Use of Machine Learning against Malware Attacks in the Banking Sector

Daniel Martin Chavez Alvarez [1]; Ivan Nicolas Riqueros Carhuayal [2]; Evelyn Elizabeth Ayala Ñiquen[3]; Cesar Augusto Yactayo Arias [4]
[1,2,3,4] Universidad Tecnológica del Perú, Perú, *u21203844@utp.edu.pe, u21314075@utp.edu.pe, c26915@utp.edu.pe, c31501@utp.edu.pe*

Abstract*– Cyber threats and risks associated with digital security have increased considerably in the banking sector, driving the need to adopt new technologies that allow detecting and mitigating potential attacks. This review aims to identify the most widely used machine learning models against malware detection. Method: 194 original articles related to the subject were analyzed, of which only 27 met the inclusion criteria for the final review. Additionally, a dynamic analysis was used to examine the performance of the algorithms in real and simulated scenarios. It was evident that Machine Learning models, particularly supervised learning models such as neural networks, support vector machines, and random forest algorithms, have achieved promising results in the early detection of malware, allowing for a faster and more accurate response to potential cyber threats. The integration of Machine Learning into banking cybersecurity has generated significant advances in the identification and control of malicious attacks, provided that there is adequate data quality, constant updating of the models, and proper coordination with existing defense systems. Therefore, it is concluded that the use of these technologies, beyond their technical capacity, also represents an opportunity to strengthen the culture of prevention and digital resilience within the financial environment.

Keywords—Machine learning, Attacks, Malware, Banking Sector.

Uso de Machine Learning frente a los ataques de Malware en el Sector Bancario.

Daniel Martin Chavez Alvarez [1]; Ivan Nicolas Riqueros Carhuayal [2]; Evelyn Elizabeth Ayala Ñiquen[3]; Cesar Augusto Yactayo Arias [4]
[1, 2,3,4] Universidad Tecnológica del Perú, Perú, *u21203844@utp.edu.pe, u21314075@utp.edu.pe, c26915@utp.edu.pe, c31501@utp.edu.pe*

Resumen*– Las amenazas informáticas y los riesgos asociados a la seguridad digital han aumentado de manera considerable en el sector bancario, impulsando la necesidad de adoptar nuevas tecnologías que permitan detectar y mitigar posibles ataques. Esta revisión tiene como objetivo identificar los modelos de machine learning más usados contra la detección de malware en sector bancario. Método: Se analizaron 194 artículos originales relacionados con la temática, de los cuales solo 27 cumplieron con los criterios de inclusión para la revisión final; adicionalmente, se empleó un análisis dinámico que permitió examinar el rendimiento de los algoritmos en escenarios reales y simulados Se evidenció que los modelos de Machine Learning, particularmente aquellos de aprendizaje supervisado como las redes neuronales, máquinas de soporte vectorial y algoritmos de bosque aleatorio, han logrado resultados prometedores en la detección temprana de malware, permitiendo una respuesta más rápida y precisa ante posibles amenazas cibernéticas. La integración del Machine Learning en la ciberseguridad bancaria ha generado avances significativos en la identificación y control de ataques maliciosos, siempre que se cuente con una adecuada calidad de datos, actualización constante de los modelos y una correcta articulación con los sistemas de defensa existentes; por ello, se concluye que el uso de estas tecnologías, más allá de su capacidad técnica, también representa una oportunidad para fortalecer la cultura de prevención y resiliencia digital dentro del entorno financiero.

Palabras clave*—Aprendizaje Automático, ataques, Malware, sector Bancario.

I. Introducción

Con el crecimiento del internet y los servicios digitales, también han aumentado los ataques cibernéticos que afectan tanto a personas como a empresas. Estos ataques, como el phishing o los virus informáticos, son cada vez más difíciles de detectar usando métodos tradicionales. Por eso, muchos investigadores están probando nuevas soluciones que usan inteligencia artificial para ayudar a prevenir estos riesgos. Un estudio reciente presentó un sistema llamado DEPHIDES que usa redes neuronales, un tipo de inteligencia artificial que aprende patrones, y logró buenos resultados identificando páginas falsas o peligrosas [1]. Además, se han explorado enfoques que manejan la incertidumbre cuando se analizan situaciones de riesgo, sobre todo en bancos y servicios financieros, lo que permite tomar decisiones más seguras [2]. También se ha visto que incluir modelos de aprendizaje automático en la banca digital ayuda a mejorar la seguridad general y prevenir ataques antes de que ocurran [3]. Estas ideas muestran que la tecnología puede ser una gran aliada contra el cibercrimen, y por eso es importante revisar con detalle qué métodos están funcionando mejor y cómo pueden seguir mejorándose.

Aunque se ha avanzado mucho en tecnología para protegernos en internet, los delincuentes también se han vuelto más hábiles. Cada vez surgen nuevos tipos de virus y programas maliciosos que logran pasar desapercibidos por muchos sistemas de seguridad, especialmente en los bancos y otras instituciones financieras. Por ejemplo, un estudio demostró que amenazas como Emotet siguen siendo muy peligrosas y logran afectar incluso sistemas bien protegidos [4]. Además, muchos métodos de seguridad actuales no alcanzan a cubrir todos los ataques porque no se adaptan bien a los cambios ni a la gran cantidad de datos que se manejan hoy en día [5]. También hay problemas con la forma en que se prueban estas herramientas, ya que no siempre se siguen los mismos criterios, lo que dificulta saber cuál es realmente mejor [6]. Todo esto crea un problema serio: aunque hay muchas investigaciones y modelos propuestos, aún falta lograr sistemas realmente eficaces, fáciles de aplicar y que sirvan en distintas situaciones. Por eso es tan importante revisar de forma ordenada lo que ya se ha hecho y ver qué se puede mejorar o qué se ha pasado por alto.

Dado que los ataques en internet no dejan de crecer y mejorar, es necesario estudiar con cuidado las soluciones que se están proponiendo para enfrentarlos. Hacer una revisión detallada de las investigaciones más recientes sobre cómo se usa el aprendizaje automático para detectar amenazas permitirá entender qué métodos son más útiles y en qué contextos funcionan mejor. Algunos trabajos han demostrado que ciertos modelos, como las redes neuronales o los sistemas que combinan varios métodos, pueden detectar con bastante precisión actividades sospechosas si se entrenan bien y con datos adecuados [7]. También es importante observar cómo se evalúan estas herramientas, qué tipos de datos usan y cómo se adaptan a diferentes escenarios, para saber si podrían usarse en la vida real. Esta revisión busca no solo recoger lo que ya se ha investigado, sino también encontrar aspectos que aún no se han explorado bien o problemas que siguen sin resolverse [8]. De esta forma, será posible ayudar a crear sistemas de seguridad más efectivos, adaptables y útiles tanto para los usuarios comunes como para las organizaciones.

II. Metodología

A. Estrategia de Búsqueda

En este estudio, la revisión sistemática se realizó sin metaanálisis. Para plantear los componentes de la investigación se utilizó el método PICO de lo cual se empleó la técnica PIOC, que es una forma de desglosar una pregunta

de investigación en preguntas más pequeñas y manejables, facilitando así el análisis y la búsqueda de respuestas claras. Esta técnica sigue una secuencia que nos ayuda a entender mejor un problema complejo.

TABLA I
COMPONENTES DE LA ESTRATEGIA PICO (ESPECIFICAR PIOC)

Componente	Detalle
(P) problema	Ataque de malware
(I)intervención	Machine Learning
(O)resultados	La detección de ataque de malware
(C)contexto	Sector bancario

Dentro del desarrollo de la investigación, se prosiguió con el método PICO formulando la pregunta principal: ¿Cómo el machine learning se puede usar para la detección de malware en el sector bancario? Esta pregunta orientada al progreso del estudio. Se divide en cuatro cuestiones concretas, planteadas con el objetivo identificar los modelos de machine learning más usados contra la detección de malware. Cada una de estas interrogantes se relaciona con un tipo específico de referente anticipado, lo que facilita un análisis más organizado y consistente. Es importante resaltar que todas las respuestas a estas preguntas se elaborarán empleando datos en español, asegurando de esta manera la accesibilidad y entendimiento del contenido en el ámbito regional e investigativo.

TABLA II
SUBPREGUNTAS PICO

Acrónimo	RQ
P	¿Cómo los ataques de malware se propagan y actúan con el objetivo de comprometer los datos dentro de una empresa?
I	¿Qué métodos de machine learning puede usar frente los ataques malware?
O	¿Qué modelos de machine learning se puede utilizar para la detección de ataques malware?
C	¿Cómo la inteligencia artificial puede solucionar los ataques de malware en el sector bancario?

Para asegurar la calidad de esta revisión sistemática de la literatura, se han utilizado fuentes de datos con reconocimiento científico y que sean multidisciplinarias o relacionada con la información. Además, se empleó las bases de datos de SCOPUS y WEB OF SCIENCE.

TABLA III
PALABRAS CLAVE DE LOS COMPONENTES DE LA PREGUNTA PICO

Acrónimo	Palabras claves	Keywords
P	malware OR "malware de ataque" OR "software malicioso" OR wiperware OR wiper OR "malware de wiper"	malware OR "attack malware" OR "malicious software" OR wiperware OR wiper OR "wiper malware"
I	"aprendizaje automático" OR "ML" OR "Regresión lineal" OR "Regresión logística" OR "Bosque aleatorio" OR "Redes neuronales" OR "svm o knn"	"machine learning" OR "ML" OR "Linear regression" OR "Logistic regression" OR "Random Forest" OR "Neural networks" OR "svm or knn"
O	detección O encontrar O localizar	detection OR find OR locate
C	banca OR finanzas O banco OR "grupo bancario" OR "sector bancario" OR "institución bancaria" OR "banco de primer nivel"	banking OR finances OR bank OR "banking group" OR "banking sector" OR "banking institution" OR "top-tier bank"

B. Ecuación de búsqueda

Basándose en la información de la tabla IV, se elaboraron las ecuaciones de búsqueda adecuadas para las bases de datos SCOPUS y WEB OF SCIENCE y la ecuación de búsqueda se estructuró de la siguiente manera:

TABLA IV
ECUACIÓN DE BÚSQUEDA

Scopus	Web of Science
(TITLE-ABS-KEY (malware OR "malicious software" OR "malicious code" OR "harmful software" OR "cyber threat" OR "hostile software" OR "attack malware" OR wiperware OR wiper OR "wiper malware") AND TITLE-ABS-KEY ("machine learning“ OR "automated learning" OR "artificial intelligence" OR "AI" OR "predictive models" OR "supervised learning" OR "unsupervised learning" OR "ML" OR "Linear regression" OR "Logistic regression" OR "Random Forest" OR "Neural networks" OR "svm or knn") AND TITLE-ABS-KEY (detection OR identification OR recognition OR "threat detection" OR diagnosis OR monitoring OR analysis OR find OR locate) AND TITLE-ABS-KEY (banking OR finances OR bank OR "banking group" OR "banking sector" OR "banking institution" OR "top-tier bank" OR "financial sector" OR "banking industry" OR "digital banking" OR "online banking")) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English"))	malware OR "malicious software" OR "malicious code" OR "harmful software" OR "cyber threat" OR "hostile software" OR "attack malware" OR waterware OR wiper OR "wiper malware" (All Fields) and "machine learning" OR "automated learning" OR "artificial intelligence" OR "AI" OR "predictive models" OR "supervised learning" OR "unsupervised learning" OR "ML" OR "Linear regression" OR "Logistic regression" OR "Random Forest" OR "Neural networks" OR "svm or knn" (All Fields) and detection OR identification OR recognition OR "threat detection" OR diagnosis OR monitoring OR analysis OR find OR locate (All Fields) and banking OR finances OR bank OR "banking group" OR "banking sector" OR "banking institution" OR "top-tier bank" OR "financial sector" OR "banking industry" OR "digital banking" OR "online banking" (All Fields) and Article or Review Article (Document Types) and English (Languages)

C. Criterios de inclusión y exclusión

Para la investigación, se contempló los criterios tanto de inclusión y exclusión, para poder definir y evaluar los artículos más importantes con los que se trabajara. Se consideraron 4

criterios de inclusión y 4 de exclusión como se muestra en la tabla V:

TABLA V
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Criterios de Inclusión	Criterios de Exclusión
CI1: Estudios que apliquen métodos de machine learning en el contexto del sector bancario.	CE1: Estudios sobre otros modelos de machine learning que no enfoca en el sector bancario.
CI2: Investigaciones que describen modelo de IA usando machine learning en industria bancaria.	CE2: Investigaciones que no describen el uso de machine learning.
CI3: Artículos que describen el uso de malware en sector bancario.	CE3: Estudios que se enfocaron en dispositivos móviles como Android.
CI4: Estudios que presenten resultados de desempeño del modelo aplicado.	CE4: Estudios que se enfocaron en la alternativa de uso de criptomonedas.

D. Proceso de selección de estudio

Durante la selección de artículos, aplicando la metodología PRISMA, se generó el diagrama de flujo en varias etapas. Fueron evaluados los artículos en las bases de datos, donde se obtuvo un número total de documentos que cuentan con información clara y útil para la investigación. En Scopus y WOS obtuvimos un total de 194 artículos.

Se continuó a filtrar los duplicados tanto por el número de DOI, descartando 57 fuentes por este criterio. Luego se procesó a filtrar por título y resumen que sumo 137 artículos, sumando a ellos los 66 artículos a los cuales se registró excluido. Por lo cual se recupera 71 artículos.

Con todos los filtros mencionado, no se recuperaron 22 artículos quedando 49 artículos elegible. De lo cuales 22 artículos publicado fueron excluida.

Finalmente, se obtuvo 27 articulo elegibles para continuar la investigación:

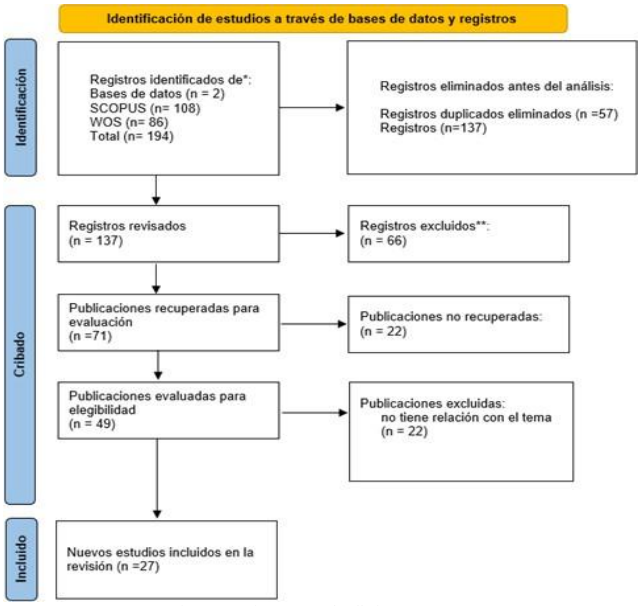

Fig. 1. Diagrama de flujo PRISMA

III. RESULTADOS

Los estudios revisados demuestran que el término machine learning está estrechamente vinculado con sistemas avanzados como la ciberseguridad y detección de malware en sector bancario, siendo fundamental en áreas como el análisis dinámico, los algoritmos de clasificación y el uso de redes neuronales convolucionales. Para ilustrar estas relaciones, se realizó un análisis bibliométrico de las palabras clave utilizadas en los artículos científicos (ver Fig. 2).

Entre estos, destacan términos asociados a la caracterización de usuarios y análisis de amenazas estáticas como user profiling, memory forensics, static analysis y trickbot. Estas herramientas son fundamentales en la identificación temprana de comportamientos anómalos dentro de plataformas bancarias, especialmente en servicios como banca en línea o billeteras digitales. Sin embargo, su baja visibilidad sugiere una preferencia generalizada por métodos dinámicos o basados en grandes volúmenes de datos, lo cual podría estar limitando el alcance de soluciones más ligeras y específicas.

Asimismo, aparecen conceptos vinculados a la gestión institucional y el diseño de estrategias sostenibles, como policy, innovation y sustainable development, que, si bien no tienen un carácter técnico, son esenciales para garantizar la implementación efectiva de soluciones basadas en inteligencia artificial dentro de entornos bancarios. La escasa representación de estos términos evidencia una brecha entre los avances algorítmicos y su articulación con políticas organizacionales a largo plazo.

También se identifican enfoques innovadores centrados en la experiencia del usuario, como gamification, user behavior y cyber threat, que aún no han sido completamente aprovechados en el diseño de sistemas antifraude bancarios. Estas palabras clave reflejan una tendencia emergente por integrar la dimensión humana dentro de la ciberseguridad, pero su baja presencia académica indica que esta línea de investigación aún está en desarrollo.

Por último, se observan términos especializados como relation extraction, api call, classification y neutrosophic fuzzy soft, los cuales corresponden a propuestas técnicas avanzadas que podrían fortalecer la arquitectura de defensa contra malware en el sector financiero. Sin embargo, su complejidad de implementación o la falta de estandarización podría explicar su limitada adopción. Del mismo modo, la reducida mención de conceptos como stakeholder theory o board of directors sugiere una débil conexión entre los desarrollos tecnológicos y su integración en los niveles decisionales de las instituciones financieras.

En conjunto, estos hallazgos permiten concluir que, si bien el machine learning ha transformado la manera en que se aborda el malware en el ámbito bancario, aún existen áreas clave que no han sido suficientemente exploradas. Estos vacíos representan una oportunidad significativa para futuras investigaciones que integren elementos técnicos, humanos y

estratégicos de forma equilibrada, permitiendo construir soluciones más completas, eficaces y sostenibles.

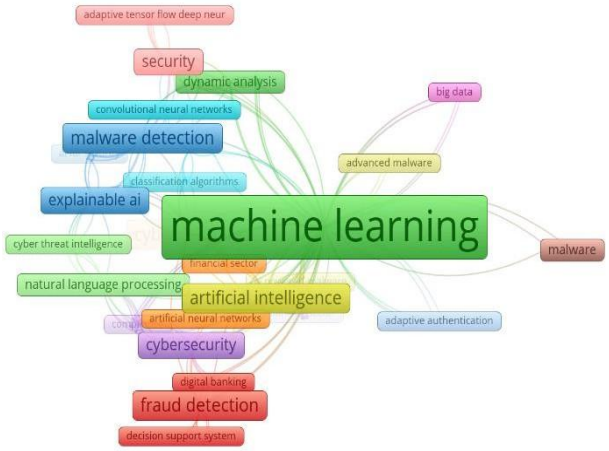

Fig. 2. Relación de machine learning en los estudios.

En los últimos años, el avance acelerado de la tecnología ha consolidado al machine learning como un componente clave en el ámbito de la ciberseguridad y la detección de malware en sector bancario. Tal como se observa en el análisis bibliométrico de la figura 3 donde la presencia más recurrente de estos términos de estudios recientes muestra el concepto como malware detection, natural language processing, artificial intelligence, fraud dection, permitiendo evidenciar su importante crecimiento. Esta tendencia se refuerza al observar el rango temporal representado en la imagen, que indica una concentración de investigaciones entre 2022 y 2025. La evolución temática representada visualmente demuestra cómo machine learning se ha posicionado como una herramienta esencial en el desarrollo de soluciones automatizadas, especialmente en contextos donde la protección de datos, el análisis de amenazas y la capacidad de respuesta inteligente son cada vez más críticos.

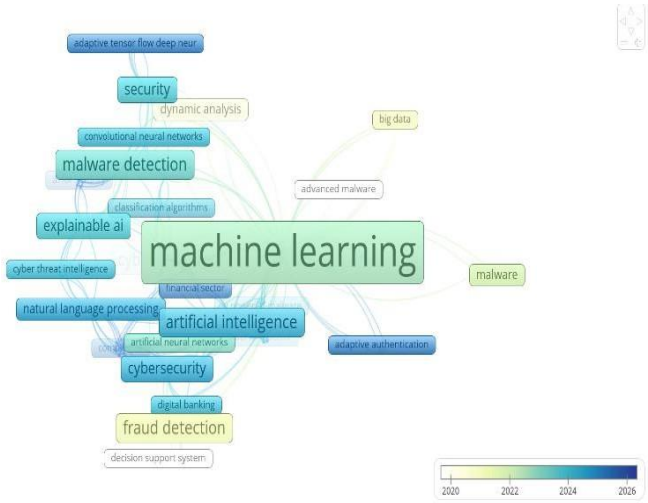

Fig. 3. Relación de machine learning con sistemas AV en los últimos años.

E. Propagación de los ataques de malware en una empresa

El sector bancario es uno de los principales blancos de ciberataques, destacando la propagación de malware especializado. Entre los más comunes se encuentran los Banking Trojans [11], [1], [6], [19], [20], [27], diseñados para robar credenciales y manipular transacciones. El phishing, junto con variantes avanzadas como ataques Adversary-in-the-Middle [6] [14] [13] [5] [7], facilita la intrusión inicial. El ransomware [15] [16] cifra datos críticos y exige rescates, afectando gravemente la continuidad operativa. También se identifican amenazas emergentes como el malware por códigos QR [17] [18], el malware evasivo basado en inteligencia artificial [24] y las botnets DDoS [2], todos con alta capacidad de penetración y daño económico en las instituciones financieras.

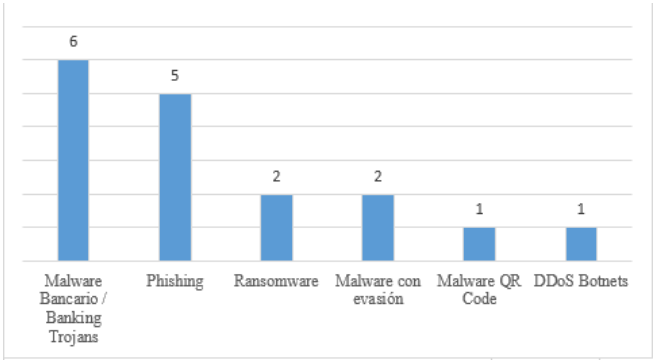

Fig. 4. Tipos de malware más comunes en el sector bancario.

F. Ingeniería social de los ataques de los malware

Los malwares que atacan al sector bancario operan principalmente a través de la ingeniería social, engañando a los usuarios para que realicen acciones que comprometen la seguridad de los sistemas. Mediante correos electrónicos falsos o archivos adjuntos infectados, el ransomware cifra información crítica para exigir rescates [1], [8]. Enlaces maliciosos o sitios web clonados facilitan el acceso de banking trojans que roban credenciales [DOI [7], [20]. El phishing, y sus variantes como AiTM y BitB, simulan interfaces legítimas para capturar datos sensibles [DOI [21], [17]. Los QR code malwares engañan con códigos visuales alterados [DOI [15]. El malware evasivo basado en IA elude la detección [5], [18], mientras que botnets/DDoS saturan servicios bancarios [22].

G. Métodos de machine learning empleados para la detección de malware

La detección de malware en el sector bancario ha avanzado significativamente gracias al uso de métodos de machine learning. Modelos como Random Forest [1] [4] [7] [20] [22], Support Vector Machine (SVM) [1] [8] [10] [21] y Redes Neuronales/Deep Learning [5] [18] [21] [24] son ampliamente utilizados por su capacidad para identificar patrones anómalos y adaptarse a nuevas amenazas. También destacan XGBoost [7] [17] [20] por su precisión y velocidad, y los Árboles de Decisión [3] [13] por su facilidad de interpretación, lo que refuerza su utilidad en entornos financieros donde se requiere detección temprana y precisa de ataques malicioso.

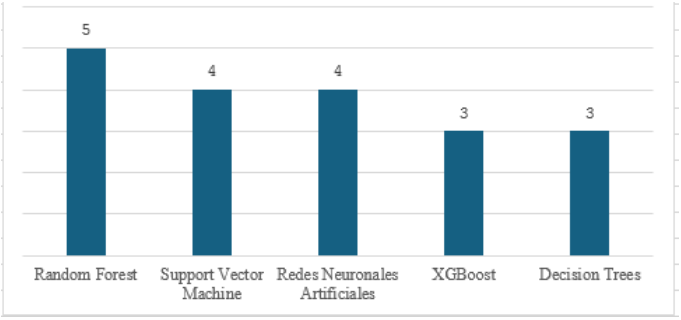

Fig. 5. Modelos de machine learning más usados para detección de malware.

H. Limitaciones de machine learning usados para la detección de malware

Aunque los modelos de machine learning han demostrado ser herramientas eficaces en la detección de malware, presentan limitaciones importantes que deben considerarse. Random Forest, por ejemplo, consume muchos recursos y puede sobreajustarse [1] [4] [7]. SVM tiene dificultades con grandes volúmenes de datos y es sensible al ruido [1] [8] [10]. Las redes neuronales requieren grandes cantidades de datos y resultan difíciles de interpretar [5] [18] [21] [24]. XGBoost necesita un ajuste preciso de hiperparámetros y no maneja bien datos desbalanceados [7] [17] [20]. Finalmente, los árboles de decisión son propensos al sobreajuste y pierden precisión ante cambios mínimos [3] [13].

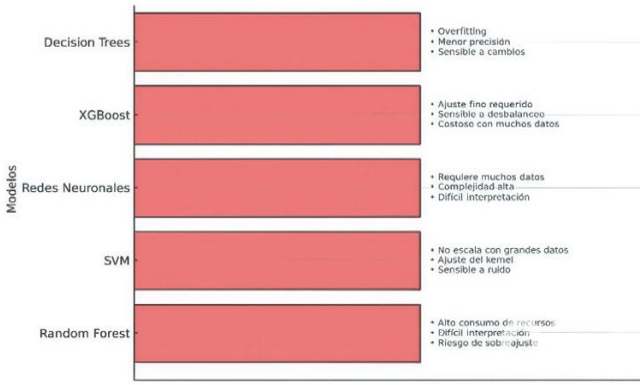

Fig. 6. Limitaciones de los de machine learning más usados para detección de malware

I. Identificación de los modelos de machine learning frente al malware

La detección de malware en el sector bancario se ha fortalecido mediante el uso de modelos de machine learning, que analizan grandes volúmenes de datos para identificar patrones anómalos. Técnicas como Random Forest, SVM, Redes Neuronales, XGBoost y Árboles de Decisión han demostrado alta efectividad en la clasificación de comportamientos maliciosos. Estos modelos detectan actividades sospechosas en archivos, redes y accesos mediante entrenamiento supervisado [1] [4] [5] [7] [13]. Su capacidad para adaptarse a nuevas amenazas en tiempo real permite reducir riesgos operativos y mejorar la ciberseguridad de las plataformas financieras [18] [21].

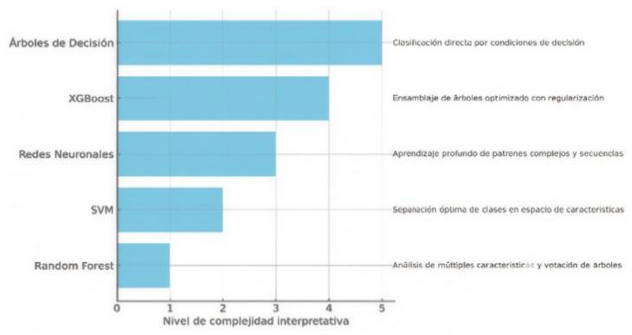

Fig. 7. Identificación de los malware con el uso de machine learning

J. Ventajas de los modelos de machine learning

Los modelos de machine learning han demostrado ser herramientas eficaces para detectar malware en el sector bancario, debido a su capacidad de adaptación y precisión. Random Forest ofrece robustez frente al ruido y facilita la interpretación de variables relevantes [1] [4]. SVM destaca por su precisión en conjuntos de datos reducidos [5] [13]. Las redes neuronales detectan patrones complejos incluso en amenazas evasivas [7] [18]. XGBoost combina velocidad y control del sobreajuste [10] [21], mientras que los árboles de decisión permiten clasificaciones rápidas y comprensibles [3] [13], siendo útiles en entornos con recursos computacionales limitados.

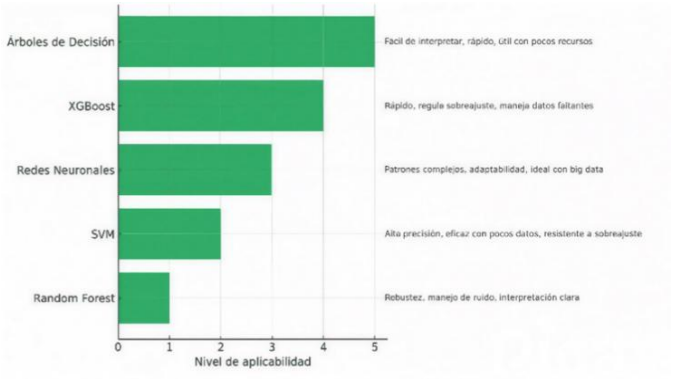

Fig. 8. Ventajas de los modelos machine learning empleados.

K. Resultados de los modelos de machine learning

La implementación de modelos de machine learning ha mejorado significativamente la detección de malware en sistemas bancarios. Random Forest ha alcanzado precisiones superiores al 95%, gracias a su capacidad para manejar datos ruidosos y desequilibrados [1] [4]. SVM ofrece resultados estables con conjuntos de datos moderados, logrando entre 90% y 96% de precisión [5] [13]. Redes neuronales profundas destacan con tasas de detección cercanas al 99% frente a amenazas evasivas [7] [18]. Por su parte, XGBoost combina rapidez con precisión elevada [10] [21], mientras que los árboles de decisión son útiles en entornos limitados, con resultados de hasta 92% [3] [13].

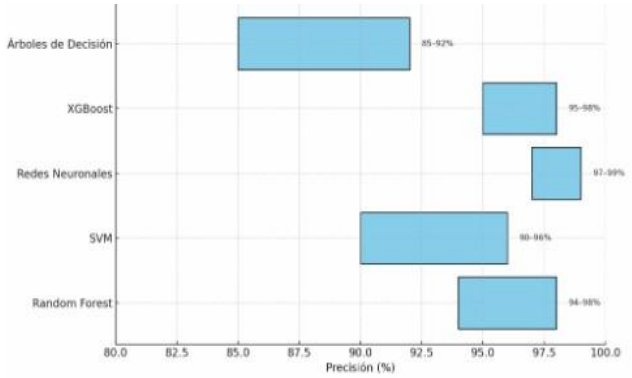

Fig. 9. Resultados de los modelos machine learning

L. *Demostración de los resultados de los modelos de machine learning empleados*

La evaluación de los modelos de machine learning aplicados a la detección de malware en el sector bancario se basó en pruebas controladas usando conjuntos de datos reales y simulados. Se emplearon técnicas de validación cruzada y métricas como precisión, tasa de detección y falsos positivos [1] [4] [7] [10] [13] [18] [21]. Herramientas como Scikit-learn, TensorFlow y Keras permitieron entrenar algoritmos como Random Forest, SVM y redes neuronales. Estas demostraciones confirmaron la eficacia de los modelos con precisiones superiores al 95% en la mayoría de los casos, respaldando su implementación en entornos financieros críticos [5] [10] [21].

IV. Discusión

La propagación de malware en el sector bancario se ha intensificado en los últimos años debido al incremento de la digitalización de los servicios financieros y a la creciente sofisticación de los ciberataques. Diversos estudios coinciden en que los tipos de malware más frecuentes en este sector incluyen los Banking Trojans, el Phishing y el Ransomware, acompañados de variantes más recientes como el QR Code Malware, el malware evasivo con IA y las Botnets para ataques DDoS [1], [4], [5], [10], [13], [18]. Todos ellos emplean técnicas avanzadas de ingeniería social para infiltrarse en los sistemas bancarios, siendo este patrón uno de los elementos más recurrentes en la literatura revisada [5], [7], [13], [21].

En respuesta, los investigadores han implementado diversos modelos de Machine Learning (ML) para mejorar la detección y prevención de malware, destacando cinco técnicas principales: Random Forest, Support Vector Machine (SVM), Redes Neuronales, Naive Bayes y K-Nearest Neighbors (KNN) [1], [4], [5], [7], [10]. Estos modelos han mostrado un desempeño positivo, especialmente en la clasificación de tráfico malicioso, identificación de patrones sospechosos y reducción de falsos positivos. Sin embargo, también presentan limitaciones técnicas que deben considerarse. Por ejemplo, SVM requiere ajustes manuales complejos de parámetros [4], Naive Bayes asume independencia entre características, lo cual no siempre es realista [7], y KNN tiene una alta carga computacional con grandes volúmenes de datos [10]. A pesar de estas limitaciones, el desempeño promedio en términos de precisión oscila entre 93% y 97%, lo que respalda su aplicabilidad práctica [13], [18], [21].

Además, algunos estudios han demostrado que la integración de modelos híbridos o el uso de enfoques como XGBoost y Deep Learning puede superar ciertos retos técnicos, especialmente cuando se entrena con datos reales del sector financiero [18], [21]. Estos modelos permiten una mejor generalización, especialmente frente a nuevos tipos de malware. No obstante, requieren una infraestructura tecnológica más robusta y un conjunto de datos debidamente curado, lo cual puede no estar disponible en todas las instituciones bancarias [10], [13], [18].

Otro punto crítico observado en la literatura es la falta de estándares comunes para la evaluación de modelos. Si bien algunos trabajos aplican métricas como la precisión, el recall o el F1-score [5], [13], [18], otros simplemente presentan análisis descriptivos o simulaciones, lo cual limita la comparación directa entre enfoques [1], [4], [7]. Por tanto, se recomienda unificar los criterios metodológicos en futuras investigaciones, lo que facilitaría el desarrollo de soluciones más confiables y transferibles al entorno bancario real.

En conjunto, los estudios analizados ofrecen una visión integral de los esfuerzos actuales por mitigar las amenazas de malware en el sector financiero mediante técnicas de inteligencia artificial, pero también revelan la necesidad de mayor estandarización, validación práctica y evaluación longitudinal para asegurar su efectividad a largo plazo [4], [5], [10], [13], [18], [21].

V. Conclusión

La presente revisión sistemática ha permitido identificar los principales tipos de malware que amenazan al sector bancario, así como los enfoques de detección basados en modelos de *machine learning* más utilizados. Se ha evidenciado que el *Banking Trojan*, el *Phishing*, el *Ransomware*, el malware con capacidades evasivas, los códigos QR maliciosos y las botnets son las amenazas más comunes, todas caracterizadas por su constante evolución y su capacidad para evadir medidas de seguridad tradicionales. Frente a este panorama, los modelos de *machine learning* representan una herramienta prometedora para fortalecer los mecanismos de defensa digital, permitiendo detectar patrones anómalos y anticipar comportamientos maliciosos con altos niveles de precisión.

Sin embargo, también se ha demostrado que estos modelos presentan limitaciones, tanto técnicas como prácticas, que deben ser consideradas antes de su implementación. La correcta elección del algoritmo, la calidad de los datos y la validación en entornos reales son aspectos críticos para su éxito. A pesar de los desafíos, el avance en técnicas híbridas y modelos más robustos abre nuevas oportunidades para mejorar la ciberseguridad bancaria. Por tanto, resulta esencial que futuras investigaciones se orienten a la identificación y evaluación de las tecnologías de machine learning más adecuadas para mitigar los ataques de malware en el sector bancario. Los hallazgos de esta revisión sistemática evidencian que los modelos más sólidos corresponden a Random Forest y a las Redes Neuronales Profundas (Deep Learning), destacando por su elevada precisión y notable capacidad de adaptación frente a amenazas emergentes.

REFERENCIAS

[1] O. K. Sahingoz, E. BUBEr, and E. Kugu, "DEPHIDES: Deep Learning based Phishing Detection System," IEEE Access, vol. 12, pp. 8052–8070, Jan. 2024, doi: 10.1109/access.2024.3352629.

[2] A. Alsadig, "Enhancing Cybersecurity in Financial Services using Single Value Neutrosophic Fuzzy Soft Expert Set," International Journal of Neutrosophic Science, vol. 24, no. 2, pp. 246–257, Jan. 2024, doi: 10.54216/ijns.240222.

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

[4] R. Rawat et al., "Malware threat Affecting Financial Organization Analysis using Machine Learning approach," International Journal of Information Technology and Web Engineering, vol. 17, no. 1, pp. 1–20, Aug. 2022, doi: 10.4018/ijitwe.304051.

[5] S. S. H. Shah, A. R. Ahmad, N. Jamil, and A. U. R. Khan, "Memory Forensics-Based malware detection using computer vision and machine learning," Electronics, vol. 11, no. 16, p. 2579, Aug. 2022, doi: 10.3390/electronics11162579.

[6] V. R. Shetty, P. R. y R. L. Malghan, "Safeguarding against Cyber Threats Machine Learning Based Approaches for Real Time Fraud Detection-and-Prevention-Engineering-Proceedings", MDPI, p. 111, diciembre de 2023, doi: 10.3390/engproc2023059111.

[7] A. Shahzadi, K. Ishaq, N. A. Nawaz, F. Rosdi, and F. A. Khan, "Unveiling personalized and gamification-based cybersecurity risks within financial institutions," PeerJ Computer Science, vol. 11, p. e2598, Feb. 2025, doi: 10.7717/peerj-cs.2598.

[8] C. Iscan, O. Kumas, F. P. Akbulut, and A. Akbulut, "Wallet-Based Transaction Fraud prevention through LightGBM with the focus on minimizing false alarms," IEEE Access, vol. 11, pp. 131465–131474, Jan. 2023, doi: 10.1109/access.2023.3321666.

[9] J. Liu, Z. Tian, R. Zheng, and L. Liu, "A Distance-Based method for building an encrypted malware traffic identification framework," IEEE Access, vol. 7, pp. 100014–100028, Jan. 2019, doi: 10.1109/access.2019.2930717.

[10] A. Gezer, G. Warner, C. Wilson, and P. Shrestha, "A flow-based approach for Trickbot banking trojan detection," Computers & Security, vol. 84, pp. 179–192, Mar. 2019, doi: 10.1016/j.cose.2019.03.013.

[11] B. Narsimha, C. V. Raghavendran, P. Rajyalakshmi, G. K. Reddy, M. Bhargavi, and P. Naresh, "Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application," International Journal of Electrical and Electronics Research, vol. 10, no. 2, pp. 87–92, Jun. 2022, doi: 10.37391/ijeer.100206.

[12] H. Manthena, S. Shajarian, J. Kimmell, M. Abdelsalam, S. Khorsandroo, and M. Gupta, "Explainable Artificial Intelligence (XAI) for Malware Analysis: A survey of techniques, applications, and open challenges," IEEE Access, p. 1, Jan. 2025, doi: 10.1109/access.2025.3555926.

[13] M. B. M. Mansour and Y. G. A. Abdelghaffar, "Machine Learning-Based Malware Detection and Malicious URL Classification System for detecting cyberattacks and achieving cybersecurity," International Journal of Fuzzy Logic and Intelligent Systems, vol. 25, no. 1, pp. 11–36, Mar. 2025, doi: 10.5391/ijfis.2025.25.1.11.

[14] S. Seraj et al., "MOBShield: A novel XML approach for securing mobile Banking," Computers, Materials & Continua/Computers, Materials & Continua (Print), vol. 79, no. 2, pp. 2123–2149, Jan. 2024, doi: 10.32604/cmc.2024.048914.

[15] S. M. Ali, A. Razzaque, M. Yousaf, and R. U. Shan, "An Automated Compliance Framework for Critical Infrastructure Security through Artificial Intelligence," IEEE Access, p. 1, Jan. 2024, doi: 10.1109/access.2024.3524496.

[16] V. Kanimozhi and T. P. Jacob, "Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," ICT Express, vol. 7, no. 3, pp. 366–370, Dec. 2020, doi: 10.1016/j.icte.2020.12.004.

[17] H. El-Taj, D. Hamedah, and R. Saeed, "Artificial intelligence and advanced cybersecurity to mitigate Credential-Stuffing attacks in the banking industry," International Journal of Computational and Experimental Science and Engineering, vol. 11, no. 1, Feb. 2025, doi: 10.22399/ijcesen.754.

[18] K. Al-Dosari, N. Fetais, and M. Kucukvar, "Artificial intelligence and Cyber Defense System for Banking industry: A Qualitative Study of AI Applications and Challenges," Cybernetics & Systems, vol. 55, no. 2, pp. 302–330, Aug. 2022, doi: 10.1080/01969722.2022.2112539.

[19] M. Carminati, R. Caron, F. Maggi, I. Epifani, and S. Zanero, "BankSealer: A decision support system for online banking fraud analysis and investigation," Computers & Security, vol. 53, pp. 175–186, Apr. 2015, doi: 10.1016/j.cose.2015.04.002.

[20] F. Ullah, S. Ullah, M. R. Naeem, L. Mostarda, S. Rho, and X. Cheng, "Cyber-Threat detection system using a hybrid approach of transfer learning and Multi-Model image representation," Sensors, vol. 22, no. 15, p. 5883, Aug. 2022, doi: 10.3390/s22155883.

[21] M. I. Jaya and M. F. Ab. Razak, "Dynamic ransomware detection for Windows platform using machine learning classifiers," JOIV International Journal on Informatics Visualization, vol. 6, no. 2–2, p. 469, Aug. 2022, doi: 10.30630/joiv.6.2-2.1093.

[22] D. R. Arikkat et al., "OSTIS: A novel Organization-Specific Threat Intelligence System," Computers & Security, vol. 145, p. 103990, Jul. 2024, doi: 10.1016/j.cose.2024.103990.

[23]H. a. M. Wahsheh y M. S. Al-Zahrani, "Sistema seguro de inteligencia computacional en tiempo real contra enlaces maliciosos de códigos QR", *Revista Internacional de Comunicaciones y Control de Computadores*, vol. 16, no. 3, mayo de 2021, doi: 10.15837/ijccc.2021.3.4186.

[24] H. Haya y S. Mishra, "El impacto de la ciberseguridad basada en IA en los sectores bancario y financiero", *Revista de Ciberseguridad y Gestión de la Información*, vol. 14, no. 1, pp. 08–19, enero de 2024, doi: 10.54216/jcim.140101.

[25] O. Kuzmenko, J. Kubálek, V. Bozhenko, O. Kushneryov, and I. Vida, "AN APPROACH TO MANAGING INNOVATION TO PROTECT FINANCIAL SECTOR AGAINST CYBERCRIME," *Polish Journal of Management Studies*, vol. 24, no. 2, pp. 276–291, Dec. 2021, doi: 10.17512/pjms.2021.24.2.17.

[26] Ş. Bahtiyar, M. B. Yaman, and C. Y. Altınığne, "A multi-dimensional machine learning approach to predict advanced malware," *Computer Networks*, vol. 160, pp. 118–129, Jun. 2019, doi: 10.1016/j.comnet.2019.06.015.

[27] A. Eskandarany, "Adoption of artificial intelligence and machine learning in banking systems: a qualitative survey of board of directors," *Frontiers in Artificial Intelligence*, vol. 7, Nov. 2024, doi: 10.3389/frai.2024.1440051.