ISBN: 978-628-96613-2-3. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LEIRD2025.1.1.419

Artificial intelligence-based detection methods in software-defined networks for identifying denial-of-service attacks. A systematic literature review

Abstract– ***As software-defined networks (SDNs) expand, so do the threats that affect them, especially denial-of-service (DoS) attacks. The ability to efficiently detect these attacks is critical to maintaining the integrity and availability of services in SDN environments. The purpose of this research is to conduct a systematic review (SR) of artificial intelligence (AI)-based detection methods used in SDN to detect DoS attacks, analyzing their technological characteristics and efficiency. To this end, 70 documents obtained from the Scopus and Web of Science databases, published between 2021 and 2025, were rigorously analyzed, including machine learning and deep learning models focused on detecting these threats. This review covers aspects such as: the characteristics of denial-of-service (DoS) attacks, the AI methods and models used, as well as the metrics and performance measures reported in the studies to evaluate the efficiency of these methods. The results show that most approaches achieve detection rates above 80% when using metrics such as accuracy, recall, and F1-score; however, limitations are identified in the detection of low-intensity attacks and in the handling of unbalanced datasets. In conclusion, it is indicated that artificial intelligence-based methods have high potential for protection in software-defined networks; however, an improvement in performance metrics and an adequate response to different attack variants are considered necessary in order to achieve greater effectiveness in real environments.***

Keywords – ***attack detection, Software-Defined Networks, artificial intelligence, efficiency metrics, network security.***

Métodos de detección basados en inteligencia artificial en redes definidas por software para la identificación de ataques de denegación de servicio. Una revisión sistemática de literatura

Resumen– ***A medida que las redes definidas por software (SDN) se van expandiendo, también lo hacen las amenazas que las afectan, especialmente los ataques de denegación de servicios (DoS). La capacidad de detectar eficientemente estos ataques es fundamental para mantener la integridad y disponibilidad de los servicios en los entornos SDN. El propósito de esta investigación es realizar una revisión sistemática de literatura (RSL) de los métodos de detección basados en inteligencia artificial (IA) utilizados en SDN para detectar ataques DoS, analizando sus características tecnológicas y su eficiencia. Para ello, se analizaron rigurosamente 70 documentos obtenidos de las bases de datos Scopus y Web of Science, publicados entre 2021 y 2025, que incluyen modelos de aprendizaje automático y profundo enfocados en la detección de estas amenazas. Esta revisión abarca aspectos como: las características de los ataques de denegación de servicio (DoS), los métodos y modelos de IA empleados, así como las métricas y medidas de rendimiento reportadas en los estudios para evaluar la eficiencia de estos métodos estudiados. En los resultados se observa que en la mayoría de los enfoques se alcanzan tasas de detección superiores al 80 % al utilizar métricas como precisión, recall y F1-score; no obstante, se identifican limitaciones en la detección de ataques de baja intensidad y en el manejo de conjuntos de datos desbalanceados. En conclusión, se indica que los métodos basados en inteligencia artificial tienen alto potencial para la protección en SDN; no obstante, se considera necesaria una mejora en las métricas de rendimiento y una respuesta adecuada ante las distintas variantes de ataques, con el fin de lograr mayor eficacia en entornos reales.***

Keywords – attack detection, Software-Defined Networks, artificial intelligence, efficiency metrics, network security.

I. Introducción

En el contexto actual, las SDN introdujeron una nueva forma de gestionar las redes. A través de su arquitectura desacoplada al separar el plano de control del plano de datos y centralizar la gestión en un controlador lógico, este modelo permite administrar los recursos de red de manera rápida, programable, flexible y escalable a diferencia de las redes tradicionales [1]. La centralización de la red genera grandes beneficios pero también se vuelve su mayor debilidad, al grado que la saturación del controlador causa el fallo generalizado de la red, ya que se vuelve un punto único de fallo [2].

Entre los ataques que aprovechan mejor las vulnerabilidades de la arquitectura desacoplada de las SDN, se encuentran los de DoS y sus variantes, las cuales pueden sobrecargar el sistema, ralentizar drásticamente o dejar completamente inoperativos los servicios de red [3]. Los DoS están evolucionando constantemente, generando la aparición de variantes más sofisticadas, volviendo obsoletos los métodos de detección tradicionales, ya que suelen depender de firmas o criterios predefinidos, que requieren actualizaciones constantes para mantenerse efectivos [4]. Como respuesta, se ha optado por utilizar métodos basados en modelos de inteligencia artificial (IA), específicamente Aprendizaje Automático (ML) y el Aprendizaje Profundo (DL). Estos métodos pueden manejar grandes volúmenes de datos, identificar anormalidades, patrones complejos de tráfico y ofrecen soluciones inteligentes y dinámicas para la detección DoS [5]. A diferencia de los métodos tradicionales, los basados en IA pueden adaptarse a nuevas variantes de ataques de forma más eficiente. No obstante, aún existen desafíos significativos como detección de ataques de baja intensidad, el manejo de conjuntos de datos desequilibrados, la interpretabilidad de los modelos y las limitaciones de recursos en los controladores SDN [6]. Además, muchas soluciones propuestas han sido evaluadas en entornos fuera de línea o con conjuntos de datos no específicos para SDN, lo que restringe su aplicabilidad en escenarios reales [4].

La adición de IA en ambientes SDN facilitará la creación de respuestas más eficientes ante ataques DoS en sitios de comercio electrónico, donde la disponibilidad constante es fundamental. Los métodos basados en IA tienen la capacidad de identificar comportamientos inusuales en tiempo real, ajustarse a nuevas amenazas y reducir los ataques antes que estos impacten en la operación [7]. De este modo, ayudan a salvaguardar ingresos, la confianza del usuario y la solidez del negocio digital.

El propósito de esta investigación es realizar una revisión RSL con el objetivo de explorar la eficiencia de los métodos basados en inteligencia artificial para la detección de ataques de denegación de servicios en el contexto de las SDN. Los resultados de esta revisión ayudarán a conocer las capacidades y limitaciones de los métodos de detección actuales, orientando futuras direcciones de investigación hacia soluciones más eficientes para las SDN.

II. METODOLOGÍA

El RSL se realizó a través de un enfoque de selección guiada, el cual fue diseñado para garantizar el análisis bibliográfico estructurado de manera clara, concisa y

específica al tema seleccionado. Este método se basó en la formulación de una pregunta principal de investigación que se enfoca en lo que se quiere conocer del tema: ¿cuál es la eficiencia de los métodos de detección basados en inteligencia artificial frente a los ataques de DoS en SDN? De la cual derivan tres preguntas específicas. La primera pregunta estudia las características de la amenaza, PE1: ¿Qué características tienen los ataques DoS en SDN?. La segunda pregunta estudia qué tecnologías se utilizan para combatir o identificar las amenazas: PE2: ¿Qué métodos de detección basados en inteligencia artificial emplean las SDN para identificar ataques DoS?. La tabla I, presenta las palabras clave empleadas para cada pregunta específica..

TABLA I
CRITERIOS DE INCLUSIÓN ESTRUCTURA DEL MÉTODO DE SELECCIÓN GUIADA

ITEM	KEYWORDS
PE1	Distributed Denial of Service, Denial of Service attack, Software Defined Network, attack y characteristics
PE2	machine learning, deep learning y methods
PE3	effectiveness, efficiency y performance

El sustento científico de los datos utilizados se basa en la búsqueda de información en las plataformas Scopus y Web of Science (WOS). Se aplicaron los siguientes filtros: año (2021–2025), acceso (Open Access), idioma (inglés, ucraniano) y tipo de documento (artículo, ponencia de conferencia, revisión). Para la recolección de información, se generó una cadena de búsqueda utilizando las palabras clave definidas previamente, la fórmula de búsqueda resultante fue la siguiente:(TITLE-ABS-KEY ((("DDoS" OR "Distributed Denial of Service" OR "DoS attack" OR "Denial of Service attack") AND ("SDN" OR "Software Defined Network" OR "Software Defined Networking") AND ("attack characteristics" OR "attack vectors" OR "impact" OR "types" OR "nature" OR "patterns" OR "features"))AND(("artificial intelligence" OR "AI" OR "machine learning" OR "deep learning" OR "neural networks")
AND ("mitigation" OR "detection" OR "protection" OR "defense" OR "countermeasure"))AND("efficiency" OR "performance" OR "effectiveness" OR "evaluation")) AND PUBYEAR > 2020 AND PUBYEAR < 2026 AND (LIMIT-TO (OA , "all"))

La búsqueda se finalizó el 4 de mayo del 2025, además se tomaron en cuenta los siguientes criterios de inclusión descritos en la tabla II y exclusión descritos en tabla III.

TABLA II
CRITERIOS DE INCLUSIÓN

ITEM	CRITERIO
CI1	Artículos de investigación que presenten métodos o propuestas para la detección de ataques DoS utilizando Inteligencia Artificial (IA)
CI2	Los estudios deben estar explícitamente enfocados y evaluados en el contexto de SDN.
CI3	Los artículos deben incluir una evaluación o análisis de la eficiencia del método propuesto.

TABLA III
CRITERIOS DE EXCLUSIÓN

ITEM	CRITERIO
CE1	Artículos que no traten ataques ataques DoS o solo los mencionan sin abordarlos específicamente.
CE2	Trabajos que utilicen exclusivamente redes tradicionales, redes de IoT, o cualquier otro tipo de arquitectura de red que no sea SDN como contexto principal de evaluación**.**
CE3	Artículos que describan un método de detección de DDoS basado en IA en SDN pero no presenten métricas de evaluación de su desempeño o eficiencia claras y cuantificables.

Se incluyeron estos criterios a la formula de busqueda , el resultado final fue:(TITLE-ABS-KEY (("DDoS" OR "Distributed Denial of Service" OR "DoS attack" OR "Denial of Service attack" OR "Distributed Flooding Attack" OR "Flood Attack" OR "Volume-based DDoS attack" OR "Layer 7 DDoS attack") AND ("SDN" OR "Software Defined Network" OR "Software Defined Networking" OR "Network Function Virtualization" OR "NFV" OR "Virtualized Networks" OR "Programmable Networks") AND ("attack characteristics" OR "attack vectors" OR "attack signatures" OR "attack methods" OR "attack behaviors" OR "impact" OR "damage" OR "effect" OR "consequences" OR "disruption" OR "performance degradation" OR "types" OR "classification" OR "variants" OR "forms" OR "categories" OR "nature" OR "properties" OR "attributes" OR "patterns" OR "trends" OR "regularities" OR "behaviors" OR "strategies" OR "features" OR "elements" OR "traits" OR "aspects")) AND TITLE-ABS-KEY (("artificial intelligence" OR "AI" OR "machine learning" OR "deep learning" OR "neural networks") AND ("mitigation" OR "detection" OR "protection" OR "defense" OR "countermeasure")) AND TITLE-ABS-KEY (("efficiency" OR

"performance" OR "effectiveness" OR "evaluation"))) AND PUBYEAR > 2020 AND PUBYEAR < 2026 AND (LIMIT-TO (OA , "all")) .

Se identificaron inicialmente 178 artículos en las bases de datos Scopus y Web of Science. Se sigue una revisión sistemática según las directrices de la declaración PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), la cual señala estándares para asegurar la presentación clara y la transparencia en estudios de este tipo [8]. Tal como muestra la Fig.1, durante la fase de identificación, se eliminaron 60 registros duplicados, quedando 118 artículos para ser cribados. En la fase de cribado, se revisaron los títulos y resúmenes, donde se excluyeron 30 registros por no cumplir con los criterios de inclusión previamente establecidos. De los 88 documentos restantes, 8 no pudieron ser recuperados por problemas de acceso. A continuación, se evaluaron 80 artículos en texto completo, con base en criterios rigurosos de inclusión y exclusión. Como resultado de esta evaluación, 10 publicaciones fueron excluidas: por no centrarse en la temática de interés, y por no cumplir con los requisitos metodológicos establecidos.

La revisión sistemática considera finalmente 70 estudios. Todos estos estudios responden a los objetivos y lineamientos definidos desde el comienzo de la investigación. Este proceso, basado en la declaración PRISMA, ofrece una estructura metodológica clara. Se favorece la transparencia, la precisión en los resultados y la posibilidad de reproducir el estudio. También se asegura un nivel adecuado de calidad y se facilita el uso de la evidencia por parte de otros investigadores en futuras actualizaciones [8].

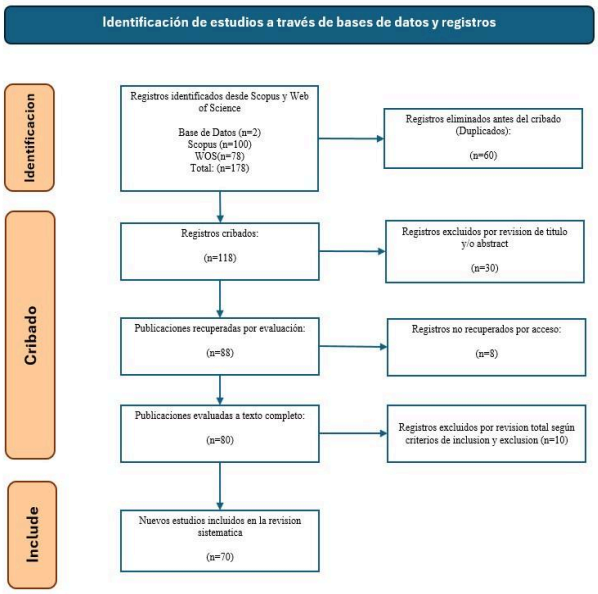

Fig 1. Diagrama PRISMA.

III. RESULTADO Y DISCUSIONES

A. Bibliometría

Tal como se muestra en Fig.2. En el 2021 se publicaron 9 documentos, se incrementó a 13 en 2022, reflejando un crecimiento del interés investigativo, el punto más alto se alcanzó en 2023 con 21 documentos, indicando un máximo de producción académica, después, la tendencia descendió a 20 documentos en 2024 y 7 en 2025 el bajo número en el último año se debe a que apenas estamos 6 de mayo.

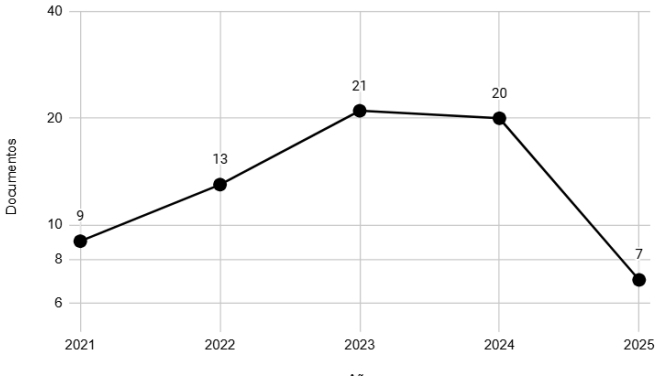

Fig.2 Documentos indizados por años.

La Fig. 3 muestra cómo se distribuyen los documentos según el país donde se publican. Estados Unidos tiene el 34.29% de las publicaciones y toma el primer lugar, este país mantiene un alto nivel de actividad científica. Basilea, en Suiza, aparece en segundo lugar con el 32.86% de las publicaciones y demuestra una presencia fuerte en la producción científica global.

Reino Unido se sitúa en tercer lugar con el 10.00% de las publicaciones, mostrando una participación destacada en la comunidad académica. Por otro lado, Países Bajos cuenta con el 8.57%, evidenciando un aporte significativo en la investigación científica. China e Indonesia aportan el 2.86% cada uno, esto indica un interés creciente en la investigación. Finalmente, Vietnam, Ucrania, Polonia, Qatar, Canadá e India aportan un 1.43% cada uno, mostrando cómo la investigación científica se extiende a diferentes regiones del mundo.

Este análisis explica cómo varios países suman aportes al conocimiento científico durante el periodo evaluado. Algunos ya tienen una presencia sólida, mientras que otros crecen y avanzan dentro de la comunidad científica internacional.

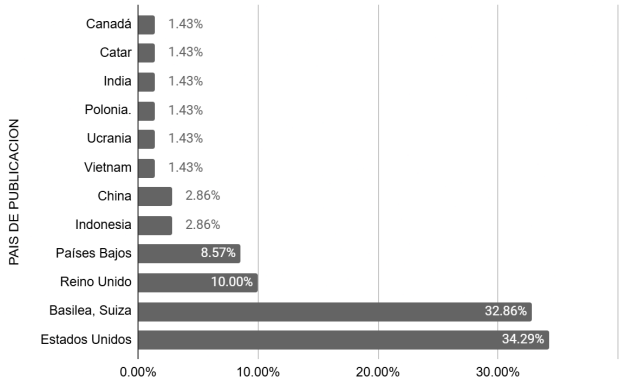

Fig.3 Documentos indizados por países.

Tal como se muestra en Tabla IV, las keywords con mayor frecuencia en los documentos son "machine learning", "denial-of-service attack" y "distributed denial of service". Estos términos aparecen con constancia y muestran el interés por estos temas en la literatura. Aunque "machine learning" tiene más ocurrencias, su total link strength es menor que el de otras como "denial-of-service attack", lo que muestra que se usa en varios contextos y no se enfoca únicamente en ciberseguridad. En cambio, "network security" y "software-defined networking" muestran una relación más fuerte con otros términos, lo que señala una conexión más directa con el eje temático.

En este contexto, la ocurrencia hace referencia a la cantidad de veces que una palabra clave aparece en los documentos analizados, mientras que el total link strength indica la fuerza total de las conexiones que esa palabra tiene con otras, es decir, cuán frecuentemente aparece junto a otras palabras clave dentro del mismo conjunto de documentos.

TABLA IV
CO-OCURRENCIA DE KEYWORDS

Keyword	Occurrences	Total link strength
denial-of-service attack	32	157
network security	26	131
distributed denial of service	29	128
software-defined networkings	24	126
denial of-service attacks	20	114
machine learning	33	111
software defined networking	24	106
deep learning	26	86
machine -learning	13	75
sdn	19	60

Nota: Elaborada a partir de los documentos analizados.

B. Preguntas Específicas

Los resultados se basan en responder las preguntas específicas planteadas en la sección II, para la PE1. ¿Qué características tienen los ataques DoS en SDN?.

Resultado del análisis sistemático de la documentación, se planteó una categorización de las variantes de los ataques DoS, específicamente los documentos [9], [10], [11] y [12], presentan clasificaciones similares, basándonos en la performance de sus ataques, agrupando las variantes para un mejor análisis de sus características.

Los clasificamos en 4 tipos, CT1: Ataques de Saturación de Ancho de Banda, son ataques ciegos en cuanto a objetivos, buscando abrumar la capacidad de los recursos de red [12], CT2: Ataques de Explotación de Protocolos, se enfoque en aprovechar las vulnerabilidades de protocolos de capa 3 y 4 del modelo OSI [12], CT3: Ataques de Explotación de Aplicaciones, están dirigidos a servicios o aplicaciones específicas, se enfocan en la capas superiores del modelo OSI de la 5 a la 7 [8], CT4: Ataques Lentos, son de alta frecuencia pero de bajo volumen, esta categoría incluye ataques que están en las tres primeras, porque tienen subtipos que se comportan como lentos [12].

La tabla V, que presentamos a continuación agrupa en las variantes en sus respectivas categoría según su performance de ataque, podemos observar la distribución de las variantes encontradas en los 70 documentos analizados. En CT1, se encuentran presentes en 50 documentos (71.43% del total de documentos), destacándose como la categoría más preponderante, las variantes que se destacan son UDP Flooding (50.00% del total de CT1), ICMP Flooding (48.00%) y TCP SYN Flood (46.00%). En CT2, se encuentra presente en 35 de documentos (50.00%), las variantes que se destacan son TCP SYN Flood (97.14% del total de CT2), Packet-in Flooding (11.43%). En CT3, se encuentra presente en 28 documentos 40.00%, las variantes que se destacan son HTTP GET/POST (HTTP GET/POST Flooding) (50.00% del total de CT3), NetBIOS (10.71%). En CT4, se encuentra presente en 19 documentos 27.14%, reflejando la poca investigación sobre estos ataque en comparación con las demás categorías, las variantes que se destacan son TCP SYN Flood (78.95% del total de CT4), UDP Flooding (73.68%) y Slowloris Attack (42.11%).

Podemos observar que la variante TCP SYN Flood aparece en tres categorías, en CT1 y CT2, algunos autores destacan que este tipo de ataque puede comportarse de ambas maneras [12]. En algunos casos, simplemente satura el ancho de banda enviando múltiples solicitudes TCP [13]; en otros, busca explotar vulnerabilidades específicas del protocolo TCP [14]. Además, también se incluye en la CT4, ya que puede enviar mensajes de bajo volumen pero con alta frecuencia, lo que le permite pasar desapercibido y evadir mecanismos de detección [15],[16]

TABLA V
VARIANTES DE DDoS POR CATEGORÍAS

Item	Subtipos	Documentos	Porcentaje
CT1	UDP Flooding	25	50.00%
	ICMP Flooding	24	48.00%
	TCP SYN flood	23	46.00%
	Ataques de reflexión(DNS Amplification)	13	26.00%
	IP-Spoofing:	5	10.00%
	Smurf Attack	4	8.00%
	otros	16	32.00%
	(*) TOTAL PARCIAL	50	71.43%
CT2	TCP SYN Flood	34	97.14%
	Packet-in Flooding	4	11.43%
	PUSH ACK Attack (o PUSH ACK Flooding)	3	8.57%
	Teardrop Attack	3	8.57%
	otros	6	17.14%
	(*) TOTAL PARCIAL	35	50.00%
CT3	HTTP GET/POST (HTTP GET/POST Flooding)	14	50.00%
	NetBIOS	3	10.71%
	GoldenEye	3	10.71%
	Otros	6	21.43%
	(*) TOTAL PARCIAL	28	40.00%
CT4	TCP SYN Flood	15	78.95%
	UDP Flooding	14	73.68%
	Slowloris Attack(Body, Header y Read)	8	42.11%
	Otros	6	31.58%
	(*) TOTAL PARCIAL	19	27.14%
TOTAL DOCUMENTOS		70	

(*) Es el total de documentos que abordan esta categoría de ataques. El porcentaje se calcula con respecto al total de documentos.

NOTA: Los porcentajes de los subtipos se calculan con respecto al total de cada categoría, no sobre el total de documentos. Un mismo documento puede analizar más de una categoría, por lo tanto, la suma de los porcentajes puede superar el 100%.

Respecto a la PE2: ¿Qué modelos y métodos de detección basados en inteligencia artificial emplean las SDN para identificar ataques DoS?

Los métodos basados en inteligencia artificial obtienen mejores resultados de precisión, por encima de lo que normalmente se espera de métodos convencionales [17]. A partir del estudio de un conjunto de 70 artículos, se creó la Tabla VI para el análisis de los modelos utilizados por los métodos en sus experimentaciones. En el contexto del aprendizaje automático (ML); el modelo *Random Forest* tuvo mayor preferencia, fue probado en el 64.71% de los artículos que analizan ML. A este modelo, con una diferencia porcentual mínima, le siguen otros algoritmos como *K-Nearest Neighbors* (KNN) con un 45.10% y el *Árbol de Decisión* (DT) con un 41.18%. Con una diferencia porcentual ligeramente más amplia, se encuentra el uso de modelos como *Support Vector Machine* (SVM) con un 31.37%, *Naive Bayes* (NB) con un 29.41%, *Regresión Logística* (LR) con un 23.53% y *XGBoost* con un 21.57%. Con menor frecuencia, se utilizaron modelos como *K-Means Clustering* y *Whale Optimization Algorithm*, con una participación menor al 10%. En cuanto al aprendizaje profundo (DL), el modelo más utilizado en los documentos fue la *Red Neuronal Convolucional* (CNN), incluyendo sus dos variantes: CNN 1D y CNN 2D, con una frecuencia del 51.11% de los estudios analizados. Le siguen *Perceptrón Multicapa* (MLP) y *Long Short-Term Memory* (LSTM), ambos algoritmos con un porcentaje de participación del 26.67%. Otros modelos con menor presencia en los artículos fueron *Gated Recurrent Unit* (GRU) y *Deep Neural Network* (DNN), ambos con un 17.78%; *Artificial Neural Network* (ANN) con un 11.11%; y *Bidirectional LSTM* (Bi-LSTM), junto con otros modelos, con menos del 10% de participación.

En cuanto a los totales parciales presentados en la Tabla VI, se observa que 51 de los 70 documentos analizados (72.86%) emplean modelos de aprendizaje automático (ML), mientras que 45 documentos (64.29%) implementan modelos de aprendizaje profundo (DL). Estos valores reflejan que muchos estudios utilizan más de un enfoque, ya sea comparando su desempeño o integrándose de forma híbrida. Asimismo, el mayor porcentaje asociado a los modelos ML se justifica por su menor requerimiento computacional, facilidad de implementación y buenos niveles de precisión en entornos controlados. Por otro lado, aunque los modelos DL demandan más recursos, su adopción en un número significativo de estudios destaca su potencial para detectar patrones complejos en grandes volúmenes de datos. Esta dualidad evidencia una tendencia hacia enfoques combinados que maximizan las fortalezas de ambos paradigmas. Para concluir, se ha destacado que las técnicas de selección de características han sido reconocidas como un mecanismo fundamental para mejorar y optimizar el rendimiento de los modelos, ya que disminuyen la dimensionalidad del conjunto de datos y facilitan la identificación de variables importantes [7], [10], [18].

TABLA VI
MODELOS ML Y DL EN LA REVISIÓN

Tipos	Modelo	Documentos	Porcentaje
ML	Random Forest (RF)	33	64.71%
	K-Nearest Neighbors (KNN)	23	45.10%
	Decision Tree (DT)	21	41.18%
	Support Vector Machine (SVM)	16	31.37%
	Naive Bayes (NB)	15	29.41%
	Regresión Logística (LR)	12	23.53%
	XGBoost (Extreme Gradient Boosting)	11	21.57%
	K-Means Clustering	4	7.84%
	Whale Optimization Algorithm (WOA) /	2	3.92%
	Otros	13	25.49%
	(1) TOTAL PARCIAL	**51**	72.86%
DL	Convolutional Neural Network (CNN, 1D y 2D)	23	51.11%
	Multilayer Perceptron (MLP)	12	26.67%
	Long Short-Term Memory (LSTM)	12	26.67%
	Gated Recurrent Unit (GRU)	8	17.78%
	Deep Neural Network (DNN)	8	17.78%
	Red Neuronal Artificial (ANN)	5	11.11%
	Bidirectional LSTM (Bi-LSTM)	3	6.67%
	Otros	7	15.56%
	(2) TOTAL PARCIAL	**45**	64.29%
TOTAL		70	

(1) Es el total de documentos que utilizan modelos ML, el porcentaje se calcula entre el total de documentos.

(2) Es el total de documentos que utilizan modelos DL, el porcentaje se calcula entre el total de documentos.

NOTA: Los porcentajes de los subtipos se calculan con respecto al total de cada tipo, no sobre el total de documentos. Un mismo documento puede utilizar varios modelos de IA, por lo tanto, la suma de los porcentajes puede superar el 100%.

En el RSL se identificó 45 métodos más relevantes, se evaluaron a partir de cuatro aspectos clave: el modelo de aprendizaje automático (ML) o aprendizaje profundo (DL) seleccionado después de concluir las pruebas, ya sea individualmente o en combinación; el dataset empleado como fuente de datos para las experimentaciones; las métricas de rendimiento reportadas, incluyendo. Accuracy (Acc): mide la proporción de predicciones correctas (benignas y maliciosas) sobre el total de predicciones, Precisión (P): Mide la proporción de verdaderos positivos (ataques maliciosos detectados correctamente), Recall (R): Mide la proporción de verdaderos positivos (ataques maliciosos detectados correctamente) y F1-score (F1): Es la media armónica de Precision y Recall. Proporciona un equilibrio entre ambas métricas, se seleccionaron estas cuatro medidas por la su frecuencia en la documentación seleccionadas; y la clasificación del análisis, categorizado como Binario(B): clasifica en tráfico en benigno o malicioso, y Multiclass(M): Identifica 3 o más clases de ataques. La Tabla VII resume los hallazgos presentando 20 de los 45 métodos analizados. Esta selección se ha realizado para destacar los trabajos más representativos, incluyendo aquellos con los rendimientos más altos en análisis binario y multiclase, así como el método que reportó los valores más bajos, ofreciendo así una visión clara del espectro de eficacia encontrado..

De los 45 métodos analizados, Existen 10 (22.22%) que combinan modelos ML y DL, Los modelos que más escogieron después después de las experimentaciones son, CNN (31.11% de los 45 métodos), RF (20.00%), LTSM (15.56%), SVM (13.33%), KNN (11.11%). A pesar de que CNN es el más popular y es de tipo DL, los modelos ML son más seleccionados con 31 métodos (68.89%) que se implementan de forma individual o conjunta solo ML y solo DL están implementados en 28 métodos (62.22%). Esto se explica por el bajo costo computacional de implementar modelos ML [19], esta tendencia se puede atribuir al menor costo computacional que generalmente implican los modelos ML [19]. No obstante, es crucial señalar que los métodos basados en DL tienen una mayor capacidad de adaptación para identificar variantes nuevas y desconocidas de ataques DoS [20].

TABLA VI1
RESUMEN EVALUACION DE METODOS

Artículo	Modelos de ML/DL	Dataset	Acc	P	R	F1	Clasificación
[10]	RF	CSE-CIC-IDS 2018	99.130 %	98.430%	99.920%	99.130 %	B
[29]	CNN	CICIDS2017	99.000 %	97.500%	96.300%	96.900 %	B
[30]	GRU	CICIDS2019,2018	97.100 %	99.400%	94.700%	97.000 %	B
[20]	CNN	NSL-KDD	95.600 %	93.000%	89.000%	90.500 %	M
[31]	KNN	CICIDS2017	99.940 %	x	99.930%	99.970 %	M
		CSE-CIC-2018	99.920 %	x	99.920%	99.960 %	

		CICIDS2019	99.970 %	x	99.900%	99.920 %	
[17]	CNN, LSTM	Mendeley Data	99.923 %	100.000 %	100.000%	100.000 %	B
		UNSW_2018_IoT_Botnet	100.000 %	100.000 %	100.000%	100.000 %	
[32]	CNN, RF, BiLSTM	InSDN	97.770 %	97.660%	97.900%	97.780 %	B
			97.120 %	96.790%	96.880%	96.790 %	M
[33]	SVM	CICIDS2017	94.010 %	x	x	97.000 %	B
		CICIDS2019	95.570 %	x	x	97.000 %	
[34]	DNN, LSTM	CICIDS2018	99.550 %	99.360%	99.440%	99.420 %	M
[35]	SVM, KNN, XGBoost, NB, RF	SDN Dataset	99.07238%	X	X	X	B
[36]	XGBoost	NSL-KDD dataset	95.950 %	92.000%	98.000%	95.550 %	M
[37]	SVM, CNN	Generados	99.370 %	99.030%	99.600%	99.090 %	B
[27]	LSTM, RF, BI-LSTM	InSDN	99.990 %	99.990%	99.990%	99.990 %	M
[28]	CNN, MLP	InSDN	97.98%	99.99%	97%	99.98	M
[22]	RF	BoT-IoT	91%	92%	90%	92%	B
			91%	92%	90%	92%	M
[25]	1D CNN, GRU, DNN	CICIDS2019	99.81%	99.96%	99.90 %	99.93%	B
		Generados	99.88%	100%	100%	100%	
[38]	SVM	NSL-KDD	99%	99%	99%	99%	B
[26]	CNN	Generados	99.99%	99.99%	99.99 %	99.99%	B
[23]	RF	Generados	100%	x	x	x	B
[24]	RF	CICIDS2019	100.00 %	100.00%	100.00%	100.00 %	B
TOTAL MÉTODOS		45					

Respecto a la PE3, ¿Qué nivel de eficiencia y eficacia tienen los métodos de detección que emplean las SDN basados en inteligencia artificial para identificar ataques DoS?.

Para el análisis se debe tener en cuenta que los métodos entrenaron a sus modelos a través de datasets públicos, datos generados o una combinación de ambos, como se muestra en la tabla VII, el dataset más empleado fue CICICIDS, mientras que la generación de datos propios permitió a los investigadores controlar las variantes de ataques DoS incluidas en el entrenamiento[21].

La Tabla VII facilita la evaluación de la eficiencia de diversos métodos, clasificados en dos categorías: análisis binario (B) y multiclass (M). En el análisis binario, que abarca 34 métodos (75.5% del total), se observan valores de (Acc) consistentemente altos, generalmente superiores al 97%, con un rango que va desde 91% ([22]) hasta 100% ([17], [23], [24]), destacando varios estudios que superan el 99.9%, especialmente [17] (CNN, LSTM) y [23] (RF), siendo el valor más bajo 91% ([22]). La (P) promedia aproximadamente 99%, con un rango de 92% ([22]) a 100% ([17], [25]), liderada por [17] y [25] (1D-CNN/GRU/DNN). El (R) tiene un promedio aproximado de 98.8%, con un rango de 90% ([22]) a 100% ([17], [25]), destacando nuevamente [17] y [25]. El (F1) promedia cerca de 98.9%, con un rango de 92% ([22]) a 100% ([17], [25], [26]), liderado por [17], [25] y [26]. Por otro lado, en el análisis multiclass, que incluye 16 métodos (35.5% del total), el (Acc) promedia aproximadamente 97.9%, con un rango de 91% ([22]) a 99.99% ([27]), liderado por [27] (LSTM/RF/BiLSTM). La (P) promedia alrededor de 97.7%, con un rango de 92% ([22]) a 99.99% ([28]), destacando [28] (CNN/MLP). El (R) promedia cerca de 97.5%, con un rango de 90% ([22]) a 99.97% ([28]), liderado por [28]. El (F1) promedia aproximadamente 97.6%, con un rango de 92% ([22]) a 99.98% ([28]), también liderado por [28]. En resumen, los 34 métodos binarios alcanzan un promedio superior al 99%, liderados por [17] y [25], mientras que los 16 métodos de multiclasificación promedian por encima del 97%, con [27] y [28] a la cabeza, evidenciando alta eficiencia en ambas categorías con variaciones según los modelos implementados.

IV. CONCLUSIONES

El análisis minucioso de la literatura sobre la eficiencia de los métodos basados en inteligencia artificial, específicamente modelos de Machine Learning y Deep Learning para la detección de ataques DoS y sus variantes en las redes definidas por software (SDN) ha revelado importantes hallazgos y tendencias relevantes. En esta revisión de 70 artículos se observó que los enfoques basados en inteligencia artificial alcanzaron tasas de detección superiores al 90%, con picos de 100%, esto indica un alto nivel de eficiencia en la detección de estas amenazas o un sobre ajuste de los modelos utilizados en por los métodos propuestos, los métodos que dan indicios sobre este sobre ajuste son [17], [23] y [24], por su rendimiento perfecto casi en todas sus métricas. Algunos de los modelos más utilizados son Random Forest, Support Vector Machine (SVM) y Convolutional Neural Network (CNN) que logran excelentes resultados incluso en algunos escenarios más complejos y con volúmenes de datos extensos. También se identificaron diferentes estrategias metodológicas centradas en mejorar el rendimiento de los sistemas. La metodología de algunos trabajos consta de comparar varios modelos de inteligencia artificial para determinar cuál ofrece mejor rendimiento en la detección de estos ataques, mientras que otros prefieren ensamblaje o esquemas de votación con el fin de aumentar la precisión y reducir falsos positivos en la detección. Por otro lado, algunos estudios optan por un enfoque híbrido que combina técnicas tanto de machine learning como de deep learning, esto con la intención de unir

fortalezas de diferentes algoritmos y reforzar la capacidad de detección

También se identificó que los modelos de inteligencia artificial funcionan con mayor eficacia frente a ataques de intensidad moderada o alta. Sin embargo, surgen dificultades al momento de identificar ataques de baja intensidad o al trabajar con conjuntos de datos desequilibrados. Las métricas más utilizadas en los estudios son precisión, recall y F1-score, lo que señala una tendencia favorable en la reducción de falsos positivos y en el aumento de la precisión en la detección.

En síntesis, se confirma que los métodos basados en inteligencia artificial poseen un potencial considerable para fortalecer la seguridad de las redes SDN frente a ataques DoS. A pesar de ello, persiste la necesidad de mejorar el rendimiento de estas técnicas frente a amenazas más sofisticadas y en situaciones con datos desbalanceados, con el propósito de alcanzar un nivel más alto de eficacia en entornos reales y en la protección de servicios críticos.

Referencias

[1] J. Buzzio-García et al., "Exploring traffic patterns through network programmability: Introducing SDNFLow, a comprehensive OpenFlow-based statistics dataset for attack detection," IEEE Access, vol. 12, pp. 42163–42180, 2024, doi: 10.1109/ACCESS.2024.3378271.

[2] M. Raza, M. Jasim Saeed, M. B. Riaz, and M. Awais Sattar, "Federated learning for privacy-preserving intrusion detection in software-defined networks," IEEE Access, vol. 12, pp. 69551–69567, 2024, doi: 10.1109/ACCESS.2024.3395997

[3] N. Anand, M. A. Saifulla, R. Babu Ponnuru, G. Reddy Alavalapati, R. Patan, and A. H. Gandomi, "Securing software defined networks: A comprehensive analysis of approaches, applications, and future strategies against DoS attacks," IEEE Access, vol. 13, pp. 64473–64515, 2025, doi: 10.1109/ACCESS.2024.3520478.

[4] N. M. Yungaicela-Naula, C. Vargas-Rosales, and 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.

[5] H. Dhadhal and P. Kotak, "Leveraging datasets for effective mitigation of DDoS attacks in software-defined networking: significance and challenges," reks, vol. 2024, no. 2, pp. 136–146, 2024, doi: 10.32620/reks.2024.2.11

[6] H. A. Butt, K. S. A. Harthy, M. A. Shah, M. Hussain, R. Amin, and M. U. Rehman, "Enhanced DDoS detection using advanced machine learning and ensemble techniques in software defined networking," Comput. Mater. Contin., vol. 81, no. 2, pp. 3003–3031, 2024, doi: 10.32604/cmc.2024.057185.

[7] Narayan, Heena, and Amit, "A collaborative approach to detecting DDoS attacks in SDN using entropy and deep learning," J. Telecommun. Inf. Technol., 2024, doi: 10.26636/jtit.2024.3.1609.

[8] M. L. Rethlefsen and M. J. Page, "PRISMA 2020 and PRISMA-S: common questions on tracking records and the flow diagram," J. Med. Libr. Assoc., vol. 110, no. 2, pp. 253–257, 2022, doi: 10.5195/jmla.2022.1449.

[9] S. A. AlSharman, O. Al-Khaleel, and M. Al-Ayyoub, "A detailed inspection of machine learning based Intrusion Detection Systems for software Defined Networks," IoT, vol. 5, no. 4, pp. 756–784, 2024, doi: 10.3390/iot5040034.

[10] Z. Liu, Y. Wang, F. Feng, Y. Liu, Z. Li, and Y. Shan, "A DDoS detection method based on feature engineering and machine learning in software-defined networks," Sensors (Basel), vol. 23, no. 13, 2023, doi: 10.3390/s23136176.

[11] A. V. Songa and G. R. Karri, "An integrated SDN framework for early detection of DDoS attacks in cloud computing," J. Cloud Comput. Adv. Syst. Appl., vol. 13, no. 1, 2024, doi: 10.1186/s13677-024-00625-9.

[12] A. Singh and B. B. Gupta, "Distributed Denial-of-Service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions," Int. J. Semant. Web Inf. Syst., vol. 18, no. 1, pp. 1–43, 2022, doi: 10.4018/IJSWIS.297143.

[13] A. A. Sadi, M. Savi, A. Melis, M. Prandini, and F. Callegati, "Unleashing dynamic pipeline reconfiguration of P4 switches for efficient network monitoring," IEEE Trans. Netw. Serv. Manag., vol. 21, no. 3, pp. 3482–3497, 2024, doi: 10.1109/TNSM.2024.3377538.

[14] H. Wang and Y. Li, "Overview of DDoS attack detection in software-defined networks," IEEE Access, vol. 12, pp. 38351–38381, 2024, doi: 10.1109/ACCESS.2024.3375395.

[15] A. A. Bahashwan et al., "HLD-DDoSDN: High and low-rates dataset-based DDoS attacks against SDN," PLoS One, vol. 19, no. 2, p. e0297548, 2024, doi: 10.1371/journal.pone.0297548.

[16] A. H. Janabi, T. Kanakis, and M. Johnson, "Survey: Intrusion detection system in software-defined networking," IEEE Access, vol. 12, pp. 164097–164120, 2024, doi: 10.1109/ACCESS.2024.3493384.

[17] A. K. Mousa and M. N. Abdullah, "An improved deep learning model for DDoS detection based on hybrid stacked autoencoder and checkpoint network," Future Internet, vol. 15, no. 8, p. 278, 2023, doi: 10.3390/fi15080278.

[18] M. S. E. Sayed, N.-A. Le-Khac, M. A. Azer, and A. D. Jurcut, "A flow-based anomaly detection approach with feature selection method against DDoS attacks in SDNs," IEEE Trans. Cogn. Commun. Netw., vol. 8, no. 4, pp. 1862–1880, 2022, doi: 10.1109/TCCN.2022.3186331.

[19] C. L. Kumar et al., "Metaparameter optimized hybrid deep learning model for next generation cybersecurity in software defined networking environment," Sci. Rep., vol. 15, no. 1, p. 14166, 2025, doi: 10.1038/s41598-025-96153-w.

[20] R. Devi, L. Shyamala, and S. Saraswathi, "Adaptive Learning based whale optimization and convolutional neural network algorithm for Distributed Denial of Service attack detection in software defined network environment," Int. J. Recent Innov. Trends Comput. Commun., vol. 10, no. 6, pp. 80–93, 2022, doi: 10.17762/ijritcc.v10i6.5557.

[21] Ö. Tonkal, H. Polat, E. Başaran, Z. Cömert, and R. Kocaoğlu, "Machine learning approach equipped with Neighbourhood Component Analysis for DDoS attack detection in Software-defined networking," Electronics (Basel), vol. 10, no. 11, p. 1227, 2021, doi: 10.3390/electronics10111227.

[22] H. Babbar, S. Rani, and M. Driss, "Effective DDoS attack detection in software-defined vehicular networks using statistical flow analysis and machine learning," PLoS One, vol. 19, no. 12, p. e0314695, 2024, doi: 10.1371/journal.pone.0314695.

[23] M. A. Mohsin and A. H. Hamad, "Performance evaluation of SDN DDoS attack detection and mitigation based Random Forest and K-nearest neighbors machine learning algorithms," Rev. D Intell. Artif., vol. 36, no. 2, pp. 233–240, 2022, doi: 10.18280/ria.360207.

[24] R. Ma, Q. Wang, X. Bu, and X. Chen, "Real-time detection of DDoS attacks based on random forest in SDN," Appl. Sci. (Basel), vol. 13, no. 13, p. 7872, 2023, doi: 10.3390/app13137872.

[25] H. Elubeyd and D. Yiltas-Kaplan, "Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks,"

Appl. Sci. (Basel), vol. 13, no. 6, p. 3828, 2023, doi: 10.3390/app13063828

[26] Y. Al-Dunainawi, B. R. Al-Kaseem, and 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.

[27] M. A. O. Rabah, H. Drid, Y. Medjadba, and M. Rahouti, "Detection and mitigation of distributed denial of service attacks using ensemble learning and honeypots in a novel SDN-UAV network architecture," IEEE Access, pp. 1–1, 2024, doi: 10.1109/ACCESS.2024.3443142.

[28] S. Mehmood, R. Amin, J. Mustafa, M. Hussain, F. S. Alsubaei, and M. D. Zakaria, "Distributed Denial of Services (DDoS) attack detection in SDN using Optimizer-equipped CNN-MLP," PLoS One, vol. 20, no. 1, p. e0312425, 2025, doi: 10.1371/journal.pone.0312425.

[29] H. S. Ilango, M. Ma, and R. Su, "A FeedForward–convolutional neural network to detect low-rate DoS in IoT," Eng. Appl. Artif. Intell., vol. 114, no. 105059, p. 105059, 2022, doi: 10.1016/j.engappai.2022.105059.

[30] M. V. O. Assis, L. F. Carvalho, J. Lloret, and M. L. Proença Jr, "A GRU deep learning system against attacks in software defined networks," J. Netw. Comput. Appl., vol. 177, no. 102942, p. 102942, 2021, doi: 10.1016/j.jnca.2020.102942.

[31] A. I. Hassan, E. A. El Reheem, and S. K. Guirguis, "An entropy and machine learning based approach for DDoS attacks detection in software defined networks," Sci. Rep., vol. 14, no. 1, p. 18159, 2024, doi: 10.1038/s41598-024-67984-w.

[32] R. Ben Said, Z. Sabir, and I. Askerzade, "CNN-BiLSTM: A hybrid deep learning approach for network intrusion detection system in software-defined networking with hybrid feature selection," IEEE Access, vol. 11, pp. 138732–138747, 2023, doi: 10.1109/ACCESS.2023.3340142.

[33] T. E. Ali, Y.-W. Chong, and S. Manickam, "Comparison of ML/DL approaches for detecting DDoS attacks in SDN," Appl. Sci. (Basel), vol. 13, no. 5, p. 3033, 2023, doi: 10.3390/app13053033.

[34] M. A. Razib, D. Javeed, M. T. Khan, R. Alkanhel, and M. S. A. Muthanna, "Cyber threats detection in smart environments using SDN-enabled DNN-LSTM hybrid framework," IEEE Access, vol. 10, pp. 53015–53026, 2022, doi: 10.1109/ACCESS.2022.3172304.

[35] M. Amitha and M. Srivenkatesh, "Design of a hypermodel using transfer learning to detect DDoS attacks in the cloud security," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 9, 2023, doi: 10.14569/IJACSA.2023.0140957

[36] A. O. Alzahrani and M. J. F. Alenazi, "Designing a network intrusion detection system based on machine learning for software defined networks," Future Internet, vol. 13, no. 5, p. 111, 2021, doi: 10.3390/fi13050111.

[37] M. W. Nadeem, H. G. Goh, Y. Aun, and V. Ponnusamy, "Detecting and mitigating botnet attacks in software-defined networks using deep learning techniques," IEEE Access, vol. 11, pp. 49153–49171, 2023, doi: 10.1109/ACCESS.2023.3277397.

[38] L. Boukraa, S. Essahraui, K. E. Makkaoui, I. Ouahbi, and R. Esbai, "Intelligent intrusion detection in software-defined networking: A comparative study of SVM and ANN models," Procedia Comput. Sci., vol. 224, pp. 26–33, 2023, doi: 10.1016/j.procs.2023.09.007

[39] A. V. Kachavimath and Narayan, "A hybrid deep learning model with consensus-based feature selection for DDoS attacks detection in SDN," Procedia Comput. Sci., vol. 252, pp. 643–652, 2025, doi: 10.1016/j.procs.2025.01.024.

[40] N. C.m., J. Katiravan, G. S., and C. E. J.i., "A novel dual optimized IDS to detect DDoS attack in SDN using hyper tuned RFE and deep grid network," Cyber Security and Applications, vol. 2, no. 100042, p. 100042, 2024, doi: 10.1016/j.csa.2024.100042.

[41] Z. A. Khan and A. S. Namin, "A survey of DDOS attack detection techniques for IoT systems using BlockChain technology," Electronics (Basel), vol. 11, no. 23, p. 3892, 2022, doi: 10.3390/electronics11233892.

[42] M. Aslam et al., "Adaptive Machine Learning based Distributed Denial-of-Services attacks detection and mitigation system for SDN-enabled IoT," Sensors (Basel), vol. 22, no. 7, p. 2697, 2022, doi: 10.3390/s22072697.

[43] A. V. Kachavimath and Narayan, "An efficient DDoS attack detection in SDN using multi-feature selection and ensemble learning," Procedia Comput. Sci., vol. 252, pp. 241–250, 2025, doi: 10.1016/j.procs.2024.12.026.

[44] Q. T. Can, T. D. Nguyen, M. B. Pham, T. T. Nguyen, T. H. A. Tran, and T. T. M. Dinh, "An innovative hybrid model for effective DDOS attack detection in software defined networks," Int. J. Comput. Netw. Commun., vol. 16, no. 6, pp. 107–125, 2024, doi: 10.5121/ijcnc.2024.16607.

[45] J. D. Gadze, A. A. Bamfo-Asante, J. O. Agyemang, H. Nunoo-Mensah, and K. A.-B. Opare, "An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers," Technologies (Basel), vol. 9, no. 1, p. 14, 2021, doi: 10.3390/technologies9010014.

[46] H. Xu, L. Bai, and W. Huang, "An optimization-inspired intrusion detection model for software-defined networking," era, vol. 33, no. 1, pp. 231–254, 2025, doi: 10.3934/era.2025012.

[47] H. A. Alamri and V. Thayananthan, "Analysis of machine learning for securing software-defined networking," Procedia Comput. Sci., vol. 194, pp. 229–236, 2021, doi: 10.1016/j.procs.2021.10.078

[48] K.-M. Ko, J.-M. Baek, B.-S. Seo, and W.-B. Lee, "Comparative study of AI-enabled DDoS detection technologies in SDN," Appl. Sci. (Basel), vol. 13, no. 17, p. 9488, 2023, doi: 10.3390/app13179488.

[49] Z. Li, B. Yang, X. Zhang, and C. Guo, "DDoS defense method in Software-Defined Space-Air-ground network from dynamic Bayesian game perspective," Secur. Commun. Netw., vol. 2022, pp. 1–13, 2022, doi: 10.1155/2022/1886516.

[50] S. Kumar et al., "DDoS detection in SDN using machine learning techniques," Comput. Mater. Contin., vol. 71, no. 1, pp. 771–789, 2022, doi: 10.32604/cmc.2022.021669.

[51] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," Information (Basel), vol. 14, no. 1, p. 41, 2023, doi: 10.3390/info14010041.

[52] A. Mansoor, M. Anbar, A. Bahashwan, B. Alabsi, and S. Rihan, "Deep learning-based approach for detecting DDoS attack on Software-defined networking controller," Systems, vol. 11, no. 6, p. 296, 2023, doi: 10.3390/systems11060296.

[53] A. T. Phu et al., "Defending SDN against packet injection attacks using deep learning," Comput. Netw., vol. 234, no. 109935, p. 109935, 2023, doi: 10.1016/j.comnet.2023.109935.

[54] H. M. Belachew, M. Y. Beyene, A. B. Desta, B. T. Alemu, S. S. Musa, and A. J. Muhammed, "Design a robust DDoS attack detection and mitigation scheme in SDN-edge-IoT by leveraging machine learning," IEEE Access, vol. 13, pp. 10194–10214, 2025, doi: 10.1109/ACCESS.2025.3526692.

[55] R. Bingu and S. Jothilakshmi, "Design of intrusion detection system using ensemble learning technique in cloud computing environment," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 5, 2023, doi: 10.14569/IJACSA.2023.0140580.

[56] A. Hirsi, L. Audah, A. Salh, M. A. Alhartomi, and S. Ahmed, “Detecting DDoS threats using supervised machine learning for traffic classification in software defined networking,” IEEE Access, vol. 12, pp. 166675–166702, 2024, doi: 10.1109/ACCESS.2024.3486034.

[57] A. O. Sangodoyin, M. O. Akinsolu, P. Pillai, and 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.

[58] K. Wang, Y. Fu, X. Duan, and T. Liu, “Detection and mitigation of DDoS attacks based on multi-dimensional characteristics in SDN,” Sci. Rep., vol. 14, no. 1, p. 16421, 2024, doi: 10.1038/s41598-024-66907-z

[59] H.-M. Chuang, F. Liu, and C.-H. Tsai, “Early detection of abnormal attacks in software-defined networking using machine learning approaches,” Symmetry (Basel), vol. 14, no. 6, p. 1178, 2022, doi: 10.3390/sym14061178.

[60] C.-H. Hsieh, W.-K. Wang, C.-X. Wang, S.-C. Tsai, and Y.-B. Lin, “Efficient detection of link-flooding attacks with deep learning,” Sustainability, vol. 13, no. 22, p. 12514, 2021, doi: 10.3390/su132212514.

[61] S. S. Samaan and H. A. Jeiad, “Feature-based real-time distributed denial of service detection in SDN using machine learning and Spark,” Bull. Electr. Eng. Inform., vol. 12, no. 4, pp. 2302–2312, 2023, doi: 10.11591/eei.v12i4.4711.

[62] 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, 2024., doi: 10.3390/telecom5020017 .

[63] M. N. Ali, M. Imran, M. S. ud Din, and B.-S. Kim, “Low Rate DDoS detection using Weighted Federated Learning in SDN control plane in IoT network,” Appl. Sci. (Basel), vol. 13, no. 3, p. 1431, 2023, doi: 10.3390/app13031431

[64] T. E. Ali, Y.-W. Chong, and S. Manickam, “Machine learning techniques to detect a DDoS attack in SDN: A systematic review,” Appl. Sci. (Basel), vol. 13, no. 5, p. 3183, 2023, doi: 10.3390/app13053183

[65] W. G. Gadallah, Faculty of Computers and Information, Assiut University, Assiut, Egypt, N. M. Omar, and H. M. Ibrahim, “Machine learning-based distributed denial of service attacks detection technique using new features in software-defined networks,” Int. J. Comput. Netw. Inf. Secur., vol. 13, no. 3, pp. 15–27, 2021, doi: 10.5815/IJCNIS.2021.03.02.

[66] O. Polat et al., “Multi-stage learning framework using convolutional neural network and decision tree-based classification for detection of DDoS pandemic attacks in SDN-based SCADA systems,” Sensors (Basel), vol. 24, no. 3, p. 1040, 2024, doi: 10.3390/s24031040.

[67] M. A. Setitra, M. Fan, B. L. Y. Agbley, and Z. E. A. Bensalem, “Optimized MLP-CNN model to enhance detecting DDoS attacks in SDN environment,” Network, vol. 3, no. 4, pp. 538–562, 2023, doi: 10.3390/network3040024.

[68] E. Fenil and P. Mohan Kumar, “ShChain_3D-ResNet: Sharding blockchain with 3D-Residual Network (3D-ResNet) deep learning model for classifying DDoS attack in Software defined network,” Symmetry (Basel), vol. 14, no. 6, p. 1254, 2022, doi: 10.3390/sym14061254.

[69] P. Karthika and K. Arockiasamy, “Simulation of SDN in mininet and detection of DDoS attack using machine learning,” Bull. Electr. Eng. Inform., vol. 12, no. 3, pp. 1797–1805, 2023, doi: 10.11591/eei.v12i3.5232.

[70] S. Khamaiseh, A. Al-Alaj, M. Adnan, and H. W. Alomari, “The robustness of detecting known and unknown DDoS saturation attacks in SDN via the integration of supervised and semi-supervised classifiers,” Future Internet, vol. 14, no. 6, p. 164, 2022, doi: 10.3390/fi14060164.

[71] S. Refa Alotaibi et al., “Two-tiered privacy preserving framework for software-defined networking driven defence mechanism for consumer platforms,” IEEE Access, vol. 13, pp. 26684–26694, 2025, doi: 10.1109/ACCESS.2025.3538331.