49807, 2022, doi: 10.1109/ACCESS.2022.3173319.

[24] H. Y. P. Huacasi, «Bosques Aleatorios», Medium. Accedido: 13 de septiembre de 2024. [En línea]. Disponible en: https://medium.com/@hpumah/bosques-aleatorios-482163ace92e

[25] Z. Su, Q. Liu, C. Zhao, y F. Sun, «A Traffic Event Detection Method Based on Random Forest and Permutation Importance», *Mathematics*, vol. 10, p. 873, mar. 2022, doi: 10.3390/math10060873.

[26] Z. Ali y A. Burhan, «Hybrid machine learning approach for construction cost estimation: an evaluation of extreme gradient boosting model», *Asian J. Civ. Eng.*, vol. 24, pp. 1-16, abr. 2023, doi: 10.1007/s42107-023-00651-z.

[27] A. Bhardwaj, V. Mangat, y R. Vig, «Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of ddos attacks in cloud», *IEEE Access*, vol. 8, pp. 181916-181929, 2020, doi: 10.1109/ACCESS.2020.3028690.

[28] S. Dwivedi, M. Vardhan, y S. Tripathi, «Distributed Denial-of-Service Prediction on IoT Framework by Learning Techniques», *Open Comput. Sci.*, vol. 10, n.º 1, pp. 220-230, 2020, doi: 10.1515/comp-2020-0009.

[29] K. S. Sahoo *et al.*, «An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks», *IEEE Access*, vol. 8, pp. 132502-132513, 2020, doi: 10.1109/ACCESS.2020.3009733.

[30] L. Seungjin, A. Abdullah, y N. Z. Jhanjhi, «A review on honeypot-based botnet detection models for smart factory», *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, n.º 6, pp. 418-435, 2020, doi: 10.14569/IJACSA.2020.0110654.

[31] A. A. Hezam, S. A. Mostafa, Z. Baharum, A. Alanda, y M. Z. Salikon, «Combining Deep Learning Models for Enhancing the Detection of Botnet Attacks in Multiple Sensors Internet of Things Networks», *Int. J. Inform. Vis.*, vol. 5, n.º 4, pp. 380-387, 2021, doi: 10.30630/JOIV.5.4.733.

[32] M. A. H. Azmi, C. F. M. Foozy, K. A. M. Sukri, N. A. Abdullah, I. R. A. Hamid, y H. Amnur, «Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms», *Int. J. Inform. Vis.*, vol. 5, n.º 4, pp. 395-401, 2021, doi: 10.30630/JOIV.5.4.734.

[33] A. O. Sangodoyin, M. O. Akinsolu, P. Pillai, y V. Grout, «Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning», *IEEE Access*, vol. 9, pp. 122495-122508, 2021, doi: 10.1109/ACCESS.2021.3109490.

[34] N. M. Yungaicela-Naula, C. Vargas-Rosales, y J. A. Perez-Diaz, «SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning», *IEEE Access*, vol. 9, pp. 108495-108512, 2021, doi: 10.1109/ACCESS.2021.3101650.

[35] F. D. S. Sumadi, A. R. Widagdo, A. F. Reza, y Syaifuddin, «SD-Honeypot Integration for Mitigating DDoS Attack Using Machine Learning Approaches», *Int. J. Inform. Vis.*, vol. 6, n.º 1, pp. 39-44, 2022, doi: 10.30630/joiv.6.1.853.

[36] R. F. Fouladi, O. Ermiş, y E. Anarim, «A DDoS attack detection and countermeasure scheme based on DWT and auto-encoder neural network for SDN», *Comput. Netw.*, vol. 214, 2022, doi: 10.1016/j.comnet.2022.109140.

[37] G. A. MM, J. N. K. S, U. M. R, y M. R. TF, «An efficient SVM based DEHO classifier to detect DDoS attack in cloud computing environment», *Comput. Netw.*, vol. 215, 2022, doi: 10.1016/j.comnet.2022.109138.

[38] Ismail *et al.*, «A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks», *IEEE Access*, vol. 10, pp. 21443-21454, 2022, doi: 10.1109/ACCESS.2022.3152577.

[39] Y. Al-Dunainawi, B. R. Al-Kaseem, y H. S. Al-Raweshidy, «Optimized Artificial Intelligence Model for DDoS Detection in SDN Environment», *IEEE Access*, vol. 11, pp. 106733-106748, 2023, doi: 10.1109/ACCESS.2023.3319214.

[40] T. Linhares, A. Patel, A. L. Barros, y M. Fernandez, «SDNTruth: Innovative DDoS Detection Scheme for Software-Defined Networks (SDN)», *J. Netw. Syst. Manag.*, vol. 31, n.º 3, pp. 1-23, jul. 2023, doi: 10.1007/s10922-023-09741-4.

[41] M. Aljebreen, H. A. Mengash, M. A. Arasi, S. S. Aljameel, A. S. Salama, y M. A. Hamza, «Enhancing DDoS Attack Detection Using Snake Optimizer With Ensemble Learning on Internet of Things Environment», *IEEE Access*, vol. 11, pp. 104745-104753, 2023, doi: 10.1109/ACCESS.2023.3318316.

[42] S. Naiem, A. E. Khedr, A. M. Idrees, y M. I. Marie, «Enhancing the Efficiency of Gaussian Naïve Bayes Machine Learning Classifier in the Detection of DDOS in Cloud Computing», *IEEE Access*, vol. 11, pp. 124597-124608, 2023, doi: 10.1109/ACCESS.2023.3328951.

[43] R. Abu Bakar, L. De Marinis, F. Cugini, y F. Paolucci, «FTG-Net-E: A hierarchical ensemble graph neural network for DDoS attack detection», *Comput. Netw.*, vol. 250, p. 110508, ago. 2024, doi: 10.1016/j.comnet.2024.110508.

[44] R. Bocu y M. Iavich, «Enhanced detection of low-rate DDoS attack patterns using machine learning models», *J. Netw. Comput. Appl.*, vol. 227, p. 103903, jul. 2024, doi: 10.1016/j.jnca.2024.103903.

[45] A. A. Alashhab *et al.*, «Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model», *IEEE Access*, vol. 12, pp. 51630-51649, 2024, doi: 10.1109/ACCESS.2024.3384398.

[46] A. Hussain, E. Marín Tordera, X. Masip-Bruin, y H. C. Leligou, «Rule-Based With Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems (CPPS)», *IEEE Access*, vol. 12, pp. 114894-114911, 2024, doi: 10.1109/ACCESS.2024.3445261.