https://doi.org/10.69639/arandu.v11i2.468

La inteligencia artificial en la seguridad informática: Una revisión literaria

Artificial Intelligence in Information Security: A Literature Review

Bernabe Ortega Tenezaca
bortega@uea.edu.ec
https://orcid.org/0000-0001-9693-6951
Universidad Estatal Amazónica
Puyo – Ecuador

Lady Rodriguez Carmona
lv.rodriguezc@uea.edu.ec
https://orcid.org/0009-0000-1570-827X
Universidad Estatal Amazónica
Puyo – Ecuador

Edgar Macías Farias
ef.maciasf@uea.edu.ec
https://orcid.org/0009-0001-6976-9024
Universidad Estatal Amazónica
Puyo – Ecuador

Janick Rodrigo Cevallos Illicachi
jr.cevallosi@uea.edu.ec
https://orcid.org/0000-0002-1138-7357
Universidad Estatal Amazónica
Puyo – Ecuador

Artículo recibido: 20 octubre 2024 - *Aceptado para publicación: 26 noviembre 2024*
Conflictos de intereses: Ninguno que declarar

RESUMEN

El presente trabajo tiene como objetivo, presentar una revisión y análisis de la literatura científica más reciente, relativa a la aplicación y uso de la inteligencia artificial, en la detección de amenazas, en el campo de la seguridad informática, mediante la aplicación de algoritmos como los de aprendizaje automático, y sus principales tendencias para enfrentar los desafíos actuales, relativas a la detección de ataques evasivos que intentan burlar los sistemas de seguridad tradicionales, tomando en cuenta las fortalezas, sus debilidades y retos que aún persisten como la identificación de patrones sospechosos, y la necesidad de grandes cantidades de datos de alta calidad para entrenar los modelos de IA. La importancia de este trabajo radica en que sirve como una guía, para investigadores, desarrolladores de software y profesionales de la seguridad informática, que se encuentren interesados en generar sistemas de detección de fallas de seguridad y amenazas, más robustos y eficientes, congruentes con las necesidades actuales.

Palabras clave: inteligencia artificial, ciberseguridad, aprendizaje automático

ABSTRACT

The purpose of this paper is to present a review and analysis of the most recent scientific literature on the application and use of artificial intelligence in threat detection in the field of computer security, through the application of algorithms such as machine learning, and its main trends to meet the current challenges, The main trends in the detection of evasive attacks that attempt to circumvent traditional security systems, taking into account the strengths, weaknesses and challenges that still persist, such as the identification of suspicious patterns, and the need for large amounts of high quality data to train AI models. The importance of this work lies in the fact that it serves as a guide for researchers, software developers and computer security professionals who are interested in generating more robust and efficient systems for detecting security flaws and threats, congruent with current needs.

Keywords: artificial intelligence, cyber security, machine learning

INTRODUCCIÓN

En el mundo actual, el impactante desarrollo de la Inteligencia Artificial (IA) enfrenta vario retos, entre ellos, en el sector de la seguridad de la información y particularmente en el campo de la ciberseguridad. La IA mejora significativamente la detección y respuesta en tiempo real, de amenazas mediante algoritmos de aprendizaje automático, incrementando el nivel y los mecanismos de defensa de un entorno de red (Sharko et al., 2024; Zhou & Liang, 2024). La evaluación de los riesgos asociados y capacidad de respuesta de la IA ante amenzas de ciberataques son cada vez son más eficientes, según estudios han logrado alcanzar un 30% más en la precisión en la detección de amenazas y en un 40% la reducción de falsos positivos en comparación los métodos tradicionales (Chaowen, 2024). El acceso a la computación de altas prestaciones, hace posible el tratamiento de grandes cantidades de datos que permiten realizar estudios con mayor precisión de patrones y anomalías relacionadas a la seguridad informática (Tairov, 2024), y permite la automatización de tareas complejas y rutinarias (Munjal et al., 2024). El despliegue de la IA, plantea problemas éticos, por lo que es imperioso establecer directrices morales que aborden los temas de toma de decisiones (Munjal et al., 2024) (Sharko et al., 2024). En el presente trabajo se presenta una revisión literaria sistemática basado en las Directrices de elementos de información preferidos para revisiones sistemáticas y meta-análisis (acrónimo en inglés PRISMA)(Yusuff, 2023). La importancia de este trabajo radica en la valoración de las oportunidades y los nuevos desafíos para el desarrollo desde el contexto académico sobre los avances de la IA y su aplicación en la seguridad informática como herramienta fundamental en la batalla contra el cibercrimen.

Terminología

Con el objetivo de preparar la base para la revisión literaria, se definen la terminología principal, que establece el contexto del desarrollo de este trabajo.

Advanced Persistent Threat APT

Las amenazas persistentes avanzadas por sus siglas en inglés APT, son ataques cibernéticos sofisticados ejecutados por grupos u organizaciones dirigidos a empresas de alto perfil o entidades de gobierno (Bokhari & Myeong, 2023). Los APT difieren del malware tradicional debido a su sofisticado mecanismo de acción con un enfoque específico (Xuan et al., 2020). Las APT contemplan una serie de pasos coordinados dentro de la redes informáticas cuya activación se asocia a grupos financiados como el crimen organizado (Bhardwaj, 2023). Las APT se centran en objetivos específicos de alto valor, para lo cual se requiere una estrategia de seguridad multicapa con mecanismos de detección avanzados (Alsanad & Altuwaijri, 2022; Hasan et al., 2023; J. Zhang et al., 2024). Las contramedidas de seguridad como Firewalls e IDS/IPS pueden ser insuficientes, requiriendo para este caso técnicas proactivas de búsqueda de

amenazas, como las que utilizan análisis forense de memoria, para identificar y mitigar las amenazas que evaden los sistemas de monitoreo estándar (Ali et al., 2024; Dau et al., 2024).

Phishing

El phishing es una de las formas delito cibernético en auge que intenta obtener información confidencial de manera fraudulenta (Ajhari et al., 2023). Mediante emite comunicaciones electrónicas haciéndose pasar por una entidad confiable que busca información como nombres de usuario, contraseñas y detalles de tarjetas de crédito, entre otros (Yunoose et al., 2022). El phishing es clasificado como una forma de estafa por Ingeniería Social, que suplantan la identidad de organizaciones legitimas mediante enlaces ilegales que dirigen al usuario a sitios web falsos HTML peligroso (Li et al., 2020). El elemento humano es una vulnerabilidad crítica en los ataques de phishing, ya que estas estafas explotan debilidades y comportamientos humanos (Mohebzada et al., 2012). La susceptibilidad al phishing sigue siendo una amenaza importante, especialmente a medida que el cibercrimen continúa evolucionando y plantea amenazas significativas para la sociedad (Ribeiro et al., 2023).

Distributed Denial of Service DDoS

Un ataque de denegación de servicio distribuido (DDoS) se define como un intento malicioso de interrumpir el funcionamiento de un servidor, servicio o una red objetivo (Alomari et al., 2024). El ataque DDoS se ejecuta sobre sistemas comprometidos, generalmente formando una botnet, que envía una cantidad masiva de tráfico al objetivo, haciendo que no responda solicitudes legitimas a sus usuarios (Dhananjay Tangtode et al., 2024). En la actualidad los ataques DDoS han incrementado su potencial de ataque con volúmenes de datos que alcanzan cientos de terabytes, dificultando su detección y mitigación (Dhananjay Tangtode et al., 2024). Las redes inalámbricas de sensores (WSN) son vulnerables a ataques DDoS debido a su naturaleza diversa y desequilibrada de datos (Reza, 2024).

Malware

El software malicioso malware es una amenaza que abarca varios tipos de amenazas como virus, gusanos, troyanos, Ransomware y spyware. El malware tiene como objetivo robar, cifrar, eliminar datos confidenciales, comprometer funciones informáticas (Rao-Kadari et al., 2024). Las técnicas tradicionales para la detección de malware basadas en firmas y heurísticas, actualmente resultan ineficaces contra nuevas variantes como virus metamórficos, cifrados y polimórficos (Christopher & Ayorinde, 2024). El estudio de contramedidas para malware es escencial dentro del mundo de la ciberseguridad que intenta comprender su comportamiento (Tilmar Jakobsern, 2024). La evolución de malware de formas tradicionales monomórficas a formas polimórficas, metamórficas y oligomórficas requiere sistemas de detección más avanzados (Supriyanto et al., 2024) .

Detección de Intrusiones

La detección de intrusiones es un tema crítico en la ciberseguridad, que monitorea el tráfico de red y los procesos de host en busca de actividades sospechosas, emitiendo alertas cuando se detectan (Bertino et al., 2023). Los modelos tradicionales de detección de intrusiones basadas en firmas para amenazas conocidas, en la actualidad son insuficientes frente al crecimiento exponencial del uso de internet y diversidad de nuevos protocolos (A. Singh et al., 2024a). Los sistemas de detección de intrusión IDS se implementan como aplicaciones de software o dispositivos de hardware, actuando como capa protectora de la infraestructura de red (Xue et al., 2021). Los IDS emiten alertas cuando se encuentran actividades sospechosas dentro de un entorno computacional (Xue et al., 2021).

Ransomware

El ransomware se categoriza como un tipo de software malicioso, desarrollado para el cibercrimen. El malware infecta un sistema informático toma control de los archivos del usuario, impidiendo el acceso a ellos hasta que se pague un rescate, generalmente en criptomonedas (Thakur et al., 2022). El creador del ransomware promete que una vez que se reciba el pago, el dueño de la información secuestrada, recibir una clave de descifrado (Thakur et al., 2022) (Hyslip & Burruss, 2023). El ransomware inicia en la década de los 2000, y por su fácil propagación pasaron de atacar a usuarios comunes a usuarios corporativos (Hyslip & Burruss, 2023). Se conoce una variante de Rasomware-as-a-service que se oferta en foros hackers y la deep-web que permite su uso a cambio de compartir el dinero de los rescates (Hyslip & Burruss, 2023). Este delito se persigue a nivel internacional y ha logrado desmantelar operaciones en ransomware-as-a-service con arrestos de alto perfil (Ahmed et al., 2022).

METODOLOGÍA

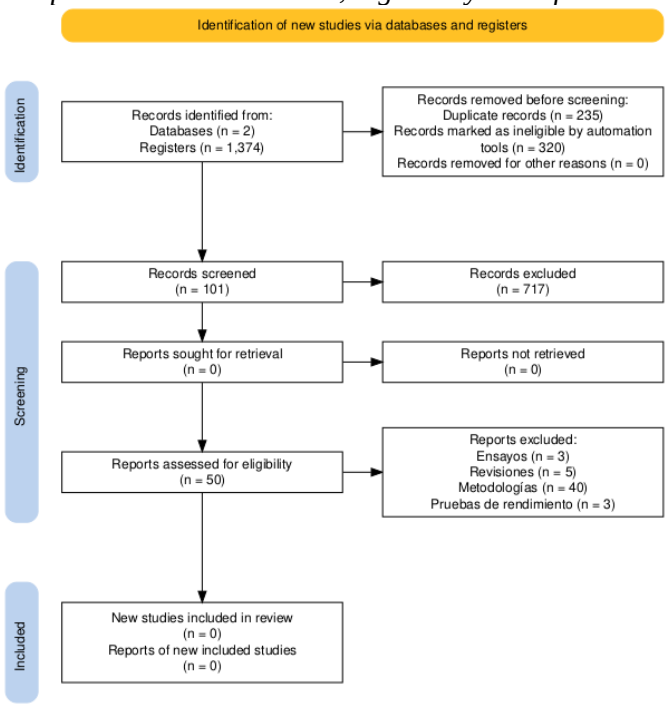
El proposito de la presente revisión literaria, es de identificar y evaluar el estado del arte de la investigación de la inteligencia artificial en la seguridad informática en sus diversas areas, y luego clasificar las investigaciones relevantes para identificar posibles oportunidades para futuras investigaciones. La revisión literaria es un enfoque válido y un paso necesario que permite establecer un campo de investigación e identificación de la conceptualización (Yusuff, 2023) (Rao, 2023).

Nuestra revisión literaria se basa en las consideraciones y terminología previamente expuestas, y sigue un proceso sistemático basado en PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) (*PRISMA Statement*, s. f.; Rico-González et al., 2021).

El proceso de análisis contiene tres etapas (*PRISMA Statement*, s. f.): Identification, Screening, Included. El proceso implica una búsqueda bibliográfica detallada en bases de datos, utilizando términos relevantes, y un diagrama de flujo para describir el proceso de cribado y selección (Yusuff, 2023).

Figura 1

Diagrama de flujo explicativo PRISMA 2020 para nuevas revisiones sistemáticas que incluyen búsquedas en bases de datos, registros y otras fuentes



Nota: El diagrama incluye los datos cuantitativos obtenidos en las diferentes búsquedas de acuerdo con el modelo de la declaración PRISMA (Haddaway et al., 2022).

Nuestra revisión bibliográfica incluye artículos de revistas revisadas por pares. En afán del rigor científico, se excluyeron documentos de trabajo no publicados, conferencias, revisiones, entrevistas, servicios, ensayos, metodologías comparativas, y documentos de conferencias. La búsqueda bibliográfica se delimito desde el año 2020. En algunos casos estrictos de conceptualización se han utilizado artículos fuera del rango descrito para definiciones clásicas.

Mediante el modelo WWH (Mohanty & Bala Das, 2018) se plantea la pregunta de investigación (PI)"¿Cómo se aplica la inteligencia artificial en la mejora de la detección y respuesta ante ciberataques, qué beneficios y desafíos se han identificado en estudios recientes?"

Para la fase de identificación (*PRISMA Statement*, s. f.), se utilizó la información más relevante y limitados a artículos científicos en las bases de datos Scopus y de Google Scholar *ver Tabla 1*. Se obtienen un total de 1374 artículos (1023 Scopus, 586 Google Scholar). Se remueven 235 artículos repetidos, y 320 artículos marcados como no elegible de manera automatizada.

Tabla 1

Sumario de métodos de búsqueda

Métodos de búsqueda	Descripción
Unidad de analisis	Las fuentes incluyen articulos indexados publicados sobre la inteligencia artificial en la seguridad informática.
Tipo de analisis	Cualitativo
Periodo de analisis	Desde el año 2019.
Motores de búsqueda.	

Palabras claves usadas en la búsqueda	Se utilizaron las siguientes bases de datos para buscar publicaciones relevantes: Elsevier (www.sciencedirect.com), Google Scholar, Scopus www.scopus.com). 1. Seguridad Informática 2. Inteligencia Artificial 3. Machine Learning 4. Aprendizaje automático 5. Algoritmos de IA.

En la fase de cribado (*PRISMA Statement*, s. f.), mediante los diversos criterios de exclusión E_i se descartan 819 artículos, y por los criterios y de inclusión I_j, se obtienen un total de 50 artículos elegidos para el análisis, *ver Tabla 2*.

Tabla 2

Criterios de exclusión

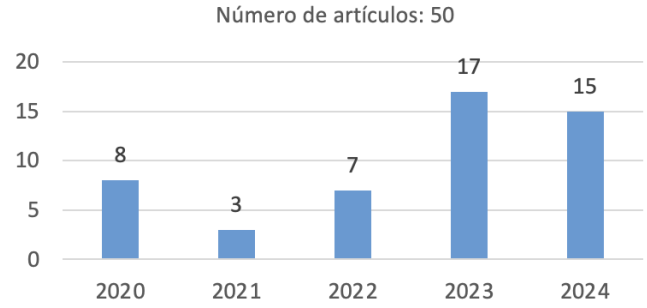
Criterio	Detalle
E_1	La públicación pertenece a la categoría de ensayo
E_2	La publicación utiliza una metodología no relacionada con la temática.
E_3	La publicación aborda el rendimiento de diferentes pruebas o servicios.
E_4	La publicación pertenece a la categoría de revisiones
I_1	La públicación pertenece a la categoría de ensayo
I_2	La publicación utiliza una metodología no relacionada con la temática.
I_3	La publicación aborda el rendimiento de diferentes pruebas o servicios.
I_4	La publicación pertenece a la categoría de revisiones

Análisis Descriptivo

En este estudio, se puede observar la tendencia de los 50 artículos seleccionados a lo largo del periodo de estudio, *ver Figura 2*. Bajo las condiciones E_i e I_j de selección, mayoritariamente se encuentra que el año 2023 tiene una mayor generación de aportes científicos, sin embargo, muy cerca el año en curso. En el 2023 los esfuerzos se ven abocados a la detección de Phising por URLs, Sistemas de Detección de Intrusos, Detección y clasificación de amenazas de nueva generación, aplicación de modelos de nueva generación, *ver Figura 3*.

Figura 2

Distribución de artículos en el tiempo

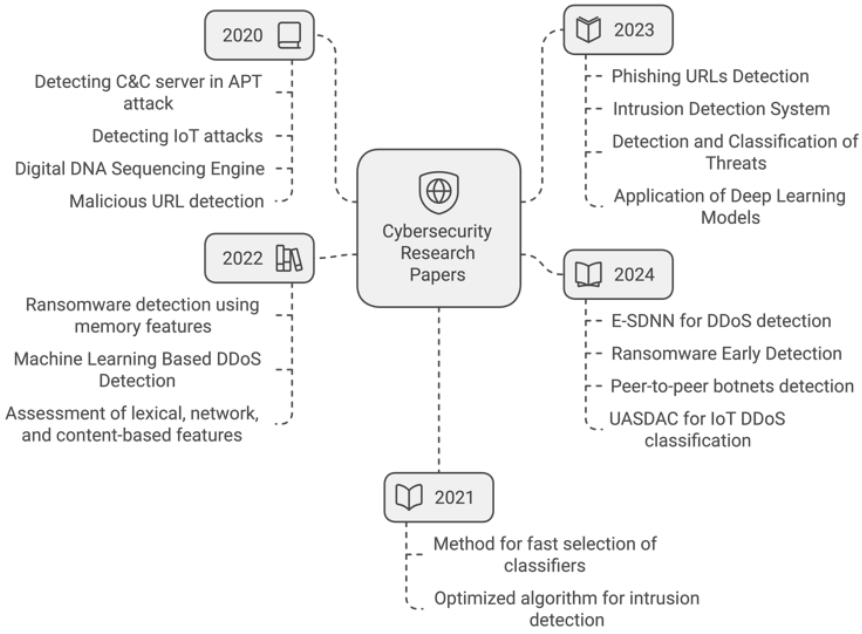


Nota: La gráfica representa 50 artículos que cumplen con las condiciones E_i e I_j para los criterios de la fase de cribado

Las tendencias para el 2024, se enmarcan en temáticas como: detección DDoS, detección temprana de Ransomware, detección de botnets, y clasificación de DDoS en sistemas del internet de las cosas IoT, *ver Figura 3*.

Figura 3

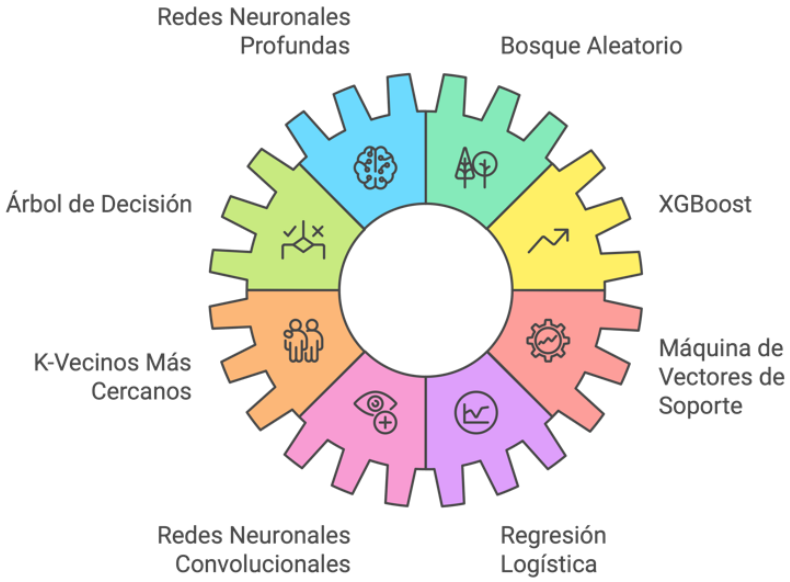
Tendencias durante el período de estudio



Los principales modelos de detección encontrados durante la exploración de los artículos seleccionados son: Random Forest, Árboles de decisión, Support Vector Machine, Logistic Regression, K-means, Neuronal Networks, etc., con sus diversas clasificaciones, *ver Figura 4*.

Figura 4

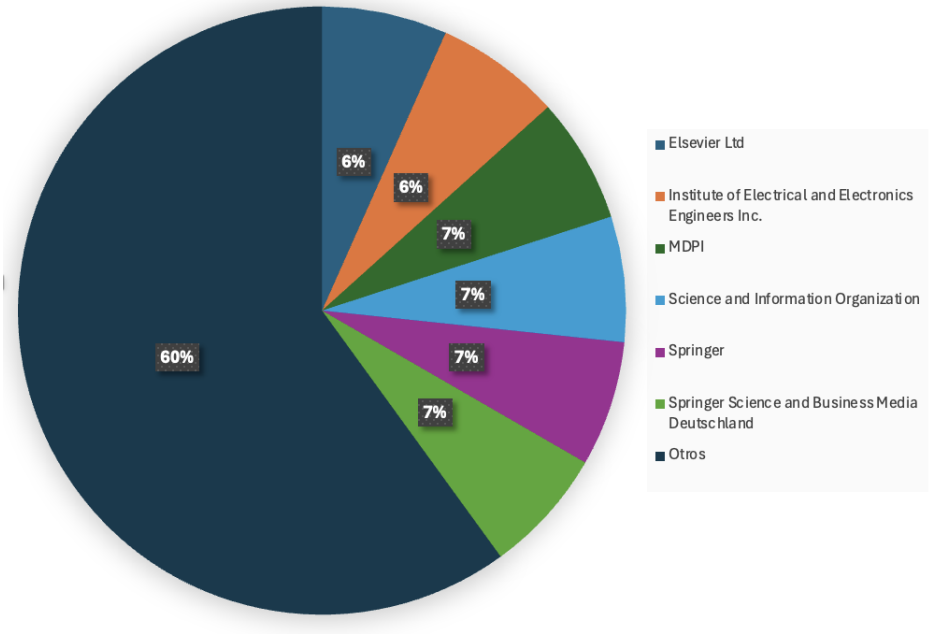
Modelos de detección de amenazas en ciberseguridad



La Figura 5, muestra los principales editores de los 50 artículos seleccionados, siendo mayoritariamente Springer, Elsevier Ltd., IEEE, MDPI, entre otros.

Figura 5

Principales revistas de la información seleccionada



RESULTADOS

La tabla 3, muestra en resumen la aplicación de diversas técnicas como contramedidas a las amenazas tratadas en el presente trabajo organizadas por año y clasificadas por los modelos de detección. La Figura 6 resume las principales técnicas de Machine Learning ML y Deep Learning DL. El aprendizaje automático (ML) es un campo de las ciencias computacionales de rápida expansión dentro de la inteligencia artificial. En el ML se desarrollan algoritmos y modelos estadísticos para el análisis e identificación de patrones (Vaishali & Kumar Tiwari, 2024). El aprendizaje profundo (DL) parte de las redes neuronales con múltiples capas para modelar patrones complejos y abstracciones de alto nivel en datos. Tiene a su alcance varios dominios como el procesamiento del lenguaje natural (PNL), reconocimiento de voz y la visión por computadora (Varatharajan et al., 2024).

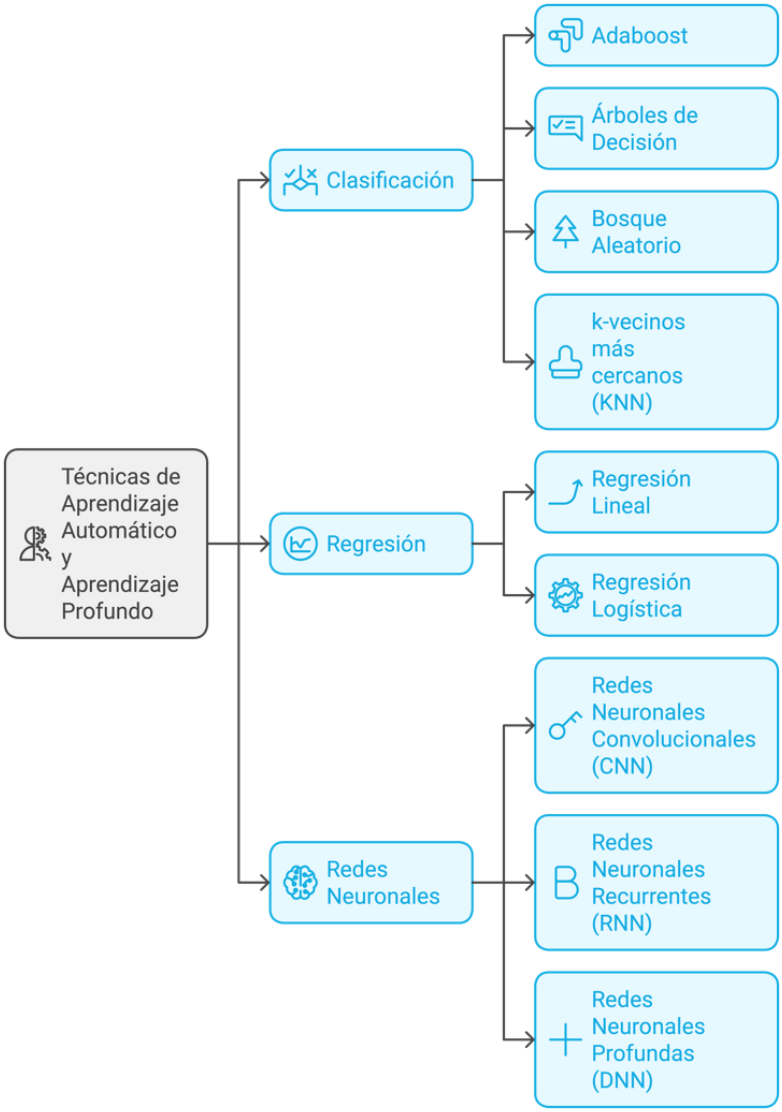
Entre los principales Técnicas de clasificación se mencionan: AdaBoost, Arboles de decisión, Bosque aleatorio (RF), K-vecinos más cercanos (KNN). Los principales algoritmos de Regresión tienen a la Regresión Lineal y Regresión Logística, y en cuanto a las Redes Neuronales, se tienen: Redes Neuronales Convolucionales (CNN), Redes Neuronales Recurrentes (RNN) y Redes Neuronales Profundas (DNN).

El Adaptive Boosting (AdaBoost), es un algoritmo de ML que mejora el rendimiento de los clasificadores débiles al combinarlos en un clasificador fuerte. AdaBoost mejora iterativamente la precisión del modelo y se aplica ampliamente en varios dominios (D. Zhang & Li, 2023).

Los árboles de clasificación son un tipo de árbol de decisión que utiliza el ML para categorizar datos en clases predefinidas de acuerdo con sus atributos de entrada. Su uso principal es la interpretabilidad y capacidad para modelar relaciones complejas, no lineales. Los árboles de clasificación funcionan dividiendo recursivamente los datos en subconjuntos basados en los atributos más informativos, los cuales se seleccionan utilizando criterios como pureza o entropía (Acito, 2023).

Figura 6

Principales técnica de Machine Learning y Deep Learning



El aumento de gradiente optimiza sus modelos de big data, mejorando la precisión y rendimiento combinando aprendices débiles como árboles de decisión. Utiliza una dinámica de cambios de peso durante la fase de entrenamiento, para diagnosticar y ajustar y mejorar la eficiencia (Starodub et al., 2021). BiLSTM-GHA-CNN es un modelo híbrido que combina la memoria bidireccional a largo plazo (BilsTM), la Red Conversarial Generativa (GAN) y la Red Neural Convolucional (CNN). BiLSTM-GHA-CNN puede aplicarse a varios dominios con la finalidad de mejorar la precisión de la predicción mediante la síntesis de datos adicionales a partir

de datos limitados (Ma et al., 2024). CatBoost utiliza técnicas de aprendizaje de conjuntos y ML basado en el impulso de gradiente sobre árboles de decisión, se utiliza para el modelado de variables operacionales, clasificador, o predicción temprana (Harish et al., 2024). Los clasificadores en IA son algoritmos que clasifican los datos en clases o categorías predefinidas, ideales para el análisis de texto, reconocimiento facial y predicción de resultados basados en datos de entrada. Los clasificadores se entrenan mediante el uso de Redes Neuronales Artificiales (ANN) (Santry, 2023). Las redes neuronales, son una categoría del ML y de la IA, su evolución ha sido muy significativa (Pires et al., 2024). Las ANN se utilizan cuando se desconoce la relación entre las variables de entrada y salida, siendo ideales para tareas de clasificación y regresión ("Neural Networks", 2023)(Pires et al., 2024). La arquitectura de las ANN multicapa, permite el desarrollo de modelos de aprendizaje profundo como redes neuronales profundas (DNN), redes neuronales convolucionales (CNN) y redes neuronales recurrentes (RNN) (Dong et al., 2024). Random Forest (RF) es un método utilizado para la clasificación, regresión entre otros. RF se basa en la construcción de una multitud de árboles de decisión sin podar durante el entrenamiento y genera el modo de las clases (clasificación) o predicción media (regresión) de los árboles individuales (Alduailij et al., 2022). La regresión logística (LGR) es ampliamente utilizado como un método estadístico en el modelamiento, donde la variable objetivo tiene dos únicas categorías posibles. A diferencia de la regresión lineal (LR) ordinaria, la (LGR) está diseñada específicamente para manejar datos binarios, cuyo resultado es la predicción en forma de probabilidades (Acito, 2023).

Tabla 3

Resumen de los principales modelos aplicados en las amenazas por año

Año	Amenaza	Uso de la IA	Referencias
2020	APT	ML	(Xuan et al., 2020)
	Malware	LSTM y CNN apiladas	(Namavar Jahromi et al., 2020)
	Phishing	RF, NPL, CNN	(Al-Alyan & Al-Ahmadi, 2020)
	Phishing y botnet	CNN	(De La Torre Parra et al., 2020)
	Ransomware	DNAact-Ran	(Khan et al., 2020)
	Spam Web	CNN, DNN	(Liu & Lee, 2020)
	URL Maliciosa	ML en big data	(Cui et al., 2018)
2021	IDS	SVM, LR, ML	(Alhayali et al., 2021)
	Phishing	RF	(Hammad et al., 2021)
	Spam	K-NN, SVM, NB	(Rapacz et al., 2021)
2022	APT	SVM,	(Alsanad & Altuwaijri, 2022)

	DDoS	RF, XGBoost, K-NN, RL	(Alduailij et al., 2022)
	Malware	RF	(A. P. Singh & Singh, 2022)
	Phishing	Arboles de clasificación	(Piñeiro & Wong Portillo, 2022)
	Sitios web maliciosos	NB	(Aljabri et al., 2022)
	Troyanos	Clasificadores	(Kanaker et al., 2022)
	URL maliciosos	ML y DL	(Alsaidi et al., 2022)
2023	APT	XGBoost	(Hasan et al., 2023)
	Botnets	GA KNN	(Ayo et al., 2023)
	Carding	KNN, LDA, y LR	(Chung & Lee, 2023)
	IDS	ML, BN, RF, Decision table, NN	(Chang et al., 2023)
	Keyloggers	RF, LightGBM, CatBoost	(Alsubaie et al., 2023)
	Malware	KNN, SVM, RF, MLP, ET, GNB	(S. Kumar & Panda, 2023)
	Phishing	RNA, SVM, DT, RF, CNN, VAE, DNN, GBC, RF, NN, NB, Adaboost, KNN, SVM, XGBoost, Decision Tree, RL	(Aljammal et al., 2023; Alnemari & Alshammari, 2023; Choudhary et al., 2023; Jha et al., 2023; Mosa et al., 2023; Nagy et al., 2023; Pandey et al., 2023; Prabakaran et al., 2023; Zaimi et al., 2023)
	Ransomware	CNN, OGCNN-RWD	(Khalid Alkahtani et al., 2023)
2024	Ataques remotos	ML	(Abdulkareem et al., 2024)
	Botnets	CNN, ML, DL	(Kabla et al., 2024)
	DDoS	E-SDNN	(Benmohamed et al., 2024; Selvam & Maheswari Balasubramanian, 2024)
	Detección de amenazas	RF	(Mambetov et al., 2024)
	IDS	Neighbors, XGBoost y AdaBoos	(A. Singh et al., 2024b)

Malware	RNC, RF, AdaBoost, XGBoost	(Gutierrez et al., 2024; J. Kumar et al., 2024)
Phishing	RN, RNC, Plazo (BiLSTM-GHA-CNN	(Bezerra et al., 2024; Nanda & Goel, 2024)
Ransomware	RF, DT, XGBoost	(Alhashmi et al., 2024; Aljabri et al., 2024)
URL maliciosa	ML, XGBoost, KNN, SVM, Decision Tree, RF NB, RL	(Aljahdalic et al., 2024; Yang et al., 2024)

CONCLUSIONES

El seguimiento del modelo PRISMA aporta a este trabajo los insumos que garantizan la rigurosidad científica y aportan las bases principales para el estudio. Mediante la revisión y análisis de los trabajos científicos, se da respuesta a la pregunta de investigación planteada. Los resultados obtenidos, garantizan la rigurosidad científica, puesto que se determina como es aplicada la IA en la mejora continua de la detección y respuesta a diferentes vectores de ciberataques, así como los beneficios y desafíos de los estudios realizados recientemente. Las técnicas descritas se basan en algoritmos de Clasificación, Regresión y Redes Neuronales de Machine Learning y Deep Learning o una combinación novedosa de ellos. La IA se encuentra en constante desarrollo, lo que implica que, existe mucho aún por hacer para desarrollar contramedidas que ayuden a mitigar el cibercrimen. Uno de los factores importantes del éxito de los ciberataques radica en el factor humano, por lo tanto, muchos esfuerzos son encaminados en crear una cultura de ciberseguridad en los usuarios. Se han realizado varios estudios para la detección en tiempo real de intrusiones no deseadas a los sistemas de información. Existen esfuerzos realizados por los proveedores de navegadores web y servidores de correo electrónico, por detener la propagación de intentos fraudulentos para obtener información crítica.

La IA también es utilizada con la intención de encubrir o esquivar los mecanismos de detección de anomalías, e intentos de intrusión a entornos privados. Se utilizan nuevos elementos computacionales para crear amenazas sofisticadas, polimórficas, metamórficas u oligomórficas que se convierten en un verdadero desafío para su detección y respuesta en tiempo real.

REFERENCIAS

Abdulkareem, A., Somefun, T. E., Mutalub, A. L., & Adeyinka, A. (2024). Experimental analysis of intrusion detection systems using machine learning algorithms and artificial neural networks. *International Journal of Electrical and Computer Engineering*, *14*(1), 983-992. Scopus. https://doi.org/10.11591/ijece.v14i1.pp983-992

Acito, F. (2023). Classification and Regression Trees. En F. Acito (Ed.), *Predictive Analytics with KNIME: Analytics for Citizen Data Scientists* (pp. 169-191). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-45630-5_8

Ahmed, S., Syed, R., Kamal, R., & ... (2022). Corporate information security policies targeting ransomw are attack. *2022 Mohammad Ali …*. https://ieeexplore.ieee.org/abstract/document/9994155/

Ajhari, A. A., Priambodo, D. F., Paradisa, R. H., & Yulianti, H. (2023). PROCTOR: A Robust URL Protection System Against Fraudulent, Phishing, and Scam Activities. *International Journal of Computing and Digital Systems*, *14*(1), 1013-1021. Scopus. https://doi.org/10.12785/IJCDS/140179

Al-Alyan, A., & Al-Ahmadi, S. (2020). Robust URL phishing detection based on deep learning. *KSII Transactions on Internet and Information Systems*, *14*(7), 2752-2768. Scopus. https://doi.org/10.3837/tiis.2020.07.001

Alduailij, M., Khan, Q. W., Tahir, M., Sardaraz, M., Alduailij, M., & Malik, F. (2022). Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method. *Symmetry*, *14*(6). Scopus. https://doi.org/10.3390/sym14061095

Alhashmi, A. A., Darem, A. A., Alshammari, A. B., Darem, L. A., Sheatah, H. K., & Effghi, R. (2024). Ransomware Early Detection Techniques. *Engineering, Technology and Applied Science Research*, *14*(3), 14497-14503. Scopus. https://doi.org/10.48084/etasr.6915

Alhayali, R. A. I., Aljanabi, M., Ali, A. H., Mohammed, M. A., & Sutikno, T. (2021). Optimized machine learning algorithm for intrusion detection. *Indonesian Journal of Electrical Engineering and Computer Science*, *24*(1), 590-599. Scopus. https://doi.org/10.11591/ijeecs.v24.i1.pp590-599

Ali, B. S., Ullah, I., Al Shloul, T., Khan, I. A., Khan, I., Ghadi, Y. Y., Abdusalomov, A., Nasimov, R., Ouahada, K., & Hamam, H. (2024). ICS-IDS: application of big data analysis in AI-based intrusion detection systems to identify cyberattacks in ICS networks. *Journal of Supercomputing*, *80*(6), 7876-7905. Scopus. https://doi.org/10.1007/s11227-023-05764-5

Aljabri, M., Alhaidari, F., Albuainain, A., Alrashidi, S., Alansari, J., Alqahtani, W., & Alshaya, J. (2024). Ransomware detection based on machine learning using memory features. *Egyptian Informatics Journal*, *25*. Scopus. https://doi.org/10.1016/j.eij.2024.100445

Aljabri, M., Alhaidari, F., Mohammad, R. M. A., Alhamed, D. H., Altamimi, H. S., & Chrouf, S. M. B. (2022). An Assessment of Lexical, Network, and Content-Based Features for Detecting Malicious URLs Using Machine Learning and Deep Learning Models. *Computational Intelligence and Neuroscience*, *2022*. Scopus. https://doi.org/10.1155/2022/3241216

Aljahdalic, A. O., Banafee, S., & Aljohani, T. (2024). URL filtering using machine learning algorithms. *Information Security Journal*, *33*(3), 193-203. Scopus. https://doi.org/10.1080/19393555.2023.2193350

Aljammal, A. H., taamneh, S., Qawasmeh, A., & Salameh, H. B. (2023). Machine Learning Based Phishing Attacks Detection Using Multiple Datasets. *International Journal of Interactive Mobile Technologies*, *17*(5), 71-83. Scopus. https://doi.org/10.3991/ijim.v17i05.37575

Alnemari, S., & Alshammari, M. (2023). Detecting Phishing Domains Using Machine Learning. *Applied Sciences (Switzerland)*, *13*(8). Scopus. https://doi.org/10.3390/app13084649

Alomari, M., Alsadah, S., Aldahmash, N., Alghulaygah, H., Alogaiel, R., & Saqib, N. A. (2024). A Comprehensive Review of Distributed Denial-of-Service (DDoS) Attacks: Techniques and Mitigation Strategies. *2024 Seventh International Women in Data Science Conference at Prince Sultan University (WiDS PSU)*, 215-222. https://doi.org/10.1109/WiDS-PSU61003.2024.00051

Alsaidi, R. A. M., Yafooz, W. M. S., Alolofi, H., Taufiq-Hail, G. A.-M., Emara, A.-H. M., & Abdel-Wahab, A. (2022). Ransomware Detection using Machine and Deep Learning Approaches. *International Journal of Advanced Computer Science and Applications*, *13*(11), 112-119. Scopus. https://doi.org/10.14569/IJACSA.2022.0131112

Alsanad, A., & Altuwaijri, S. (2022). Advanced Persistent Threat Attack Detection using Clustering Algorithms. *International Journal of Advanced Computer Science and Applications*, *13*(9), 640-649. Scopus. https://doi.org/10.14569/IJACSA.2022.0130976

Alsubaie, M. S., Atawneh, S. H., & Abual-Rub, M. S. (2023). Building Machine Learning Model with Hybrid Feature Selection Technique for Keylogger Detection. *International Journal of Advances in Soft Computing and Its Applications*, *15*(2), 32-53. Scopus. https://doi.org/10.15849/IJASCA.230720.03

Ayo, F. E., Awotunde, J. B., Folorunso, S. O., Adigun, M. O., & Ajagbe, S. A. (2023). A genomic rule-based KNN model for fast flux botnet detection. *Egyptian Informatics Journal*, *24*(2), 313-325. Scopus. https://doi.org/10.1016/j.eij.2023.05.002

Benmohamed, E., Thaljaoui, A., Elkhediri, S., Aladhadh, S., & Alohali, M. (2024). E-SDNN: encoder-stacked deep neural networks for DDOS attack detection. *Neural Computing and*

Applications, *36*(18), 10431-10443. Scopus. https://doi.org/10.1007/s00521-024-09622-0

Bertino, E., Bhardwaj, S., Cicala, F., Gong, S., Karim, I., Katsis, C., Lee, H., Li, A. S., & Mahgoub, A. Y. (2023). Detection. En E. Bertino, S. Bhardwaj, F. Cicala, S. Gong, I. Karim, C. Katsis, H. Lee, A. S. Li, & A. Y. Mahgoub (Eds.), *Machine Learning Techniques for Cybersecurity* (pp. 79-104). Springer International Publishing. https://doi.org/10.1007/978-3-031-28259-1_6

Bezerra, A., Pereira, I., Rebelo, M. Â., Coelho, D., Oliveira, D. A. D., Costa, J. F. P., & Cruz, R. P. M. (2024). A case study on phishing detection with a machine learning net. *International Journal of Data Science and Analytics*. Scopus. https://doi.org/10.1007/s41060-024-00579-w

Bhardwaj, A. (2023). *Sophisticated-Sinister-Stealth Attacks* (sophisticated-sinister-stealth-attacks) [Chapter]. Https://Services.Igi-Global.Com/Resolvedoi/Resolve.Aspx?Doi=10.4018/979-8-3693-1528-6.Ch002; IGI Global. https://doi.org/10.4018/979-8-3693-1528-6.ch002

Bokhari, S. A. A., & Myeong, S. (2023). The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective. *IEEE Access*, *11*, 69783-69797. Scopus. https://doi.org/10.1109/ACCESS.2023.3293480

Chang, V., Boddu, S., Xu, Q. A., & Doan, L. M. T. (2023). Intrusion detection and prevention with machine learning algorithms. *International Journal of Grid and Utility Computing*, *14*(6), 617-631. Scopus. https://doi.org/10.1504/IJGUC.2023.135306

Chaowen, C. (2024). Research on computer network security situation awareness warning mechanism based on artificial intelligence. *2024 IEEE 4th International Conference on Electronic Technology, Communication and Information (ICETCI)*, 748-753. https://doi.org/10.1109/ICETCI61221.2024.10594283

Choudhary, T., Mhapankar, S., Bhddha, R., Kharuk, A., & Patil, R. (2023). A Machine Learning Approach for Phishing Attack Detection. *Journal of Artificial Intelligence and Technology*, *3*(3), 108-113. Scopus. https://doi.org/10.37965/jait.2023.0197

Christopher, L. U., & Ayorinde, I. T. (2024). Malware Detection Using Hidden Markov Model. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *12*(2), 37-46. https://doi.org/10.22624/AIMS/DIGITAL/V11N2P4

Chung, J., & Lee, K. (2023). Credit Card Fraud Detection: An Improved Strategy for High Recall Using KNN, LDA, and Linear Regression. *Sensors*, *23*(18). Scopus. https://doi.org/10.3390/s23187788

Cui, B., He, S., Shi, P., & Yao, X. (2018). Malicious URL detection with feature extraction based on machine learning. *International Journal of High Performance Computing and Networking*, *12*(2), 166-178. Scopus. https://doi.org/10.1504/ijhpcn.2018.094367

Dau, D.-D., Lee, S., & Kim, H. (2024). A comprehensive comparison study of ML models for multistage APT detection: Focus on data preprocessing and resampling. *Journal of Supercomputing*, *80*(10), 14143-14179. Scopus. https://doi.org/10.1007/s11227-024-06010-2

De La Torre Parra, G., Rad, P., Choo, K.-K. R., & Beebe, N. (2020). Detecting Internet of Things attacks using distributed deep learning. *Journal of Network and Computer Applications*, *163*. Scopus. https://doi.org/10.1016/j.jnca.2020.102662

Dhananjay Tangtode, Shayan Sayyad, Omkar Gelye, Sarthak Sawant, & Prof. Girisha Bombale. (2024). DDOS Attack Detection. *International Journal of Advanced Research in Science, Communication and Technology*, 248-251. https://doi.org/10.48175/IJARSCT-15547

Dong, Q., Chen, X., & Huang, B. (2024). Chapter 11—Neural networks. En Q. Dong, X. Chen, & B. Huang (Eds.), *Data Analysis in Pavement Engineering* (pp. 223-245). Elsevier. https://doi.org/10.1016/B978-0-443-15928-2.00009-4

Gutierrez, R., Villegas-Ch, W., Godoy, L. N., Mera-Navarrete, A., & Lujan-Mora, S. (2024). Application of Deep Learning Models for Real-Time Automatic Malware Detection. *IEEE Access*, *12*, 107742-107756. Scopus. https://doi.org/10.1109/ACCESS.2024.3436588

Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. *Campbell Systematic Reviews*, *18*(2), e1230. https://doi.org/10.1002/cl2.1230

Hammad, M., Hewahi, N., & Elmedany, W. (2021). T-SNERF: A novel high accuracy machine learning approach for Intrusion Detection Systems. *IET Information Security*, *15*(2), 178-190. Scopus. https://doi.org/10.1049/ise2.12020

Harish, M., Kumar, V., Rajasekarnan, p, & Poovizhi, P. (2024, diciembre 10). *Analysis on Early Prediction of Cotton Plant Leaf Diseases Using CatBoost Algorithm | IEEE Conference Publication | IEEE Xplore*. https://ieeexplore.ieee.org/document/10624844

Hasan, M. M., Islam, M. U., & Uddin, J. (2023). Advanced Persistent Threat Identification with Boosting and Explainable AI. *SN Computer Science*, *4*(3). Scopus. https://doi.org/10.1007/s42979-023-01744-x

Hyslip, T. S., & Burruss, G. W. (2023). Ransomware. En *Handbook on Crime and Technology* (pp. 86-104). Edward Elgar Publishing. https://www.elgaronline.com/edcollchap/book/9781800886643/book-part-9781800886643-13.xml

Jha, A. K., Muthalagu, R., & Pawar, P. M. (2023). Intelligent phishing website detection using machine learning. *Multimedia Tools and Applications*, *82*(19), 29431-29456. Scopus. https://doi.org/10.1007/s11042-023-14731-4

Kabla, A. H. H., Thamrin, A. H., Anbar, M., Manickam, S., & Karuppayah, S. (2024). Peer-to-peer botnets: Exploring behavioural characteristics and machine/deep learning-based detection. *Eurasip Journal on Information Security*, *2024*(1). Scopus. https://doi.org/10.1186/s13635-024-00169-0

Kanaker, H., Karim, N. A., Awwad, S. A. B., Ismail, N. H. A., Zraqou, J., & Al ali, A. M. F. (2022). Trojan Horse Infection Detection in Cloud Based Environment Using Machine Learning. *International Journal of Interactive Mobile Technologies*, *16*(24), 81-106. Scopus. https://doi.org/10.3991/ijim.v16i24.35763

Khalid Alkahtani, H., Mahmood, K., Khalid, M., Othman, M., Al Duhayyim, M., Osman, A. E., Alneil, A. A., & Zamani, A. S. (2023). Optimal Graph Convolutional Neural Network-Based Ransomware Detection for Cybersecurity in IoT Environment. *Applied Sciences (Switzerland)*, *13*(8). Scopus. https://doi.org/10.3390/app13085167

Khan, F., Ncube, C., Ramasamy, L. K., Kadry, S., & Nam, Y. (2020). A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning. *IEEE Access*, *8*, 119710-119719. Scopus. https://doi.org/10.1109/ACCESS.2020.3003785

Kumar, J., Rajendran, B., & Sudarsan, S. D. (2024). Zero-Day Malware Classification and Detection Using Machine Learning. *SN Computer Science*, *5*(1). Scopus. https://doi.org/10.1007/s42979-023-02404-w

Kumar, S., & Panda, K. (2023). SDIF-CNN: Stacking deep image features using fine-tuned convolution neural network models for real-world malware detection and classification. *Applied Soft Computing*, *146*. Scopus. https://doi.org/10.1016/j.asoc.2023.110676

Li, X., Zhang, D., & Wu, B. (2020). Detection method of phishing email based on persuasion principle. *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, *1*, 571-574. https://doi.org/10.1109/ITNEC48623.2020.9084766

Liu, D., & Lee, J.-H. (2020). Cnn based malicious website detection by invalidating multiple web spams. *IEEE Access*, *8*, 97258-97266. Scopus. https://doi.org/10.1109/ACCESS.2020.2995157

Ma, Z., Sun, Y., Ji, H., Li, S., Nie, S., & Yin, F. (2024). A CNN-BiLSTM-Attention approach for EHA degradation prediction based on time-series generative adversarial network. *Mechanical Systems and Signal Processing*, *215*, 111443. https://doi.org/10.1016/j.ymssp.2024.111443

Mambetov, S., Begimbayeva, Y., Gurko, O., Doroshenko, H., Joldasbayev, S., Fridman, O., Kulambayev, B., Babenko, V., Ilhe, I., & Neronov, S. (2024). DETECTION AND CLASSIFICATION OF THREATS AND VULNERABILITIES ON HACKER FORUMS BASED ON MACHINE LEARNING. *Eastern-European Journal of*

Enterprise Technologies, *3*(9(129)), 16-27. Scopus. https://doi.org/10.15587/1729-4061.2024.306522

Mohanty, R., & Bala Das, S. (2018). A Proposed What-Why-How (WWH) Learning Model for Students and Strengthening Learning Skills Through Computational Thinking. En P. K. Sa, M. N. Sahoo, M. Murugappan, Y. Wu, & B. Majhi (Eds.), *Progress in Intelligent Computing Techniques: Theory, Practice, and Applications* (pp. 135-141). Springer. https://doi.org/10.1007/978-981-10-3376-6_15

Mohebzada, J. G., Zarka, A. E., Bhojani, A. H., & Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. *2012 International Conference on Innovations in Information Technology (IIT)*, 249-254. https://doi.org/10.1109/INNOVATIONS.2012.6207742

Mosa, D. T., Shams, M. Y., Abohany, A. A., El-Kenawy, E.-S. M., & Thabet, M. (2023). Machine Learning Techniques for Detecting Phishing URL Attacks. *Computers, Materials and Continua*, *75*(1), 1271-1290. Scopus. https://doi.org/10.32604/cmc.2023.036422

Munjal, G., Paul, B., & Kumar, M. (2024). Application of Artificial Intelligence in Cybersecurity: En P. K. Goel, H. M. Pandey, A. Singhal, & S. Agarwal (Eds.), *Advances in Information Security, Privacy, and Ethics* (pp. 127-146). IGI Global. https://doi.org/10.4018/979-8-3693-1431-9.ch006

Nagy, N., Aljabri, M., Shaahid, A., Ahmed, A. A., Alnasser, F., Almakramy, L., Alhadab, M., & Alfaddagh, S. (2023). Phishing URLs Detection Using Sequential and Parallel ML Techniques: Comparative Analysis. *Sensors*, *23*(7). Scopus. https://doi.org/10.3390/s23073467

Namavar Jahromi, A., Hashemi, S., Dehghantanha, A., Choo, K.-K. R., Karimipour, H., Newton, D. E., & Parizi, R. M. (2020). An improved two-hidden-layer extreme learning machine for malware hunting. *Computers and Security*, *89*. Scopus. https://doi.org/10.1016/j.cose.2019.101655

Nanda, M., & Goel, S. (2024). URL based phishing attack detection using BiLSTM-gated highway attention block convolutional neural network. *Multimedia Tools and Applications*, *83*(27), 69345-69375. Scopus. https://doi.org/10.1007/s11042-023-17993-0

Pandey, M. K., Singh, M. K., Pal, S., & Tiwari, B. B. (2023). Prediction of phishing websites using machine learning. *Spatial Information Research*, *31*(2), 157-166. Scopus. https://doi.org/10.1007/s41324-022-00489-8

Piñeiro, J. J. M. L., & Wong Portillo, L. R. (2022). Web architecture for URL-based phishing detection based on Random Forest, Classification Trees, and Support Vector Machine. *Inteligencia Artificial*, *25*(69), 107-121. Scopus. https://doi.org/10.4114/intartif.vol25iss69pp107-121

Pires, P. B., Santos, J. D., Pereira, I. V., Pires, P. B., Santos, J. D., & Pereira, I. V. (2024). *Artificial Neural Networks: History and State of the Art* (artificial-neural-networks) [Chapter]. Https://Services.Igi-Global.Com/Resolvedoi/Resolve.Aspx?Doi=10.4018/978-1-6684-7366-5.Ch037; IGI Global. https://doi.org/10.4018/978-1-6684-7366-5.ch037

Prabakaran, M. K., Meenakshi Sundaram, P., & Chandrasekar, A. D. (2023). An enhanced deep learning-based phishing detection mechanism to effectively identify malicious URLs using variational autoencoders. *IET Information Security*, *17*(3), 423-440. Scopus. https://doi.org/10.1049/ise2.12106

PRISMA statement. (s. f.). PRISMA Statement. https://www.prisma-statement.org

Rao, S. C. (2023). An Introduction to Systematic Reviews and Meta-Analyses. *APIK Journal of Internal Medicine*, *11*(3), 141. https://doi.org/10.4103/ajim.ajim_36_23

Rao-Kadari, S., Radhika, G., M. Shekar, Shankar, R., & Madhu, C. (2024). A Study on the Key Applications of Malware. *International Journal of Advanced Research in Science, Communication and Technology*, 481-485. https://doi.org/10.48175/IJARSCT-19359

Rapacz, S., Chołda, P., & Natkaniec, M. (2021). A method for fast selection of machine-learning classifiers for spam filtering. *Electronics (Switzerland)*, *10*(17). Scopus. https://doi.org/10.3390/electronics10172083

Reza, F. (2024). DDoS-Net: Classifying DDoS Attacks in Wireless Sensor Networks with Hybrid Deep Learning. *2024 6th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT)*, 487-492. https://doi.org/10.1109/ICEEICT62016.2024.10534545

Ribeiro, L. Q., Guedes, I., Cardoso, C., Ribeiro, L. Q., Guedes, I., & Cardoso, C. (2023). *Phishing: A Theoretical Approach and the Innovative Tools* (phishing) [Chapter]. Https://Services.Igi-Global.Com/Resolvedoi/Resolve.Aspx?Doi=10.4018/978-1-6684-8422-7.Ch005; IGI Global. https://doi.org/10.4018/978-1-6684-8422-7.ch005

Rico-González, M., Pino-Ortega, J., Clemente, F., & Arcos, A. L. (2021). Guidelines for performing systematic reviews in sports science. *Biology of Sport*, *39*(2), 463-471. https://doi.org/10.5114/biolsport.2022.106386

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, *117*, 345-357. Scopus. https://doi.org/10.1016/j.eswa.2018.09.029

Santry, D. (2023, diciembre 1). *Training Classifiers—Demystifying Deep Learning—Wiley Online Library*. https://onlinelibrary.wiley.com/doi/10.1002/9781394205639.ch4

Selvam, S., & Maheswari Balasubramanian, U. (2024). UASDAC: An Unsupervised Adaptive Scalable DDoS Attack Classification in Large-Scale IoT Network Under Concept Drift. *IEEE Access*, *12*, 64701-64716. Scopus. https://doi.org/10.1109/ACCESS.2024.3397512

Sharko, A. D., Sharko, G., & Qose, S. (2024). Artificial Intelligence In Cybersecurity Applications. *2024 IEEE 28th International Conference on Intelligent Engineering Systems (INES)*, 000175-000180. https://doi.org/10.1109/INES63318.2024.10629129

Singh, A. P., & Singh, M. (2022). Classification of Malware in HTTPs Traffic Using Machine Learning Approach. *El-Cezeri Journal of Science and Engineering*, *9*(2), 644-655. Scopus. https://doi.org/10.31202/ecjse.990318

Singh, A., Prakash, J., Kumar, G., Jain, P. K., & Ambati, L. S. (2024a). Intrusion Detection System: A Comparative Study of Machine Learning-Based IDS. *Journal of Database Management (JDM)*, *35*(1), 1-25. https://doi.org/10.4018/JDM.338276

Singh, A., Prakash, J., Kumar, G., Jain, P. K., & Ambati, L. S. (2024b). Intrusion Detection System: A Comparative Study of Machine Learning-Based IDS. *Journal of Database Management*, *35*(1). Scopus. https://doi.org/10.4018/JDM.338276

Starodub, A., Eliseeva, N., & Georgiev, M. (2021). Gradient-Based Algorithm for Tracking the Activity of Neural Network Weights Changing. *EPJ Web of Conferences*, *248*, 01012. https://doi.org/10.1051/epjconf/202124801012

Supriyanto, C., Rafrastara, F. A., Amiral, A., Amalia, S. R., Fahreza, M. D. A., & Abdollah, M. F. (2024). Malware Detection Using K-Nearest Neighbor Algorithm and Feature Selection. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *8*(1), Article 1. https://doi.org/10.30865/mib.v8i1.6970

Tairov, I. (2024). Artificial Intelligence Applications for Confronting Cybersecurity Issues. *Research Papers*, *64*(3), 121-132. https://doi.org/10.37075/RP.2024.3.08

Thakur, S., Chaudhari, S., & Joshi, B. (2022). Ransomware: Threats, Identification and Prevention. En *Cyber Security and Digital Forensics* (pp. 361-387). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119795667.ch16

Tilmar Jakobsern, A. (2024). Malware Analysis. En *Practical Cyber Intelligence* (pp. 167-175). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781394256129.ch12

Vaishali, J., & Kumar Tiwari, S. (2024). OVERVIEW: MACHINE LEARNING. En *OVERVIEW: MACHINE LEARNING*. IIP Series. https://iipseries.org/

Varatharajan, N., Lavanya, S., Suganya, A., & Vikkram, R. (2024). Deep Learning: Overview, Applications and Computing Devices. En *Deep Learning Concepts in Operations Research*. Auerbach Publications.

Xuan, C. D., Duong, L. V., & Tisenko, V. N. (2020). Detecting C&C server in the APT attack based on network traffic using machine learning. *International Journal of Advanced Computer Science and Applications*, *11*(5), 22-27. Scopus. https://doi.org/10.14569/IJACSA.2020.0110504

Xue, Y., Onzo, B., & Neri, F. (2021). Intrusion Detection System Based on an Updated ANN Model. En Y. Tan & Y. Shi (Eds.), *Advances in Swarm Intelligence* (pp. 472-479). Springer International Publishing. https://doi.org/10.1007/978-3-030-78811-7_44

Yang, S., Chen, Z., Xu, Y., & Liu, J. (2024). Research on Malicious Web Page Identification Method Based on Deep Learning and Feature Fusion. *Journal of Cyber Security*, *9*(3), 176-190. Scopus. https://doi.org/10.19363/J.cnki.cn10-1380/tn.2024.05.12

Yunoose, A., Varghese, Y., R, A., Prakash, A., & Babu, D. (2022). International Journal of Engineering Technology and Management Sciences. *International Journal of Engineering Technology and Management Sciences*, *5*(6), 574-579. https://doi.org/DOI:10.46647/ijetms.2022.v06i05.092

Yusuff, H. (2023). Systematic review and meta-analysis. *Journal of Global Medicine*, *3*(S1), Article S1. https://doi.org/10.51496/jogm.v3.S1.133

Zaimi, R., Hafidi, M., & Lamia, M. (2023). A deep learning approach to detect phishing websites using CNN for privacy protection. *Intelligent Decision Technologies*, *17*(3), 713-728. Scopus. https://doi.org/10.3233/IDT-220307

Zhang, D., & Li, H. (2023). Application of Adaboost Algorithm in Enterprise Financial Risk Analysis Model. *2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE)*, 1-5. https://doi.org/10.1109/AIKIIE60097.2023.10389905

Zhang, J., Zheng, J., Zhang, Z., Chen, T., Tan, Y.-A., Zhang, Q., & Li, Y. (2024). ATT&CK-based Advanced Persistent Threat attacks risk propagation assessment model for zero trust networks. *Computer Networks*, *245*. Scopus. https://doi.org/10.1016/j.comnet.2024.110376

Zhou, Y., & Liang, Y. (2024). Application of artificial intelligence technology in network security. *Highlights in Science, Engineering and Technology*, *92*, 479-485. https://doi.org/10.54097/1mrvaw84