ISBN: 978-628-96613-1-6. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2025.1.1.475

APPLICATION OF MACHINE LEARNING TECHNIQUES FOR RISK MANAGEMENT AGAINST MALWARE ATTACKS IN THE BUSINESS SECTOR

Huancahuari Curitomay Rony[1]; Castilla Rojas, Wladimir José[2]; Navas Gotopo Soratna Veronica[3] Luis Enrique Ramírez Calderon[4]

[1,2,3,4] Universidad Tecnológica del Perú, Lima, Perú.
U20307755@utp.edu.pe , 1530964@utp.edu.pe , C19491@utp.edu.pe, C19975@utp.edu.pe,

Abstract: ***This study aims to analyze the use of machine learning for detecting and preventing malware attacks in key technological environments such as IoT, enterprise networks, and critical systems. A comprehensive review of deep learning techniques and models applied in cybersecurity is conducted, evaluating their effectiveness, accuracy, and the limitations they face against emerging threats. The review also aims to identify the most innovative solutions that integrate artificial intelligence to enhance cyber defenses. To carry out this RSL, a methodological approach was followed, which included collecting relevant articles from academic databases, applying inclusion and exclusion criteria to ensure the quality of the selected studies. Key data was extracted and analyzed from the reviewed works, organized by the machine learning techniques used and the specific areas of application. The results showed that deep learning techniques and hybrid models have significantly improved the detection and mitigation of advanced attacks, such as ransomware and APTs. However, important challenges in implementing these technologies were identified, especially in sectors with resource limitations andresistance to organizational change. In conclusion, the use of machlearning has proven to be highly effective in improving cybersecurity, although its widespread adoption still faces barriers such as the lack of trained personnel and adequate infrastructure. This study highlights the need for further research into integrating these technologies with emerging solutions and improving their adaptability across different organizational contexts.***

Keywords: ***Cybersecurity, Supervised learning, Neural networks, Automation, and Organizations.***

APLICACIÓN DE TÉCNICAS DE MACHINE LEARNING PARA LA GESTIÓN DE RIESGOS ANTE ATAQUES DE MALWARE EN EL SECTOR EMPRESARIAL

Ronny [1]; Josue Antonio Sánchez Mato[2]; Navas Gotopo Soratna Veronica[3] Luis Enrique Ramírez Calderon[4]

[1,2,3,4] Universidad Tecnológica del Perú, Lima, Perú.
U20307755@utp.edu.pe , 1530964@utp.edu.pe , C19491@utp.edu.pe, C19975@utp.edu.pe,

Resumen: ***Este estudio tiene como propósito exminar el uso de machine learning en la detección y prevención de ataques de malware en diversos entornos tecnológicos, como IoT, redes empresariales y sistemas críticos. Se lleva a cabo una revisión detallada de las técnicas y modelos de deep learning aplicados en el ámbito de la ciberseguridad, evaluando su efectividad, precisión y las limitaciones que enfrentan frente a amenazas emergentes. Además, se identifican las soluciones más innovadoras que integran inteligencia artificial para fortalecer las defensas cibernéticas. La metodología utilizada consistió en una revisión sistemática de artículos académicos seleccionados de bases de datos especializadas, aplicando criterios específicos para garantizar la calidad de los estudios incluidos. Se extrajeron y analizaron datos relevantes, organizándolos según las técnicas de machine learning utilizadas y las aplicaciones específicas en los diferentes sectores. Los resultados mostraron que las técnicas de deep learning y los modelos híbridos han mejorado significativamente la capacidad para detectar y mitigar ataques avanzados, como ransomware y APT. No obstante, también se identificaron desafíos importantes en la implementación de estas tecnologías, particularmente en industrias con limitaciones de recursos y resistencia al cambio organizacional. En conclusión, el uso de machine learning ha demostrado ser una herramienta eficaz para mejorar la ciberseguridad, aunque su adopción generalizada sigue enfrentando obstáculos relacionados con la falta de personal capacitado y la infraestructura adecuada. Este estudio destaca la necesidad de continuar investigando en la integración de estas tecnologías con soluciones emergentes y en su adaptación a distintos contextos organizacionales.***

Palabras claves: Ciberseguridad, Aprendizaje supervisado, Redes neuronales, Automatización y Organizaciones

I. INTRODUCCIÓN

Hoy en día, el sector empresarial se ha visto obligado a intervenir en nuevos métodos digitales, debido a toda esta situación cambiante de mayor involucración con la tecnología, La rápida proliferación de estos cambios ha presentado desafíos considerables para mantener la ciberseguridad. A medida que los ecosistemas de IoT se expanden, atraen cada vez más ataques como el malware [1]. La seguridad informática se ha vuelto fundamental para salvaguardar la información y los recursos digitales. La implementación de métodos de aprendizaje automático en la gestión de riesgos ante ataques de malware ha cobrado relevancia en los últimos años gracias a su habilidad para identificar patrones complejos y predecir comportamientos maliciosos en tiempo real [2]. Las soluciones tradicionales basadas en firmas de malware han demostrado ser insuficientes frente a la creciente sofisticación de los ataques, lo que ha resultado en una mayor adopción de enfoques basados en ML para mejorar la defensa cibernética en las organizaciones.

A medida que la tecnología se integra más en nuestras vidas, la protección de datos contra ataques se vuelve esencial. La ciberseguridad ha cobrado relevancia para individuos, empresas y gobiernos debido a la evolución constante del cibercrimen. Con el aumento de ciberataques, los expertos en seguridad enfrentan dificultades para reaccionar y predecir nuevas amenazas. Las soluciones tradicionales, como cortafuegos y software antivirus, son cada vez menos efectivas ante nuevas vulnerabilidades, lo que hace que el uso de técnicas de aprendizaje automático sea fundamental. En este contexto, se ha propuesto un protocolo de enrutamiento basado en confianza habilitado por ML (TrustML-RP) que identifica nodos atacantes en ataques DDoS y de supresión de paquetes, utilizando una combinación de algoritmos de aprendizaje automático para mejorar la seguridad de la red [3].

Aunque el Machine Learning ha avanzado considerablemente en la detección del programa maligno, aún hay varias áreas que carecen de una visión completa, lo que dificulta la evaluación efectiva de la gestión de riesgos. La dependencia de técnicas de reducción de dimensionalidad podría pasar por alto características importantes, afectando la capacidad de los modelos para manejar diferentes tipos de malware. Además, la evaluación se limita a un único conjunto de datos, lo que podría no reflejar adecuadamente la diversidad de malware en el mundo real [4], lo que impide una comprensión más amplia de cómo estas metodologías pueden implementarse en la administración de riesgos dentro del contexto empresarial.

El incremento que se ha observado tras esta migración digital sobre los niveles de ataque cibernéticos dirigidos al sector empresarial y la complejidad de los modelos de amenazas subraya una necesidad de indagar la creación de un sistema sólido de gestión de riesgos. Según SOPHOS citado en [5] En 2021 cerca de 37% de todas las organizaciones mundiales fueron afectados por ataques de ransomware, virus alineado al malware, que afectó en gran medida a los dispositivos de la red. Asimismo, indica que la demanda del pago tras el rescate de estos datos robados para el 2020 superaron más de 230 millones de dólares a nivel mundial. Tras esta situación surge la necesidad de consolidar el conocimiento ya existente con las nuevas técnicas a desarrollar sobre Machine Learning y proporcionar una guía eficiente para los medios de seguridad informática. Los resultados de esta revisión no solo ayudaran a entender las fortalezas y limitaciones que están presentes ahora, adicional, ofrecer una estructura sólida para futuras investigaciones y el poder desarrollar cada vez mejores soluciones efectivas para contrarrestar estas amenazas de ciberseguridad.

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

El objetivo de esta revisión sistemática de la literatura (RSL) es proporcionar un análisis detallado y actualizado sobre el uso de machine learning para la detección y prevención de ataques de malware, con un enfoque en áreas como IoT, redes empresariales y sistemas críticos. La revisión tiene como propósito identificar y evaluar las principales técnicas y modelos de deep learning aplicados en la ciberseguridad, destacando su efectividad y las limitaciones a las que se enfrentan al tratar con amenazas emergentes. Además, se pretende analizar las soluciones más innovadoras que integran inteligencia artificial en sistemas de defensa, y proporcionar una reflexión sobre su impacto en la seguridad digital. Este trabajo busca organizar y clasificar los estudios previos, proporcionando una base sólida para futuras investigaciones y desarrollos en el campo de la ciberseguridad.

El documento está estructurado de la siguiente manera: En primer lugar, la Sección 2: Metodología presenta el enfoque adoptado para realizar la revisión sistemática de la literatura (RSL). Aquí se describen las preguntas de investigación que guían el estudio, los criterios utilizados para seleccionar los artículos incluidos en la revisión y el proceso seguido para extraer y analizar los datos clave de los estudios revisados. En la Sección 3: Resultados, se presentan los hallazgos obtenidos a partir del análisis de los artículos seleccionados. Esta sección organiza los resultados según las técnicas de machine learning que se utilizan en los estudios, las áreas específicas de aplicación (como IoT, redes empresariales, etc.), y los principales resultados relacionados con la efectividad, precisión y las limitaciones de los enfoques utilizados. La Sección 4: Discusión se dedica a analizar de manera crítica los estudios revisados, abordando las tendencias actuales, las innovaciones tecnológicas que se han implementado y señalando las posibles discrepancias o vacíos en el conocimiento que aún existen. También se discuten las implicaciones prácticas de estos hallazgos para la implementación de machine learning en sistemas de ciberseguridad y se plantean posibles líneas de investigación futura. Finalmente, en la Sección 5: Conclusiones, se resumen los hallazgos más relevantes de la revisión, se discuten las limitaciones del estudio y se proponen áreas de investigación futura, destacando los aspectos más importantes que podrían contribuir al avance en la integración de machine learning para la protección contra el malware.

II METODOLOGÍA

Es importante señalar que, para llevar a cabo esta revisión sistemática de la literatura, se ha empleado una estrategia basada en el componente PIOC, lo que facilitó la estructuración y el enfoque de la investigación de manera eficaz. A continuación, se presenta la pregunta formulada con el modelo PIOC: **Población** (P): ¿Cómo afectan los ciberataques, específicamente el malware, a las empresas que implementan soluciones basadas en aprendizaje automático? **Intervención**(I): ¿Qué tan efectivas son las técnicas de aprendizaje automático en la detección y prevención de ataques de malware en el entorno empresarial? **Resultados** (O): ¿Qué tan efectivas son las técnicas de aprendizaje automático en la reducción del riesgo asociado a ataques de malware en el sector empresarial? **Contexto** (C): ¿Cómo influyen los ataques de malware en las estrategias de seguridad de las empresas que adoptan técnicas de aprendizaje automático para la protección de sus sistemas?

TABLA I.
Modelo PIOC

Población	Empresas tecnológicamente avanzadas, Ciberseguridad empresarial	"Ciberseguridad" "aprendizaje automático" "detección de malware"	"cybersecurity" "Machine learning" "malware detection"
Intervención	Técnicas de aprendizaje automático, Detección de malware	"Aprendizaje supervisado" "redes neuronales" "aprendizaje no supervisado"	"Supervised learning" "Neural networks" "Unsupervised learning"
Resultados	Eficacia en reducción de ataques de malware	"Automatización" "defensa" "prevención"	"automation" "defense" "prevention"
Contexto	Organizaciones empresariales	"Organizaciones" "negocios" "empresas"	"organizations" "businesses" "companies"

En relación con los términos empleados para la búsqueda relevante de la literatura se utilizó la siguiente ecuación:(TITLE-ABS-KEY (“cybersecurity" OR "machine learning" OR "malware detection”) AND TITLE-ABS-KEY ("Supervised learning" OR "Neural networks" OR " unsupervised learning") AND TITLE-ABS-KEY ("automation" OR "defense" OR "prevention") AND TITLE-ABS-KEY ("organizations" OR "businesses" OR "companies"))

La búsqueda se realizó en la base de datos Scopus utilizando la ecuación mencionada anteriormente. Se llevó a cabo un filtrado inicial que consistió en seleccionar fuentes a partir de los títulos y resúmenes de los artículos, descartando aquellos que no cumplían con los criterios de inclusión. Los estudios que superaron este filtro fueron revisados en su totalidad para verificar su relevancia y adecuación a los objetivos de la revisión. Posteriormente, se extrajeron datos clave de los artículos seleccionados, incluyendo información sobre la población estudiada, las técnicas de Machine Learning empleadas, los beneficios observados y los factores contextuales que influyeron en los resultados. Esta información fue analizada en profundidad, lo que permitió identificar patrones, temas recurrentes y hallazgos clave relacionados con la efectividad de las técnicas de Machine Learning en la gestión de riesgos cibernéticos. Finalmente, se sintetizaron y organizaron los hallazgos para ofrecer una visión crítica sobre el estado actual del conocimiento en este ámbito y señalar las áreas que requieren mayor atención investigativa.

Criterios de Inclusión y Exclusión

Para garantizar que los estudios seleccionados sean relevantes y de alta calidad, se establecieron los siguientes criterios de inclusión y exclusión:

1. Población (P): Criterios de Inclusión: Estudios que se centren en empresas o sectores empresariales que han sido afectados por ataques de malware o han implementado soluciones de ciberseguridad; asimismo, artículos que evalúen riesgos de malware en sistemas empresariales (corporaciones, grandes empresas, pymes, etc.). Criterios de Exclusión: Estudios que se centren en otros sectores no relacionados con el entorno empresarial (gobiernos, usuarios domésticos, ONGs no comerciales, etc.).

2. Intervención (I): Criterios de Inclusión: Artículos que apliquen técnicas de machine learning (aprendizaje automático) para la detección, prevención o mitigación de ataques de malware en el ámbito empresarial. Criterios de Exclusión: Trabajos que utilicen únicamente métodos tradicionales de ciberseguridad (como sistemas basados en firmas o heurísticos) sin integración de machine learning;

también, estudios donde la intervención no esté directamente relacionada con la aplicación de machine learning.

3. Resultados (O): Criterios de Inclusión: Artículos que evalúen o midan la efectividad de las técnicas de machine learning para mitigar riesgos y reducir ataques de malware en las empresas; del mismo modo, estudios que reporten métricas claras como reducción en la cantidad de ataques, mejoras en la seguridad o mitigación de riesgos. Criterios de Exclusión: Estudios donde los resultados no estén relacionados con la ciberseguridad empresarial o la protección contra malware.

4. Contexto (C): Criterios de Inclusión: Estudios cuyo contexto sean ataques de malware en sistemas empresariales o corporativos y su relación con la adopción de machine learning para la ciberseguridad. Criterios de Exclusión: Estudios que se centren en sistemas no empresariales o en usuarios individuales sin un enfoque en las empresas.

5. Año: Criterios de Inclusión: Artículos publicados de los últimos 5 años (2020-2024). Criterios de Exclusión: Artículos publicados antes del 2020.

Para asegurar la transparencia y rigor en la selección de los estudios incluidos en esta revisión sistemática de la literatura, se utilizó la metodología PRISMA. Este enfoque facilitó la documentación detallada del proceso de identificación, cribado, elegibilidad e inclusión de los artículos revisados. A continuación, se presentan las diferentes etapas del proceso de selección de estudios:

Para garantizar la transparencia y rigurosidad en la selección de los estudios incluidos en esta revisión sistemática de la literatura, se siguió la metodología PRISMA. Este diagrama permitió documentar de manera detallada el proceso de identificación, cribado, la elegibilidad e inclusión de los artículos revisados. A continuación, se ilustran las diferentes etapas del proceso de selección de estudios:

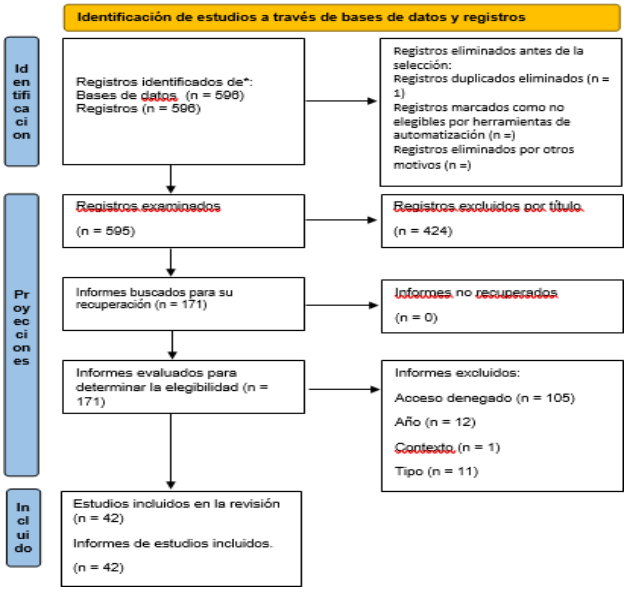

Fig.1 Diagrama de flujo PRISMA

Es importante señalar que la recopilación de información se realizó en la base de datos Scopus, utilizando la ecuación de búsqueda mencionada anteriormente. Se llevó a cabo un primer filtrado inicial, que consistió en seleccionar fuentes basadas en los títulos y resúmenes de los artículos, descartando aquellos que claramente no cumplían con los criterios de inclusión. Después, los estudios que pasaron este primer filtro fueron revisados en su totalidad para verificar su relevancia y adecuación a los objetivos de la revisión. Posteriormente, se extrajeron datos clave de los artículos seleccionados, incluyendo información sobre la población estudiada, las técnicas de gamificación utilizadas, los beneficios observados y los factores contextuales que influyeron en los resultados.

Esta información fue analizada de manera exhaustiva, lo que permitió identificar patrones, temas recurrentes y hallazgos clave relacionados con el impacto de la gamificación en la mejora de los procesos de innovación empresarial. Los hallazgos obtenidos fueron sintetizados y organizados para ofrecer una perspectiva reflexiva y crítica sobre el estado actual del conocimiento en este ámbito, así como para señalar las áreas que requieren una mayor atención investigativa.

III RESULTADOS

En esta sección se presentan los resultados de la revisión de estudios recientes, los cuales se guiaron por las preguntas PIOC. Para llevar a cabo el proceso de selección, se siguieron las directrices de la declaración PRISMA. Como resultado, se seleccionaron 42 artículos de la base de datos Scopus, los cuales ayudaron a aumentar la efectividad y viabilidad del estudio mediante la aplicación de diversos enfoques y métodos estadísticos.

Cabe destacar que en la revisión sistemática de la literatura se recopilaron datos de un total de 47 artículos, lo que facilita una comprensión integral del impacto de la gamificación en los procesos de formación e innovación empresarial. Es importante señalar que estos artículos seleccionados ofrecen estudios empíricos y análisis teóricos que demuestran cómo se han implementado diversas técnicas de gamificación en contextos organizacionales, proporcionando una base sólida de datos y experiencias prácticas. Este enfoque variado en la selección de fuentes permitió una exploración exhaustiva y contextualizada del tema, garantizando que los hallazgos sean tanto relevantes como aplicables.

Fig. 2: Publicaciones por año

En la figura 2, se ilustra la cantidad de publicaciones por año, las cuales revelan información de los años 2020, 2021, 2022, 2023 y 2024, también mostramos el número significativo de investigaciones, aunque en menor medida, este patrón sugiere un incremento en la tendencia tras el interés por el tema, lo cual es positivo para el desarrollo de futuras investigaciones en este campo. La variabilidad en las cifras de publicaciones entre estos años, reflejan cambios en las

prioridades de investigación, la evolución de las metodologías utilizadas, o el impacto de la pandemia en la producción académica. En relación con la pregunta PIOC, se desarrollaron sub-preguntas que facilitaron la recopilación de información a partir de los artículos de investigación. Cabe mencionar que las mismas permitieron afinar y construir los ítems del estudio de manera precisa y eficiente. A continuación, se presenta la Tabla de extracción de información

TABLA II.
SUBPREGUNTAS PARA FORMULARIOS DE EXTRACCIÓN DE INFORMACIÓN

SUBPREGUNTAS	ITEMS DE EXTRACCIÓN
RQ1: ¿Cómo afectan los ciberataques, específicamente el malware, a las empresas que implementan soluciones basadas en aprendizaje automático?	¿Cómo mejora el machine learning la detección de malware en comparación con métodos tradicionales?
	¿Cómo afectan los ataques de malware a la infraestructura tecnológica de empresas que usan machine learning?
	¿Cómo varían los daños financieros y operativos en empresas con machine learning frente a las que no lo usan?
RQ2: ¿Qué tan efectivas son las técnicas de aprendizaje automático en la detección y prevención de ataques de malware en el entorno empresarial?	¿Qué precisión tienen las técnicas de machine learning en la detección de malware?
	¿Cómo previene el machine learning los ataques de malware en empresas?
	¿Cuáles son las técnicas de machine learning más efectivas para la prevención de malware?
RQ3: ¿Qué tan efectivas son las técnicas de aprendizaje automático en la reducción del riesgo asociado a ataques de malware en el sector empresarial?	¿Cómo reduce el machine learning el riesgo de malware en empresas?
	¿Qué impacto tiene el machine learning en la mitigación de riesgos de malware?
	¿Cómo mejora el machine learning la seguridad empresarial frente a malware?
RQ4: ¿Cómo influyen los ataques de malware en las estrategias de seguridad de las empresas que adoptan técnicas de aprendizaje automático para la protección de sus sistemas?	¿Cómo afectan los ataques de malware a las empresas que usan machine learning?
	¿Cómo ajustan las empresas sus estrategias de seguridad ante el malware usando machine learning?
	¿De qué forma influye el malware en la adopción de machine learning para la protección empresarial?

En el contexto de esta revisión sistemática de literatura, se abordaron las preguntas surgidas a partir de la formulación PIOC. A continuación, se detallan las respuestas donde se presenta un análisis exhaustivo de cada aspecto relevante, mediante tablas que enuncian las categorías y su respectiva descripción.

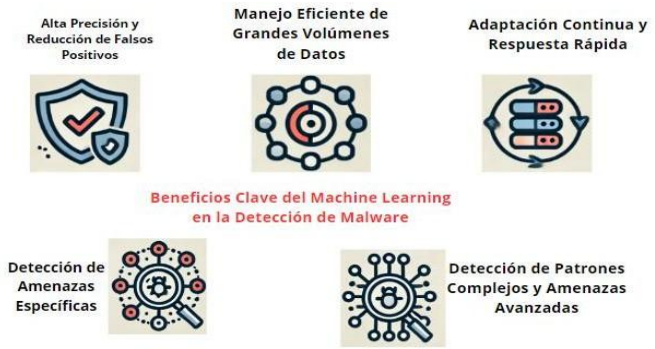

Fig. 3: Beneficios del aprendizaje automático en la detección de malware

¿Cómo afectan los ciberataques, específicamente el malware, a las empresas que implementan soluciones basadas en aprendizaje automático?

Machine learning mejora la detección de malware frente a métodos tradicionales mediante mayor precisión y reducción de falsos positivos [4], [2], [14], [36], permitiendo adaptación continua y respuesta rápida [4], [18], [27], [29] a nuevas amenazas. Su capacidad para manejar grandes volúmenes de datos [1], [9], [16], [36], [40] lo hace ideal para redes IoT, donde se especializa en identificar amenazas como phishing y DDoS [19], [20], [27], [28], [30], [39].

En la infraestructura tecnológica, machine learning reduce el impacto en dispositivos IoT y redes críticas [1], [6], [18], [26], ofreciendo protección y mitigación en la nube [8], [17], [20], [21], [27] contra ataques como ransomware. Facilita la contención rápida de ataques de ingeniería social [7], [15], [19], [25], [30] y mejora la resiliencia frente a DDoS y APTs [3], [8], [14], [32].

Para las empresas, el uso de machine learning implica reducción de interrupciones operativas [1], [4], [32], [12], [5] y menores costos de recuperación [3], [4], [5], [17], [20] al responder rápidamente a ataques. Esto también disminuye pérdidas financieras [3], [19], [5], [14], [27] y protege la reputación de la marca [3], [4], [8], [10], [12], [27], optimizando así costos operativos [3], [4], [18], [27], [32] al reducir la frecuencia y gravedad de los ataques

Fig. 4: Impacto del Machine Learning en la Seguridad Empresarial

¿Qué tan efectivas son las técnicas de aprendizaje automático en la detección y prevención de ataques de malware en el entorno empresarial?

El machine learning mejora la detección de malware con alta precisión al identificar patrones complejos mediante redes neuronales y transformadores [1],[2],[4],[5],[11],[19],[27],[30]. Técnicas como deep learning y aprendizaje semi-supervisado logran más del 90% de

precisión, y modelos especializados en phishing, DDoS y ransomware optimizan la detección [1],[2],[4],[5],[27],[30]. La selección de características puede aumentar la precisión hasta un 98%, y en entornos IoT e industriales se alcanzan más del 95% [4],[11],[27],[30].

Además, machine learning permite la detección proactiva de amenazas en tiempo real, bloqueando ataques antes de causar daños [1],[4],[5],[11],[27]. Monitorea redes y dispositivos IoT, filtra correos maliciosos y mitiga intrusiones en aplicaciones [1],[6],[8],[18],[20],[19],[30],[39],[4],[5],[11],[12],[29],[32].

También protege contra ataques avanzados y APTs [1],[3],[4],[14],[32]. Las técnicas más efectivas incluyen redes neuronales profundas y convolucionales (CNN y DNN), que detectan patrones en tráfico de red [1],[4],[6],[8],[18],[27],[30],[32]. Los enfoques híbridos mejoran la detección de ataques complejos [2],[3],[4],[8],[10],[27],[29],[30],[32],[46], y el aprendizaje federado permite colaboración segura en sistemas de recomendación [10],[12],[19],[20].

TABLA III

¿QUÉ TAN EFECTIVAS SON LAS TÉCNICAS DE APRENDIZAJE AUTOMÁTICO EN LA REDUCCIÓN DEL RIESGO ASOCIADO A ATAQUES DE MALWARE EN EL SECTOR EMPRESARIAL?

SUBPREGUNTA	CATEGORÍA EMERGENTE	DESCRIPCIÓN DE LA CATEGORÍA
¿Cómo reduce el machine learning el riesgo de malware en empresas?	Detección temprana y respuesta proactiva [1], [2], [4], [6], [7], [18], [24], [27]	Machine learning identifica y mitiga amenazas en tiempo real, reduciendo el riesgo de infiltración en la infraestructura empresarial.
	Prevención de intrusiones en redes IoT y tráfico de red: [1],[6],[8],[9],[16] ,[18],[26],[33]	Monitoreando el tráfico de red y dispositivos IoT, machine learning detecta patrones maliciosos y minimiza la exposición al malware.
	Protección contra phishing y enlaces sospechosos [7],[15],[19],[30] ,[39]	Bloquea correos y URLs sospechosas antes de que los empleados interactúen, previniendo la entrada de malware por phishing.
	Bloqueo de ataques avanzados y rutas de ataque [1], [4], [3], [20], [23], [26], [31], [32], [37], [43]	Identifica y neutraliza rutas de ataque complejas, como inyecciones SQL y XSS, antes de comprometer datos críticos.
	Reducción de falsos positivos y carga de seguridad [2], [4], [7], [11], [16], [22], [24], [30], [35], [42], [47]	Al mejorar la precisión de detección y reducir falsos positivos, aligerar la carga sobre equipos de seguridad, permitiendo respuestas más rápidas.
¿Qué impacto tiene el machine learning en la mitigación de riesgos de malware?	Detección temprana y bloqueo preventivo de amenazas [1], [2], [4], [5], [6], [7], [11], [12], [18], [19], [22]	Detecta y neutraliza ataques como phishing y ransomware antes de afectar la red.
	Mejora en la respuesta y reducción de tiempos de inactividad [1], [4], [18], [27], [26], [32]	Reacciones rápidas ante incidentes, reduciendo inactividad y pérdidas financieras.
	Protección proactiva en redes IoT y SDN [1],[6],[9],[17] ,[20],[26]	Modelos de aprendizaje supervisado mejoran la seguridad en redes IoT y SDN.
	Adaptabilidad y manejo de grandes volúmenes de datos [1], [4], [9], [10], [11], [13], [14], [18], [22], [24], [26], [27], [29]	Defensas adaptables que analizan grandes cantidades de datos en tiempo real.
	Capacitación y análisis de riesgos para el personal [15], [19], [25], [30], [44]	Sistemas predictivos reducen riesgos mediante análisis proactivo y formación sobre amenazas.
¿Cómo mejora el machine learning la seguridad empresarial frente a malware?	Detección temprana y respuesta proactiva [1],[2],[3],[4],[5]} ,[6],[8],[14],[25]	Inteligencia artificial identifica amenazas actuando antes de que causen daños.
	Automatización de la seguridad en tiempo real [1],[2],[3],[4],[6] ,[14],[27],[30],[32]	La automatización de detección y respuesta a incidentes mejora la gestión de seguridad en redes IoT y SDN.
	Protección contra ataques de ingeniería social y phishing [19],[30],[25] ,[7],[14],[28]	Soluciones de aprendizaje profundo bloquean URLs y correos sospechosos.
	Defensa avanzada en redes y bases de datos [3],[4],[12],[14] ,[27],[32]	Modelos de machine learning optimizan la seguridad en redes y bases de datos, identificando patrones de inyección SQL y actividades anómalas.
	Fortalecimiento de infraestructuras críticas y resiliencia	La adaptación a amenazas emergentes y el mapeo de rutas de ataque complejas aseguran la integridad de sistemas empresariales clave.

El machine learning es fundamental para reducir el riesgo de malware en las empresas, al permitir detección temprana y respuesta proactiva, lo que minimiza la infiltración en la infraestructura

[1],[2],[4],[6],[7],[18],[24],[27]. Facilita la prevención de intrusiones en redes IoT al monitorear el tráfico y detectar patrones maliciosos [1],[6],[8],[9],[16],[18],[26],[33], y bloquea correos y URLs sospechosas, protegiendo contra phishing [7],[15],[19],[30],[39]. Además, neutraliza rutas de ataque complejas como inyecciones SQL antes de comprometer datos críticos [1],[4],[3],[20],[23],[26],[31],[32],[37],[43], aliviando la carga sobre equipos de seguridad al mejorar la precisión de detección y reducir falsos positivos [2],[4],[7],[11],[16],[22],[24],[30],[35],[42],[47].

En la mitigación de riesgos, el machine learning permite la detección y bloqueo preventivo de amenazas, neutralizando ataques antes de afectar la red [1],[2],[4],[5],[6],[7],[11],[12],[18],[19],[22]. Mejora la respuesta ante incidentes, reduciendo tiempos de inactividad y pérdidas financieras [1],[4],[18],[27],[26],[32]. También fortalece la seguridad en redes IoT mediante modelos de aprendizaje supervisado [1],[6],[9],[17],[20],[26], y ofrece defensas adaptables al manejar grandes volúmenes de datos en tiempo real [1],[4],[9],[10],[11],[13],[14],[18],[22],[24],[26],[27],[29]. La capacitación del personal en análisis proactivo de amenazas mejora la preparación general [15],[19],[25],[30],[44].

TABLA IV

¿CÓMO INFLUYEN LOS ATAQUES DE MALWARE EN LAS ESTRATEGIAS DE SEGURIDAD DE LAS EMPRESAS QUE ADOPTAN TÉCNICAS DE APRENDIZAJE AUTOMÁTICO PARA LA PROTECCIÓN DE SUS SISTEMAS?

SUBPREGUNTA	CATEGORÍA EMERGENTE	DESCRIPCIÓN DE LA CATEGORÍA
¿Cómo afectan los ataques de malware a las empresas que usan machine learning?	Reducción de daños y tiempo de recuperación [1],[2],[4],[12], [14],[27]	La detección temprana ayuda a las empresas a mitigar ataques DDoS y phishing, acelerando recuperaciones.
	Disminución de la frecuencia de ataques exitosos [2],[4],[5],[10] ,[19],[27],[32]	Los sistemas inteligentes detectan proactivamente amenazas, minimizando daños de malware y ransomware.
	Mitigación de vulnerabilidades en redes y bases de datos [1],[4],[5],[8], [14],[29],[32]	La detección anticipada fortalece redes IoT y SDN, reduciendo interrupciones operativas.
	Mejor capacidad de gestión ante amenazas avanzadas [1], [3], [4], [5], [6], [12], [14], [27], [32], [39]	Las defensas automatizadas gestionan las consecuencias de ataques APT.
	Mayor resiliencia frente a intentos de intrusión y manipulación [1],[3],[4],[5],[14] ,[18],[26],[32],[35]	Modelos colaborativos aumentan la resistencia ante envenenamientos de datos.
¿Cómo ajustan las empresas sus estrategias de seguridad ante el malware usando machine learning?	Enfoque proactivo y monitoreo continuo [1],[3],[4],[5],[6] ,[8],[17],[27]	Las empresas implementan protección continua mediante la supervisión de dispositivos IoT.
	Integración de análisis predictivo y modelos adaptativos [3],[4],[14],[24],[29]	Modelos predictivos mejoran la respuesta a amenazas emergentes.
	Colaboración y manejo seguro de datos [3],[5],[6],[14] ,[17],[30],[39]	Estrategias colaborativas comparten información sobre amenazas, fortaleciendo defensas.
	Uso de técnicas resistentes a manipulaciones [4],[6],[8],[14] ,[24],[32],[39]	Redes neuronales gráficas enfrentan envenenamientos y protegen datos sensibles.
	Capacitación y actualización de políticas de seguridad [1],[2],[3],[4], [5],[27]	Las empresas educan sobre phishing y adoptan políticas de seguridad flexibles.
¿De qué forma influye el malware en la adopción de machine learning para la protección empresarial?	Aumento de ataques en IoT y redes empresariales [1], [6], [8], [18], [27], [32]	La complejidad de ataques en IoT impulsa la integración de machine learning.
	Creciente sofisticación de amenazas avanzadas [1],[3],[4],[5],[14], [27],[32],[34],[39]	Ataques APT y DDoS fomentan el uso de técnicas avanzadas de aprendizaje.
	Necesidad de defensa en tiempo real y detección predictiva [3],[6],[8],[14] ,[19],[29],[32],[47]	La rápida evolución de amenazas incentiva el uso de machine learning en tiempo real.
	Protección de datos y modelos críticos [3],[4],[12],[16],[30]	Malware en bases de datos lleva a mejorar la protección de datos.
	Incremento en ataques de phishing y ransomware [19],[30],[3],[4] ,[27],[39],[15]	La prevalencia de phishing y ransomware impulsa el análisis de correos sospechosos.

Las empresas adaptan sus estrategias de seguridad contra el malware utilizando machine learning a través de un enfoque proactivo y monitoreo continuo, lo que incluye la supervisión de dispositivos IoT [1],[3],[4],[5],[6],[8],[17],[27]. Incorporan análisis predictivo y modelos adaptativos para responder mejor a amenazas emergentes [3],[4],[14],[24],[29].

La colaboración y el manejo seguro de datos son clave, ya que permiten compartir información sobre amenazas y fortalecer defensas [3],[5],[6],[14],[17],[30],[39]. Además, aplican técnicas resistentes a manipulaciones, como redes neuronales gráficas, para proteger datos sensibles [4],[6],[8],[14],[24],[32],[39], y capacitan al personal sobre phishing y seguridad [1],[2],[3],[4],[5],[27]. El malware impulsa la adopción de machine learning en la protección empresarial al aumentar la frecuencia de ataques en IoT y redes, lo que fomenta su integración [1],[6],[8],[18],[27],[32]. La sofisticación de amenazas avanzadas, como APT y DDoS, promueve el uso de técnicas de aprendizaje avanzadas [1],[3],[4],[5],[14],[27],[32],[34],[39]. También se destaca la necesidad de defensa en tiempo real y

detección predictiva, ya que la rápida evolución de las amenazas requiere el uso de machine learning [3],[6],[8],[14],[19],[29],[32],[47]. Finalmente, el malware en bases de datos lleva a mejorar la protección de datos críticos [3],[4],[12],[16],[30], y el aumento de ataques de phishing y ransomware incentiva el análisis de correos sospechosos [19],[30],[3],[4],[27],[39],[15].

IV Discusiones

La revisión de la literatura resalta la importancia del aprendizaje automático (ML) y las técnicas avanzadas de Deep learning en la identificación y mitigación de los ataques de malware en diferentes entornos tecnológicos, como IoT, redes empresariales y sistemas críticos. Estas herramientas se han vuelto esenciales debido a su capacidad para manejar grandes volúmenes de datos, detectar patrones complejos y predecir comportamientos anómalos en tiempo real. Los estudios revisados muestran que no solo permiten detectar amenazas de manera temprana, sino que también facilitan una respuesta mucho más eficaz ante ataques dirigidos. Esto se refleja en investigaciones como las de [1][3][4], que destacan el uso de modelos avanzados basados en redes neuronales profundas y métodos explicables. Estas técnicas permiten entender y justificar las decisiones de los modelos, lo que es clave para generar confianza en los sistemas automatizados de seguridad y para cumplir con las regulaciones que exigen transparencia. El Deep learning no solo aumenta la precisión de la detección, sino que también juega un papel crucial en la reducción de falsos positivos, un reto importante en la detección de malware. Métodos como la selección de características mediante algoritmos híbridos, que combinan enfoques como algoritmos genéticos y deep learning, no solo mejoran la precisión, sino que también permiten optimizar el rendimiento de los modelos, incluso en escenarios con grandes volúmenes de datos y redes con recursos limitados, como en el caso de IoT [6][24]. Además, el uso de redes neuronales gráficas ha demostrado un potencial significativo para identificar patrones complejos en ataques avanzados persistentes (APT), que se ocultan dentro de tráfico legítimo, lo que ayuda a las empresas a adelantarse a las amenazas antes de que puedan causar daños considerables [7][27].

En otro sentido, las estrategias basadas en machine learning, como las arquitecturas híbridas y el aprendizaje por transferencia, han mostrado ser especialmente eficaces para abordar ciber amenazas específicas, como los ataques de ransomware y los fraudes en tiempo real. Estas estrategias combinan modelos previamente entrenados con grandes conjuntos de datos, adaptándose a contextos específicos, lo que permite una protección más sólida frente a datos cifrados y URL maliciosas, como se observa en [27][39]. Este tipo de enfoques no solo favorece la detección temprana, sino que también hace posible mitigar los efectos de los ataques antes de que generen daños graves, lo cual es crucial para las empresas, especialmente en sectores como el financiero. El aprendizaje por transferencia, particularmente para ransomware, aprovecha los grandes conjuntos de datos preexistentes para entrenar modelos que luego se pueden ajustar a las necesidades particulares de cada empresa. Este enfoque es especialmente útil cuando las amenazas son dinámicas y cambian rápidamente, algo común en sectores altamente competitivos como el financiero y en la infraestructura crítica [30][31].

A pesar de las múltiples ventajas que ofrecen las tecnologías basadas en machine learning, su implementación exitosa depende de diversos factores contextuales. Uno de los mayores desafíos para las empresas tradicionales es la resistencia al cambio organizacional. Muchos sectores, especialmente los más conservadores, encuentran dificultades para adoptar nuevas tecnologías debido a la falta de personal capacitado, recursos financieros limitados y, en algunos casos, una falta de conciencia sobre la importancia de la ciberseguridad [22][34]. Sin embargo, estudios recientes, como el de [32], sugieren que a través de una formación adecuada y colaborando con proveedores de soluciones de seguridad, las empresas pueden superar estos obstáculos, adoptando eficazmente tecnologías de ciberseguridad basadas en ML sin comprometer su eficiencia operativa.

Para superar estas barreras, es crucial implementar programas de capacitación continua que involucren a expertos en seguridad cibernética, ingenieros de software e inteligencia artificial. De esta forma, se facilitaría la integración de tecnologías avanzadas y se garantizaría que los equipos de seguridad comprendan tanto las ventajas como las limitaciones de los modelos predictivos. Además, fomentar un trabajo colaborativo interdisciplinario en las organizaciones, uniendo especialistas de diversas áreas, será esencial para maximizar los beneficios de las tecnologías basadas en ML. Según los estudios de [3][7][50], la colaboración entre disciplinas es clave para crear sistemas de seguridad más robustos, capaces de adaptarse a la evolución constante de las amenazas cibernéticas.

El análisis también resalta la importancia de los modelos basados en clustering y el aprendizaje no supervisado para detectar anomalías en el tráfico de red, especialmente en entornos industriales y de IoT [16][33]. Estas técnicas son útiles cuando las amenazas no siguen patrones preestablecidos, lo que las hace difíciles de detectar con métodos supervisados tradicionales. En investigaciones como [11][40], se ha demostrado que la combinación de clustering con selección de características clave y clasificación supervisada mejora significativamente la precisión y la eficacia en la detección de amenazas avanzadas persistentes (APT), sobre todo en sistemas de control industrial, que son objetivos frecuentes de ciberataques debido a su importancia estratégica [41].

Además, los modelos de clustering permiten identificar comportamientos anómalos en redes de alto tráfico, lo que es especialmente útil en situaciones donde las amenazas no son fácilmente detectables mediante firmas o patrones predefinidos. La optimización de características también juega un papel esencial en la mejora de la eficacia de los modelos, adaptándolos a las condiciones cambiantes de las redes y ayudando a las empresas a mitigar riesgos de manera más eficiente [42][43]. Por último, el éxito de estas tecnologías no solo depende de la tecnología en sí, sino también de la capacidad de las organizaciones para medir su impacto y rendimiento. La definición de métricas claras y la creación de sistemas de evaluación estandarizados son fundamentales para medir la efectividad de las soluciones basadas en machine learning. Estas métricas no solo deben centrarse en la precisión de detección, sino también en aspectos como la reducción de falsos positivos, el tiempo de respuesta y la eficacia frente a nuevas amenazas [44][45].

V CONCLUSIONES

Un primer aspecto para resaltar es el papel fundamental que desempeñan el aprendizaje automático y las técnicas avanzadas de deep learning en la detección y mitigación de ataques de malware. La evidencia recopilada demuestra que estas tecnologías han evolucionado hasta convertirse en herramientas clave para abordar

amenazas complejas en diversos entornos, como IoT, redes empresariales y sistemas industriales críticos. En particular, la implementación de arquitecturas basadas en redes neuronales profundas y enfoques explicables ha demostrado ser eficaz en la identificación de patrones maliciosos, ofreciendo soluciones sólidas y adaptativas.

Adicionalmente, las investigaciones destacan el potencial de técnicas específicas como modelos convolucionales diluidos, redes de decisión profunda y algoritmos híbridos de selección de características. Estos enfoques permiten abordar desafíos técnicos, como el desequilibrio en los datos, y maximizan la precisión en escenarios de ciberataques diversificados, especialmente en redes IoT. Este avance es especialmente relevante en un panorama de amenazas dinámico, donde la adaptabilidad de los sistemas se convierte en un diferenciador crítico.

Otro hallazgo relevante es la efectividad de las estrategias híbridas, como el aprendizaje por transferencia y los modelos de machine learning adaptativos, para combatir amenazas emergentes como el ransomware y los fraudes en tiempo real. Estas técnicas han demostrado un impacto significativo en la protección de datos y la detección temprana de amenazas, consolidándose como soluciones integrales en la defensa cibernética. Por otra parte, se resalta el valor de los modelos no supervisados, como los sistemas basados en clustering, para identificar anomalías en el tráfico de red, especialmente en entornos industriales e IoT. Estas estrategias, reforzadas por técnicas de clasificación supervisada y optimización de características, resultan eficaces para detectar amenazas avanzadas y persistentes, lo que subraya la necesidad de enfoques integrados en estos contextos. Sin embargo, la implementación exitosa de estas tecnologías no está exenta de desafíos. Los resultados de la revisión apuntan a que factores como la madurez tecnológica, la infraestructura disponible y la cultura organizacional de las empresas juegan un papel decisivo en la adopción de estas herramientas. Sectores más tradicionales enfrentan barreras como la resistencia al cambio y la escasez de personal capacitado, lo que limita su capacidad para aprovechar plenamente estas tecnologías.

En este contexto, se enfatiza la necesidad de promover la capacitación continua y la colaboración interdisciplinaria como pilares esenciales para superar estas barreras. Además, es crucial desarrollar métricas claras y sistemas de evaluación que permitan medir el impacto de estas tecnologías, facilitando su mejora continua y alineación con los objetivos estratégicos de cada organización. Finalmente, la revisión evidencia la necesidad de fomentar la investigación futura, particularmente en la integración de estas herramientas con tecnologías emergentes, como la inteligencia artificial explicable y la computación perimetral, para maximizar su impacto. La adopción de estas estrategias permitirá a las organizaciones no solo mitigar riesgos cibernéticos, sino también construir entornos digitales más resilientes y seguros frente a las amenazas en constante evolución.

REFERENCIAS

[1] (Siraj Uddin Qureshi, Jingsha He, Saima Tunio, Nafei Zhu, Ahsan Nazir, Ahsan Wajahat, Faheem Ullah, Abdul Wadud 2024). Systematic review of deep learning solutions for malware detection and forensic analysis in IoT. https://doi.org/10.1016/j.jksuci.2024.102164

[2] (Akshit Kamboj, Priyanshu Kumar, Amit Kumar Bairwa, Sandeep Joshi, 2023) Detection of malware in downloaded files using various machine learning models. https://doi.org/10.1016/j.eij.2022.12.002

[3] Ahmed, A., Awais, M., Siraj, M., & Umar, M. (2023). Enhancing cybersecurity with trust-based machine learning: A defense against DDoS and packet suppression attacks. https://doi.org/10.55549/epstem.1368266

[4] (E. Baghirov, 2024). A Comprehensive Investigation into Robust Malware Detection with Explainable AI. https://doi.org/10.1016/j.csa.2024.100072

[5] P. Maniriho, A. N. Mahmood, and M. J. M. Chowdhury, "A systematic literature review on Windows malware detection: Techniques, research issues, and future directions" https://doi.org/10.1016/j.jss.2023.111921.

[6] Karthick M., Samsudeen S., Thomas L., Darsini P.V., and Prabaakaran K., "Cybersecurity Warning System Using Diluted Convolutional Neural Network Framework for IOT Attack Prevention," doi: 10.22266/ijies2024.0229.66.

[7] Mini T.V., John J., and Siji P.D., "Unmasking Deception: Artificial Neural Networks in Smishing Detection for Cyber Security Fortification," doi: 10.14445/23488549/IJECE-V11I7P114.

[8] AlSaleh I., Al-Samawi A., and Nissirat L., "Novel Machine Learning Approach for DDoS Cloud Detection: Bayesian-Based CNN and Data Fusion Enhancements," doi: 10.3390/s24051418.

[9] Hang F., Xie L., Zhang Z., Guo W., and Li H., "Research on the application of network security defence in database security services based on deep learning integrated with big data analytics," doi: 10.1016/j.ijin.2024.02.006.

[10] Qiu P., Zhang X., Ji S., Li C., Pu Y., Yang X., and Wang T., "Hijack Vertical Federated Learning Models as One Party," doi: 10.1109/TDSC.2024.3358081.

[11] Sugin S.V. and Kanchana M., "Enhancing intrusion detection with imbalanced data classification and feature selection in machine learning algorithms," doi: 10.19101/IJATEE.2023.10101620.

[12] Shieh C.-S., Ho F.-A., Horng M.-F., Nguyen T.-T., and Chakrabarti P., "Open-Set Recognition in Unknown DDoS Attacks Detection with Reciprocal Points Learning," doi: 10.1109/ACCESS.2024.3388149.

[13] Avci C., Tekinerdogan B., and Catal C., "Design tactics for tailoring transformer architectures to cybersecurity challenges," doi: 10.1007/s10586-024-04355-0.

[14] Becerra-Suarez F.L., Fernández-Roman I., and Forero M.G., "Improvement of Distributed Denial of Service Attack Detection through Machine Learning and Data Processing," doi: 10.3390/math12091294.

[15] Loh P.K.K., Lee A.Z.Y., and Balachandran V., "Towards a Hybrid Security Framework for Phishing Awareness Education and Defense," doi: 10.3390/fi16030086.

[16] Vaarandi R. and Guerra-Manzanares A., "Stream clustering guided supervised learning for classifying NIDS alerts," doi: 10.1016/j.future.2024.01.032.

[17] Asmar M. and Tuqan A., "Integrating machine learning for sustaining cybersecurity in digital banks," doi: 10.1016/j.heliyon. 2024.e37571.

[18] Alkhonaini M.A., Mazroa A.A., Aljebreen M., Ben Haj Hassine S., Allafi R., Dutta A.K., Alsubai S., and Khamparia A., "Hybrid Sine-Cosine Chimp optimization-based feature selection with deep learning model for threat detection in IoT sensor networks," doi: 10.1016/j.aej.2024.05.051.

[19] Bezerra A., Pereira I., Rebelo M.Â., Coelho D., Oliveira D.A.D., Costa J.F.P., and Cruz R.P.M., "A case study on phishing detection with a machine learning net," doi: 10.1007/s41060-024-00579-w.

[20] Arun Prasad P.B., Mohan V., and Vinoth Kumar K., "Hybrid Metaheuristics with Deep Learning Enabled Cyberattack Prevention in Software Defined Networks," doi: 10.17559/TV-20230621000752.

[21] Baker T., Li T., Jia J., Zhang B., Tan C., and Zomaya A.Y., "Poison-Tolerant Collaborative Filtering Against Poisoning Attacks on Recommender Systems," doi: 10.1109/TDSC.2024.3354462.

[22] Krishnan M., Lim Y., Perumal S., and Palanisamy G., "Detection and defending the XSS attack using novel hybrid stacking ensemble learning-based DNN approach," doi: 10.1016/j.dcan.2022.09.024.

[23] Jmal H., Hmida F.B., Basta N., Ikram M., Kaafar M.A., and Walker A., "SPGNN-API: A Transferable Graph Neural Network for Attack Paths Identification and Autonomous Mitigation," doi: 10.1109/TIFS.2023.3338965.

[24] Alrayes F.S., Zakariah M., and Driss M., "Deep Neural Decision Forest (DNDF): A Novel Approach for Enhancing Intrusion Detection Systems in Network Traffic Analysis," doi: 10.3390/s23208362.

[25] Shetty V.R., R P., and Malghan R.L., "Safeguarding against Cyber Threats: Machine Learning-Based Approaches for Real-Time Fraud Detection and Prevention †," doi: 10.3390/engproc2023059111.

[26] Mahalingam A., Perumal G., Subburayalu G., Albathan M., Altameem A., Almakki R.S., Hussain A., and Abbas Q., "ROAST-IoT: A Novel Range-Optimized Attention Convolutional Scattered Technique for Intrusion Detection in IoT Networks," doi: 10.3390/s23198044.

[27] Singh A., Mushtaq Z., Abosaq H.A., Mursal S.N.F., Irfan M., and Nowakowski G., "Enhancing Ransomware Attack Detection Using Transfer Learning and Deep Learning Ensemble Models on Cloud-Encrypted Data," doi: 10.3390/electronics12183899.

[28] Alarfaj F.K. and Khan N.A., "Enhancing the Performance of SQL Injection Attack Detection through Probabilistic Neural Networks," doi: 10.3390/app13074365.

[29] Ravindran S. and Sarveshwaran V., "Deep Learning Towards Intrusion Detection System (IDS): Applications, Challenges and Opportunities," doi: 10.13052/jmm1550-4646.1958.

[30] Aldakheel E.A., Zakariah M., Gashgari G.A., Almarshad F.A., and Alzahrani A.I.A., "A Deep Learning-Based Innovative Technique for Phishing Detection in Modern Security with Uniform Resource Locators," doi: 10.3390/s23094403.

[31] Li D., Liu D., Guo Y., Ren Y., Su J., and Liu J., "Defending against model extraction attacks with physical unclonable function," doi: 10.1016/j.ins.2023.01.102.

[32] Imran M., Siddiqui H.U.R., Raza A., Raza M.A., Rustam F., and Ashraf I., "A performance overview of machine learning-based defense strategies for advanced persistent threats in industrial control systems," doi: 10.1016/j.cose.2023.103445.

[33] Guo J. and Shen Y., "Online Anomaly Detection of Industrial IoT Based on Hybrid Machine Learning Architecture," doi: 10.1155/2022/8568917.

[34] Lin Q., Ming R., Zhang K., and Luo H., "Privacy-Enhanced Intrusion Detection and Defense for Cyber-Physical Systems: A Deep Reinforcement Learning Approach," doi: 10.1155/2022/4996427.

[35] Bilot T., Madhoun N.E., Agha K.A., and Zouaoui A., "Graph Neural Networks for Intrusion Detection: A Survey," doi: 10.1109/ACCESS.2023.3275789.

[36] Meng L., "Internet of Things Information Network Security Situational Awareness Based on Machine Learning Algorithms," doi: 10.1155/2022/4146042.

[37] Note J. and Ali M., "Comparative Analysis of Intrusion Detection System Using Machine Learning and Deep Learning Algorithms," doi: 10.33166/AETiC.2022.03.003.

[38] Padmapriya V. and Srivenkatesh M., "Digital Twins for Smart Home Gadget Threat Prediction using Deep Convolution Neural Network," doi: 10.14569/IJACSA.2023.0140270.

[39] Mosa D.T., Shams M.Y., Abohany A.A., El-Kenawy E.-S.M., and Thabet M., "Machine Learning Techniques for Detecting Phishing URL Attacks," doi: 10.32604/cmc.2023.036422.

[40] Kasongo S.M. and Sun Y., "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," doi: 10.1186/s40537-020-00379-6.

[41] Zhang Y., Yasaei R., Chen H., Li Z., and Faruque M.A.A., "Stealing Neural Network Structure through Remote FPGA Side-Channel Analysis," doi: 10.1109/TIFS.2021.3106169.

[42] Al-Imran M. and Ripon S.H., "Network Intrusion Detection: An Analytical Assessment Using Deep Learning and State-of-the-Art Machine Learning Models," doi: 10.1007/s44196-021-00047-4.

[43] Nhu C.-N. and Park M., "Two-phase deep learning-based edos detection system," doi: 10.3390/app112110249.

[44] Al-Khater W.A., Al-Maadeed S., Ahmed A.A., Sadiq A.S., and Khan M.K., "Comprehensive review of cybercrime detection techniques," doi: 10.1109/ACCESS.2020.3011259.

[45] Zimba A., Chen H., Wang Z., and Chishimba M., "Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics," doi: 10.1016/j.future.2020.01.032.

[46] Nazih W., Hifny Y., Elkilani W.S., Dhahri H., and Abdelkader T., "Countering ddos attacks in sip based voip networks using recurrent neural networks," doi: 10.3390/s20205875.

[47]Naseer S., Ali R.F., Dominic P.D.D., and Saleem Y., "Learning representations of network traffic using deep neural networks for network anomaly detection: A perspective towards oil and gas it infrastructures," doi: 10.3390/sym12111882.