Revista Micaela
ISSN: 2955-8646 (en línea) / **2709-8990 (Impresa)**
Universidad Nacional Micaela Bastidas de Apurímac
Vice Rectorado de Investigación – Perú

Vol. 5 Num. 2 (2024) - Publicado: 22/03/24
DOI: https://doi.org/10.57166/micaela.v5.n2.2024
Páginas: 17 - 24
Recibido 20/08/2024; Aceptado 04/09/2024

https://doi.org/10.57166/micaela.v5.n2.2024.151

Autores:

1. ORCID iD https://orcid.org/0009-0009-1881-5455 Jhoel Alan Huaraca Núñez, egresado de la Universidad Nacional Micaela Bastidas De Apurímac, Pe 181212@unamba.edu.pe.

2. ORCID iD https://orcid.org/0009-0009-6766-7938 Alfredo Cervantes Ccasa, egresado de la Universidad Nacional Micaela Bastidas De Apurímac, Pe 172138@unamba.edu.pe

3. ORCID iD https://orcid.org/0000-0002-2552-5669 Mario Aquino Cruz a, docente en la Universidad micaela bastidas de Apurímac, Pe. maquino@unamba.edu.pe

Técnicas de machine learning para la detección de intrusos en redes: Una revisión sistemática de la literatura

Machine learning techniques for network intrusion detection: A systematic review of the literature

Jhoel Alan Huaraca-Nuñez[1], Alfredo Cervantes-Ccasa-[2], Mario Aquino-Cruz[3]

Resumen. La ciberseguridad es uno de los principales desafíos del mundo moderno debido al rápido avance tecnológico, que aunque ha mejorado la calidad de vida, también ha expuesto a las redes a nuevas amenazas. El objetivo de este estudio es evaluar el impacto de los sistemas de detección de intrusiones (IDS) en la protección de datos y analizar cómo estas técnicas se han adaptado a las amenazas emergentes, mejorando la detección de actividades maliciosas. Para lograr esto, se realizó una revisión sistemática de artículos publicados entre 2018 y 2024 en bases de datos como IEEE, ACM, ScienceDirect y Scopus, siguiendo la metodología de Barbara Kitchenham, utilizando la herramienta Parsifal para generar búsquedas y formular preguntas de investigación. Los resultados iniciales indican un creciente interés en la aplicación de técnicas de Machine Learning para la detección de intrusiones en los últimos seis años, con un pico de publicaciones en 2023, especialmente en la base de datos IEEE, lo que demuestra una evolución significativa en la eficacia de estas técnicas para hacer frente a las amenazas cibernéticas.

Palabras Clave: Algoritmos, Detección de Intrusos, Redes, Machine Learning.

Abstract. Cybersecurity is one of the main challenges of the modern world due to the rapid technological advancement, which, although it has improved the quality of life, has also exposed networks to new threats. The objective of this study is to evaluate the impact of intrusion detection systems (IDS) on data protection and to analyze how these techniques have adapted to emerging threats, improving the detection of malicious activities. To achieve this, a systematic review of articles published between 2018 and 2024 in databases such as IEEE, ACM, ScienceDirect and Scopus was conducted, following Barbara Kitchenham's methodology, using the Parsifal tool to generate searches and formulate research questions. Initial results indicate a growing interest in the application of Machine Learning techniques for intrusion detection over the last six years, with a peak of publications in 2023, especially in the IEEE database, demonstrating a significant evolution in the effectiveness of these techniques to address cyber threats.

Keywords: Algorithms, Intrusion Detection, Machine Learning, Networks.

1 Introducción

La seguridad de las redes se ha convertido en una preocupación crítica en la era digital, donde el número de dispositivos conectados y la cantidad de datos intercambiados continúan creciendo exponencialmente. Según Cybersecurity Ventures estima que el costo global del crimen cibernético superará los 10.5 billones de dólares anualmente para 2025, lo que resalta aún más la urgencia de establecer estrategias efectivas para la protección de sistemas de información y de redes. En este sentido, el creciente panorama de amenazas ha llevado a la necesidad no solo de soluciones reactivas, sino también de soluciones que pudieran ser proactivas en la identificación y mitigación de riesgos [1]. La

detección de intrusiones en redes (IDS) es otra de las formas de defensa más importante contra el ciberataque. Tradicionalmente, los (IDS) se basan en métodos heurísticos y el uso de firmas, que, aunque pueden ser útiles para detectar amenazas ya identificadas, estos mecanismos están destinados a fallar para los ataques nuevos y sofisticados, los investigadores también señalan, que estos métodos no pueden adaptarse rápidamente a los cambios en el comportamiento de los atacantes, lo que aumenta la vulnerabilidad de las redes frente a intrusiones emergentes [2]. En consecuencia, los investigadores y profesionales de la seguridad recurren a Machine Learning para mejorar la detección de intrusiones. Maching Learning ofrece el aprendizaje de los datos históricos y se adaptan a las nuevas amenazas en tiempo real, lo que permite un enfoque más dinámico y eficiente para la protección de la red [3]. El estudio de Britos propone una solución para detectar intrusiones en redes mediante redes neuronales y modelos estadísticos. Utilizando simuladores de redes y software en C, el sistema analiza el tráfico con funciones de densidad de probabilidad y clasificadores multivariables. Con un bajo error de aprendizaje (0,56%) y generalización (1,97%), el enfoque es eficaz para detectar anomalías en tiempo real y mejorar la seguridad de infraestructuras críticas mediante su integración con un firewall [4]. Gonzalo Valdezate realizó un estudio sobre sistemas de detección de intrusos basados en Machine Learning utilizando el conjunto de datos NSL-KDD. El objetivo fue comparar la eficacia de varios algoritmos en la clasificación de ataques, midiendo métricas como precisión y tasa de falsos positivos. Usando Scikit-Learn y Plotly, se entrenaron y evaluaron los algoritmos, destacando los árboles de decisión por su precisión. El estudio resalta la importancia de la selección de características para mejorar el rendimiento y la eficacia en la detección de intrusiones [5].

Rivero Pérez realizó un estudio sobre técnicas de aprendizaje automático para la detección de intrusos en redes, revisando enfoques recientes y destacando el uso de algoritmos híbridos. Se aplicaron modelos de reducción de dimensionalidad y clasificación en conjuntos de datos como KDD Cup 99, utilizando técnicas de preprocesamiento como selección y discretización de atributos. Los resultados indican que la hibridación de estos algoritmos mejora la detección de ataques basados en contenido, aumentando la precisión y reduciendo falsos positivos [6].

El objetivo del presente artículo es llevar a cabo una revisión sistemática de las técnicas de Machine Learning para la detección de intrusiones en redes. Para tal fin, se empleará la metodología propuesta por Barbara Kitchenham, la cual permite estructurar y analizar la información de manera rigurosa. En la sección de resultados, se examinará la información extraída de los artículos seleccionados, destacando las técnicas y algoritmos más pertinentes en este ámbito.

2 Método

Para el desarrollo del presente artículo se aplicó como inspiración la metodología de Barbara Kitchenham, es importante destacar que ayuda de manera significativa en trabajos relacionados a la revisión sistemática de la literatura, a continuación, se describen las fases que ayudaron a desarrollar el presente estudio.

a) Planificar la revisión sistemática de literatura con el uso de la herramienta Parsifal.

- Identificar las preguntas de investigación.
- Crear un proceso de búsqueda.
- Definir los criterios de inclusión y exclusión para los artículos.
- Elegir las fuentes de consulta
- Cadenas de búsqueda.

b) Desarrollar la revisión sistemática de literatura con la planificación definida.

- Buscar artículos.
- Selección de los artículos definitivos para el análisis de la información.
- Análisis y clasificación de la información.

c) Documentar e interpretar los resultados de la revisión.

d) Herramientas:

- Mendeley: Es una herramienta de gestión de referencias y colaboración académica que ayuda a los investigadores a organizar, leer, y citar artículos científicos.
- Parsifal: Es una herramienta online que permitió el desarrollo de la SRL, ayudando así a automatizar y optimizar el tiempo que lleva el proceso de obtención y selección de información.

3 Resultados

3.1 Planificar la revisión sistemática de literatura

A continuación, se describen las tareas llevadas a cabo durante la fase de planificación de la revisión sistemática de la literatura.

a) Identificar las preguntas de investigación

Para definir las preguntas de investigación en la revisión sistemática de la literatura (SLR), se llevó a cabo una búsqueda exploratoria relacionados con el tema de estudio. En base al propósito del presente artículo se plantean 3 preguntas de investigación.

- ¿Cuántos estudios se han publicado en los últimos siete años acerca de las Técnicas de Machine learning para la Detección de Intrusos en Redes?
- ¿En que año se publicaron la mayoría de los artículos y cuál es su interpretación?
- ¿Cómo contribuyen las técnicas de Machine Learning a mejorar la detección de intrusiones en redes?

b) Crear un proceso de búsqueda

Se emplearon términos clave utilizando el método PICOC para delimitar el alcance de la revisión sistemática. Este enfoque abarca cinco elementos principales: población, intervención, comparación, resultados y contexto. A través de este método, se definieron las expresiones que componen las cadenas de búsqueda, las cuales se describen a continuación.

- Población (P): (“Intrusion Detection") AND ("Computer Networks”)
- Intervención (I): "Machine Learning"
- Comparación (C): No aplica
- Resultados (O): Algorithms" OR "Techniques
- Contexto (C): "Intelligence Artificial"

c) Definir los criterios de inclusión y exclusión para los artículos

Luego de obtener los resultados preliminares de las búsquedas, se establecieron 4 criterios de inclusión (IC) y 4 de exclusión (EC) para seleccionar estudios relevantes y acordes a los objetivos de la investigación. A continuación, se describen dichos criterios.

Criterio de inclusión (IC):

- IC1: Artículos publicados desde el 2018 en adelante.
- IC2: Artículos que contengan información de Técnicas de Machine Learning para la detección de intrusos en redes
- IC3: Artículos escritos en idioma inglés o español.
- IC4: Artículos que hayan sido publicados en revistas científicas, artículos científicos y conferencias.

Criterio de exclusión (EC):

- EC1: Artículos cuyo título no tenga relación con el objeto de estudio.
- EC2: Artículos duplicados.
- EC3: Capítulos de libros, manuales, literatura gris
- EC4: Artículos que no pertenecen al área Ciencias y Computación.

d) Elegir las fuentes de consulta

De acuerdo con los lineamientos de Barbara Kitchenham se seleccionaron 4 fuentes de búsqueda, como se indica en la Tabla 1, seleccionadas por su accesibilidad y capacidad para realizar consultas avanzadas.

Tabla 1. Base de datos científicos

Base de Datos	URL
ACM	http://portal.acm.org
IEEE	http://ieeexplore.ieee.org
ScienceDirect	http://www.sciencedirect.com
Scopus	http://www.scopus.com

e) Cadena de búsqueda

A partir de una revisión preliminar de artículos, se definieron las palabras clave siguiendo el método PICOC, y se emplearon operadores lógicos "AND" y "OR" para crear las cadenas de búsqueda. La herramienta Parsifal generó una cadena de búsqueda general, que se ajustó según cada base de datos. Todas las palabras clave se establecieron en inglés y se detallan en la Tabla 2.

Tabla 2. Cadena de búsqueda

Base de Datos	Cadena de búsqueda
Parsifal	("Intrusion Detection") AND ("Computer Networks") AND ("Machine Learning") AND ("Algorithms" OR "Techniques")
ACM	("Intrusion Detection") AND ("Computer Networks") AND ("Machine Learning") AND ("Algorithms" OR "Techniques")
IEEE	("Intrusion Detection") AND ("Computer Networks") AND ("Machine Learning") AND ("Algorithms" OR "Techniques")
ScienceDirect	("Intrusion Detection") AND ("Computer Networks") AND ("Machine Learning") AND ("Algorithms" OR "Techniques")
Scopus	("Intrusion Detection") AND ("Computer Networks") AND ("Machine Learning") AND ("Algorithms" OR "Techniques")

3.2 Desarrollar la revisión sistemática de la literatura

a) Buscar artículos

La cadena de búsqueda se implementó en las bases de datos seleccionadas (ACM, IEEE, ScienceDirect y Scopus), obteniendo un total de 1089 artículos. Tras realizar las búsquedas, se generaron archivos en formato .bib, los cuales fueron cargados en la herramienta Parsifal para facilitar la gestión de los resultados. Durante el proceso, se descartaron 45 artículos duplicados, quedando 1044 artículos para una revisión más detallada. De estos, se ignoraron aquellos que no cumplían con los criterios de inclusión o que no eran relevantes para el campo de estudio, seleccionando finalmente 21 artículos para una revisión exhaustiva.

b) Selección de artículos definitivos para el análisis de información

Según la metodología de Barbara Kitchenham, lo habitual en esta etapa es que los artículos pasen por una evaluación de calidad mediante una serie de preguntas, con el fin de seleccionar aquellos que mejor contribuyan al objetivo de la investigación. No obstante, dado que se identificaron únicamente 21 artículos que cumplen con los criterios de inclusión, se optó por incluirlos todos en el análisis final de la información.

c) Análisis y clasificación de la información

Análisis de algoritmos: Se consideró la cantidad total de artículos que mencionan los algoritmos utilizados, y esta información se representó en porcentajes para visualizar de manera más clara los datos.

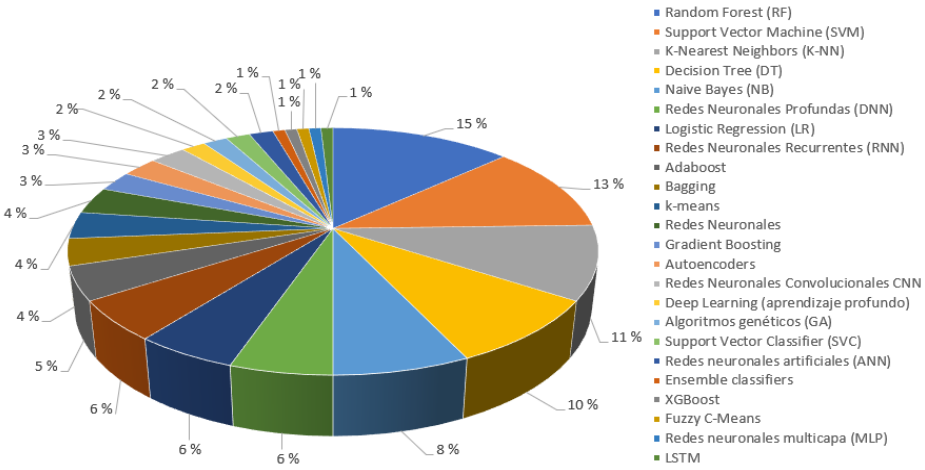


Fig. 1. Algoritmos utilizados

Al observar y analizar la Fig. 1 se puede determinar lo siguiente:

- El algoritmo Random Forest (RF) es el más utilizado, mencionado en el 15% de los artículos como técnica de machine learning para la detección de intrusos en redes.
- Support Vector Machine (SVM) con un 13%, y K-Nearest Neighbors (K-NN) que aparece en el 11% de los estudios. Decision Tree (DT) es referenciado en el 10%, mientras que Naive Bayes (NB) alcanza un 8% de uso en los artículos analizados.
- El 6% es alcanzado por Redes Neuronales Profundas (DNN), Logistic Regression (LR) y Redes Neuronales Recurrentes (RNN).
- Adaboost está en el 5%, Bagging, k-means y Redes Neuronales en el 4%, Gradient Boosting y Autoencoders en el 3%, y CNN, Deep Learning, GA, LSTM, XGBoost y ANN entre el 2% y 1%.

Fuentes de información: Utilizando la herramienta Parsifal, se generó la Fig. 2, esta representación gráfica, expresada en porcentajes, permite analizar con mayor precisión el impacto y la relevancia de las distintas bases de datos en la recolección de artículos y datos relevantes para el estudio.

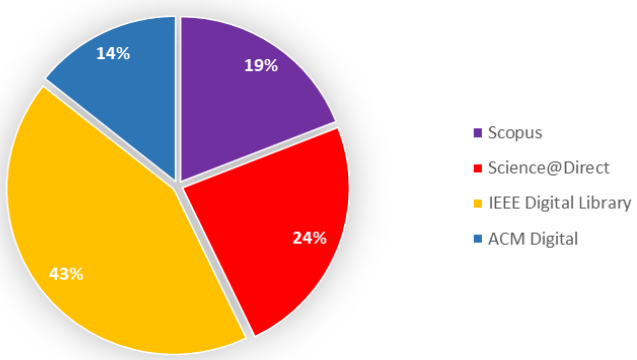


Fig. 2. Fuentes de información

A continuación, se destacan los puntos más importantes.

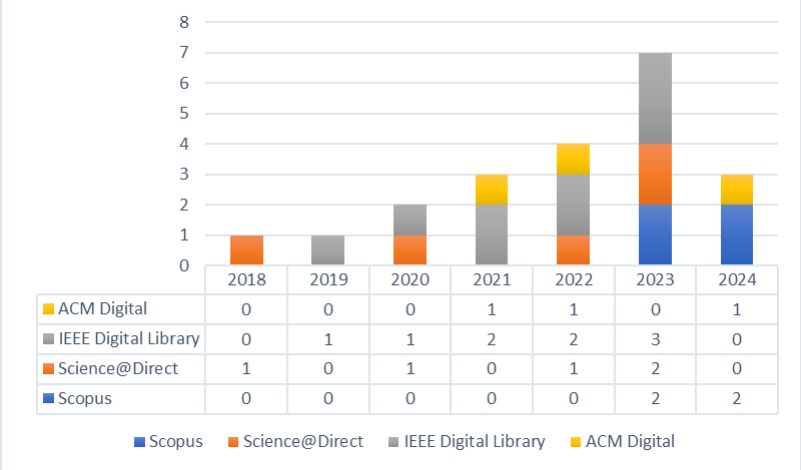
- La IEEE Digital Library es la fuente más relevante en este estudio, con una contribución del 43%, en este grupo están: [7], [8], [9], [10], [11], [12], [13], [14], [15].
- La fuente de información de ScienceDirect con 24% de nivel de aporte para el presente artículo, en este grupo se encuentran: [16], [17], [18], [19], [20].
- Con un 19% de los artículos, Scopus, desempeña un papel importante en el análisis. A este grupo pertenecen: [21], [22], [23], [24]
- ACM, aunque tiene la menor participación con un 14%, sigue siendo una fuente valiosa para el conjunto de artículos examinados que son: [25], [26], [27].

3.3 Documentar e interpretar los resultados de la revisión

Esta fase se enfoca en analizar e interpretar la información obtenida durante la revisión. En este proceso, se proporcionan respuestas a las preguntas de investigación planteadas, lo que permite un mejor entendimiento.

a) ¿Cuántos estudios se han publicado en los últimos siete años acerca de las Técnicas de Machine learning para la detección de intrusos en redes?

En 2018, se registró 1 artículo en ScienceDirect. En 2019, hubo 1 publicación en IEEE. En 2020, se mantuvo el mismo patrón con 1 artículo en IEEE y 1 en ScienceDirect. En 2021, se publicaron 1 artículo en ACM, 2 artículos en IEEE. En 2022, hubo un total de 4 artículos, en ScienceDirect, IEEE Digital Library y ACM. El mayor número de publicaciones ocurrió en 2023, con 2 estudios en Scopus, 2 en ScienceDirect y 3 en IEEE. Finalmente, en 2024, se han registrado 2 estudios en Scopus y 1 en ACM. En la Fig. 3 podemos ver detalladamente el progreso de las publicaciones en este ámbito de estudio.



	2018	2019	2020	2021	2022	2023	2024
ACM Digital	0	0	0	1	1	0	1
IEEE Digital Library	0	1	1	2	2	3	0
Science@Direct	1	0	1	0	1	2	0
Scopus	0	0	0	0	0	2	2

Fig. 3. Artículos seleccionados en los últimos 7 años

b) ¿En qué año se publicaron la mayoría de los artículos y cuál es su interpretación?

El análisis revela que en 2023 se alcanzó el mayor número de publicaciones, con 7 artículos, creciendo de manera constante desde 2018. Esto refleja un creciente interés en el uso de técnicas de Machine Learning para la detección de intrusos en redes, impulsado por avances tecnológicos y una mayor preocupación por la seguridad digital. La complejidad creciente de las amenazas cibernéticas ha hecho que este campo sea una prioridad para los investigadores, en la Fig. 4 se muestra más detallado.

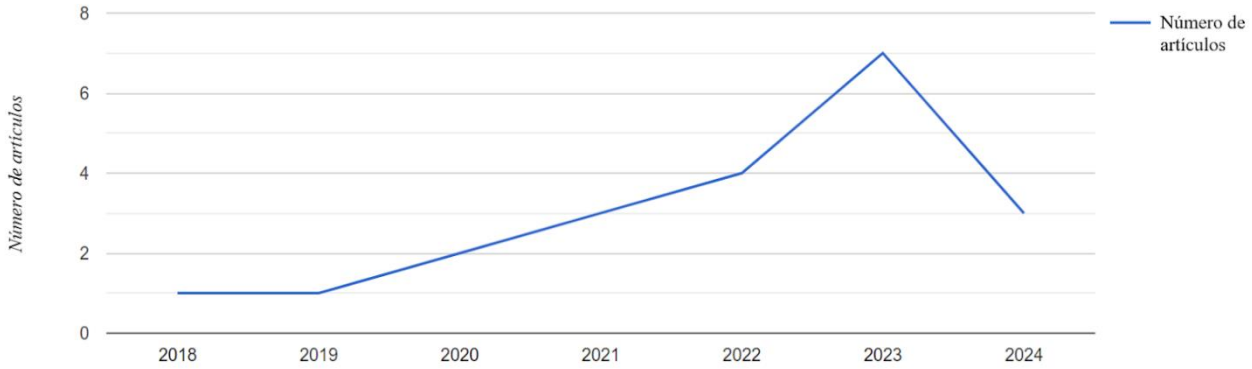


Fig. 4. Artículos publicados por años

c) ¿Cómo contribuyen las técnicas de Machine Learning a mejorar la detección de intrusiones en redes?

Según la revisión de varios artículos sobre Machine Learning aplicado a la detección de intrusiones en redes, la mayoría de las investigaciones se centran en mejorar la precisión y reducir los falsos positivos en la detección de ataques cibernéticos. Los métodos más utilizados incluyen Redes Neuronales, Máquinas de Soporte Vectorial (SVM) y Árboles de Decisión, que permiten clasificar patrones anómalos en el tráfico de red de manera más eficiente que los enfoques tradicionales.

Un gran porcentaje de los estudios se enfocan en detectar amenazas como ataques de denegación de servicio, inundaciones de paquetes, y otras actividades maliciosas que se basan en patrones repetitivos o desconocidos. Otro grupo de trabajos se concentra en la optimización de los algoritmos, aplicando técnicas novedosas como el aprendizaje profundo y el aprendizaje no supervisado para identificar amenazas emergentes sin requerir grandes conjuntos de datos etiquetados.

4 Discusiones y Conclusiones

La información obtenida permitió identificar que la principal fuente de estudios proviene de IEEE, con el año 2023 como el de mayor cantidad de publicaciones relevantes en los últimos siete años. En el análisis de resultados, los algoritmos más utilizados fueron Random Forest (RF), Support Vector Machine (SVM) y K-Nearest Neighbors (K-NN). Además, se mencionaron otros algoritmos importantes como Decision Tree (DT), Naive Bayes (NB), Redes Neuronales Profundas (DNN) y Logistic Regression (LR) entre otros algoritmos son utilizados en un solo artículo. La investigación ha demostrado que al utilizar Machine Learning son cruciales para la detección de intrusos en redes, en el ámbito de la seguridad permitieron identificar proactivamente ataques, descubrir patrones específicos generados por el malware que pueden alterar los sistemas.

Se concluye:

Todos los estudios enfatizan la eficacia de diversos algoritmos, como árboles de decisión, máquinas de soporte vectorial y redes neuronales, para clasificar y detectar intrusiones, aprovechando conjuntos de datos variados que incluyen tráfico de red, registros de eventos y características de comportamiento del usuario. Sin embargo, también se observaron diferentes métodos, mientras que algunos estudios se centraron en el rendimiento de algoritmos de detección de ataques específicos, otros abordaron desafíos como el desequilibrio de clases de datos y la adaptación a nuevas amenazas.

5 Biografías

- Jhoel Alan Huaraca Núñez, Egresado en Ingeniería informática y sistemas de la Universidad Micaela Bastidas de Apurímac.
- Alfredo Cervantes Ccasa, Egresado en Ingeniería informática y sistemas de la Universidad Micaela Bastidas de Apurímac.
- Mario Aquino Cruz, Docente en la Universidad Nacional Micaela Bastidas de Apurímac Perú, MSc. en informática, investigador en las áreas informáticas educativa, IoT, inteligencia artificial y ciberseguridad.

6 Referencias

[1] cybersecurityventures, “Cybercrime To Cost The World $10.5 Trillion Annually By 2025.” [Online]. Available: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[2] M. Aljanabi, M. Arfian, H. Abdulkaree, and J. Sulaiman, “Intrusion Detection : A Review,” no. 1–4, 2021, doi: 10.58496/MJCS/2021/001.

[3] G. Valdezate and cardeñoso Valentín, “Sistemas de Deteccion de Intrusos ´ Basados en Tecnicas de Machine Learning,” pp. 1–52, [Online]. Available: https://uvadoc.uva.es/bitstream/handle/10324/44228/TFG-G4680.pdf?sequence=1

[4] B. J. Daniel, A. Silvia, and V. Laura, “Detección de Intrusiones mediante el uso de Redes Neuronales,” p. 6, doi: 10.1109/TLA.2007.4378531.

[5] J. Luis and R. Pérez, “Técnicas de aprendizaje automático para la detección de intrusos en redes de computadoras,” vol. 8, no. 4, pp. 52–73, 2014, Accessed: Oct. 08, 2024. [Online]. Available: http://scielo.sld.cu/pdf/rcci/v8n4/rcci03414.pdf

[6] A. Pérez, S. Rodríguez, and J. Maritenez, “Detección de Intrusiones en Redes de Computadores Usando Redes Neuronale,” *Revista de Tecnología y Seguridad Informática*, vol. 12, no. 44–58, 2021.

[7] H. Hacilar, Z. Aydin, and V. Çağri Güngör, “Network intrusion detection based on machine learning strategies: performance comparisons on imbalanced wired, wireless, and software-defined networking (SDN) network traffics,” vol. 32, pp. 623–640, 2024, doi: 10.55730/1300-0632.4091.

[8] I. H. Hassan, A. Mohammed, and M. A. Masama, “Metaheuristic algorithms in network intrusion detection,” *Comprehensive Metaheuristics: Algorithms and Applications*, pp. 95–129, Jan. 2023, doi: 10.1016/B978-0-323-91781-0.00006-5.

[9] Q. Liu and T. Zhang, “Deep learning technology of computer network security detection based on artificial intelligence,” *Computers and Electrical Engineering*, vol. 110, p. 108813, Sep. 2023, doi: 10.1016/J.COMPELECENG.2023.108813.

[10] C. Kalimuthan and J. Arokia Renjit, "Review on intrusion detection using feature selection with machine learning techniques," *Mater Today Proc*, vol. 33, pp. 3794–3802, Jan. 2020, doi: 10.1016/J.MATPR.2020.06.218.

[11] H. Jmila and M. I. Khedher, "Adversarial machine learning for network intrusion detection: A comparative study," *Computer Networks*, vol. 214, p. 109073, Sep. 2022, doi: 10.1016/J.COMNET.2022.109073.

[12] U. S. Musa, M. Chhabra, A. Ali, and M. Kaur, "Intrusion Detection System using Machine Learning Techniques: A Review," in *Proceedings - International Conference on Smart Electronics and Communication, ICOSEC 2020*, Institute of Electrical and Electronics Engineers Inc., Sep. 2020, pp. 149–155. doi: 10.1109/ICOSEC49089.2020.9215333.

[13] V. Gancheva, "Application of Machine Learning Techniques for Software Anomaly Detection," pp. 57–62, doi: 10.1109/ICAMCS59110.2023.00016.

[14] A. Sareh, R. Shreif, and E. Heba, "Efficient Feature Selection for Intrusion Detection Systems," pp. 1029–1034, 2019, doi: 10.1109/UEMCON47517.2019.8992960.

[15] J. Lansky, S. Ali, and M. Mohammadi, "Deep Learning-Based Intrusion Detection Systems: A Systematic Review," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3097247.

[16] H. A. Abdullah Abdulwali, M. H. Saleh Al-Humaidi, H. Z. Abdullah Al-Asri, A. F. Mansour Al-Saidi, and A. A. Al-Himiary, "Intrusions Detection System Using Machine Learning Algorithms," *2023 3rd International Conference on Emerging Smart Technologies and Applications, eSmarTA 2023*, pp. 1–8, 2023, doi: 10.1109/ESMARTA59349.2023.10293386.

[17] U. S. Musa, S. Chakraborty, M. M. Abdullahi, and T. Maini, "A review on intrusion detection system using machine learning techniques," *Proceedings - IEEE 2021 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2021*, pp. 541–549, Feb. 2021, doi: 10.1109/ICCCIS51004.2021.9397121.

[18] S. V. Amanoul and A. M. Abdulazeez, "Intrusion Detection System Based on Machine Learning Algorithms: A Review," *2022 IEEE 18th International Colloquium on Signal Processing and Applications, CSPA 2022 - Proceeding*, pp. 79–84, 2022, doi: 10.1109/CSPA55076.2022.9782043.

[19] M. Halim, B. A. Pratomo, and B. Jati Santoso, "Comparative Analysis of Novelty Detection Algorithms in Network Intrusion Detection Systems," *2023 International Conference on Advanced Mechatronics, Intelligent Manufacture and Industrial Automation, ICAMIMIA 2023 - Proceedings*, pp. 306–310, 2023, doi: 10.1109/ICAMIMIA60881.2023.10427625.

[20] A. A. Yilmaz, "Intrusion Detection in Computer Networks using Optimized Machine Learning Algorithms," *3rd International Informatics and Software Engineering Conference, IISEC 2022*, pp. 1–5, 2022, doi: 10.1109/IISEC56263.2022.9998258.

[21] M. Komisarek, M. Pawlicki, M. Kowalski, A. Marzecki, R. Kozik, and M. Choraś, "Network Intrusion Detection in the Wild - The Orange use case in the SIMARGL project," *ACM International Conference Proceeding Series*, Aug. 2021, doi: 10.1145/3465481.3470091.

[22] Z. Rachidi, K. Chougdali, A. Kobbane, and J. Ben-Othman, "Network intrusion detection using Machine Learning approach," *ACM International Conference Proceeding Series*, pp. 13–17, Jul. 2022, doi: 10.1145/3551690.3551693.

[23] M. J. Rani and D. Singh, "Machine Learning Algorithm for Intrusion Detection: Performance Evaluation and Comparative Analysis," *7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2023 - Proceedings*, pp. 779–784, 2023, doi: 10.1109/I-SMAC58438.2023.10290491.

[24] B. Beridze and M. Donadze, "Network Anomaly Detection Utilizing Machine Learning Methods," *2023 IEEE East-West Design and Test Symposium, EWDTS 2023 - Proceedings*, 2023, doi: 10.1109/EWDTS59469.2023.10297059.

[25] Z. H. Salim and S. O. Hasoon, "Intrusion Detection Using Artificial Intelligence Techniques: Review," *International Conference on Artificial Intelligence, Computer, Data Sciences, and Applications, ACDSA 2024*, 2024, doi: 10.1109/ACDSA59508.2024.10467524.

[26] A. Verma and V. Ranga, "Statistical analysis of CIDDS-001 dataset for Network Intrusion Detection Systems using Distance-based Machine Learning," *Procedia Comput Sci*, vol. 125, pp. 709–716, Jan. 2018, doi: 10.1016/J.PROCS.2017.12.091.

[27] I. A. Najm and A. H. Saeed, "Enhanced Network Traffic Classification with Machine Learning Algorithms," pp. 322–327, 2024, doi: 10.1145/3660853.3660935.