Revisión de la implementación del machine learning en la seguridad de la información

Review of the implementation of machine learning in information security

Recibido: noviembre 23 de 2022 | Revisado: noviembre 26 de 2022 | Aceptado: noviembre 29 de 2022

Cristhian Alvarado[1]
Carlos Pingo[2]
Alberto Mendoza[3]

Resumen

La presente revisión tiene como objetivo dar a conocer cómo se está implementando el machine learning en la seguridad de la información. Por tal motivo se optó por la metodología PRISMA para identificar artículos en diferentes bases de datos en los últimos cinco años. Se utilizó las siguientes bases de datos: Scopus, Science Direct, Research Gate y Google Académico. Posteriormente, se aplicaron los criterios de inclusión y exclusión, dando un resultado de 16 artículos donde se implementa el machine learning en la seguridad de la información para dar respuesta a las preguntas planteadas. De esta manera, las diversas técnicas y/o algoritmos del machine learning aplicados en la seguridad de la información es una necesidad de las organizaciones en la actualidad para la protección de la información, siendo unos de los algoritmos más usados las redes neuronales artificiales y el área donde mayormente se implementa el machine learning para la seguridad de la información es internet de las cosas.

Palabras clave: Aprendizaje Automático; Seguridad de la Información; Aprendizaje Profundo; Inteligencia Artificial

Abstract

This review aims to make known how machine learning is being implemented in information security. For this reason, the PRISMA methodology was chosen to identify articles in different databases in the last 5 years. The following databases were obtained: Scopus, Science Direct, Research Gate and Google Scholar. Subsequently, the inclusion and exclusion criteria will be applied, giving a result of 16 articles where machine learning is implemented in information security to answer the questions raised. In conclusion, the various techniques and/or algorithms of machine learning applied in information security is a need for organizations today for the protection of information, one of the most used algorithms being artificial neural networks. and the area where machine learning is most widely deployed for information security is the internet of things.

Keywords: Machine Learning; Security of the information; Deep Learning; Artificial intelligence

1 Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, Trujillo, Perú
2 Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, Trujillo, Perú
3 Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, Trujillo, Perú

Autor de correspondencia:
cfalvarado@unitru.edu.pe

https://doi.org/10.24265/campus.2022.v27n34.13

Introducción

Actualmente, la mayoría de la población conoce las tecnologías de la información, dado que fueron involucradas en mayor porcentaje durante y después de la pandemia que azotó al mundo. Es un hecho que la tecnología nos ayuda a ser más productivos y nos permite acceder a una gran cantidad y volúmenes de información con tan solo un clic, pero a la vez esto conlleva a una gran cantidad de problemas de seguridad porque no sabemos si en cualquier momento nuestra información puede ser expuesta por ciberdelincuentes. (Vega Briceño, 2021)

La sociedad actual se encuentra en el proceso de desarrollar un sentido de responsabilidad y seguridad corporativas, lo cual es imprescindible para las organizaciones donde se deben disponer de servicios avanzados de consultoría para lograr una completa seguridad corporativa. Asimismo, adoptar buenas prácticas y políticas de seguridad que garanticen la seguridad de la información. (Shrivastava & Kumar, 2019).

En ese contexto, una de las últimas técnicas para garantizar la seguridad de la información que están usando las organizaciones es el machine learning, dónde se implementan diferentes algoritmos, métodos, teorías de aprendizaje automático para solucionar los problemas de seguridad de la información y prevenirlos. El machine learning cada vez está siendo muy popular en las organizaciones ya que nos ofrece una "inteligencia" similar a la del humano y está siendo aplicado en diferentes sectores, áreas y actividades relacionadas a la encriptación, autentificación, reconocimiento, visión computacional, prevención, entre otras. (Iqbal H. Sarker, 2022).

Según (Shrivastava & Kumar, 2019), "machine learning" está enfocado en los diversos cambios en los sistemas de ejecución de tareas asociadas con inteligencia artificial que se refiere a la capacidad de una máquina para poseer inteligencia como la humana. Las diversas tareas mencionadas, anteriormente, implican el diagnóstico, planificación, reconocimiento, control de robots, previsión y predicción. Estos cambios implican la evolución de nuevos sistemas o mejora en los sistemas existentes. Así mismo, según ISO/IEC 27001, la "seguridad de la información" consiste en mantener la confidencialidad, integridad y disponibilidad de la información. Son buenas prácticas y metodologías que buscan proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o eliminación no autorizada; en otras palabras, proteger los datos y recursos de infraestructura tecnológica de una organización. Además, otras cualidades están involucradas como la autenticidad, responsabilidad, confiabilidad y el no repudio. (Vega Briceño, 2021)

El objetivo principal de esta revisión fue analizar la implementación del machine learning en la seguridad de la información en los últimos cinco años. Para ello, se desarrollaron algunas preguntas previas: ¿Qué importancia tiene el machine learning en la seguridad de la información?, ¿Qué algoritmos de machine learning son usados para la seguridad de la información?, ¿En qué áreas se usa el machine learning para la seguridad de la información de las organizaciones?

Método

Para la investigación realizada se hizo una revisión sistemática en base a la metodología PRISMA (Preferred Reporting Items for Systematic Review and Meta-Analyses). La pregunta de investigación establecida para esta revisión sistemática fue la siguiente: ¿Cómo se está implementando el machine learning en la seguridad de la información en los últimos cinco años?

Según (Quispe et al., 2021) una revisión sistémica es una revisión de la literatura científica donde se lleva a cabo un proceso planificado, con el objetivo de analizar artículos publicados anteriormente para responder a una pregunta específica. La literatura encontrada debe ser relevante y se debe ajustar a los criterios de inclusión/exclusión establecidos posteriormente. Los hallazgos son de confiabilidad, las conclusiones ayudan a la toma de decisiones a los próximos investigadores.

Adicionalmente, para Blanco Gómez et al., 2020 el objetivo de la metodología PRISMA es reducir el riesgo de sesgo tanto en la fase que selecciona la literatura científica relevante para incluir en la revisión sistemática, como en la fase de análisis posterior. Para ellos se deben establecer criterios de inclusión y exclusión que se aplican en la fase de selección final.

Para el proceso de búsqueda de información hemos extraído las palabras claves de nuestro tema de investigación, que son las siguientes: "Aprendizaje Automatizado", "Algoritmos del Aprendizaje Automatizado" y "Seguridad de la Información". Asimismo, una vez identificadas las palabras claves, se buscaron por su traducción al inglés: "Machine Learning", "Machine Learning Algorithms" y "Security of Information".

Se realizó la indagación en diferentes bases de datos científicos. Para segmentarla, limitamos las publicaciones hasta hace cinco años (2018-2022) con la finalidad de conocer cómo está la situación actual del machine learning aplicado a la seguridad de la información.

La combinación de términos en español que usamos para la búsqueda de publicaciones fue la siguiente: [("aprendizaje automatizado) AND ("seguridad de la información") AND (LIMIT-TO (PUBYEAR, 2022) OR LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018))]. Además, la combinación de términos en inglés que usamos para la búsqueda de publicaciones fue la siguiente: [("machine learning") AND ("security of information") AND (LIMIT-TO (PUBYEAR, 2022) OR LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018))].

Para el desarrollo de esta investigación se hizo una búsqueda en las bases de datos como Scopus, Science Direct, ResearchGate y Google Académico donde se pudo encontrar diversos tipos de publicaciones como: artículos, conferencias y libros entre los años 2018-2022 relacionados al tema de investigación.

Figura 1

Resultados por tipo de publicación

En cuanto a los criterios de exclusión e inclusión, se consideraron los siguientes como se muestra en la Tabla 1.

Tabla 1

Criterios de exclusión e inclusión

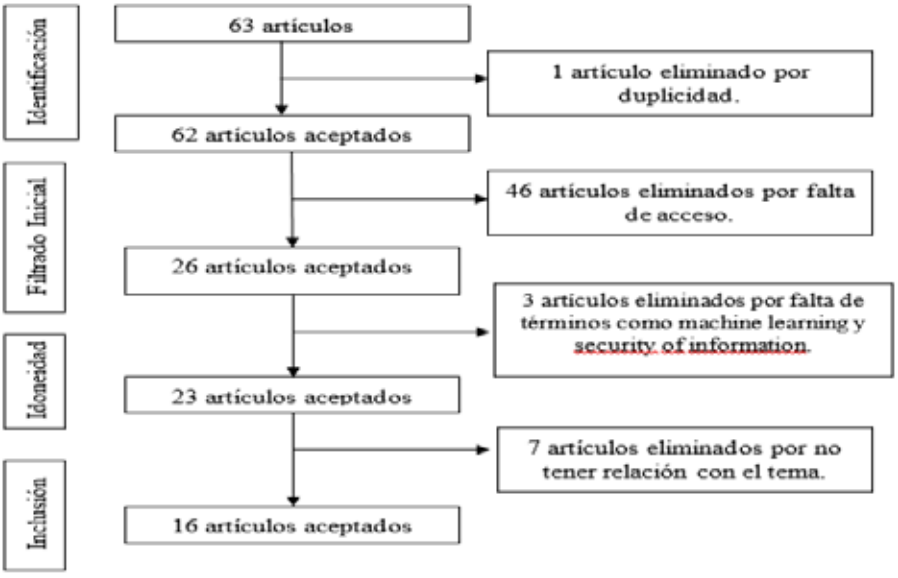
Exclusión	Inclusión
No tiene relación el machine learning con la seguridad de la información	Publicaciones con información del machine learning aplicados a la seguridad de la información
Publicaciones con más de cinco años de antigüedad	Publicaciones dentro del rango del año 2018 al 2022
Por duplicidad	Artículos publicados en los idiomas español e inglés
Por falta de acceso	

Resultados y Discusión

En la búsqueda de publicaciones se estableció un intervalo de tiempo desde hace cinco años atrás en las bases de datos seleccionadas que arrojaron un total de 63 artículos entre el año 2018 – 2022 distribuidos de la siguiente manera: Scopus: 23 artículos, Science Direct 27 artículos, Research Gate cinco artículos y Google Académico 18 artículos.

Figura 2

Flujograma del proceso de selección de artículos



De 63 artículos seleccionados, aplicando la metodología PRISMA y haciendo uso del flujograma para la selección de artículos en base a los criterios de inclusión y exclusión, se escogieron 16 artículos, de los cuales seis pertenecen a Google Académico, que significa el 37,50% como mayoría de los artículos seleccionados, lo cual se evidencia en la Figura 3.

Figura 3

Cantidad de artículos por base de datos

Se obtuvieron los siguientes artículos según la base de datos: Scopus, tres artículos; Science Direct, cinco artículos; Research Gate, dos artículos y Google Académico, seis artículos. Posteriormente, de los 16 artículos seleccionados, se procedió a hacer la identificación de la situación actual del machine learning en la seguridad de la información, lo cual se puede evidenciar en la Tabla 2.

Tabla 2

Resultado de búsqueda final

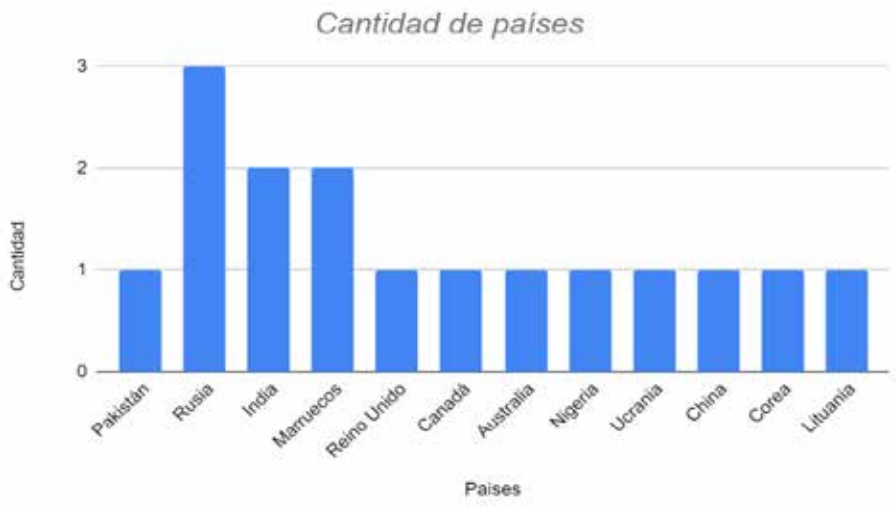
Nro.	Autor	Título de Investigación	País	Año
01	(Naseer et al., 2018)	Enhanced network anomaly detection based on deep neural networks	Pakistán	2018
02	(Sokolov et al., 2019)	Applying of digital signal processing techniques to improve the performance of machine learning-based cyber-attack detection in industrial control system	India	2019
03	(Ikrissi & Mazri, 2021)	IOT-BASED SMART ENVIRONMENTS: STATE of the ART, SECURITY THREATS and SOLUTIONS	Marruecos	2021
04	(Zapechnikov, 2020)	Privacy-Preserving Machine Learning as a Tool for Secure Personalized Information Services	Rusia	2020
05	(Applebaum et al., 2021)	Signature-based and Machine-Learning-based Web Application Firewalls: A Short Survey	Reino Unido	2021
06	(Domashova & Kripak, 2021)	Identification of non-typical international transactions on bank cards of individuals using machine learning methods	Rusia	2021
07	(Thorat et al., 2021)	TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification	India	2021
08	(Bahassi et al., 2022)	Toward an exhaustive review on Machine Learning for Cybersecurity	Marruecos	2022

09	(Hazratifard et al., 2022)	Using Machine Learning for Dynamic Authentication in Telehealth: A Tutorial	Canadá	2022
10	(Iqbal H. Sarker, 2022)	Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects	Australia	2022
11	(ADETUNMBI A.O. et al., 2018)	A Machine Learning Approach for Information System Security	Nigeria	2018
12	(Tolubko et al., 2018)	Method for Determination of Cyber Threats Based on Machine Learning for Real-Time Information System	Ucrania	2018
13	(Zhang et al., 2020)	Multicriteria Decision and Machine Learning Algorithms for Component Security Evaluation: Library-Based Overview	China	2020
14	(Raviteja et al., 2020)	Implementation Of Machine Learning Algorithms for Detection Of Network Intrusion	India	2020
15	(Butt et al., 2020)	A Review of Machine Learning Algorithms for Cloud Computing Security	Corea	2020
16	(Damaševičius et al., 2021)	Ensemble-Based Classification Using Neural Networks and Machine Learning Models for Windows PE Malware Detection	Lituania	2021

Tomando en cuenta los artículos seleccionados, se procedió a revisar cómo se está implementando el machine learning para mejorar la seguridad de la información. Con respecto a los países que lideran las publicaciones se obtuvo que el país con más artículos es Rusia con tres publicaciones, seguido por la India y Marruecos con dos publicaciones. El resto de los países tiene una publicación, lo cual se puede evidenciar en la Figura 4.

Figura 4

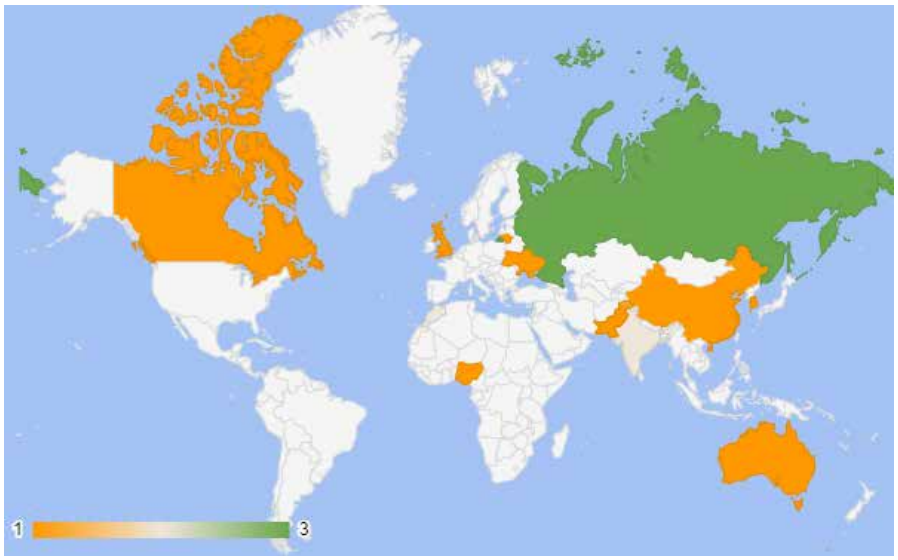
Cantidad de artículos por países



A continuación, se muestra la ubicación geográfica de los países donde se encontraron los artículos en los cuales se está aplicando el machine learning para mejorar la seguridad de la información que se puede evidenciar en la Figura 5.

Figura 5

Ubicación geográfica de los países



Para la mayoría de los artículos, un párrafo bien desarrollado que resuma el principal hallazgo de la investigación es suficiente, aunque en algunos casos se puede requerir una conclusión de dos o tres párrafos, tal vez con una oración corta con las implicaciones para posteriores investigaciones.

Implementación del machine learning en la seguridad de la información

En la literatura revisada, los autores coinciden en que la seguridad de la información es uno de los mayores desafíos en el que se enfrentan las organizaciones e instituciones. Además con la pandemia de COVID-19, la mayoría de los servicios se ha trasladado al modo online y remoto, lo que aumenta más los peligros de ciberataques y malwares (Damaševičius et al., 2021).

En lo que respecta a infraestructura de red, como defensa principal, se espera un sistema de detección de intrusos que se adapte al panorama de amenazas que varía constantemente. Por eso, en las últimas tres décadas, las técnicas de aprendizaje automático se aplicaron como un enfoque convencional para desarrollar modelos de detección de anomalías de red. (Naseer et al., 2018)

Las técnicas tradicionales para construir sistemas de detección de ataques, como la técnica basada en firmas, no permiten detectar ataques en el día cero.

Para mejorar el rendimiento de la detección de ataques, se recurre al uso de métodos de aprendizaje automático, en particular, redes neuronales. (Sokolov et al., 2019). En los sistemas de control industrial, los enfoques basados en machine learning para la detección de ciberataques, son una alternativa a la técnica de firma clásico que impiden la detección de nuevos ataques. Con los resultados obtenidos utilizando redes neuronales profundas, muchos investigadores han propuesto el uso de las redes neuronales para detectar intrusiones en los sistemas de control industrial. (Sokolov et al., 2019).

Por otro lado, el cibercrimen ha aumentado en los últimos años y cada día surgen nuevas formas de robar, modificar y destruir información o desactivar los sistemas de información. Una forma de acceso a los sistemas de información en la que se procesa información confidencial es el malware ya que el objetivo principal de este moderno campo de investigación en seguridad de la información es crear métodos y algoritmos de seguridad que puedan detectar y neutralizar el malware desconocido.

El tamaño de las listas grises aumenta, constantemente, con el avance de las técnicas de escritura y producción de malware. Se necesita con urgencia nuevos métodos inteligentes para la detección automática de malware. (Damaševičius et al., 2021).

Asimismo, con la expansión de la información general en la nube, también se ha migrado información delicada en la nube, motivando mayor seguridad en Clod Computing contra amenazas de integridad disponibilidad y confidencialidad. Por esto, machine learning es tan importante en la nube que cada nube utilizará machine learning en un futuro próximo. (Butt et al., 2020)

En la industria de la Salud, con la introducción del servicio de telesalud que utiliza las tecnologías de telecomunicaciones y dispositivos de Internet de las cosas (IoT) para poder brindar servicios médicos en línea, es en estos sistemas, donde se recopilan los datos del paciente y se envían a los profesionales de la salud para comprender el estado del paciente en cualquier momento y en cualquier lugar.

En el año 2019, solo el 1% de los pacientes utilizaban los servicios de telesalud; mientras que en el año 2020, con la pandemia originada por el COVID-19, más del 38% de los especialistas en salud hizo consultas a los pacientes a través de sistemas de tele salud. En un entorno médico, descuidar la seguridad y la privacidad de los datos puede ser fatal, por lo que las capacidades del ML en biometría se pueden usar para mejorar la seguridad de la telemedicina, ya que el aprendizaje automático facilita la autenticación continua y sensible al contexto (Hazratifard et al., 2022).

Si hablamos de la nube, no debemos olvidar el campo de IoT, donde los entornos inteligentes se han vuelto vulnerables a una serie de amenazas de seguridad en varias capas de la arquitectura de IoT.

Entre las técnicas de machine learning aplicadas para solucionar los problemas de seguridad de IoT tenemos: algoritmos de aprendizaje supervisado y no supervisado para detectar la presencia de una botnet, brindar seguridad en WSN y detectar numerosos ataques en redes Wi-Fi. (Ikrissi & Mazri, 2021). Debido a la transformación digital y el Internet de las cosas (IoT), el mundo electrónico, actualmente, tiene una gran cantidad de datos que necesitan estar protegidos. La mitigación eficaz de las anomalías y ataques cibernéticos se está convirtiendo en una preocupación creciente en la industria actual de la seguridad cibernética en todo el mundo. A medida que proliferan múltiples tipos de ciberataques y amenazas, las soluciones de seguridad tradicionales son insuficientes para abordar los desafíos de seguridad actuales.

El uso de la inteligencia artificial, especialmente del aprendizaje automático (ML), es esencial para proporcionar un sistema de seguridad dinámicamente mejorado, automatizado y actualizado a través del análisis de datos de seguridad. (Iqbal H. Sarker, 2022).

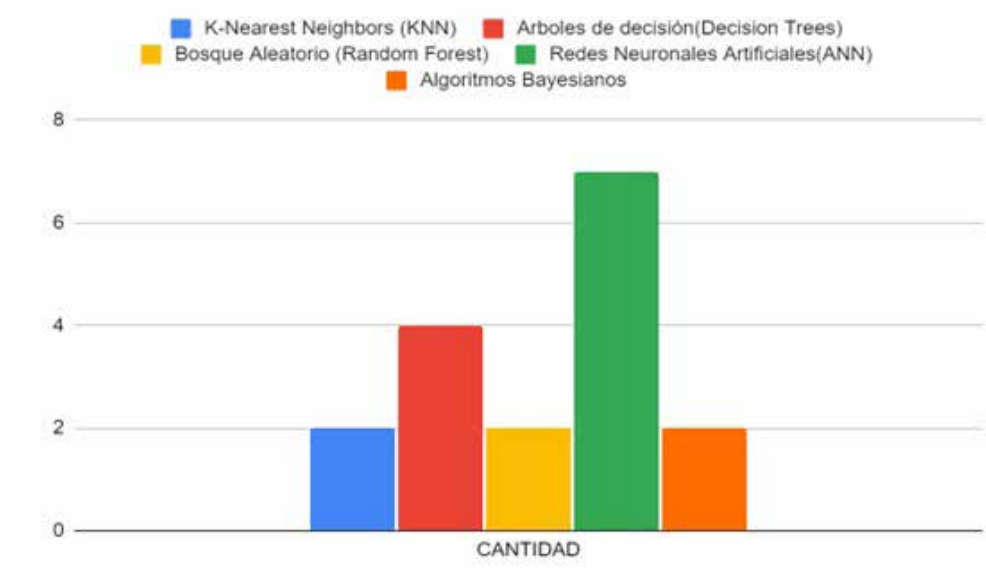
Las instituciones financieras están interesadas en el desarrollo e implementación de nuevos sistemas efectivos de monitoreo de fraude que minimicen el riesgo de aprobar transacciones ilegales. Actualmente, para detectar transacciones ilegales, los sistemas antifraude existentes utilizan información de pago, datos de tarjetas bancarias, involucrados en la transacción, información sobre el dispositivo desde el cual se realizó el pago, información sobre la ubicación del remitente en el momento de la transferencia, etc. Debido a esto se ha desarrollado un algoritmo para detectar transacciones fraudulentas que permite detectar transferencias internacionales de dinero atípicas en tiempo real. De esta manera se está reduciendo, así el volumen total de pérdidas por transacciones ilegales y minimizando el daño a la reputación causado a la organización (Domashova & Kripak, 2021).

Según (Naseer et al., 2018) ,la aplicación de redes neuronales profundas para la solución de problemas de seguridad de la información es un área de investigación relativamente nueva.

De las investigaciones revisadas se identificaron los siguientes algoritmos y/o técnicas del machine learning usados para la seguridad de la información; árboles de decisión (Decision Trees), algoritmos bayesianos, redes neuronales artificiales (ANN), bosque aleatorio (random forest) y K-Nearest neighbors (KNN). Es posible apreciar que el algoritmo más usado del machine learning en la seguridad de la información es el de las Redes Neuronales Artificiales (ANN). Esto debido a que tienen una gran de capacidad para aprender tareas basadas en un entrenamiento, lo cual se puede evidenciar en la Figura 6.

Figura 6

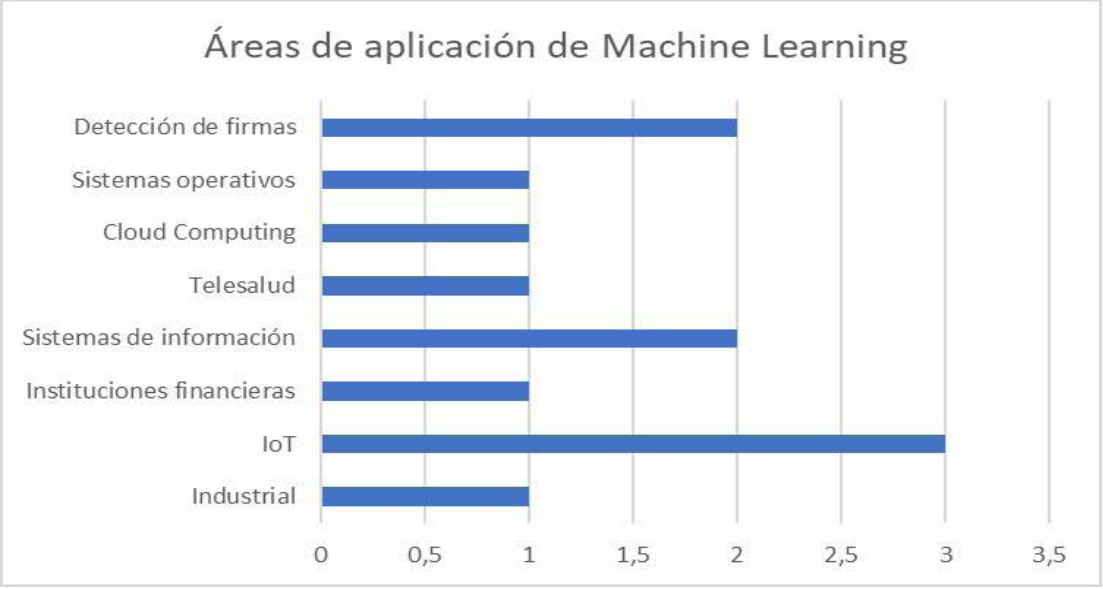
Algoritmos más usados del machine learning en la seguridad de la información



Asimismo, en las investigaciones revisadas se identificaron las siguientes áreas de la seguridad de la información donde se implementa el machine learning: detección de firmas, sistemas operativos, cloud computing, tele salud, sistemas de información, instituciones financieras, IoT y en sistemas de tipo industrial; siendo el área de IoT donde mayormente se implementa el machine learning en cuestión de seguridad de la información. Lo cual se puede evidenciar en la Figura 7.

Figura 7

Áreas donde se implementa el machine learning para la seguridad de la información



Discusión

De esta revisión vemos como las revistas académicas nos brindan una visión general de cómo se están implementando las diferentes técnicas y/o algoritmos del machine learning para mejorar la seguridad de la información en el nuevo contexto actual que ha cambiado con el avance acelerado de la transformación digital debido a la pandemia de Covid-19.

Después de analizar los resultados podemos decir que la aplicación del machine learning para soluciones de seguridad de la información es un campo de aplicación relativamente nuevo y que está siendo altamente demandado por el creciente desarrollo de nuevas amenazas que afectan la vulnerabilidad de los sistemas.

Bahassi et al., 2022 nos dice que los ataques cibernéticos son cada vez más diversos y sofisticados. Además, tienen un gran impacto en las personas y sus organizaciones y con el uso generalizado del aprendizaje automático (ML) en varias áreas se puede agregar valor a la ciberseguridad. Teniendo en cuenta los sistemas industriales coincidimos con el autor (Raviteja et al., 2020) el cual concluye que la seguridad de los sistemas de información será un desafío para la industria con acceso abierto a los sistemas. (Naseer et al., 2018) para la detección de intrusos se implementó

los modelos basados en redes neuronales DCNN y LSTM los cuales lograron mostrar un rendimiento excepcional en detección de intrusos con una precisión del 85% y 89% respectivamente en el conjunto de datos de prueba, lo que demuestra que el machine learning no solo es una tecnología viable sino más bien prometedora para aplicaciones de seguridad de la información.

Damaševičius et al., 2021 indican que hay un aumento en la demanda de métodos inteligentes que detectan nuevas variantes de malware, porque los métodos existentes consumen mucho tiempo y son vulnerables a muchos errores. La presente investigación identificó cómo se está implementando, en diferentes áreas, las técnicas y/o algoritmos de machine en la seguridad de la información partiendo de la revisión de publicaciones académicas en las bases de Datos como Scopus, Science Direct, Research Gate y Google Académico de los últimos cinco años, en donde se observa que la técnica más usada del machine learning son las redes neuronales artificiales (ANN), lo cual se puede evidenciar en la Figura 6.

Conclusión

La presente revisión sistémica ayudó a conocer cómo se encuentra la implementación del machine learning en las distintas áreas y actividades de la seguridad de la información; así como, también las técnicas y/o algoritmos usados en la seguridad de la información. El área de IoT es donde mayormente se implementa el machine learning para la seguridad de la información, y el algoritmo y/o técnica más usada, las redes neuronales artificiales (ANN), datos obtenidos de las publicaciones revisadas.

De nuestra revisión de publicaciones en las bases de datos como Scopus, Science Direct, ResearchGate y Google Académico en los últimos cinco años, el país con mayor número de investigaciones sobre el uso de machine learning en la seguridad de la información es Rusia.

En cuanto a las limitaciones, la presente investigación no pudo recabar más información de artículos porque estos no eran de acceso gratuito; es decir, la presente investigación puede ser ampliada teniendo en cuenta los artículos de paga. Por otra parte, los resultados obtenidos de esta revisión sistemática, sirven de referencia sobre el desarrollo del machine learning en la seguridad de la información y como se están aplicando a distintas áreas. De la misma manera, los resultados pueden ser utilizados como referencia al momento de seleccionar un algoritmo y/o técnica del machine learning para su implementación en la seguridad de la información en cierta área de interés del experto u organización. Asimismo, se espera continuar ampliando la información en investigaciones futuras, dado que el campo del machine learning se desarrolla y avanza cada vez más y aún queda mucho por conocer sobre este tema.

Referencias

ADETUNMBI A. O., ALESE B. K., & OLASEHINDE Olayemi O. (2018). *A Machine Learning Approach for Information System Security*. https://sites.google.com/site/ijcsis/

Applebaum, S., Gaber, T., & Ahmed, A. (2021). Signature-based and Machine-Learning-based Web Application Firewalls: A Short Survey. *Procedia Computer Science*, *189*, 359–367. https://doi.org/10.1016/J.PROCS.2021.05.105

Bahassi, H., Edddermoug, N., Mansour, A., & Mohamed, A. (2022). Toward an exhaustive review on Machine Learning for Cybersecurity. *Procedia Computer Science*, *203*, 583–587. https://doi.org/10.1016/J.PROCS.2022.07.083

Blanco Gómez, D., Rubio, E. M., Marin, M. M., & de Agustina, B. (2020). *Propuesta metodológica para revisión sistemática en el ámbito de la ingeniería basada en PRISMA Additive Manufacturing: Technologies and Optimization View project Design and experimental validation of smooth pocketing toolpaths View project*. 1–12. https://www.researchgate.net/publication/348705198

Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Waqas Shaukat, M., Raza, S. M., Suh, D. Y., & Piran, M. J. (2020). A Review of Machine Learning Algorithms for Cloud Computing Security. Electronics, 9(9), 1379. https://doi.org/10.3390/ELECTRONICS9091379

Damaševičius, R., Venčkauskas, A., Toldinas, J. & Grigaliūnas, Š. (2021). Ensemble-Based Classification Using Neural Networks and Machine Learning Models for Windows PE Malware Detection. *Electronics,* 10(4), 485. https://doi.org/10.3390/ELECTRONICS10040485

Domashova, J., & Kripak, E. (2021). Identification of non-typical international transactions on bank cards of individuals using machine learning methods. *Procedia Computer Science*, *190*, 178–183. https://doi.org/10.1016/J.PROCS.2021.06.023

Hazratifard, M., Gebali, F., & Mamun, M. (2022). Using Machine Learning for Dynamic Authentication in Telehealth: A Tutorial. *Sensors*, *22*(19), 7655. https://doi.org/10.3390/S22197655

Ikrissi, G., & Mazri, T. (2021). IOT-BASED SMART ENVIRONMENTS: STATE of the ART, SECURITY THREATS and SOLUTIONS. *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives*, *46*(4/W5-2021), 279–286. https://doi.org/10.5194/ISPRS-ARCHIVES-XLVI-4-W5-2021-279-2021

Iqbal H. Sarker. (2022). *Machine*

Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. https://www.researchgate.net/publication/363274652_Machine_Learning_for_Intelligent_Data_Analysis_and_Automation_in_Cybersecurity_Current_and_Future_Prospects

Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K. (2018). Enhanced network anomaly detection based on deep neural networks. *IEEE Access*, *6*, 48231–48246. https://doi.org/10.1109/ACCESS.2018.2863036

Quispe, A. M., Hinojosa-Ticona, Y., Miranda, H. A., & Sedano, C. A. (2021). Serie de Redacción Científica: Revisiones Sistemáticas Scientific Writing Series: Systematic Review. *Revista Del Cuerpo Médico Del HNAAA*, *14*(1), 1–6. https://doi.org/10.35434/rcmhnaaa.2021.141.906

Raviteja, P., Satya Venkata, M., Devi, S., Gowri, M., Vamsi, M., Jayalakshmi, S., Dolai, N., Lokeshwar, K., Sravan, K., San…, K., Krishna, S., & Prabhakar, V. S. (2020). Implementation Of Machine Learning Algorithms For Detection Of Network Intrusion. *International Journal of Computer Science Trends and Technology (IJCST)*, *8*. www.ijcstjournal.org

Shrivastava, V., & Kumar, S. (2019). Utilizing Block Chain Technology in Various Application Areas of Machine Learning. *Proceedings of the International Conference on Machine Learning, Big Data, Cloud and Parallel Computing: Trends, Prespectives and Prospects, COMITCon 2019*, 167–171. https://doi.org/10.1109/COMITCON.2019.8862203

Sokolov, A. N., Ragozin, A. N., Pyatnitsky, I. A., & Alabugin, S. K. (2019). Applying of digital signal processing techniques to improve the performance of machine learning-based cyber-attack detection in industrial control system. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3357613.3357637

Thorat, O., Parekh, N., & Mangrulkar, R. (2021). TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification. *International Journal of Information Management Data Insights*, *1*(2), 100048. https://doi.org/10.1016/J.JJIMEI.2021.100048

Tolubko, V., Vyshnivskyi, V., Mukhin, V., Haidur, H., Dovzhenko, N., Ilin, O., & Vasylenko, V. (2018). Method for Determination of Cyber Threats Based on Machine Learning for Real-Time Information System. *Intelligent Systems and Applications*, *8*, 11–18. https://doi.org/10.5815/ijisa.2018.08.02

Vega Briceño, E. (2021). *Seguridad de la información.* Editorial Área de Innovación y Desarrollo, S.L. https://doi.org/https://doi.org/10.17993/tics.2021.4

Zapechnikov, S. (2020). Privacy-Preserving Machine Learning as a Tool for Secure Personalized Information Services. *Procedia Computer Science*, *169*, 393–399. https://doi.org/10.1016/J.PROCS.2020.02.235

Zhang, J., Nazir, S., Huang, A., & Alharbi, A. (2020). Multicriteria Decision and Machine Learning Algorithms for Component Security Evaluation: Library-Based Overview. *Security and Communication Networks*, *2020*. https://doi.org/10.1155/2020/8886877