Técnicas de protección contra malware impulsadas por IA en entorno móviles

AI-driven malware protection techniques in mobile environments

Recibido: octubre 17 de 2024 | Revisado: noviembre 04 de 2024 | Aceptado: noviembre 29 de 2024

Giovani Salcedo Quispe[1]
Leonardo Sacramento Benites[1]
Alberto Mendoza de los Santos[1]

Resumen

En la actualidad, los dispositivos móviles son una parte esencial de la vida diaria, lo que los convierte en un objetivo atractivo para ataques de malware. Las técnicas tradicionales de protección contra malware, aunque son efectivas, se enfrentan a crecientes desafíos debido a la evolución constante de las amenazas. Este artículo explora las técnicas de protección contra malware impulsadas por inteligencia artificial (IA) en entornos móviles, evaluando su eficacia en comparación con los métodos tradicionales. A través de un análisis sistemático de la literatura, se destacan las ventajas del uso de IA, como el aprendizaje automático y profundo, para mejorar la detección y mitigación de malware en dispositivos móviles. Además, se identifican las limitaciones y los desafíos de implementar estas técnicas avanzadas.

Palabras clave: nteligencia artificial; malware; dispositivos móviles; seguridad; aprendizaje automático; detección de malware

Abstract

Today, mobile devices are an essential part of daily life, making them an attractive target for malware attacks. Traditional malware protection techniques, while effective, face increasing challenges due to constantly evolving threats. This article explores artificial intelligence (AI)-powered malware protection techniques in mobile environments, evaluating their effectiveness compared to traditional methods. Through a systematic analysis of the literature, the advantages of using AI, such as machine and deep learning, to improve malware detection and mitigation on mobile devices are highlighted. Additionally, limitations and challenges of implementing these advanced techniques are identified.

Keywords: Artificial intelligence, malware, mobile devices, security, machine learning, malware detection

1 Universidad Nacional de Trujillo, Perú

Correo electrónico de contacto:
t1513300321@unitru.edu.pe

https://doi.org/10.24265/campus.2024.v29n38.04

Introducción

Con la reciente aparición de la inteligencia artificial en el mundo tecnológico, varias áreas se han visto afectadas por su influencia. Inherentemente, esta nueva tecnología está siendo utilizada para cometer múltiples delitos o ciberataques. Sin embargo, así como se le ha encontrado un uso para vulnerar datos y dispositivos, también se ha utilizado como método o como un producto para hacerle frente a estas amenazas. Poniendo el foco de atención en las aplicaciones móviles dado que estos medios tecnológicos son los dispositivos más utilizados en el país, se busca identificar los métodos que se están utilizando para la seguridad de los datos en los dispositivos móviles.

Conociendo el hecho de que ya existían varias formas de poder protegerse contra el malware en dispositivos móviles, siempre es bueno ver las opciones que ya existen, siendo alguna de ellas: Escaneo y Detección de Malware Basado en Firmas; Análisis Estático y Dinámico de Aplicaciones; y Sistemas de Detección de Intrusos Móviles (Mobile IDS).

Escaneo y detección de malware basado en firmas, se basa en el hecho de que el malware tiene su propia firma en un archivo de bits (signature), el cual ya está previamente identificado, por lo que el programa encuentra esta firma y luego la identifica (Venugopal & Hu, 2008). Sin embargo, tiene una debilidad muy grande, la cual está en su propia forma de trabajar; no puede hacer mucho contra una alguna nueva firma que no haya sido identificada en ese momento. Otra gran debilidad de esta técnica es que los propios desarrolladores del malware pueden hacer mínimos cambios a esta firma, volviéndola inútil.

El análisis estático analiza los datos que el programa proporciona pero sin la necesidad de ser instalado en el dispositivo o se ejecute (Esmail, 2023), proporcionando una evidente ventaja debido a que no pone en riesgo el dispositivo. Sin embargo, un código malicioso con varias capas de encriptación o un código ofuscado son una de las formas para poder superar esta barrera de seguridad (Bhan *et al.*, 2023), forzando a improvisar opciones más dinámicas.

Diferenciando con el análisis estático, el análisis dinámico necesita que el dispositivo se ejecute (Esmail, 2023), por lo que lo realiza de manera segura; a veces utilizando un sandbox o un entorno virtual aparte para que no afecte de verdad al dispositivo que se busca proteger. Sin embargo, se han tenido que enfrentar a desarrolladores de malware cada vez más preparados que plantearon formas de evitar que el programa fuese ejecutado en un entorno virtual aparte (Lee *et al.*, 2024), logrando así superar la barrera de seguridad de ese método.

Por otro lado, los Sistemas de Detección de Intrusos (IDS), trabajan en la red y están enfocados en los ataques DDOS, por ejemplo (Rahman *et al.*, 2023). Estos sistemas trabajan de distintas formas: fuera de línea y en tiempo real, siendo la gran diferencia entre ambas la ventaja en la frase "tiempo real" dado que las redes actuales son cada vez más rápidas y no se pueden dar el lujo de detenerse por un momento para analizar si los datos provienen de ataques o no. Aún así, el sistema no es perfecto, dado que a veces suele reportar falsas alarmas o

simplemente, falla en detectar el ataque, dejando vulnerable al dispositivo que se quiere proteger.

Entonces, con todo lo anterior puesto en escena, se puede plantear: ¿Cuáles son las técnicas impulsadas por IA para la protección contra malware en la seguridad de los datos en entornos móviles? y ¿Cómo estas técnicas mejoran la seguridad de los datos en entornos móviles en comparación con los métodos tradicionales?

Se consideraron los siguientes objetivos:

- Dar a conocer las nuevas técnicas de protección mejoradas con IA.
- Establecer una comparativa y poder determinar si hay una verdadera mejora después del apoyo en las IAs.

Método

Se llevó a cabo un análisis documental guiado por la metodología PRISMA para realizar una revisión sistemática. Las siguientes preguntas de investigación fueron formuladas como objetivos del estudio: ¿Cuáles son las técnicas impulsadas por IA para la protección contra malware en la seguridad de los datos en entornos móviles? y ¿Cómo estas técnicas mejoran la seguridad de los datos en entornos móviles en comparación con los métodos tradicionales?

Criterio de inclusión y exclusión

Como criterios de inclusión, se seleccionaron los artículos publicados entre 2021 y 2024, pertenecientes a las áreas de Ciencias de la Computación, Ingeniería y Ciencias de Materiales. Además, se consideró que los estudios incluyan los términos "Aprendizaje profundo", "Aplicaciones móviles", "Aprendizaje automático" y "Sistemas de aprendizaje". Los artículos debían estar disponibles en español o inglés para asegurar una revisión más completa.

Por otro lado, los criterios de exclusión contemplaron aquellos artículos que no detallaron de manera práctica el uso de las técnicas o que no tuvieran una relación clara entre las técnicas de protección y la IA. Para facilitar la comprensión, los criterios se resumen en la Tabla 1.

Tabla 1
Criterios de inclusion y exclusion

CRITERIOS DE INCLUSIÓN	CRITERIOS DE EXCLUSIÓN
Artículos publicados en el periodo de 2021 - 2024.	No se detalla de forma práctica el uso de la técnica.
Idioma en español o inglés	No existe una relación de la técnica de protección con IA.
Se muestra la aplicación de una tecnología y/o técnica IA.	

Recolección de datos

El proceso de búsqueda y recolección de datos se realizó utilizando una combinación de palabras clave como: "Encriptación", "Inteligencia Artificial", "Aprendizaje automático", "Dispositivos móviles" y "Aplicaciones móviles". Se empleó un enfoque riguroso y transparente para acceder a fuentes científicas, utilizando plataformas como SciELO y Scopus.

En SciELO, se utilizó el término de búsqueda "malware", obteniendo un total de 15 artículos, de los cuales, tras aplicar los criterios de inclusión y exclusión, se seleccionó uno.

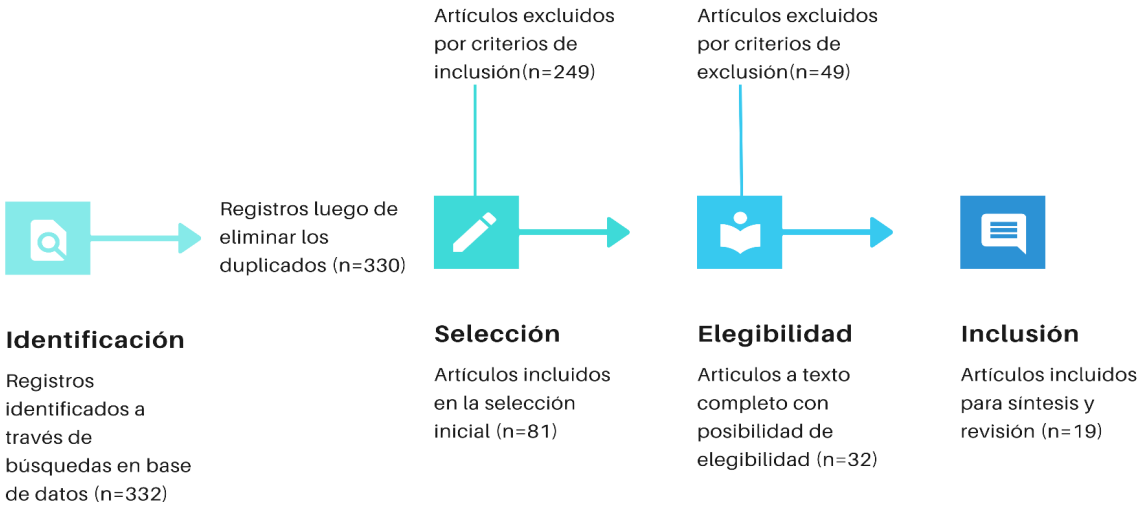
Para Scopus, se realizó una búsqueda avanzada con la siguiente cadena: "(TITLE-ABS-KEY ("end-to-end encryption" OR "asymmetric encryption" OR "symmetric encryption" OR "AES" OR "RSA" OR "Elliptic Curve Cryptography" OR "ECC" OR "multi-factor authentication" OR "MFA" OR "Diffie-Hellman" OR "homomorphic encryption" OR "public key cryptography" OR "tokenization" OR "TLS" OR "Transport Layer Security" OR "wireless network security" OR "data integrity" OR "cryptographic key management" OR "artificial intelligence" OR "AI-driven encryption" OR "machine learning encryption") AND TITLE-ABS-KEY ("mobile data protection" OR "mobile encryption" OR "mobile devices" OR "mobile applications" OR "mobile storage" OR "messaging encryption")) AND PUBYEAR > 2020 AND PUBYEAR < 2026 AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English") OR LIMIT-TO (LANGUAGE , "Spanish")) AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "MATE")) AND (LIMIT-TO (EXACTKEYWORD , "Mobile Applications") OR LIMIT-TO (EXACTKEYWORD , "Machine Learning") OR LIMIT-TO (EXACTKEYWORD , "Deep Learning") OR LIMIT-TO (EXACTKEYWORD , "Learning Systems") OR LIMIT-TO (EXACTKEYWORD , "Machine-learning"))". Esta búsqueda arrojó un total de 317 artículos, de los cuales se seleccionaron 18 tras aplicar los criterios de inclusión y exclusión, como se detalla en la Tabla 2.

Tabla 2
Bases de datos y artículos seleccionados

Bases de datos	Resultados	Seleccionados
Scopus	317	18
SciELO	15	1

Figura 1

*Proceso de selección de artículos / Flujograma PRISMA***Tabla 3**



Resultados

Con los artículos seleccionados y la posterior revisión, se obtuvieron resultados de cada uno de ellos y estos son presentados en la Tabla 3, donde se muestra el(los) autor(es), técnica, país y resultados.

Tabla 3

Resultados de artículos seleccionados

N.º	Autor(es)	Técnica	País	Resultados
1	(Poornima & Mahalakshmi, 2024)	Deep learning y Machine learning	India	La solución propuesta MAD-NET (Malware Attack Detection using Deep Belief Network) logró conseguir resultados de 99.83% utilizando varias métricas de rendimiento como precisión, recall, F1-score y exactitud.
2	Alkhtani, H; Aldhyani, T. H. H. (2022)	Soporte de máquina de vectores (SVM), k-nearest neighbors (KNN), Análisis de discriminación lineal (LDA), Redes Neuronales de Memoria a Largo Plazo (LSTM), red neuronal convolucional - memoria a largo y corto plazo (CNN-LSTM) y algoritmo de autocodificador.	Arabia Saudita	Muestra que las técnicas SVM, LSTM y CNN-LSTM son las que más eficiencia poseen al momento de detectar malware en entornos móviles.

3	Xing, Xiaofei *et al.* (2022)	Autocodificador en deep learning.	China	La idea propuesta por los autores demuestra ser muy superior a los demás métodos que utilizaron la misma técnica, teniendo un 96% de precisión en Android.
4	Faria, N., Gad, R., Unal, D., Al-Ali, A. K., & Suganthan, P. N. (2024)	Aprendizaje federado	Qatar	El artículo concluye que el aprendizaje federado es una técnica prometedora para la detección de malware en dispositivos móviles, ya que aborda los desafíos de privacidad y seguridad asociados con el entrenamiento de modelos en conjuntos de datos distribuidos. Además, destaca que, aunque presenta oportunidades, el aprendizaje federado también conlleva riesgos en cuanto a seguridad y plantea desafíos únicos debido a la arquitectura de los sistemas operativos móviles.
5	Vanjire, S. S., & Lakshmi, M. (2024)	Redes neuronales de convolución (CNN) y XAI	India	El enfoque combina CNN y técnicas de inteligencia artificial explicable (XAI), logrando una clasificación precisa de aplicaciones benignas y maliciosas en dispositivos Android. La integración de XAI proporciona explicaciones claras sobre las decisiones del modelo, facilitando la identificación de características críticas que determinan la maliciosidad de las aplicaciones.
6	Maray, M., Maashi, M., Alshahrani, H. M., Aljameel, S. S., Abdelbagi, S., & Salama, A. S. (2024)	Reconocimiento de Patrones Inteligente usando Optimizador de Equilibrio con Aprendizaje Profundo (IPR-EODL)	Arabia Saudita	El enfoque IPR-EODL mejora la detección y clasificación de malware en dispositivos Android, utilizando técnicas de aprendizaje profundo como redes neuronales recurrentes (RNN) y convolucionales (CNN) para identificar patrones de comportamiento en datos de aplicaciones. La técnica incluye el uso de atención del canal de memoria a largo plazo (CA-LSTM) y optimización de hiperparámetros con el algoritmo de Equilibrio (EO). Los resultados experimentales demuestran un desempeño significativo en la detección de malware, contribuyendo a la seguridad del ecosistema Android.
7	Jayagopalan, S., Alkhouli, M., & Aruna, R. (2023)	Modelo Keras Xception (KX-DLS) con esquema de cifrado simétrico de búsqueda dinámica (DSSE)	Emiratos Árabes Unidos	El enfoque KX-DLS permite la preservación de la privacidad en el contexto de sistemas de salud basados en IoT, asegurando que los datos de salud almacenados en la nube se analicen sin comprometer la información personal de los usuarios. El modelo ha mostrado una alta integridad de datos y pocas violaciones de privacidad, siendo más eficaz en comparación con técnicas de vanguardia anteriores. Este sistema es especialmente útil para dispositivos móviles con recursos limitados que requieren acceso a servicios de salud virtual en la nube.

8	CU, O. K., Gajendran, S., Bhavadharini, R. M., Suguna, M., & Krithiga, R. (2023)	Aprendizaje federado con DQRE-SCnet y cifrado homomórfico (FL-DQRE-SCnet)	India	El enfoque FL-DQRE-SCnet mejora la preservación de la privacidad de los registros de salud electrónicos (EHR) mediante el aprendizaje profundo y el intercambio de información, logrando una alta precisión en el diagnóstico de enfermedades. Este método minimiza las rondas de comunicación necesarias para la actualización del modelo global y garantiza la protección de datos mediante cifrado homomórfico. Los resultados muestran un rendimiento superior en comparación con métodos de referencia, alcanzando una precisión del 95%, una precisión de 94,9%, una recuperación del 94,94% y una medida F del 93,94%. Además, se obtuvo una tasa de error de 0,46 y un tiempo de ejecución de 1400 segundos.
9	Deng, X., Pei, X., Tian, S., & Zhang, L. (2022).	Marco de seguridad jerárquica para la detección de malware IIoT basado en computación de borde con un modelo Two-Stream Attention-Caps	China	Se propone un sistema de detección de malware que permite el análisis casi en tiempo real al descargar tareas de inteligencia artificial desde dispositivos móviles a servidores de borde. Este enfoque mejora la detección de malware, logrando un rendimiento superior al de los sistemas de última generación en cuatro conjuntos de datos de referencia. La estrategia de descarga computacional asegura un retraso mínimo, optimizando la coordinación de la detección entre múltiples usuarios.
10	(Iadarola *et al.*, 2021)	Deep learning	Italia	El sistema propuesto para detectar ciertos tipos de familia malware en los móviles utilizando deep learning obtuvo resultados del 96% al 97% de precisión en una muestra de 8446 móviles con Android.
11	(Bai *et al.*, 2021)	Selección automatizada de conjuntos de redes neuronales profundas (AES)	China	Se logró, de manera eficiente, que el algoritmo escoja los mejores DNN para mejorar el rendimiento de los dispositivos móviles en las situaciones que se requieran.
12	(Zeroual *et al.*, 2021)	Deep learning	Argelia	Al combinar el cifrado homomórfico con la combinación de LTP y deep learning logran adaptar el reconocimiento facial para dispositivos de bajos recursos, consiguiendo resultados al 98.7% de aprobación.
13	(Yi *et al.*, 2022)	Aprendizaje Federado (FL)	China	El método propone una solución para la seguridad de los datos en el aprendizaje federado utilizando las bases de un videojuego llamado Stackelberg, obteniendo resultados positivos en el equilibrio de Nash.

14	(Yoon, Kim, & Lee, 2022)	Machine learning	Corea del Sur	El método propone utilizar machine learning para la detección de reseñas falsas en aplicaciones, logrando así detectar aplicaciones maliciosas o no seguras. Logrando puntuaciones F1 promedio de 0.738 para reseñas falsas, 0.723 para reseñas reales y 0.730 en general, lo que indica un buen desempeño de los modelos de detección.
15	Bayazit, E. C., Sahingoz, O. K., & Dogan, B. (2023)	Aprendizaje profundo	Turquía	Se revisan técnicas de análisis estático y dinámico para la detección de malware en Android, destacando cómo los modelos de aprendizaje profundo se utilizan para mejorar la clasificación y detección de malware. El informe examina la arquitectura de Android, los conjuntos de datos empleados en la detección y los desafíos como el embalaje, la ofuscación y el cifrado de código por parte de los atacantes. Los resultados subrayan la necesidad de seguir investigando modelos avanzados para superar estas barreras de seguridad.
16	Aslam, N., Khan, I.U., Bader, S.A., Alansari, A., Alaqeel, L.A. *et al.* (2023)	Modelo de clasificación explicable basado en aprendizaje automático (ML), utilizando características de API y permisos, con técnicas de manejo de desequilibrio de datos como RandomOverSampler y explicabilidad con Shapley Values	Arabia Saudita	Se emplearon algoritmos de ML para la clasificación de aplicaciones, destacando el Extra Trees Classifier (ET), que alcanzó una precisión del 99.53% en la detección de malware con un tiempo de ejecución de solo 0.0198 segundos.
17	Sahoo, R. K., Pradhan, S., Sethi, S., & Udgata, S. K. (2023)	Aprendizaje automático (ML).	India	Se logró una precisión inicial del 99.79% con Random Forest para garantizar la integridad de los datos, mejorada al 100% usando análisis costo-beneficio en validación cruzada.
18	(Ma *et al.*, 2024)	Multilayer Perceptron (MLP) y Redes Neuronales Convolucionales (CNN)	China	Propone un proyecto llamado MCADS que busca detectar malware en el sistema operativo Android siendo más ligero, logrando alcanzar un 98.12% de precisión cuando fue puesto a prueba.
19	(AlSobeh *et al.*, 2024)	Marco de Aprendizaje Automático Consciente del Tiempo (TAML)	Jordania	El sistema propuesto logró alcanzar cifras muy prometedoras: En un entorno agnóstico al tiempo, el modelo logró una impresionante precisión con una puntuación F1 del 99.98%; y en experimentos conscientes del tiempo, que consideran los datos anuales, superan consistentemente a los modelos tradicionales, alcanzando una puntuación F1 media del 91% y una puntuación máxima del 99%.

Figura 2
Mapamundi de los artículos seleccionados

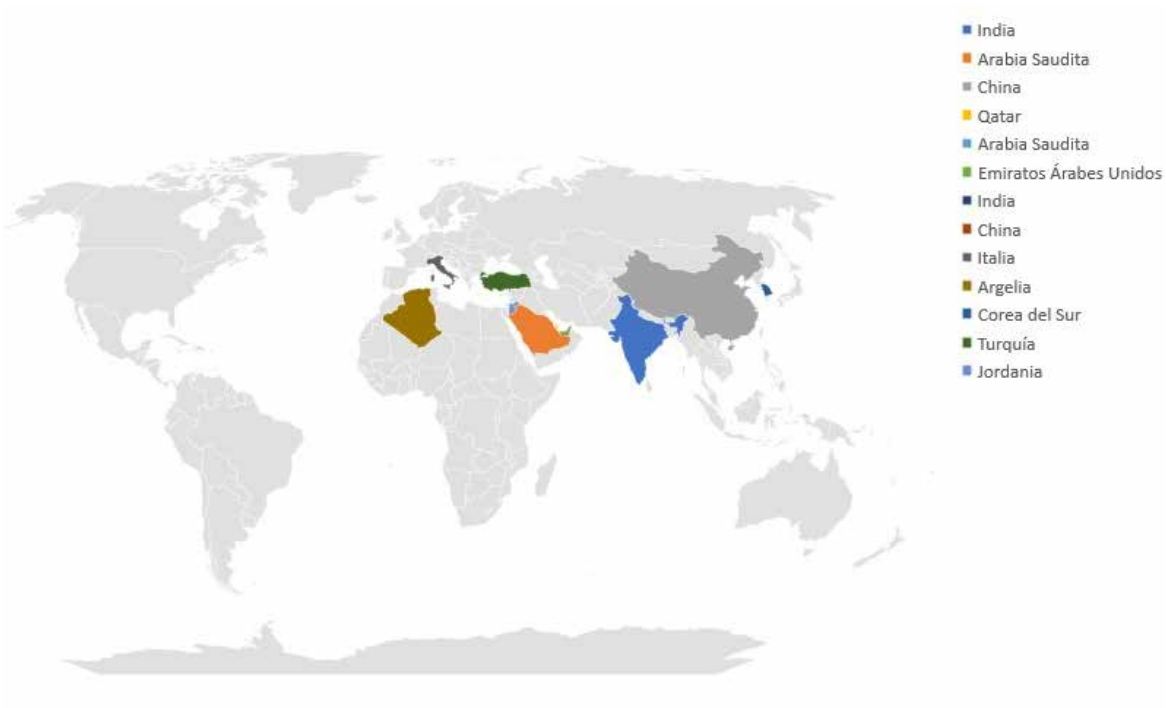


Figura 3
Gráfico de barras de las técnicas utilizadas en las propuestas

Discusión

La creciente amenaza de malware en dispositivos móviles ha llevado a un aumento significativo en la investigación de métodos de detección eficientes y precisos. Las técnicas basadas en aprendizaje automático y profundo han

demostrado ser fundamentales en esta lucha, aportando resultados prometedores. Por ejemplo, el trabajo de Poornima y Mahalakshmi (2024) demuestra que el modelo MAD-NET, que combina redes neuronales profundas, logra una precisión del 99.83% en la detección de malware, destacando la efectividad de los enfoques de deep learning en entornos móviles. Esto es consistente con los hallazgos de Iadarola *et al.* (2021), quienes reportaron precisiones entre 96% y 97% al aplicar deep learning en dispositivos Android, lo que resalta la robustez de estos métodos en la detección de malware.

Otro hallazgo importante proviene de Alkhtani *et al.* (2022), quienes observaron que las técnicas de SVM y LSTM, junto con CNN-LSTM, son particularmente efectivas para la detección de malware en entornos móviles. Esto sugiere que una combinación de métodos puede ofrecer resultados superiores en comparación con enfoques unidimensionales. Este enfoque híbrido es respaldado por Vanjire y Lakshmi (2024), que integran redes neuronales de convolución (CNN) con técnicas de inteligencia artificial explicable (XAI), mejorando la interpretación de los resultados del modelo y facilitando la identificación de características maliciosas en aplicaciones.

El aprendizaje federado se presenta como una alternativa prometedora, ya que aborda preocupaciones de privacidad al entrenar modelos en datos distribuidos. Faria *et al.* (2024) destacan que este enfoque no solo es efectivo en la detección de malware, sino que también se enfrenta a desafíos de seguridad únicos. Esto se alinea con los resultados de CU *et al.* (2023), quienes muestran que el aprendizaje federado, combinado con cifrado homomórfico, logra un balance entre precisión y privacidad, alcanzando tasas de precisión del 95% y 94.9% en la detección de enfermedades en registros de salud electrónicos.

A pesar de los logros, también se identifican desafíos significativos en la detección de malware. Bayazit *et al.* (2023) subrayan la necesidad de investigar más en modelos avanzados para superar obstáculos como la ofuscación y el empaquetado por parte de atacantes. La necesidad de sistemas que sean ligeros y eficientes también es un punto crítico, como lo demuestra el proyecto MCADS propuesto por Ma *et al.* (2024), que busca lograr una alta precisión (98.12%) mientras se mantiene la eficiencia en dispositivos con recursos limitados.

Finalmente, el trabajo de Aslam *et al.* (2023) sobre modelos de clasificación explicable resalta la importancia de no solo detectar el malware, sino también de entender cómo y por qué se toman las decisiones, lo que es esencial para la confianza del usuario en las tecnologías de detección. Este enfoque complementa los métodos tradicionales y ofrece una visión integral hacia el desarrollo de soluciones más efectivas en la lucha contra el malware en dispositivos móviles.

Conclusiones

Las técnicas de protección contra malware impulsadas por IA representan un avance significativo en la seguridad de dispositivos móviles. El aprendizaje automático y profundo, junto con técnicas como el aprendizaje federado, proporcionan herramientas efectivas para la detección y prevención de amenazas.

No obstante, la implementación de estas soluciones aún enfrenta desafíos, como la necesidad de equilibrar el consumo de recursos y la efectividad de la detección en dispositivos de baja capacidad. A medida que las amenazas evolucionan, las soluciones basadas en IA deben continuar desarrollándose para garantizar la seguridad de los datos en entornos móviles. Una estrategia prometedora es la combinación de estas técnicas con enfoques tradicionales, como la criptografía y la autenticación multifactor, para lograr una protección más robusta y completa.

De cara al futuro, es esencial continuar investigando la optimización del consumo de recursos, permitiendo que las soluciones basadas en IA sean más eficientes en dispositivos con limitaciones de hardware y energía sin comprometer su efectividad. Además, la IA debe seguir mejorándose para que sus modelos se adapten rápidamente a nuevas amenazas y reduzcan la tasa de falsos positivos.

Referencias

Alkahtani, H., & Aldhyani, T. H. H. (2022). Artificial Intelligence Algorithms for Malware Detection in Android-Operated Mobile Devices. Sensors, 22(6), 2268. https://doi.org/10.3390/s22062268

AlSobeh, A. M. R., Gaber, K., Hammad, M. M., Nuser, M., & Shatnawi, A. (2024). Android malware detection using time-aware machine learning approach. Cluster Computing. https://doi.org/10.1007/s10586-024-04484-6

Aslam, N., Khan, I.U., Bader, S.A., Alansari, A., Alaqeel, L.A. *et al.* (2023). Explainable classification model for android malware analysis using API and permission-based features. Computers, Materials & Continua, 76(3), 3167-3188. https://doi.org/10.32604/cmc.2023.039721

Bai, Y., Chen, L., Abdel-Mottaleb, M., & Xu, J. (2021). Automated Ensemble for Deep Learning Inference on Edge Computing Platforms. IEEE Internet Of Things Journal, 9(6), 4202-4213. https://doi.org/10.1109/jiot.2021.3102945

Bayazit, E. C., Sahingoz, O. K., & Dogan, B. (2023). Protecting Android Devices from Malware Attacks: A State-of-the-Art Report of Concepts, Modern Learning Models and Challenges. IEEE Access.https://doi.org/10.1109/ACCESS.2023.3323396

Bhan, R., Faruki, P., & Pamula, R. (2023). Detection of Sensitive Malicious Android Functionalities using Inter-component Control-flow Analysis. IEEE Access, 1-1. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3321383

Cinar, A. C., & Kara, T. B. (2023). The current state and future of mobile security in the light of the recent mobile security threat reports. Multimedia Tools And Applications, 82(13), 20269-20281. https://doi.org/10.1007/s11042-023-14400-6

CU, O. K., Gajendran, S., Bhavadharini, R. M., Suguna, M., & Krithiga, R. (2023). EHR privacy preservation using federated learning with DQRE-Scnet for healthcare application domains. Knowledge-Based Systems, 275, 110638. https://doi.org/10.1016/j.knosys.2023.110638

Deng, X., Pei, X., Tian, S., & Zhang, L. (2022). Edge-based IIoT malware detection for mobile devices with offloading. IEEE Transactions on Industrial Informatics, 19(7), 8093-8103.https://doi.org/10.1109/TII.2022.3216818

Esmail, H. M. (2023). Android Malware Detection and Protection Systems.

Jayagopalan, S., Alkhouli, M., & Aruna, R. (2023). Intelligent privacy preserving deep learning model for securing IoT healthcare system in cloud storage. J. Intell. Fuzzy Syst., 45(4), 5223-5238.https://doi.org/10.3233/JIFS-231713

Lee, S., Shin, Y., Choi, M., Cho, H., & Yi, J. H. (2024). Hybrid Dynamic Analysis for Android Malware Protected by Anti-Analysis Techniques with DOOLDA. Journal of Internet Technology, 25(2), Art. 2.

Ma, R., Yin, S., Feng, X., Zhu, H., & Sheng, V. S. (2024). A lightweight deep learning-based android malware detection framework. Expert Systems With Applications, 255, 124633. https://doi.org/10.1016/j.eswa.2024.124633

Maray, M., Maashi, M., Alshahrani, H. M., Aljameel, S. S., Abdelbagi, S., & Salama, A. S. (2024). Intelligent Pattern Recognition using Equilibrium Optimizer with Deep Learning Model for Android Malware Detection. IEEE Access.https://doi.org/10.1109/ACCESS.2024.3357944

Nawshin, F., Gad, R., Unal, D., Al-Ali, A. K., & Suganthan, P. N. (2024). Malware detection for mobile computing using secure and privacy-preserving machine learning approaches: A comprehensive survey. *Computers and Electrical Engineering*, *117*, 109233. https://doi.org/10.1016/j.compeleceng.2024.109233

Poornima, S., & Mahalakshmi, R. (2024). Automated malware detection using machine learning and deep learning approaches for android applications. Measurement Sensors, 32, 100955. https://doi.org/10.1016/j.measen.2023.100955

Sahoo, R. K., Pradhan, S., Sethi, S., & Udgata, S. K. (2023). Enhancing Data Integrity in Mobile Crowdsensing Environment with Machine Learning and Cost-Benefit Analysis. International

Journal of Computing and Digital Systems, 14(1), 1-1.http://dx.doi.org/10.12785/ijcds/140122

Vanjire, S. S., & Lakshmi, M. (2024). A novel method of detecting malware on Android mobile devices with explainable artificial intelligence. Bulletin of Electrical Engineering and Informatics, 13(3), 2019-2026.https://doi.org/10.11591/eei.v13i3.6986

Venugopal, D., & Hu, G. (2008). Efficient Signature Based Malware Detection on Mobile Devices. Mobile Information Systems, 4(1), 712353. https://doi.org/10.1155/2008/712353

Yi, Z., Jiao, Y., Dai, W., Li, G., Wang, H., & Xu, Y. (2022). A Stackelberg Incentive Mechanism for Wireless Federated Learning With Differential Privacy. *IEEE Wireless Communications Letters*, *11*(9), 1805-1809. https://doi.org/10.1109/lwc.2022.3181509

Xing, X., Jin, X., Elahi, H., Jiang, H., & Wang, G. (2022). A Malware Detection Approach Using Autoencoder in Deep Learning. IEEE Access, 10, 25696-25706. https://doi.org/10.1109/access.2022.3155695

Yoon, J., Kim, C., & Lee, J. (2022). Feature analysis for detecting mobile application review generated by AI-based language model. *Journal of Information Processing Systems*, 18(5), 650-660. https://doi.org/10.3745/JIPS.02.0182

Zeroual, A., Amroune, M., Derdour, M., & Bentahar, A. (2021). Lightweight deep learning model to secure authentication in Mobile Cloud Computing. Journal Of King Saud University - Computer And Information Sciences, 34(9), 6938-6948. https://doi.org/10.1016/j.jksuci.2021.09.016