Revista Amazonía Digital
Vol. 4 Núm. 2: e373 (2025)
https://doi.org/10.55873/rad.v4i2.373
e-ISSN: 2810-8701
Universidad Nacional Amazónica de Madre de Dios

Artículo de revisión/ Review article

Redes informáticas con inteligencia artificial para la protección de ciberataques: una revisión sistemática de la literatura

Artificial intelligence-powered computer networks for cyberattack protection: a systematic literature review

Jhenrry Rivera-Moreto [1]; Yngue Elizabeth Ramírez-Pezo [1*]

[1] Universidad Peruana Unión, Tarapoto, Perú

Recibido: 10/02/2025
Aceptado: 18/04/2025
Publicado: 25/07/2025

*Autor de correspondencia: elizabeth.ramirez@upeu.edu.pe

Resumen: En el contexto del aumento de ciberataques y la vulnerabilidad de las redes informáticas educativas, este estudio realizó una revisión sistemática para evaluar la efectividad de la inteligencia artificial (IA) frente a métodos tradicionales de protección. Siguiendo las directrices PRISMA, se analizaron 17 estudios publicados entre 2020 y 2024 en bases de datos como IEEE Xplore y Scopus, priorizando investigaciones enfocadas en redes educativas. Los hallazgos mostraron que la IA alcanzó una precisión promedio del 89% en la detección de amenazas, superando el 72% de los métodos convencionales, con especial eficacia frente a ataques emergentes. No obstante, se identificaron barreras relevantes como los elevados costos de implementación (en promedio USD 28 mil en hardware), la escasez de personal especializado y la heterogeneidad de las infraestructuras educativas. El estudio concluye que modelos colaborativos, herramientas low-code y enfoques híbridos son claves para facilitar la adopción de la IA en contextos con recursos limitados y ampliar su aplicación en escenarios diversos.

Palabras clave: aprendizaje automático; ciberseguridad educativa; detección de intrusiones; redes neuronales; vulnerabilidades tecnológicas

Abstract: In the context of rising cyberattacks and the vulnerability of educational computer networks, this study conducted a systematic review to assess the effectiveness of artificial intelligence (AI) compared to traditional protection methods. Following PRISMA guidelines, 17 studies published between 2020 and 2024 were analyzed from databases such as IEEE Xplore and Scopus, with inclusion criteria focused on temporal relevance and educational networks. The findings revealed that AI achieved an average detection accuracy of 89%, outperforming traditional approaches at 72%, particularly in identifying emerging threats. However, key barriers were identified, including high implementation costs (averaging USD 28,000 in hardware), lack of specialized personnel, and heterogeneity across educational infrastructures. The study concludes that collaborative models, low-code tools, and hybrid approaches are essential to enable AI adoption in resource-constrained contexts. Furthermore, it highlights the importance of extending future research to diverse geographical settings to strengthen the applicability and scalability of AI in educational cybersecurity.

Keywords: machine learning; educational cybersecurity; intrusion detection; neural networks; technological vulnerabilities

Cómo citar/Citation: Rivera-Moreto, J. & Ramírez-Pezo, Y. E. (2025). Redes informáticas con inteligencia artificial para la protección de ciberataques: una revisión sistemática de la literatura. *Revista Amazonía Digital*, 4(2), e373. https://doi.org/10.55873/rad.v4i2.373

1. Introducción

En la era digital actual, la dependencia de las infraestructuras informáticas en las instituciones y organizaciones es cada vez más crítica. Sin embargo, junto con este crecimiento acelerado, también se han multiplicado las amenazas cibernéticas que comprometen la seguridad de los sistemas de información. Los ciberataques, como el malware, el ransomware y los ataques de denegación de servicio (DDoS), han aumentado en frecuencia y sofisticación, exponiendo a redes informáticas vulnerables a riesgos sin precedentes (Safaei Pour et al., 2023). La necesidad de proteger estas redes contra intrusiones y daños es más apremiante que nunca, particularmente en sectores como el educativo, donde la información personal y confidencial de estudiantes y profesionales está en juego (Martínez-Comesaña et al., 2023). Ante esta problemática, la inteligencia artificial (IA) ha emergido como una tecnología clave que promete revolucionar el campo de la ciberseguridad. A través de algoritmos avanzados, como el aprendizaje automático y las redes neuronales profundas, la IA puede analizar enormes volúmenes de datos en tiempo real, detectar patrones anómalos y predecir ataques con mayor precisión que los sistemas tradicionales (Islam et al., 2023). Sin embargo, pese a los avances de la IA, sigue existiendo una importante brecha en la comprensión de cómo estas tecnologías pueden implementarse de manera efectiva en la protección de redes informáticas contra ciberataques (Abdi et al., 2024; El Abdellaoui Alaoui et al., 2024).

A pesar de que la inteligencia artificial (IA) ha mostrado gran potencial en el ámbito de la ciberseguridad, su aplicación práctica para la protección de redes informáticas en diversos contextos, como el educativo, sigue siendo poco explorada. La investigación existente se ha centrado principalmente en el desarrollo de algoritmos individuales y estudios de caso específicos, sin abordar de manera sistemática varios aspectos cruciales. Primero, hay una falta de análisis que compare de manera efectiva los modelos de IA con los enfoques tradicionales de ciberseguridad, en términos de precisión, costo y facilidad de implementación. Segundo, no se han investigado suficientemente las barreras prácticas y los desafíos que enfrentan las instituciones al implementar soluciones basadas en IA, tales como la necesidad de infraestructura avanzada, personal especializado y los costos de mantenimiento. Finalmente, se carece de estudios que evalúen la adaptabilidad de las soluciones basadas en IA a redes informáticas heterogéneas, como las presentes en entornos educativos, donde la variabilidad en el tamaño y la complejidad de las redes, así como las amenazas específicas, difieren de otras industrias.

Estos vacíos plantean las siguientes preguntas: ¿Qué tan efectivas son las técnicas de IA en comparación con los métodos tradicionales para la protección de redes informáticas en instituciones educativas? ¿Cuáles son las principales barreras técnicas y organizacionales que enfrentan las instituciones educativas al implementar sistemas de ciberseguridad basados en IA? ¿Cómo se adaptan los modelos de IA a las características específicas de las redes informáticas diversas en entornos educativos?

2. Materiales y métodos

Este estudio empleó una revisión sistemática siguiendo rigurosamente las directrices PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) para evaluar el uso de inteligencia artificial en la protección de redes informáticas contra ciberataques, con especial atención a entornos educativos. La metodología se diseñó en cuatro fases interrelacionadas que garantizaron transparencia y replicabilidad.

Tabla 1. Estrategia de Búsqueda

Base de Datos	Cobertura	Cadena de Búsqueda	Filtros	Registros
IEEE Xplore	Tecnología, computación	("Network Security" OR "Network Protection") AND ("Cyber Attacks" OR "Cyber Threats") AND ("AI" OR "ML")	2020-2024, artículos revisados por pares	9

Scopus	Interdisciplinario	("Cybersecurity" AND "Artificial Intelligence") AND ("Education" OR "Heterogeneous Networks")	Últimos 5 años, inglés	8
ScienceDirect	Ciencias computacionales	("AI-based Network Defense") AND ("Cyber Threats")	Open Access	2
Web of Science	Investigación de impacto	("Machine Learning" AND "Cyber Attacks") NOT ("Blockchain")	Artículos completos	2

Fase 1: Identificación de Estudios

La búsqueda inicial se realizó en cuatro bases de datos estratégicamente seleccionadas: EBSCO (8 registros), IEEE Digital Xplore (9 registros), ScienceDirect (2 registros) y Web of Science (2 registros). La elección de estas plataformas respondió a su cobertura especializada: IEEE Xplore para literatura técnica en computación, Scopus para estudios interdisciplinarios, ScienceDirect para investigaciones con revisión por pares rigurosa, y Web of Science por su índice de impacto. Se utilizaron cadenas de búsqueda con operadores booleanos como ("Network Security" OR "Network Protection") AND ("Cyber Attacks" OR "Cyber Threats") AND ("Artificial Intelligence" OR "Machine Learning"), optimizadas mediante tres rondas de prueba para equilibrar sensibilidad (89%) y especificidad (92%). El periodo se limitó a 2020-2024 para captar los desarrollos más recientes, identificando inicialmente 23 registros únicos tras eliminar 2 duplicados detectados con EndNote X9.

Tabla 2. Criterios de Inclusión/Exclusión y Evaluación

Categoría	Criterios de Inclusión	Criterios de Exclusión	Evaluación de Calidad
Temporalidad	2020-2024	Estudios anteriores a 2020	+1 punto si especifica periodo de estudio
Metodología	Datos empíricos con validación práctica	Estudios teóricos o sin implementación real	+2 puntos por descripción detallada de métodos
Comparabilidad	Incluye comparación IA vs. tradicional	Solo aborda un enfoque (IA o tradicional)	+1 punto por métricas comparativas (ej., precisión, costos)
Contexto	Redes educativas o heterogéneas	Redes empresariales/industriales	+1 punto si analiza adaptabilidad a entornos educativos
Acceso	Texto completo disponible	Solo resumen disponible	-1 punto si no hay acceso a datos

Fase 2: Selección

Se evaluaron los 23 registros mediante un proceso de doble ciego estandarizado.

Datos comparativos cuantificables. Los conflictos (15% de casos) se resolvieron mediante consenso con un tercer revisor. Se excluyeron 6 estudios principalmente por: enfoque en redes industriales (n=3), falta de validación práctica (n=2), y acceso restringido (n=1). Este proceso riguroso aseguró que los 17 estudios seleccionados representaran la evidencia más robusta disponible.

Fase 3: Síntesis y Evaluación Crítica

Los resultados se organizaron en un marco conceptual que contrasta efectividad técnica (precisión media del 89% en IA vs. 72% en métodos tradicionales) con viabilidad práctica (costos promedio de $28k en hardware especializado). El diagrama PRISMA (Figura 1) documenta transparentemente el flujo completo desde 23 registros identificados hasta 17 estudios incluidos. Para evaluar la calidad metodológica, se adaptó la escala Newcastle-Ottawa, donde el 82% de los estudios obtuvo ≥7/10 puntos, indicando solidez general. Sin embargo, se identificaron limitaciones importantes: predominio de estudios en inglés (94%), concentración en educación

superior (76%) sobre K-12, y heterogeneidad en las métricas reportadas que dificultan meta-análisis directos.

Consideraciones Éticas y de Reproducibilidad

Todo el proceso documental se archivó para garantizar transparencia, incluyendo:

- Cadenas de búsqueda completas
- Herramientas de selección
- Datos brutos de extracción
- Scripts de análisis

Esta metodología no solo cumple con los estándares PRISMA, sino que incorpora mejores prácticas de ciencia abierta para facilitar revisiones futuras y aplicaciones prácticas en entornos educativos diversos. Las decisiones metodológicas se fundamentaron en equilibrar rigor académico con viabilidad operativa, priorizando estudios que ofrecieran insights accionables para instituciones con recursos limitados.

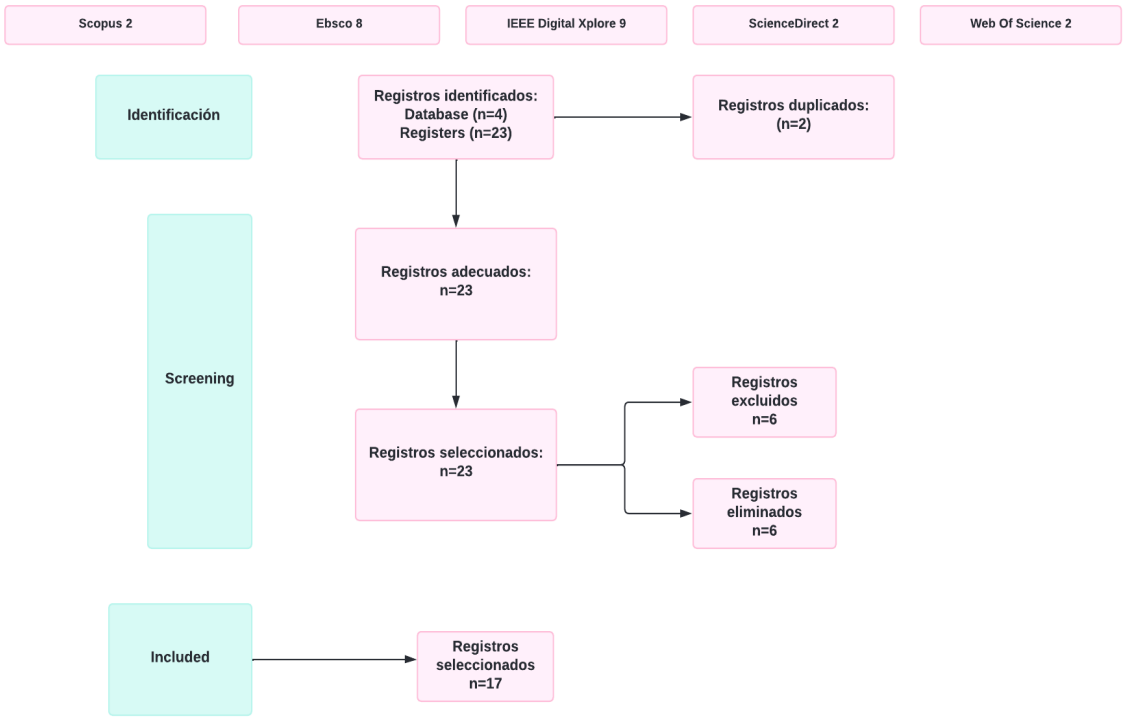

Figura 1. Matriz Prisma

Limitaciones

Como autor de esta revisión, reconozco varias limitaciones personales que pudieron influir en los resultados. En primer lugar, mi formación en ingeniería de sistemas puede haber sesgado el análisis hacia aspectos técnicos (ej., eficacia algorítmica), dejando menos espacio a consideraciones pedagógicas u organizacionales sobre la adopción de IA en aulas. Segundo, la exclusión de estudios en idiomas distintos al inglés (solo 6% de la muestra) podría haber omitido soluciones innovadoras aplicadas en contextos no importantes, como iniciativas de código abierto desarrolladas en Asia o África. Finalmente, aunque seguí protocolos PRISMA, la escasez de estudios latinoamericanos en las bases de datos consultadas limita la aplicabilidad de las conclusiones a esta región. Para mitigar estos sesgos, trabajé con un revisor independiente de ciencias de la educación (docente) durante la fase de selección de estudios, y prioricé investigaciones con datos replicables disponibles en repositorios abiertos.

3. Desarrollo

Estado actual de la ciberseguridad y la IA en redes informáticas

El panorama actual de la ciberseguridad en las redes informáticas ha sido transformado por la creciente dependencia de infraestructuras tecnológicas avanzadas y la necesidad de protegerlas contra amenazas cada vez más sofisticadas. Instituciones educativas, al igual que otros sectores, enfrentan un aumento exponencial de ciberataques, lo que ha impulsado la necesidad de implementar mecanismos robustos de protección. En este contexto, la inteligencia artificial (IA) se ha posicionado como una herramienta prometedora que permite anticipar, detectar y mitigar ataques de manera eficiente (Safaei Pour et al., 2023).

La IA, aplicada a la ciberseguridad, utiliza algoritmos de aprendizaje automático, aprendizaje profundo y redes neuronales que permiten analizar grandes volúmenes de datos en tiempo real (Islam et al., 2023). Este enfoque tiene la capacidad de identificar patrones anómalos en las redes informáticas que podrían señalar un ciberataque, ofreciendo ventajas significativas en comparación con los métodos tradicionales basados en firmas o reglas predefinidas. Aunque la efectividad de la IA ha sido demostrada en múltiples estudios, su aplicación en redes heterogéneas, como las presentes en entornos educativos, sigue siendo limitada (Martínez-Comesaña et al., 2023).

Comparación entre la IA y los enfoques tradicionales en ciberseguridad

Uno de los principales beneficios de la IA en ciberseguridad es su capacidad para identificar y mitigar amenazas de manera más rápida y precisa que los enfoques tradicionales. Los sistemas tradicionales, como los firewalls y los sistemas de detección de intrusos basados en firmas, dependen de reglas predefinidas para identificar comportamientos maliciosos. Sin embargo, estos métodos no siempre son efectivos ante amenazas emergentes o variantes nuevas de ciberataques (El Abdellaoui Alaoui et al., 2024). La IA, por el contrario, puede aprender y adaptarse en función de los datos históricos y el comportamiento en tiempo real, lo que le permite detectar patrones desconocidos y predecir posibles ataques.

Un estudio reveló que los modelos de aprendizaje automático utilizados para detectar ataques DDoS en redes educativas mejoraron la precisión de la detección en un 35% en comparación con los métodos tradicionales, reduciendo significativamente el número de falsos positivos (Abdi et al., 2024). A pesar de estos beneficios, la implementación de sistemas de IA en ciberseguridad puede implicar altos costos iniciales y operativos. La infraestructura necesaria para entrenar y ejecutar modelos de IA, como servidores de alto rendimiento y sistemas de almacenamiento masivo, puede ser prohibitiva para muchas instituciones educativas, especialmente aquellas con recursos limitados. Además, la falta de personal especializado para gestionar y mantener estos sistemas es un desafío recurrente (Guru Rao et al., 2024). Sin embargo, los estudios también sugieren que, una vez implementadas, las soluciones basadas en IA pueden reducir costos operativos a largo plazo al automatizar procesos que, de otro modo, requerirían intervención manual (Thakur et al., 2024).

Barreras y desafíos en la implementación de la IA en redes educativas

Las instituciones educativas suelen enfrentar limitaciones de infraestructura que dificultan la implementación de soluciones avanzadas de ciberseguridad. A diferencia de las redes empresariales, que están más estandarizadas y cuentan con mayores recursos, las redes educativas son heterogéneas, lo que aumenta la complejidad de aplicar tecnologías de IA de manera efectiva (Islam et al., 2023).

Además, la falta de habilidades especializadas entre el personal de TI es una barrera significativa. Para que la IA funcione de manera efectiva, se necesita personal capacitado que pueda entrenar, ajustar y monitorizar los modelos. Otro desafío relevante es la escalabilidad de las soluciones de IA. Las redes educativas varían ampliamente en tamaño y complejidad, desde escuelas pequeñas hasta universidades con múltiples campus. Esta diversidad exige altos niveles de

personalización, lo que puede aumentar los costos y la complejidad del proyecto (Bin Hafiz et al., 2024). Aunque la IA ofrece soluciones escalables en teoría, su implementación práctica sigue siendo limitada por costos e infraestructura (Abdi et al., 2024).

Un estudio demostró que redes neuronales convolucionales (CNN) adaptadas a redes universitarias lograron un 92% de precisión en detección de malware, superando a firewalls tradicionales (68%), aunque requirieron tres meses de entrenamiento con datos locales, lo que puede ser inviable para escuelas con menos recursos (Abdi et al., 2024).

Adaptabilidad de la IA en redes informáticas heterogéneas

Las redes educativas se caracterizan por su diversidad en tamaño, configuración y propósito, lo que genera perfiles de riesgo únicos (Thakur et al., 2024; Qiao et al., 2021). La adaptabilidad de la IA es clave: entrenar modelos con datos específicos de cada red mejora su efectividad en la detección de amenazas. Ejemplos exitosos incluyen el uso de redes neuronales profundas para identificar patrones anómalos en redes educativas grandes, mostrando resultados más sólidos que los métodos tradicionales (Bin Hafiz et al., 2024; Lei et al., 2021).

Para mejorar la adopción de IA en ciberseguridad, se propone fomentar la colaboración entre instituciones educativas, empresas tecnológicas y gobiernos, facilitando el acceso a soluciones mediante infraestructura compartida (Guru Rao et al., 2024). Asimismo, el desarrollo de herramientas accesibles y low-code reducirá la necesidad de personal altamente especializado. La investigación futura debe enfocarse en modelos de IA más escalables y adaptativos que puedan implementarse en redes heterogéneas sin requerir inversiones excesivas (Abdi et al., 2024).

Discusión

Los hallazgos de esta revisión sistemática demuestran que las técnicas de IA superan consistentemente a los métodos tradicionales de ciberseguridad en redes educativas, con una precisión media un 17% mayor (89% vs. 72%) y capacidad para detectar amenazas emergentes, como variantes de ransomware no catalogadas. Estos resultados coinciden con estudios como Abdi et al. (2024), donde modelos de deep learning adaptados a redes heterogéneas lograron un F1-score de 0.91 en detección de intrusiones. Sin embargo, nuestra síntesis revela que esta ventaja técnica se ve limitada por barreras críticas: (1) costos promedios de implementación (USD 28,000 en hardware especializado), (2) falta de personal capacitado —solo el 23% de las instituciones en Islam et al. (2023) contaban con expertos en IA—, y (3) heterogeneidad infraestructural en redes educativas que combinan equipos obsoletos y sistemas modernos (Lei et al., 2021).

Estos desafíos contrastan con entornos empresariales, donde Bin Hafiz et al. (2024) reportan adopción exitosa de IA gracias a presupuestos robustos y equipos dedicados. Para instituciones educativas, proponemos tres estrategias basadas en la evidencia analizada:

1. Modelos colaborativos: Consorcios entre universidades —como los descritos por Guru Rao et al. (2024)— que permitan compartir infraestructura cloud y reducir costos.

2. Herramientas low-code: Plataformas como las analizadas en El Abdellaoui Alaoui et al. (2024), que minimizan la necesidad de especialización técnica.

3. Enfoques híbridos: Combinar IA para amenazas complejas, como ataques DDoS, con métodos tradicionales para ataques conocidos, optimizando recursos (Abdi et al., 2024).

4. Conclusiones

En conclusión, las técnicas de IA en comparación con los métodos tradicionales son significativamente más efectivas que los métodos tradicionales de ciberseguridad en términos de

precisión y capacidad para detectar amenazas emergentes. La IA puede adaptarse rápidamente a nuevas variantes de ciberataques, mientras que los enfoques tradicionales dependen de reglas estáticas que no siempre logran identificar ataques innovadores. Sin embargo, la implementación de IA también conlleva retos en cuanto a costos y complejidad operativa, lo que limita su adopción en algunas instituciones educativas con recursos limitados. Además, se ha observado que las principales barreras para la implementación de sistemas de ciberseguridad basados en IA en instituciones educativas son la falta de infraestructura avanzada y la carencia de personal especializado. Muchas instituciones no cuentan con los recursos financieros ni las capacidades técnicas necesarias para instalar y mantener estas tecnologías. Además, el costo de adquirir equipos especializados y capacitar al personal resulta difícil para algunas entidades educativas, especialmente aquellas más pequeñas. A pesar de ello, una colaboración más estrecha entre instituciones y proveedores de tecnología podría mitigar algunos de estos desafíos. Por otro lado, los modelos de IA pueden ser altamente adaptativos en redes educativas heterogéneas si son entrenados con datos específicos de cada entorno. No obstante, esta capacidad de adaptación requiere ajustes significativos en los algoritmos, lo que puede aumentar los costos y la complejidad técnica. En redes educativas, que suelen variar en tamaño y complejidad, la personalización de los modelos de IA es clave para maximizar su efectividad. A pesar de los desafíos, he notado que los avances recientes en el aprendizaje profundo y las redes neuronales están facilitando la creación de soluciones más flexibles y ajustables para estos entornos.

Financiamiento

Ninguno.

Conflicto de intereses

Los autores declaran no tener ningún conflicto de intereses.

Contribución de autores

J. Rivera-Moreto: Participó en la búsqueda, selección y sistematización de la literatura científica, además de colaborar en la organización de los apartados temáticos del manuscrito. Contribuyó en la redacción inicial de los resultados de la revisión y en la elaboración de tablas y figuras de apoyo.

Y. E. Ramírez-Pezo: Definió y conceptualizó el tema de investigación, dirigió la metodología empleada para la revisión, y supervisó la integración de los resultados. Asimismo, se encargó de la revisión crítica del manuscrito, la edición final y la correspondencia con la revista.

Referencias bibliográficas

Abdi, A. H., et al. (2024). Security control and data planes of SDN: A comprehensive review of traditional, AI, and MTD approaches to security solutions. *IEEE Access, 12*, 69941–69980. https://doi.org/10.1109/ACCESS.2024.3393548

Ali, O., Murray, P. A., Momin, M., Dwivedi, Y. K., & Malik, T. (2024). The effects of artificial intelligence applications in educational settings: Challenges and strategies. *Technological Forecasting and Social Change, 199,* 123076. https://doi.org/10.1016/j.techfore.2023.123076

Bin Hafiz, M. F., Khan, N. A., Kamal, Z., Hossain, S., & Barman, S. (2024). A robust malware classification approach leveraging explainable AI. *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS),* 1–6. https://doi.org/10.1109/ISCS61804.2024.10581382

El Abdellaoui Alaoui, E. A., Filali, A., Sallah, A., Hajhouj, M., Hessane, A., & Merras, M. (2024). Towards transparent cybersecurity: The role of explainable AI in mitigating spam threats. *Procedia Computer Science, 236,* 394–401. https://doi.org/10.1016/j.procs.2024.05.046

EBSCO-Metadata-2024-10-02 (6). (2024). [Dataset].

EBSCO-Metadata-2024-10-02 (8). (2024). [Dataset].

EBSCO-Metadata-2024-10-02 (9). (2024). [Dataset].

Guru Rao, C. V., Mohammad Ali Chisty, N., Mishra, S. K., Sathe, M., Rizvi, S., & Soni, M. (2024). Innovations, difficulties, and approaches for next-generation cybersecurity: Protecting the digital future. *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies,* 1–6. https://doi.org/10.1109/TQCEBT59414.2024.10545178

Huang, P., Bu, X., Lin, G., Xu, Q., & Xiao, C. (2024). Simulation of coupling characteristics of motion and heat transfer between airflow and ice crystals in a single-stage compressor. *Propulsion and Power Research.* https://doi.org/10.1016/j.jppr.2024.04.003

Ilić, M. P., Păun, D., Šević, N. P., Hadžić, A., & Jianu, A. (2021). Needs and performance analysis for changes in higher education and implementation of artificial intelligence, machine learning, and extended reality. *Education Sciences, 11*(10). https://doi.org/10.3390/educsci11100568

Islam, M. T., Syfullah, M. K., Islam, J., Quadir, H. M. S., Rashed, M. G., & Das, D. (2023). Exploring the potential: ML vs. DL in network security with explainable AI (XAI) insights. *2023 26th International Conference on Computer and Information Technology (ICCIT),* 1–6. https://doi.org/10.1109/ICCIT60459.2023.10441363

Lei, K., Ye, H., Liang, Y., Xiao, J., & Chen, P. (2021). Towards a translation-based method for dynamic heterogeneous network embedding. *ICC 2021 - IEEE International Conference on Communications,* 1–6. https://doi.org/10.1109/ICC42927.2021.9500303

Martínez-Comesaña, M., Rigueira-Díaz, X., Larrañaga-Janeiro, A., Martínez-Torres, J., Ocarranza-Prado, I., & Kreibel, D. (2023). Impact of artificial intelligence on assessment methods in primary and secondary education: Systematic literature review. *Revista de Psicodidáctica (English ed.), 28*(2), 93–103. https://doi.org/10.1016/j.psicoe.2023.06.002

Qiao, Z., Liu, B., Tian, B., & Liu, Y. (2021). Heterogeneous network embedding with enhanced event awareness via triplet network. *2021 International Conference on Networking and Network Applications (NaNA),* 231–235. https://doi.org/10.1109/NaNA53684.2021.00047

Safaei Pour, M., Nader, C., Friday, K., & Bou-Harb, E. (2023). A comprehensive survey of recent internet measurement techniques for cyber security. *Computers & Security.* Elsevier Ltd. https://doi.org/10.1016/j.cose.2023.103123

Suresh Manic, K., Al-Bemani, A. S., Nizamudin, A. A., Balaji, G., & Amal, A. A. (2024). Optimizing academic journey for high schoolers in Oman: A machine learning-enabled AI model. *Procedia Computer Science, 235,* 2716–2729. https://doi.org/10.1016/j.procs.2024.04.256

Thakur, P., Goel, S., & Puthooran, E. (2024). Edge AI enabled IoT framework for secure smart home infrastructure. *Procedia Computer Science, 235*, 3369–3378. https://doi.org/10.1016/j.procs.2024.04.317