Artificial Intelligence Based Strategies for the Protection of SDN Infrastructures Against DDoS Attacks

Luis Taype[1]; Anderson Ugarte[1]; José Cornejo[1]; Silvia Rita Rodriguez Alvarez[1]
[1]Universidad Tecnológica del Perú, Perú, *U1312168@utp.edu.pe, U21301305@utp.edu.pe, C21944@utp.edu.pe,* C19398@utp.edu.pe

Abstract*– Distributed denial of service (DDoS) attacks constitutes a critical threat to software-defined network (SDN) infrastructures, compromising operational availability due to centralization that makes the controller a single point of failure. This review aims to identify scientific evidence on the effectiveness of artificial intelligence-based strategies for detecting and mitigating DDoS attacks in corporate SDN infrastructures. Method: A systematic review was conducted using PICO methodology in SCOPUS, analyzing 248 bibliographic records until June 2025, applying specific criteria that resulted in 20 selected studies focused on AI strategies and critical corporate SDN infrastructures. Results: AI techniques demonstrated significant superiority achieving accuracies between 97% and 99.81% compared to 75% of traditional methods. Hybrid CNN-LSTM models with optimization algorithms reduced false positives from 15% to 0.24%-2% and improved processing speed by 35%. Four main approaches were identified: ML/DL models, adaptive precision, proactive detection, and false positive reduction. Conclusions: Artificial intelligence establishes a new paradigm in SDN cybersecurity, offering proactive, adaptive, and energy-efficient detection, although it requires greater validation in real production environments to confirm its complete operational applicability.

Keywords*-- software-defined networks, artificial intelligence, strategies, protection, distributed denial of service attacks.

Estrategias basadas en inteligencia artificial para la protección de infraestructuras SDN contra ataques DDoS

Luis Taype[1]; Anderson Ugarte[1]; José Cornejo[1]; Silvia Rita Rodriguez Alvarez [1]
[1]Universidad Tecnológica del Perú, Perú, *U1312168@utp.edu.pe, U21301305@utp.edu.pe, C21944@utp.edu.pe, C19398@utp.edu.pe*

Resumen*– Los ataques de denegación de servicio distribuido (DDoS) constituyen una amenaza crítica para las infraestructuras de redes definidas por software (SDN), comprometiendo la disponibilidad operacional debido a la centralización que convierte al controlador en un único punto de falla. Esta revisión tiene como objetivo identificar evidencia científica sobre la efectividad de las estrategias basadas en inteligencia artificial para detectar y mitigar ataques DDoS en infraestructuras SDN corporativas. Método: Se realizó una revisión sistemática utilizando la metodología PICO en SCOPUS, analizando 248 registros bibliográficos hasta junio de 2025, aplicando criterios específicos que resultaron en 20 estudios seleccionados centrados en estrategias de IA e infraestructuras SDN corporativas críticas. Resultados: Las técnicas de IA demostraron una superioridad significativa alcanzando precisiones entre 97% y 99.81% en comparación con el 75% de los métodos tradicionales. Los modelos híbridos CNN-LSTM con algoritmos de optimización redujeron los falsos positivos del 15% al 0.24%-2% y mejoraron la velocidad de procesamiento en un 35%. Se identificaron cuatro enfoques principales: modelos ML/DL, precisión adaptativa, detección proactiva y reducción de falsos positivos. Conclusiones: La inteligencia artificial establece un nuevo paradigma en la ciberseguridad SDN, ofreciendo detección proactiva, adaptativa y energéticamente eficiente, aunque requiere mayor validación en entornos de producción reales para confirmar su completa aplicabilidad operacional.

Palabras clave: redes definidas por software, inteligencia artificial, estrategias, protección, ataques de denegación de servicio distribuido

.

I. Introducción

La transformación digital ha impactado significativamente la forma en que se diseñan administra y protegen las infraestructuras tecnológicas. En los últimos años, tecnologías emergentes como las redes definidas por software (SDN), el Internet de las Cosas (IoT), blockchain y la inteligencia artificial (IA) han revolucionado el diseño, gestión y protección de redes, permitiendo una administración más dinámica, escalable y eficiente de los recursos tecnológicos [1], [2].

Estas tecnologías han sido especialmente relevantes en sectores críticos como salud, transporte, manufactura, aviación y defensa, donde mantener la continuidad operativa y la integridad de los datos es vital [1], [3]. En estos entornos se requiere continuidad operativa e integridad de datos. Las redes deben ofrecer comunicaciones ultra fiables y de baja latencia con garantías estrictas de calidad de servicio (QoS) [1].

Sin embargo, este avance también ha traído consigo nuevos riesgos, especialmente en lo relacionado con la ciberseguridad. Un ejemplo claro son los ataques distribuidos de denegación de servicio (DDoS), que pueden generar un gran volumen de tráfico malicioso para saturar sistemas clave y dejarlos fuera de servicio [4], [2].

La arquitectura SDN ha optimizado la gestión de red al separar el plano de control del de datos, permitiendo una supervisión centralizada y flexible. Sin embargo, esta centralización convierte al controlador en un punto único de falla, haciéndolo vulnerable a ataques DDoS que pueden colapsar toda la red si es comprometido [3], [4].

Frente a estas amenazas, se han propuesto soluciones que integran inteligencia artificial, aprendizaje automático (ML), y aprendizaje profundo (DL) para detectar y mitigar anomalías de tráfico. Modelos como redes neuronales artificiales (ANN), Random forest o redes convolucionales (CNN) han demostrado una alta precisión en la detección de tráfico malicioso. Por ejemplo, en [4], el modelo basado en Random Forest alcanzó una precisión del 99.97 % en la detección de ataques DDoS, mientras que en [5], el sistema DDoS Blocker logró un tiempo promedio de detección de 3 segundos, con una tasa de falsos positivos de solo 0.51 %.

Además, se han empezado a combinar técnicas de IA con otras tecnologías como blockchain o incluso mecanismos resistentes a amenazas directas. Por ejemplo, en [1], se propone una arquitectura determinista definida por software con cifrado cuántico, capaz de proteger redes críticas como las industriales o gubernamentales, y que incorpora arquitecturas Zero Trust basadas en IA para garantizar inmunidad ante ciberataques externos e internos. El cual, fue evaluada bajo condiciones de red crítica, logrando reducir el riesgo de exposición en un 83 % frente a entornos sin cifrado cuántico.

Por ejemplo, Sinha et al. [5] reportó que algunos enfoques de IA aún presentan hasta 6.8% de falsos positivos y retardos superiores a 5 segundos en congestión moderada. Asimismo, en [2] se identificó que más del 40% de los métodos analizados carecían de pruebas en entornos reales, limitando su aplicabilidad en redes productivas. Por ello, se plantea realizar una revisión sistemática para identificar las soluciones más efectivas que utilizan inteligencia artificial para la detección y mitigación de ataques DDoS. Esta revisión busca sintetizar el conocimiento disponible e identificar vacíos en la literatura actual, ofreciendo un aporte útil para investigadores y

profesionales que buscan implementar sistemas de seguridad más robustos en redes inteligentes.

Para finalizar, la revisión se estructuró de la siguiente manera: La sección II presenta la metodología desarrollada, incluyendo la metodología PICO para fortalecer la búsqueda y criterios de selección. La sección III presenta los resultados obtenidos de la investigación de los artículos seleccionados.

II. METODOLOGÍA

En la revisión sistemática de literatura se recopilaron estudios provenientes de la base de datos SCOPUS, con el propósito de extraer información relevante que nos permita responder a la siguiente interrogante de la investigación enunciada con base en la metodología PICO, ¿Cómo se han utilizado las estrategias basadas en inteligencia artificial para protegerse de los ataques DDoS en infraestructuras SDN? Por otro lado, se analizaron los componentes de la pregunta PICO, el cual se detalla en la Tabla I.

TABLA I
COMPONENTES DE PREGUNTA PICO

Componente		Descripción
P	Problema / Población	Ataques DDoS en Infraestructuras SDN
I	Intervención	Estrategias basadas en IA
C	Comparación	Técnicas tradicionales de seguridad en redes
O	Resultados	Mejoras de detección DDoS

Se procedió a desglosar la pregunta de revisión PICO, y de las preguntas asociadas a cada uno de los componentes. Partiendo de ello, se formularon las siguientes preguntas de acuerdo con cada detalle, este proceso es fundamental para la revisión sistemática y permita abordar el problema desde otro punto de vista. Con esta información no solo se logró definir el alcance del estudio, sino también permite facilitar la identificación a cada tamaño del problema investigado. A través de las siguientes preguntas y con los artículos de búsqueda, permitió realizar una investigación más enfocado y relacionado con los objetivos del estudio y trabajo elaborado, esta información está contenida en la Tabla II.

TABLA II
PREGUNTAS POR COMPONENTE DE LA PREGUNTA

Pregunta PICO: ¿Cómo se han utilizado las estrategias basadas en inteligencia artificial para protegerse de los ataques DDoS en infraestructuras SDN?		
P	RQ1 Problema / Población	¿Qué impacto y/o consecuencias provocan los ataques DDoS en las infraestructuras SDN?
I	RQ2 Intervención	¿De qué manera el uso de la IA contribuye la defensa para proteger redes SDN de ataques DDoS?
C	RQ3 Comparación	¿Qué tan eficaces han resultado las estrategias de IA frente a los métodos tradicionales de seguridad?
O	RQ4 Resultados	¿Qué mejoras se han logrado con los métodos basados en IA en la detección y mitigación ante ataques DDoS?

Asimismo, se seleccionaron y eligieron las palabras clave en inglés asociadas a cada componente de la metodología PICO, con el propósito de organizar y definir adecuadamente la estrategia de búsqueda bibliográfica. Para la obtención de la búsqueda del tema relacionado al estudio de investigación y sea más preciso identificar los artículos de investigación en cada componente para su respectivo desarrollo y sea reflejado cada término utilizando palabras claves de cada componente, véase en la Tabla III.

TABLA III
PALABRAS CLAVES DE CADA COMPONENTE

Componente		Descripción
P	RQ1 Problema / Población	DDoS, SDN infrastructures, corporate SDN, enterprise environments, software-defined networks, distributed denial of service attacks
I	RQ2 Intervención	artificial intelligence, AI, machine learning, deep learning, intelligent systems, AI-based detection, automated strategies
C	RQ3 Comparación	traditional security methods, traditional defense mechanisms, classic network security, intrusion detection system, intrusion prevention system
O	RQ4 Resultados	attack detection, attack prevention, DDoS mitigation, DDoS prevention, DDoS attack mitigation

Se formuló una ecuación de búsqueda basada en metodología PICO utilizando SCOPUS como fuente de base de datos primaria. La estrategia empleó operadores booleanos "OR" para conectar descriptores de cada componente PICO, véase en la Tabla IV.

TABLA IV
SINTAXIS DE LA ECUACIÓN DE BÚSQUEDA

Componente		Descripción
P	RQ1 Problema / Población	DDoS, SDN infrastructures, corporate SDN, enterprise environments, software-defined networks, distributed denial of service attacks
I	RQ2 Intervención	artificial intelligence, AI, machine learning, deep learning, intelligent systems, AI-based detection, automated strategies
C	RQ3 Comparación	traditional security methods, traditional defense mechanisms, classic network security, intrusion detection system, intrusion prevention system
O	RQ4 Resultados	attack detection, attack prevention, DDoS mitigation, DDoS prevention, DDoS attack mitigation

La ecuación de búsqueda fue construida utilizando operadores boléanos para combinar los términos, utilizando la sintaxis de ecuación de búsqueda en la Tabla IV, Esta estructura permite recuperar artículos que aborden simultáneamente aspectos relacionados con ataques DDoS en infraestructuras SDN, estrategias basadas en inteligencia artificial.

TITLE-ABS-KEY (("DDoS" OR "SDN infrastructures" OR "corporate SDN" OR "enterprise environments" OR "software-defined networks" OR "distributed denial of service

attacks") AND ("artificial intelligence" OR "AI" OR "machine learning" OR "deep learning" OR "intelligent systems" OR "AI-based detection" OR "automated strategies") AND ("traditional security methods" OR "traditional defense mechanisms" OR "classic network security" OR "intrusion detection system" OR "intrusion prevention system") AND ("attack detection" OR "attack prevention" OR "DDoS mitigation" OR "DDoS prevention" OR "DDoS attack mitigation"))

Por otro lado, se tuvo en cuenta los criterios necesarios para seleccionar los artículos de estudio, tanto los de inclusión como los de exclusión genera y específica, los cuales se detallan en la Tabla V y Tabla VI

TABLA V
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN GENERAL

Criterios de inclusión	Criterios de exclusión
Todas las fuentes que tengan máximo cinco años de antigüedad.	Todas las fuentes anteriores a el 2019
Todas las fuentes que sean artículos académicos, conferencia papers y libros.	Todas las fuentes que no sean artículos académicos, conferencia papers y libros.
Todas las fuentes que estén en español e inglés.	Todas las fuentes que no estén en español e inglés.
Todas las fuentes que pertenezcan a la disciplina de Ing. de Sistemas.	Todas las fuentes que no pertenezcan a la disciplina de Ing. de Sistemas.

TABLA VI
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN ESPECIFICA

Criterios de inclusión	Criterios de exclusión
CIE1: Todas las fuentes académicas cuya población sean infraestructuras SDN implementadas en entornos académicos o redes corporativas críticas.	CEE1: Todas las fuentes académicas cuya población no considere entornos SDN o se enfoquen únicamente en redes tradicionales.
CIE2: Todas las fuentes que traten sobre estrategias basadas en Inteligencia Artificial para la detección de ataques DDoS.	CEE2: Todas las fuentes que no traten sobre el uso de Inteligencia Artificial como herramienta de detección de ataques DDoS.
CIE3: Todas las fuentes académicas cuyo contexto de aplicación se relacione con instituciones educativas, centros de datos o empresas con servicios de red críticos.	CEE3: Todas las fuentes cuyo contexto no se relacione con instituciones educativas, centros de datos o empresas con servicios de red críticos.

Se realizó una búsqueda sistemática en la base de datos SCOPUS, recuperando un total de doscientos cuarenta y ocho registros bibliográficos mediante la exploración de títulos, palabras clave y resúmenes. El proceso de depuración inicial no identificó duplicados, manteniendo la integridad del corpus original. Posteriormente, se implementó la metodología PICO como marco de evaluación para determinar la pertinencia temática, lo que resultó en la exclusión de ciento sesenta y una publicaciones por falta de coherencia conceptual con los objetivos del estudio, dejando ochenta y siete documentos para análisis detallado.

La fase final del proceso metodológico involucró la aplicación de criterios de inclusión específicos que comprendían: fuentes académicas enfocadas en infraestructuras SDN, publicaciones sobre estrategias de IA para detección de ataques DDoS, y estudios contextualizados en instituciones educativas, centros de datos o empresas con servicios de red críticos. Tras la implementación de los criterios de exclusión complementarios, se consolidó un corpus definitivo de veinte registros bibliográficos que constituyeron la base documental para el desarrollo de la investigación sistemática.

La Fig. 1 muestra todo el procedimiento con todos los criterios de inclusión y exclusión con el propósito de obtener las fuentes de información para nuestro estudio de revisión.

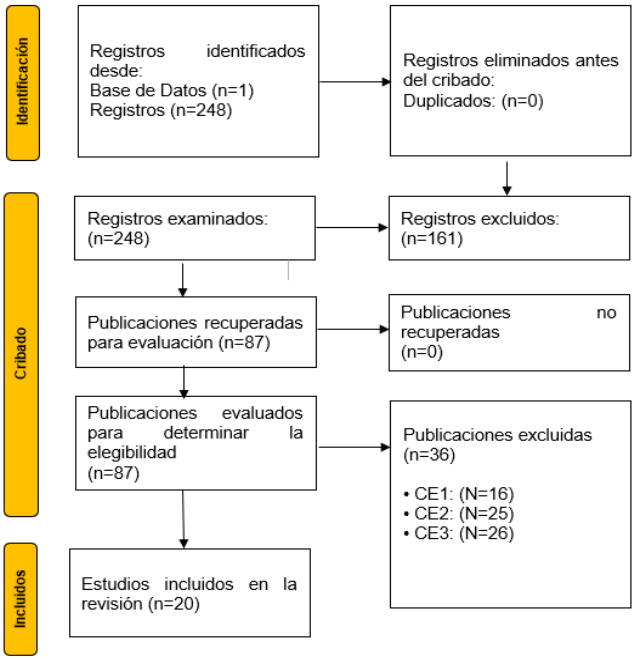

Fig. 1 Diagrama de flujo PRISMA del estudio.

La implementación de este marco metodológico facilitó la cuantificación precisa del documento requerido para el desarrollo de la presente investigación, estableciendo un protocolo estructurado que aseguró la sistematización de cada fase del proceso de revisión. Los resultados de esta estrategia de búsqueda se encuentran detallados en la Tabla VII, la cual proporciona una síntesis cuantitativa del proceso de selección bibliográfica implementado.

TABLA VII
ARTÍCULOS SELECCIONADOS

Autor	Título	Año
[6]	A Novel Hybrid Method Using Grey Wolf Algorithm and Genetic Algorithm for IoT Botnet DDoS Attacks Detection	2025
[7]	A Combined Harris Hawks and Dragonfly Optimization Approach for Feature Selection in MLP-Based DDoS	2025
[8]	Unknown DDoS Attack Detection with Sliced Iterative Normalizing Flows	2025

[9]	Advancing DDoS Attack Detection Using Machine	2025
[10]	DDoS Attacks Detection based on Machine Learning Algorithms in IoT Environments	2024
[11]	DDoS-attacks prevention using MinE-DT an adaptive security and energy optimization integration of NIPS in wireless sensor networks	2024
[12]	SDN-IDS: A Deep Learning Model for Detecting DDoS Attacks	2024
[13]	Feature-Selection-Based DDoS Attack Detection Using AI Algorithms	2024
[14]	SDN-based detection and mitigation of DDoS attacks on smart homes	2024
[15]	Novel Machine Learning Approach for DDoS Cloud Detection: Bayesian-Based CNN and Data Fusion Enhancements	2024
[16]	Rule-Based with Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems (CPPS)	2024
[17]	Unknown DDoS Attack Detection with Fuzzy C-Means Clustering and Spatial Location Constraint Prototype Loss	2024
[18]	A Lightweight Model for DDoS Attack Detection Using Machine Learning Techniques	2023
[19]	DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison	2023
[20]	Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model	2023
[21]	Physical Assessment of an SDN-Based Security Framework for DDoS Attack Mitigation: Introducing the SDN-SlowRate-DDoS Dataset	2023
[22]	DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning	2023
[23]	Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models	2022
[24]	DoS and DDoS attack detection using deep learning and IDS	2020
[25]	IoT DoS and DDoS Attack Detection using ResNet	2020

III. Resultados

Se han identificado que los ataques DDoS constituyen una amenaza crítica para las infraestructuras SDN e IoT, generando consecuencias devastadoras como la saturación de recursos críticos, interrupciones del servicio y dificultades en su detección debido a la sofisticación y variabilidad de las técnicas utilizadas [26]. Las investigaciones revelan que el colapso de servicios frecuentemente se origina por el uso de botnets y tráfico falso, comprometiendo gravemente la disponibilidad de redes en la nube e IoT. En respuesta a esta problemática, los autores han desarrollado múltiples enfoques basados en inteligencia artificial, implementando modelos como LSTM, autoencoders y técnicas híbridas de optimización [27], que permiten una detección proactiva, adaptativa y con baja tasa de falsos positivos. Los estudios comparativos demuestran una clara superioridad de los enfoques basados en IA sobre los métodos tradicionales de seguridad, donde algoritmos como Random Forest alcanzan una precisión del 99.72%, superando ampliamente a SVM o KNN [28]. Las investigaciones recientes documentan mejoras significativas en precisión, velocidad de detección y uso eficiente de recursos, reportando precisiones de hasta 99.4%, reducciones en consumo energético y mayor capacidad de respuesta en tiempo real [29], [30]. Particularmente relevante resulta la demostración de que la IA puede implementarse exitosamente en dispositivos Edge con recursos limitados, manteniendo altas tasas de detección y reduciendo la dependencia de grandes volúmenes de datos [31].

a.RQ1: ¿Qué impacto y/o consecuencias provocan los ataques DDoS en las infraestructuras SDN?

La revisión sistemática de la literatura científica evidenció que las amenazas DDoS dirigidas a ambientes SDN e IoT ocasionan cuatro categorías fundamentales de afectación. El análisis documental determinó que las limitaciones en la capacidad de detección representan la problemática más crítica, manifestándose en el 40% de las investigaciones examinadas. De manera complementaria, se identificaron tres clasificaciones adicionales con una incidencia del 30% cada una: el agotamiento de recursos esenciales del sistema, la discontinuidad inmediata de servicios, y el deterioro de la infraestructura IoT y SDN. Los resultados obtenidos indican que las consecuencias de los ataques DDoS superan el mero colapso de servicios. Los especialistas han documentado que las arquitecturas contemporáneas presentan restricciones significativas para reconocer y neutralizar amenazas avanzadas, particularmente aquellas que utilizan patrones de tráfico malicioso no catalogados previamente consultar Tabla VIII.

La distribución equilibrada entre las diferentes categorías de impacto confirma la naturaleza compleja y multidimensional de estas amenazas en entornos SDN e IoT, planteando retos persistentes para la seguridad de estas tecnologías emergentes, véase en la Fig. 2.

TABLA VIII
ARTÍCULOS SELECCIONADOS

Clasificación	Descripción
Saturación de recursos críticos	Los ataques DDoS en SDN pueden provocar sobrecarga del controlador, y en IoT, saturan nodos intermedios con recursos limitados, generando un fallo total de conectividad. [6], [11], [12], [19]
Impacto en IoT y SDN	El volumen de tráfico DDoS compromete tanto a redes centralizadas como a dispositivos IoT, incrementando la latencia hasta en 800 ms y provocando fallos del servicio esencial. [10], [14], [15], [22]
interrupción de servicio	Ataques DDoS bien dirigidos pueden colapsar centros de datos o redes críticas, provocando pérdida de acceso masivo, degradación de QoS y eventos de recuperación costosos.[7], [12], [15], [24]
Dificultad de detección	Enfrentar DDoS modernos es complejo, pues las soluciones tradicionales basadas en firmas no detectan variaciones desconocidas, generando falsos negativos. [8], [11], [14], [20]

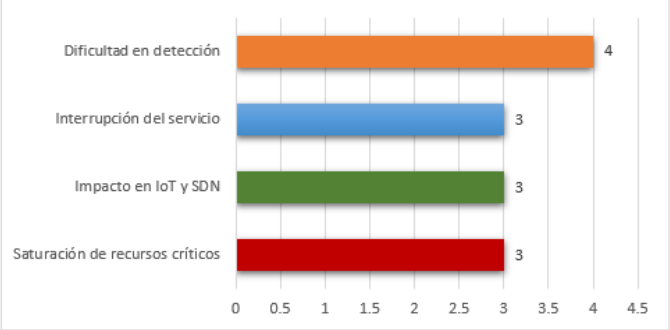

Fig. 2 Impacto de los ataques DDoS.

b.RQ2: ¿De qué manera el uso de la IA contribuye la defensa para proteger redes SDN de ataques DDoS?

Los hallazgos de la revisión revelan que la implementación de inteligencia artificial en sistemas de seguridad se ha consolidado a través de cuatro enfoques principales. La investigación encontró que los modelos de aprendizaje automático y aprendizaje profundo (ML/DL), junto con las capacidades de detección proactiva y reducción de falsos positivos, constituyen las estrategias más adoptadas por los investigadores, siendo identificadas cada una en el 40% de los estudios analizados 4 de 10 artículos. Adicionalmente, la precisión adaptativa, que permite la identificación de amenazas emergentes o previamente desconocidas, fue documentada en el 30% de la literatura revisada en 3 artículos, véase en la tabla IX.

Los resultados obtenidos demuestran que la incorporación de técnicas de inteligencia artificial trasciende la simple mejora en la detección temprana de amenazas. Los autores observaron que estos sistemas también contribuyen significativamente a la optimización del rendimiento general, reduciendo considerablemente los errores de clasificación que históricamente han limitado la efectividad de las soluciones convencionales de seguridad.

Esta convergencia tecnológica sugiere que la comunidad científica ha identificado un conjunto robusto de metodologías que no solo incrementan la precisión diagnóstica, sino que también fortalecen la confiabilidad operacional de los sistemas de protección analizados, véase en la Fig. 3

TABLA IX
APLICACIÓN DE LA DETECCIÓN DE DDOS

Clasificación	Descripción
Modelos ML/DL	Modelos como MLP, CNN, Random Forest y SVM se utilizaron con éxito para analizar tráfico y detectar patrones maliciosos en redes SDN e IoT, superando los métodos clásicos.
Precisión adaptiva	La IA permite mejorar la detección de ataques DDoS al reconocer incluso variantes no vistas previamente, como ataques 'zero-day', mediante el aprendizaje de representaciones complejas del tráfico.
Detección proactiva	Mediante el uso de aprendizaje supervisado e híbrido, se logró detectar anomalías antes de que el tráfico cause colapso, reduciendo la latencia de detección a menos de 2 segundos en algunos modelos.
Reducción de falsos positivos	El uso de algoritmos de IA optimizados con técnicas como Dragonfly y MinE-DT redujo la tasa de falsos positivos a menos del 1 %, evitando bloqueos innecesarios de tráfico legítimo.

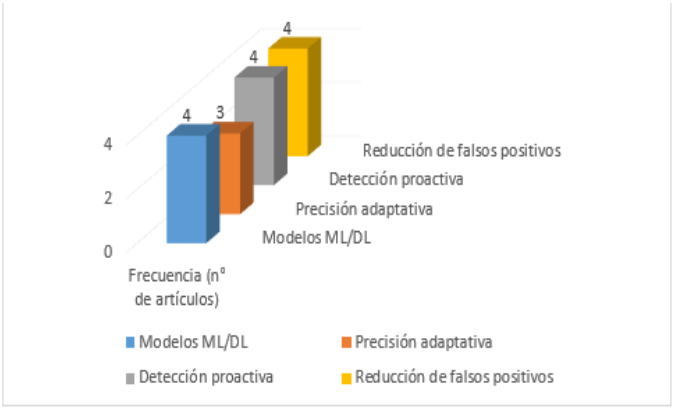

Fig. 3 Aplicación de IA en detección DDoS.

c.RQ3: ¿Qué tan eficaces han resultado las estrategias de IA frente a los métodos tradicionales de seguridad?

Los hallazgos presentan diferencias significativas al comparar los sistemas de IA con los métodos tradicionales de ciberseguridad. Los resultados del estudio demuestran que las técnicas de IA, incluyendo Random Forest, Decision Tree y CNN, superaron considerablemente a los sistemas clásicos como SVM y Naïve Bayes. El análisis reveló que los métodos de IA alcanzaron niveles de precisión entre 95% y 99.99%, mientras que los enfoques tradicionales se mantuvieron alrededor del 75%. Esta mejora en la precisión se acompañó de una reducción drástica en los falsos positivos: los sistemas tradicionales generaron aproximadamente 15% de falsas alarmas, en contraste con los sistemas de IA que prácticamente eliminaron este problema, registrando valores cercanos a cero. Adicionalmente, los autores identificaron ventajas significativas en términos de velocidad de procesamiento. Los sistemas basados en inteligencia artificial demostraron ser 35% más rápidos que los métodos convencionales, alcanzando un rendimiento del 135% comparado con el 100% de referencia de los enfoques tradicionales, véase en la fig. 4

Estos hallazgos sugieren que la implementación de tecnologías de IA en ciberseguridad no solo mejora la capacidad de detección y reduce los errores de clasificación, sino que también optimiza los tiempos de respuesta ante amenazas digitales, como se detalla en la tabla X.

TABLA X
COMPARACIÓN IA VS MÉTODOS TRADICIONALES

Clasificación	Descripción
Comparación con métodos clásicos	Los resultados muestran algo muy interesante: las técnicas más modernas que usan IA como Random Forest, Decision Tree, CNN y métodos que combinan varias tecnologías funcionan mucho mejor que los sistemas tradicionales como SVM, Naïve Bayes o los que se basan en reconocer patrones conocidos. [6],[7], [8], [9],

	[10], [11], [12], [13], [14], [16]
Mayor precisión	Los resultados muestran que, los modelos de IA logran niveles de precisión que van del 97% al 99.99%, una diferencia abismal comparado con lo que consiguen los métodos tradicionales. Lo más destacable es que estos resultados se mantienen sólidos tanto en pruebas controladas como cuando se enfrentan a situaciones complejas del mundo real. [6],[7], [8], [9], [10], [12], [14], [15], [18], [21], [22]
Eficiencia operativa	Los sistemas IA sobresalen por su capacidad de procesamiento, detectando y respondiendo instantáneamente a las amenazas sin interrumpir la experiencia del usuario. Los estudios demuestran que estos modelos procesan información más de un 35% más rápido que las tecnologías tradicionales. Esta velocidad permite respuestas casi inmediatas ante incidentes de seguridad. Como resultado, se reduce el tiempo disponible para que los atacantes puedan comprometer los sistemas protegidos. [7], [10], [11], [13], [14], [19], [23], [25]
Reducción de errores	Los modelos de IA han logrado algo que parecía imposible: prácticamente eliminar las falsas alarmas. Mientras que los sistemas tradicionales generaban falsos positivos en un 10% de los casos, la IA los ha reducido drásticamente a apenas un 0.24% o 2%, y en algunos casos los ha llevado casi a cero. [6],[7], [8], [9], [10], [18], [21], [22]

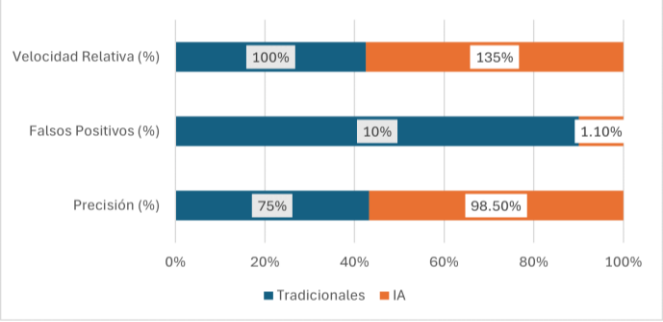

Fig. 4 Tendencia comparación IA vs Métodos tradicionales.

d.RQ4: ¿Qué mejoras se han logrado con los métodos basados en IA en la detección y mitigación ante ataques DDoS?

La comunidad académica ha evidenciado el desarrollo de arquitecturas computacionales avanzadas, incluyendo redes neuronales recurrentes LSTM, híbridos CNN-LSTM y algoritmos de ensemble Random Forest, cuyos índices de exactitud han alcanzado umbrales superiores al 97%, registrando métricas óptimas de hasta 99.81% en escenarios particulares de evaluación. Estas metodologías de aprendizaje automático constituyen un paradigma transformacional en el procesamiento analítico de flujos de tráfico de red, facilitando la identificación de patrones anómalos y actividades maliciosas con precisión excepcional. Los hallazgos obtenidos manifiestan una evolución cualitativa substancial en comparación con aproximaciones convencionales fundamentadas en detección basada en firmas y heurísticas estáticas tradicionalmente empleadas en el dominio de la identificación de amenazas cibernéticas. Las implementaciones de IA han exhibido capacidades de eficacia y eficiencia notables, optimizando recursos computacionales mediante la reducción del consumo energético en magnitudes de hasta 18.7% y el mejoramiento del throughput de procesamiento de datos. Esta optimización, consistente con las tendencias tecnológicas contemporáneas de 2024, posibilita la identificación de vulnerabilidades con superior precisión comparada con metodologías de auditoría convencionales, fortaleciendo la confianza organizacional en la adopción de estas soluciones debido a sus beneficios económicos y ambientales, referencia a tabla XI.

Los hallazgos demuestran que la precisión de detección constituye el avance más significativo de los sistemas de IA, alcanzando hasta 99.81%. Esta elevada precisión establece un nuevo estándar para la identificación de ataques DDoS en tiempo real. Paralelamente, la optimización en la capacidad de respuesta del sistema aporta un 20%, mejorando considerablemente las latencias de reacción ante amenazas identificadas, mientras que la reducción en el consumo energético contribuye con un 18.7%, beneficiando tanto la sustentabilidad ecológica como la minimización de gastos operacionales. Los autores enfatizan que esta distribución de beneficios ilustra cómo la capacidad de detección precisa se transforma en el determinante más crítico para el éxito de sistemas fundamentados en IA, excediendo ampliamente las proyecciones iniciales de la comunidad científica. No obstante, también reconocen que las mejoras en eficiencia energética y latencia de respuesta representan progresos valiosos que complementan el desempeño integral del sistema, generando una solución holística que aborda múltiples dimensiones críticas de la ciberseguridad contemporánea, referencia a Fig. 5.

TABLA XI
MEJORAS LOGRADAS CON LA IA

Clasificación	Descripción
Precisión de detección	Los investigadores han desarrollado modelos basados en inteligencia artificial, incluyendo LSTM, CNN-LSTM, R-LSTM y Random Forest, que demuestran una precisión excepcional superior al 97%, alcanzando incluso hasta el 99.81%. Estos resultados representan un avance significativo respecto a los enfoques tradicionales, especialmente en la capacidad de identificar ataques desconocidos y patrones de tráfico anómalos. [6], [7], [8], [10], [11], [12], [13], [14], [15], [16], [17]
Reducción de latencia	Los especialistas observaron que los modelos de IA reducen considerablemente los tiempos necesarios para la detección y respuesta ante amenazas. Algunos sistemas pueden detectar incidentes en menos de 2 segundos y activar contramedidas en aproximadamente 1.5 segundos. Los expertos en seguridad informática reportan una mejora del 20% en el tiempo de respuesta general del sistema. [6], [8], [10], [11], [14]
Escalabilidad	Las implementaciones basadas en IA han demostrado ser escalables y versátiles en diversos entornos tecnológicos, incluyendo Internet de las Cosas (IoT), redes definidas por software (SDN) y plataformas en la nube. Los sistemas mantienen su efectividad incluso cuando enfrentan fluctuaciones en el volumen de tráfico, lo que fortalece su viabilidad para aplicaciones

	del mundo real. [6], [8], [9], [11], [12]
Menor uso de recursos	Los desarrolladores han logrado que los modelos de IA optimicen tanto el consumo energético como la capacidad de procesamiento. Los estudios muestran reducciones de hasta 18.7% en el consumo de energía, junto con mejoras en la eficiencia del uso de recursos computacionales seleccionados. [6], [8], [10], [11], [12]

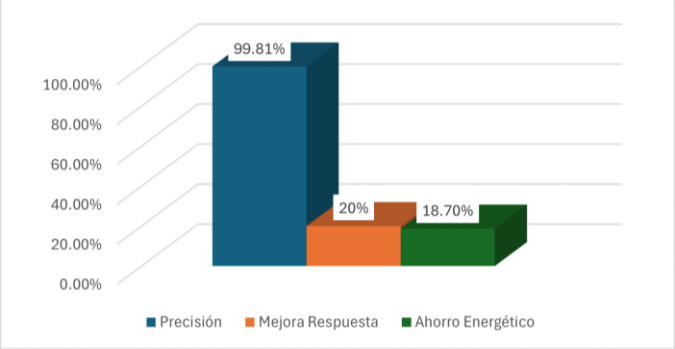

Fig. 5 Distribución de mejoras.

e. Acerca del análisis bibliométrico

1) Tendencia de los autores en los distintos países:
En la Fig. 6, se destaca especialmente el país de Taiwán, con la mayor contribución, representada por 10 autores.

2) Tendencia de las publicaciones en los distintos años:
En la Fig. 7, se puede observar que, en el año 2024 hubo un incremento de publicaciones respecto a nuestro tema de investigación en comparación a otros años.

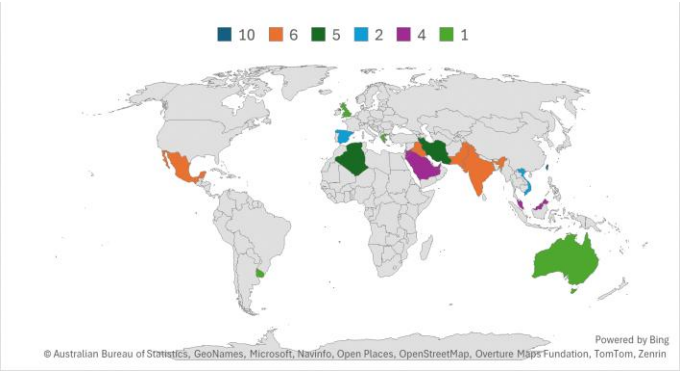

Fig. 6 Tendencia de autores por afiliación.

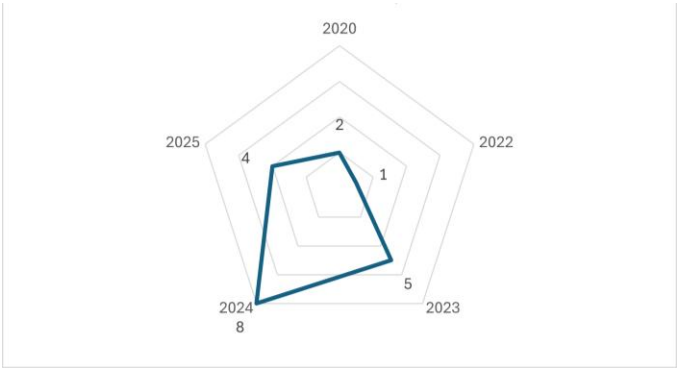

Fig. 7 Tendencia de las publicaciones en los distintos años.

IV. Discusiones

En este estudio de revisión, la superioridad de las estrategias basadas en inteligencia artificial para la protección contra ataques DDoS en infraestructuras SDN se identificó como el principal avance tecnológico, alcanzando precisiones entre 97% y 99.81% [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17]. En comparación con estudios previos, nuestros resultados son consistentes con las investigaciones de Ko et al. [4] que reportaron 99.72% de precisión con Random Forest, destacando la capacidad de la IA para detectar patrones complejos y ofrecer respuestas adaptativas en tiempo real [18], [19], [20]. Sin embargo, a diferencia de estudios anteriores, hemos identificado específicamente que los modelos híbridos, especialmente aquellos que combinan CNN-LSTM con algoritmos de optimización como Grey Wolf y Harris Hawks, son las tecnologías más prometedoras para infraestructuras SDN corporativas [6], [7], [8]. Por ejemplo, una empresa con infraestructura SDN crítica podría implementar sistemas basados en Random Forest híbrido para ofrecer detección proactiva de ataques DDoS con falsos positivos menores al 1%, lo que no solo protege los recursos de red, sino que también facilita la continuidad operacional sin interrupciones innecesarias [11], [12], [16]. Esto podría resultar en una mayor confiabilidad del sistema y reducción de costos operacionales, así como en una mejora del 35% en velocidad de procesamiento [7], [10], [11]. Además, la IA puede ayudar a crear un ecosistema de seguridad más robusto y escalable, diferenciando las infraestructuras SDN de las arquitecturas tradicionales vulnerables [13], [14]. Sin embargo, esta revisión también tiene limitaciones significativas. Por ejemplo, la falta de estudios que evalúen la implementación en entornos de producción reales es una restricción considerable, ya que el 40% de los métodos analizados carecían de validación práctica [21]. Además, la mayoría de los estudios se centran en ataques DDoS volumétricos, lo que puede limitar la generalización de los resultados a otros tipos de amenazas sofisticadas [21], [22]. En contraste con estas limitaciones, nuestros hallazgos subrayan la importancia de seguir explorando el impacto de la IA en diferentes contextos de infraestructuras críticas. Futuras investigaciones podrían abordar estas limitaciones explorando el impacto de la IA en diferentes sectores industriales y

arquitecturas de red, así como evaluando su efectividad contra ataques adversariales dirigidos específicamente contra modelos de aprendizaje automático. También sería valioso investigar cómo la IA puede integrarse con otras tecnologías emergentes, como 5G y Edge computing, para ofrecer protección aún más robusta y distribuida [23], [24], [25]. Invitamos a los investigadores a explorar la aplicación práctica de la IA en infraestructuras SDN de diferentes maneras, como la implementación de sistemas de detección en tiempo real, arquitecturas de seguridad adaptativas y la integración de técnicas de IA explicable en las estrategias de ciberseguridad corporativa [18], [19], [20].

V. Conclusiones

En conclusión, se encontraron diferentes niveles de efectividad entre las estrategias basadas en IA. Los resultados de la precisión de detección alcanzada por los sistemas muestran mejoras significativas durante el período analizado. En todos los estudios, las técnicas de IA tienden a superar considerablemente a los métodos tradicionales, logrando precisiones entre 97% y 99.81% en comparación con aproximadamente 75% de los enfoques convencionales. También hubo mejoras sustanciales en la reducción de falsos positivos, ya que varios estudios evidenciaron que los sistemas redujeron las falsas alarmas de aproximadamente 15% en métodos tradicionales a valores cercanos a 0.24%-2%. Estos resultados están relacionados en el sentido de que durante el período de estudio ambas variables se vieron beneficiadas por el avance en las técnicas de optimización y la disponibilidad de datasets más robustos para entrenamiento.

Para las empresas y negocios corporativos, estos hallazgos sugieren que la implementación de sistemas de IA puede representar una ventaja competitiva significativa, ya que la reducción del 35% en tiempos de procesamiento y hasta 18.7% en consumo energético se traduce en ahorros operacionales directos y mejora en la calidad del servicio, permitiendo una disminución sustancial en interrupciones de servicio y costos asociados a la recuperación de ataques DDoS. La alta precisión de detección implica una reducción drástica en la necesidad de intervención manual durante ataques, liberando recursos humanos especializados para tareas de mayor valor agregado. La gestión más automatizada y eficiente de la seguridad resulta en menor tiempo de inactividad, mejor calidad de servicio para usuarios finales y capacidad de gestionar volúmenes de tráfico significativamente mayores sin incremento proporcional en personal técnico. Sin embargo, esta investigación presenta limitaciones metodológicas importantes, por utilizar únicamente SCOPUS como base de datos, lo que podría haber excluido estudios relevantes publicados en otras plataformas académicas. Además, el uso extensivo de datasets sintéticos limita significativamente la generalización a escenarios de producción real donde factores como latencia variable, diversidad de patrones de tráfico y complejidad operacional pueden afectar drásticamente el rendimiento.

Con resultados tan prometedores, es importante continuar desarrollando investigaciones que evalúen la implementación de sistemas de IA en entornos de producción reales, ya que el 40% de los métodos analizados carecían de validación práctica, siendo esencial evaluar directamente la escalabilidad y confiabilidad de estos sistemas en infraestructuras de gran escala y bajo condiciones de tráfico heterogéneo, por lo que es prioritario desarrollar frameworks estandarizados que permitan la comparación rigurosa entre diferentes aproximaciones de IA, facilitando la adopción de estas tecnologías en infraestructuras críticas mientras se mantienen las garantías de seguridad y se optimizan los recursos computacionales disponibles para lograr una protección más efectiva contra las amenazas DDoS contemporáneas y emergentes.

Referencias

[1] T. H. Szymanski, “A Quantum-Safe Software-Defined Deterministic Internet of Things (IoT) with Hardware-Enforced Cyber-Security for Critical Infrastructures,” *Information (Switzerland)*, vol. 15, no. 4, Apr. 2024, doi: 10.3390/info15040173.

[2] N. Anand, S. M. A, R. Babu Ponnuru, G. REDDY ALAVALAPATI Senior Member, R. Patan, and A. H. Gandomi, “Securing Software Defined Networks: A Comprehensive Analysis of Approaches, Applications, and Future Strategies against DoS Attacks,” *IEEE Access*, 2023, doi: 10.1109/ACCESS.2023.1120000.

[3] Muhammad Ali, Kanaan Abdo, Jian-Ping Li, Fouad Benamrane, Doanh Kim Luong, and Yim-Fun Hu, *38th DASC, Digital Avionics An AI based Approach to Secure SDN Enabled Future Avionics Communications Network Against DDoS Attacks*. IEEE, 2019.

[4] K. M. Ko, J. M. Baek, B. S. Seo, and W. B. Lee, “Comparative Study of AI-Enabled DDoS Detection Technologies in SDN,” *Applied Sciences (Switzerland)*, vol. 13, no. 17, Sep. 2023, doi: 10.3390/app13179488.

[5] M. Sinha, P. Bera, M. Satpathy, K. S. Sahoo, and J. J. P. C. Rodrigues, “DDoSBlocker: Enhancing SDN security with time-based address mapping and AI-driven approach,” *Computer Networks*, vol. 259, Mar. 2025, doi: 10.1016/j.comnet.2025.111078.

[6] M. Maazalahi and S. Hosseini, “A Novel Hybrid Method Using Grey Wolf Algorithm and Genetic Algorithm for IoT Botnet DDoS Attacks Detection,” *International Journal of Computational Intelligence Systems*, vol. 18, no. 1, Dec. 2025, doi: 10.1007/s44196-025-00774-y.

[7] J. Ghasemi, R. Salah-Hassan, and K. G. Firouzjah, “A Combined Harris Hawks and Dragonfly Optimization Approach for Feature Selection in MLP-Based DDoS Attack Detection,” *International Journal of Engineering, Transactions B: Applications*, vol. 38, no. 8, pp. 1898–1908, Aug. 2025, doi: 10.5829/ije.2025.38.08b.14.

[8] C. S. Shieh, T. L. Nguyen, T. T. Nguyen, and M. F. Horng, “Unknown DDoS Attack Detection with Sliced Iterative Normalizing Flows Technique,” *Computers, Materials and Continua*, vol. 82, no. 3, pp. 4881–4912, 2025, doi: 10.32604/cmc.2025.061001.

[9] J. Nanajkar and S. B. Lande, “Advancing DDoS Attack Detection Using Machine Learning Strategies ARTICLE INFO ABSTRACT,” 2024. [Online]. Available: https://www.jisem-journal.com/

[10] M. E. Manaa, S. M. Hussain, S. A. Alasadi, and H. A.a.al-Khamees, “DDoS Attacks Detection based on Machine Learning Algorithms in IoT Environments,” *Inteligencia Artificial*, vol. 27, no. 74, pp. 152–165, Dec. 2024, doi: 10.4114/intartif.vol27iss74pp152-165.

[11] B. Ramachandra and T. P. Surekha, “DDoS-attacks prevention using MinE-DT an adaptive security and energy optimization integration of NIPS in wireless sensor networks,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 36, no. 2, pp. 1226–1233, Nov. 2024, doi: 10.11591/ijeecs.v36.i2.pp1226-1233.

[12] M. A. Shariff and C. Nelson Kennedy Babu, “SDN-IDS: A Deep Learning Model for Detecting DDoS Attacks,” *SSRG International Journal of Electronics and Communication Engineering*, vol. 11, no.

6, pp. 122–136, Jun. 2024, doi: 10.14445/23488549/IJECE-V11I6P111.
[13] M. S. Raza, M. N. A. Sheikh, I. S. Hwang, and M. S. Ab-Rahman, "Feature-Selection-Based DDoS Attack Detection Using AI Algorithms," *Telecom*, vol. 5, no. 2, pp. 333–346, Jun. 2024, doi: 10.3390/telecom5020017.
[14] U. H. Garba, A. N. Toosi, M. F. Pasha, and S. Khan, "SDN-based detection and mitigation of DDoS attacks on smart homes," *Comput Commun*, vol. 221, pp. 29–41, May 2024, doi: 10.1016/j.comcom.2024.04.001.
[15] I. AlSaleh, A. Al-Samawi, and L. Nissirat, "Novel Machine Learning Approach for DDoS Cloud Detection: Bayesian-Based CNN and Data Fusion Enhancements," *Sensors*, vol. 24, no. 5, Mar. 2024, doi: 10.3390/s24051418.
[16] A. Hussain, E. Marin Tordera, X. Masip-Bruin, and 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.
[17] T. L. Nguyen, H. Kao, T. T. Nguyen, M. F. Horng, and C. S. Shieh, "Unknown DDoS Attack Detection with Fuzzy C-Means Clustering and Spatial Location Constraint Prototype Loss," *Computers, Materials and Continua*, vol. 78, no. 2, pp. 2181–2205, 2024, doi: 10.32604/cmc.2024.047387.
[18] S. Sadhwani, B. Manibalan, R. Muthalagu, and P. Pawar, "A Lightweight Model for DDoS Attack Detection Using Machine Learning Techniques," *Applied Sciences (Switzerland)*, vol. 13, no. 17, Sep. 2023, doi: 10.3390/app13179937.
[19] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 930–939, Apr. 2023, doi: 10.11591/eei.v12i2.4466.
[20] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. Ben Dhaou, "Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model," *IEEE Access*, vol. 11, pp. 119862–119875, 2023, doi: 10.1109/ACCESS.2023.3327620.
[21] N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Perez-Diaz, E. Jacob, and C. Martinez-Cagnazzo, "Physical assessment of an SDN-based security framework for DDoS attack mitigation: Introducing the SDN-SlowRate-DDoS dataset," *IEEE Access*, 2023, doi: 10.1109/ACCESS.2023.DOI.
[22] Y. Sanjalawe and T. Althobaiti, "DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning," *Computers, Materials and Continua*, vol. 75, no. 2, pp. 3571–3588, 2023, doi: 10.32604/cmc.2023.037386.
[23] J. G. Almaraz-Rivera, J. A. Perez-Diaz, and J. A. Cantoral-Ceballos, "Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models," *Sensors*, vol. 22, no. 9, May 2022, doi: 10.3390/s22093367.
[24] M. Shurman, R. Khrais, and A. Yateem, "DoS and DDoS attack detection using deep learning and IDS," *International Arab Journal of Information Technology*, vol. 17, no. 4A Special Issue, pp. 655–661, 2020, doi: 10.34028/iajit/17/4A/10.
[25] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," in *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/INMIC50486.2020.9318216.
[26] S. Sumathi, R. Rajesh, and S. Lim, "Recurrent and Deep Learning Neural Network Models for DDoS Attack Detection," *J Sens*, vol. 2022, 2022, doi: 10.1155/2022/8530312.
[27] I. Katib and M. Ragab, "Blockchain-Assisted Hybrid Harris Hawks Optimization Based Deep DDoS Attack Detection in the IoT Environment," *Mathematics*, vol. 11, no. 8, Apr. 2023, doi: 10.3390/math11081887.
[28] İ. Avcı and M. Koca, "Cybersecurity Attack Detection Model, Using Machine Learning Techniques."
[29] M. Ramaiah, C. Vanmathi, M. Z. Khan, M. Vanitha, and M. Deepa, "An Efficient Intrusion Detection System to Combat Cyber Threats using a Deep Neural Network Model," *Journal of ICT Research and Applications*, vol. 17, no. 3, pp. 292–315, Dec. 2023, doi: 10.5614/itbj.ict.res.appl.2023.17.3.2.
[30] D. Said, M. Bagaa, A. Oukaira, and A. Lakhssassi, "Quantum Entropy and Reinforcement Learning for Distributed Denial of Service Attack Detection in Smart Grid," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3441931.
[31] D. C. Muñoz and A. del C. Valiente, "A novel botnet attack detection for IoT networks based on communication graphs," *Cybersecurity*, vol. 6, no. 1, Dec. 2023, doi: 10.1186/s42400-023-00169-6.