Ingeniería Investiga

Vol. 6, e1022, año 2024
ISSN – Online: 2708-3039
DOI: https://doi.org/10.47796/ing.v6i00.1022

Artículo de revisión

Las principales herramientas de Inteligencia Artificial para el control de acceso: una revisión sistemática

The Main Artificial Intelligence Tools for Access Control: A Systematic Review

Joan Rodriguez-Asto[1]
https://orcid.org/0000-0002-8006-1182

Segundo Samana-Rodríguez[2]
https://orcid.org/0009-0000-9298-8236

Alberto Carlos Mendoza de los Santos[3]
https://orcid.org/0000-0002-0469-915X

Recibido: 02/10/2024
Aceptado: 03/11/2024
Publicado: 13/11/2024

[1,2]Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, La Libertad, Perú
[3]Departamento de Ingeniería de Sistemas, Universidad Nacional de Trujillo, La Libertad, Perú

E-mail: [1]jrodriguezas@unitru.edu.pe, [2]ssamana@unitru.edu.pe, [3]amendozad@unitru.edu.pe

Facultad de Ingeniería
Publicación Oficial

Resumen

La creciente digitalización y automatización de sistemas incrementa la necesidad de métodos de control de acceso más avanzados y seguros. El objetivo del estudio fue identificar y sintetizar las principales herramientas de inteligencia artificial (IA) utilizadas en el control de acceso, mediante una revisión de la literatura en bases de datos como Scopus, SciELO y IEEE Xplore, empleando la metodología PRISMA y el software VOSviewer. El análisis bibliométrico destacó el liderazgo investigativo de China, India, Estados Unidos y Corea del Sur, así como términos clave como *machine learning*, *deep learning*, criptografía y biometría, junto a tecnologías emergentes como *blockchain* e IoT, que prometen revolucionar el sector de seguridad. En el análisis sistemático, *machine learning* y *deep learning* surgieron como las técnicas más aplicadas en control de acceso, siendo la lógica difusa y las redes neuronales especialmente efectivas. Las herramientas de IA facilitan el reconocimiento de patrones de comportamiento y la previsión de riesgos, y tecnologías como *blockchain* aportan transparencia y confiabilidad en la gestión de datos sensibles. Sin embargo, desafíos como el alto costo, la necesidad de grandes volúmenes de datos y las preocupaciones de privacidad limitan su implementación. Se sugiere optimizar IA, reducir dependencia de datos y explorar métodos híbridos para mejorar seguridad, transparencia y eficiencia en control de acceso, promoviendo una adopción más amplia de estas tecnologías.

Palabras clave: control de acceso; IA; sistemas de seguridad; tecnología de la información.

Abstract

The growing digitalization and automation of systems increase the need for more advanced and secure access control methods. The study aimed to identify and synthesize the main artificial intelligence (AI) tools used in access control through a literature review of databases such as Scopus, SciELO, and IEEE Xplore, using the PRISMA methodology and VOSviewer software. The bibliometric analysis highlighted the research leadership of China, India, the United States, and South Korea, as well as key terms like machine learning, deep learning, cryptography, and biometrics, alongside emerging technologies such as blockchain and IoT, which promise to revolutionize the security sector. In the systematic analysis, machine learning and deep learning emerged as the most applied techniques in access control, with fuzzy logic and neural networks proving particularly effective. AI tools facilitate behavior pattern recognition and risk prediction, while technologies like blockchain provide transparency and reliability in managing sensitive data. However, challenges such as high costs, the need for large data volumes, and privacy concerns limit implementation. It is suggested to optimize AI, reduce data dependency, and explore hybrid methods to improve security, transparency, and efficiency in access control, promoting wider adoption of these technologies.

Keywords: access control; AI; security systems; information technology.

1. Introducción

En las últimas décadas, el avance de la tecnología ha transformado múltiples aspectos de la vida cotidiana, desde la forma en que las personas se comunican hasta cómo gestionan la seguridad en sus entornos (Mothino y Cavique, 2023). En este contexto, la inteligencia artificial (IA) se presenta como una herramienta influyente que impulsa una amplia gama de industrias. Dentro de esta variedad de innovaciones, el control de acceso se destaca como uno de los campos que experimenta mejoras significativas debido a la IA. Este concepto abarca desde la protección física de instalaciones y edificios hasta el acceso a sistemas informáticos y redes virtuales. A medida que las amenazas a la seguridad evolucionan, lo hacen también las estrategias y tecnologías diseñadas para mitigar estos riesgos. La IA, con su capacidad de aprendizaje automático y adaptación continua, resulta esencial en la creación de sistemas de control de acceso más seguros y eficientes (Kaur et al., 2023).

Tradicionalmente, los sistemas de control de acceso se fundamentaban en métodos como contraseñas, tarjetas magnéticas o códigos de acceso, que, aunque efectivos en su momento, presentan limitaciones importantes en cuanto a seguridad y conveniencia (Psarra et al., 2024). Las vulnerabilidades de estos métodos convencionales fueron expuestas mediante ataques cibernéticos y físicos, lo que llevó a la búsqueda de soluciones más avanzadas. Es en este contexto donde la IA ha adquirido protagonismo. Con la capacidad de procesar grandes volúmenes de datos, identificar patrones y aprender de manera continua, los sistemas de IA aportan soluciones más seguras y personalizadas para el control de acceso (Rubio-Medrano et al., 2024). Uno de los avances significativos en este ámbito fue la incorporación del reconocimiento facial y otras modalidades biométricas. Estos sistemas basados en IA no solo identifican características físicas de los individuos, sino que también analizan aspectos de su comportamiento, añadiendo una capa adicional de seguridad (El-Bandy et al., 2024). La biometría demuestra claras ventajas frente a los métodos tradicionales. Por ejemplo, mientras que una tarjeta de acceso puede ser robada o una contraseña deducida, las características biométricas, como el reconocimiento facial o de huellas dactilares, son únicas para cada persona, dificultando considerablemente la suplantación de identidad. Además, se observan mejoras significativas en la precisión de estos sistemas, ya que la IA reduce los falsos positivos y negativos gracias a su capacidad de aprendizaje y perfeccionamiento (Ogbanufe y Kim, 2018).

No obstante, aunque las aplicaciones de IA en el control de acceso resultan favorablemente, también presentan desafíos. Uno de los más relevantes es la privacidad. Al implementar sistemas de reconocimiento facial o análisis de comportamiento, surge la preocupación sobre el posible uso indebido de los datos personales. Las organizaciones deben garantizar que las tecnologías empleadas para mejorar la seguridad no comprometan los derechos de privacidad de los individuos, lo que genera la necesidad de regulaciones más estrictas que equilibren la seguridad con la privacidad (Arguelles y Amaro, 2022). En particular, el uso de datos biométricos plantea riesgos adicionales en cuanto a la privacidad y el manejo de información personal, lo que exige la implementación de medidas que minimicen el impacto sobre los derechos individuales (Lucero et al., 2020). Además de las inquietudes sobre la privacidad, se presentan desafíos técnicos. La implementación de sistemas de IA para el control de acceso exige una inversión considerable en infraestructura y mantenimiento. Pese a los avances en precisión, aún persisten problemas como el sesgo algorítmico, que afecta la equidad y confiabilidad de estos sistemas, lo cual podría tener implicaciones sociales y éticas relevantes.

Por lo tanto, el objetivo del estudio fue identificar y sintetizar las principales herramientas de inteligencia artificial utilizadas en el control de acceso entre los años 2019 y 2024. Así como, analizar su efectividad, aplicaciones, desafíos y tendencias emergentes en el campo que facilite la adopción de tecnologías más seguras y efectivas en el futuro.

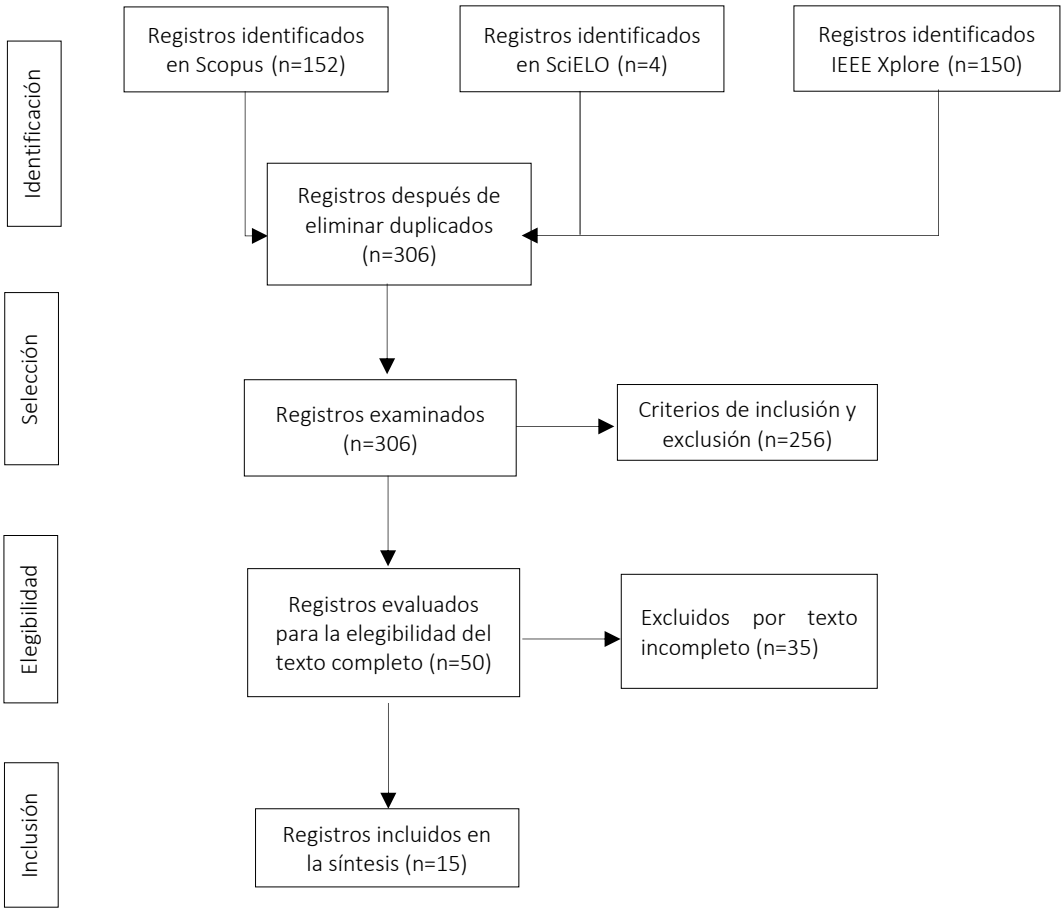
2. Metodología

Para llevar a cabo la búsqueda de los artículos, se empleó la metodología PRISMA, la cual, según Cajal et al. (2020), es una herramienta diseñada principalmente para informar sobre revisiones sistemáticas de estudios aleatorizados, aunque también es útil para estudios no aleatorizados. Por otro lado, Page et al. (2021) menciona que la declaración PRISMA es por sus siglas en ingles *Preferred Reporting Items for Systematic reviews and Meta-Analyses*, y que puede ofrecer un resumen del estado actual del conocimiento en un área específica, lo cual permite identificar prioridades para futuras investigaciones.

La recolección de datos se realizó el 25 de septiembre del 2024, a partir de búsquedas en tres bibliotecas digitales: Scopus, SciELO y IEEE Xplore, utilizando los siguientes términos relacionados con el objetivo de la investigación: "inteligencia artificial", "control de acceso", "artificial intelligence", "access control". Luego, se siguió el diagrama de flujo de PRISMA, así como se aprecia en la Figura 1, donde se indica el número de registros identificados, incluidos y excluidos, y las razones de exclusión.

Figura 1

Secuencia metodológica mediante el diagrama de flujo PRISMA



Mientas que la Tabla 1, presenta las diferentes bases de datos empleados para el estudio, junto a sus respectivas ecuaciones de búsquedas avanzadas y el operador booleano AND. Los resultados detallan el número de artículo encontrados y seleccionados para el análisis correspondiente. Una vez recopilados los documentos se procedió al proceso de filtración, utilizando los siguientes criterios de inclusión y exclusión, presentados en la Tabla 2. Además, se evaluaron los criterios de calidad, con el objetivo de realizar el último filtro, se evaluó si las investigaciones cumplían con un objetivo claro y que guarde relación, resultados que presentan respecto a las principales herramientas de IA para el control de acceso, y que las conclusiones de los estudios respondan al objetivo.

Tabla 1

Términos de búsqueda de diferentes bases de datos

Base de dato	Ecuaciones de búsqueda	Resultados	Seleccionados
Scopus	(Title-Abs-Key ("artificial intelligence") AND Title-Abs-Key ("access control")) AND Pubyear > 2018 AND Pubyear < 2024 AND (Limit-To (Doctype, "ar")).	152	10
SciELO	(artificial intelligence) AND (access control).	4	1
IEEE Xplore	("All Metadata": artificial intelligence) AND ("All Metadata": access control).	150	4

Tabla 2

Criterios evaluados

Criterios de inclusión	Criterios de exclusión
Estudios que aborden herramientas de inteligencia artificial para control de acceso.	Artículos publicados fuera del rango de 2019 a 2024.
Documentos con contenido relevante que responda a la pregunta de investigación.	Documentos que no sean de tipo artículo original.
Artículos escritos en español, chino, portugués e inglés.	Estudios que estén fuera del área tecnológica.

Por otro lado, para el análisis bibliométrico de los artículos seleccionados se empleó la herramienta VOSviewer, diseñada para construir y visualizar mapas bibliométricos basados en redes de publicaciones, autores o términos. Su objetivo es mejorar la interpretación visual de los datos bibliométricos, facilitando el análisis de co-citación, co-ocurrencia de palabras clave y otros aspectos mediante representaciones gráficas claras y adaptables. Estas visualizaciones ayudan a identificar relaciones clave y temas influyentes en un campo de investigación, proporcionando una comprensión más profunda del contenido bibliográfico (van Eck y Waltman, 2010).

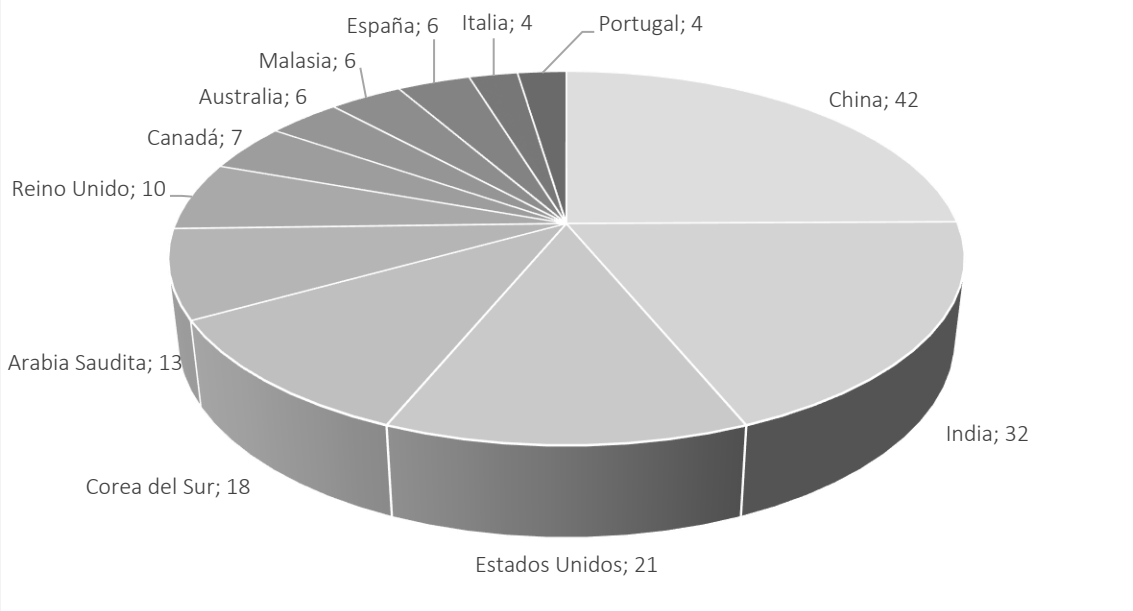
3. Resultados

3.1. Análisis bibliométrico

La Figura 2 presenta la distribución de publicaciones, destacando la participación de varios países. En primer lugar, China se posiciona como líder con 42 publicaciones, lo que indica un fuerte enfoque en el desarrollo y aplicación de tecnologías avanzadas en el ámbito de la seguridad y el control de acceso. Además, esto sugiere que China no solo está a la vanguardia en la investigación, sino que también está implementando soluciones innovadoras que podrían influir en el futuro del control de acceso a nivel global. India sigue como segundo con 32 publicaciones, evidenciando su creciente interés en esta área, mientras que Estados Unidos ocupa el tercer lugar con 21 publicaciones, subrayando su relevancia histórica en el ámbito tecnológico. Así mismo, dos de las naciones son consideradas potencias mundiales. Corea del Sur sigue de cerca, con 18 publicaciones, evidenciando su compromiso con la innovación en tecnologías de inteligencia artificial. Por otro lado, Arabia Saudita muestra un creciente interés en esta área con 13 publicaciones, lo que puede estar vinculado a sus esfuerzos por modernizar su infraestructura tecnológica y diversificar su economía.

Figura 2

Cantidad de artículos encontrados por países



La Figura 3, muestra un mapa de co-ocurrencia de términos que ilustra las interrelaciones entre conceptos clave. Los nodos, que representan distintos términos de investigación, se agrupan en colores que indican categorías temáticas específicas. En el grupo rojo destacan "inteligencia artificial" y "control de acceso", sugiriendo que estos son conceptos centrales en la investigación actual, lo que resalta la importancia de la IA en la optimización de los sistemas de acceso. El grupo azul incluye términos como "ciberseguridad" y "seguridad de red", evidenciando la necesidad de integrar medidas de protección en los sistemas de control de acceso. El grupo verde, relacionado con el "Internet de las cosas" (IoT), indica que la conectividad de dispositivos está influyendo en el desarrollo de estas soluciones. Finalmente,

el grupo amarillo abarca conceptos como "blockchain" y "criptografía", señalando un interés creciente en tecnologías de seguridad descentralizadas.

Figura 3

Análisis de búsqueda por palabras claves

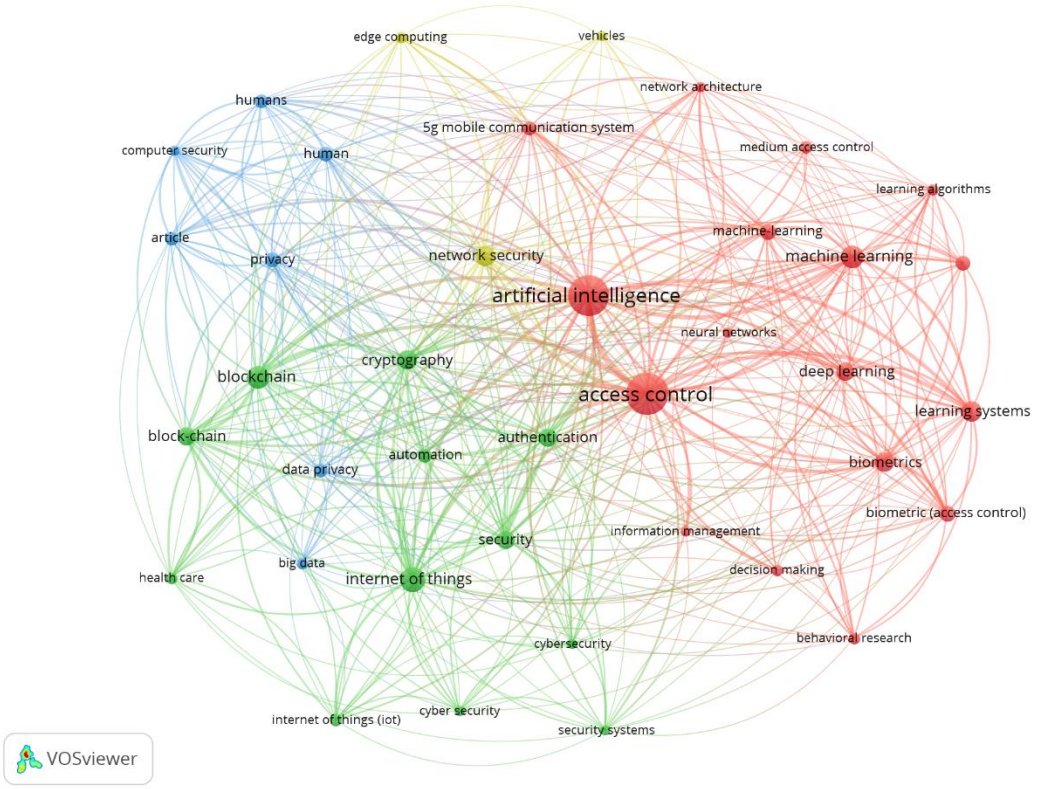
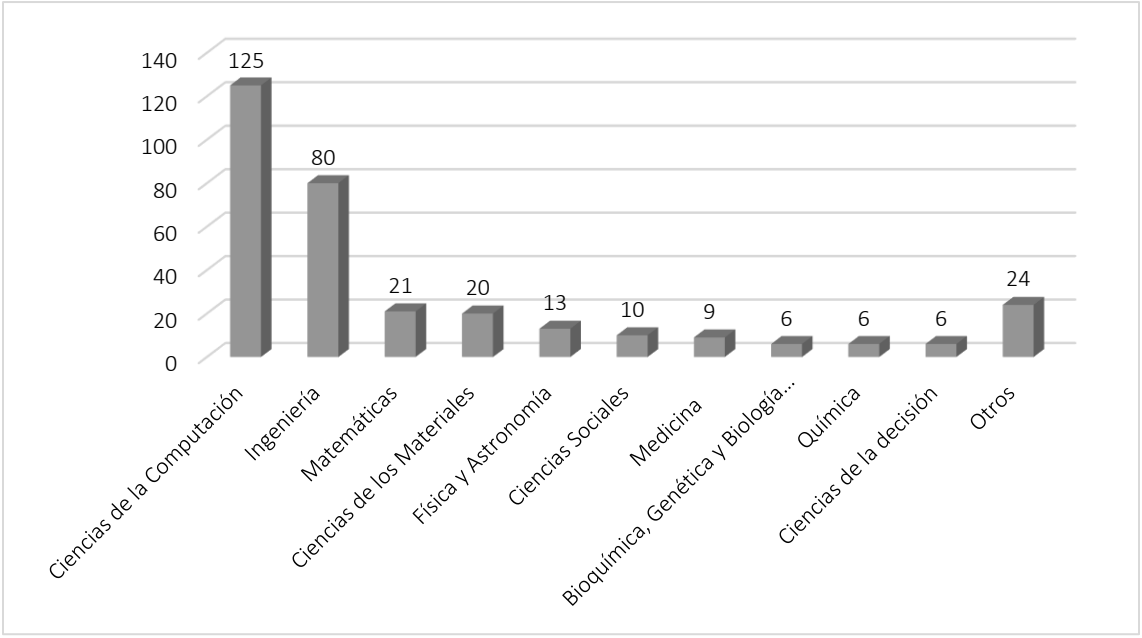


Figura 4

Número de documentos por área temática



La Figura 4, ilustra la distribución de publicaciones en diversas disciplinas científicas. Destaca que Ciencias de la Computación lidera con 125 publicaciones, seguida por Ingeniería con 80. Las Matemáticas y Ciencias de los Materiales tienen 21 y 20 publicaciones, respectivamente, lo que indica un interés moderado. A continuación, Física y Astronomía (13), Ciencias Sociales (10) y Medicina (9) reflejan niveles de investigación más bajos. Las áreas de Biociencia, Genética y Biología, Química y Ciencias de la Decisión cuentan con 6 publicaciones cada una, mientras que la categoría de Otros suma 24 publicaciones.

3.2. Análisis sistemático

Después de analizar los artículos seleccionados para la revisión, se procedió a extraer los datos relevantes, los cuales se resumen en la Tabla 3 que se presenta a continuación.

Tabla 3

Registros de temperaturas y valores de coeficientes letales para la conserva

ID	Autor/Año Herramienta IA	Uso
1	Bouramdane (2023) Deep learning	Enfoque de toma de decisiones multicriterio (MCDM) usando el proceso de jerarquía analítica (AHP). Para esto se usó Deep learning como técnica más efectiva para mejorar la ciberseguridad en las redes inteligentes. Especialmente en control de acceso y autenticación.
2	Wang et al. (2023) IA + blockchain	El uso de tecnologías de IA junto con la cadena de bloques (blockchain) se implementa en el modelo de control de acceso (CA) dinámico de dominios cruzados para mejorar la confidencialidad, integridad, disponibilidad y eficiencia del control de acceso en comparación con otros modelos tradicionales como el CA basado en control de acceso basado en identidad.
3	Khan y Kadri (2023) Random forest y modelo de regresión lineal. (Machine learning)	En este caso, la herramienta de IA usada para el control de acceso es el aprendizaje automático (*machine learning*). Los modelos específicos mencionados son random forest (RF) y el modelo de regresión lineal, que se emplean para predecir características y optimizar el protocolo MAC, mejorando la gestión de recursos en redes de área doméstica inteligentes y abordando problemas como la escalabilidad y la eficiencia en un entorno de IoT.
4	Marwan et al. (2023) Random Forest, Factorizacion de matriz no negativa, Fuzzy C-means y Correlacion de Pearson	Se propuso un nuevo esquema de autenticación de dos factores (2FA) basado en la criptografía de curva elíptica (ECC) y la función hash unidireccional para el control de acceso. Más interesante aún, usamos factorización de matriz no negativa (NMF), Fuzzy C-Means (FCM), Random Forest (RF) y correlación de Pearson (PC) para mejorar la precisión y latencia de los modelos tradicionales de filtrado de datos.

Tabla 3 (Continuación/1)

ID	Autor/Año Herramienta IA	Uso
5	Kadam et al. (2023) Lógica difusa, algoritmo de optimización (ACO)	Una técnica de enrutamiento liviano para expresar políticas de control de acceso de la red con el fin de garantizar mayor fiabilidad con mínima latencia y sobrecarga. El Protocolo de Enrutamiento Basado en Clustering Consciente de Confianza (TACR) resuelve los problemas de seguridad y fiabilidad de la comunicación en IoV, mientras reduce los costos computacionales y la latencia. La funcionalidad de TACR se basa en métodos de gestión de confianza para la selección óptima del cabeza de clúster (CH) y del retransmisor (encargado de reenviar datos). Los puntajes de confianza directa e indirecta de cada vehículo se calculan durante el clustering. La función de aptitud del algoritmo de Optimización de Colonia de Hormigas (ACO) utiliza el valor de confianza híbrido de cada vehículo. El algoritmo ACO elige vehículos estables para ser el mejor CH.
6	Liu et al. (2023) Red neuronal artificial (ANN)	La ANN se utiliza para procesar las salidas de cálculo que ayudan a decidir si sondear un hub y determinar el conteo de retroceso inicial de cada hub. También ayuda a optimizar el proceso de acceso al canal, reduciendo la latencia al minimizar el sondeo innecesario de hubs vacíos y aliviando las colisiones durante el período de contienda.
7	Motroni et al. (2023) Máquina de soporte vectorial (SVM), Red neuronal de memoria a corto y largo plazo (LSTM-NN)	La SVM de usa para clasificar el estado de las etiquetas en función de las características extraídas de la señal. Y LSTM-NN, se entrena con los datos de la etiqueta para mejorar la precisión de clasificación, logrando un 98 % de precisión en el escenario simulado. Ambas se emplean en el sistema de control de acceso en identificación por radiofrecuencia (RFID) para mejorar la clasificación y la solidez frente a interferencias.
8	Dong et al. (2023) Representational Learning	El modelo de control de acceso computable basado en incrustaciones (ECAC) utiliza el aprendizaje de representaciones (representational learning) para incrustar reglas de control de acceso en un espacio vectorial, permitiendo operaciones matemáticas para determinar la seguridad sin necesidad de consultas tradicionales.
9	Bera et al. (2021) IA + blockchain	En un marco de control de acceso basado en inteligencia artificial y concebido en blockchain para la detección y mitigación de ataques maliciosos con el fin de asegurar el entorno de Internet of Everything (IoE).

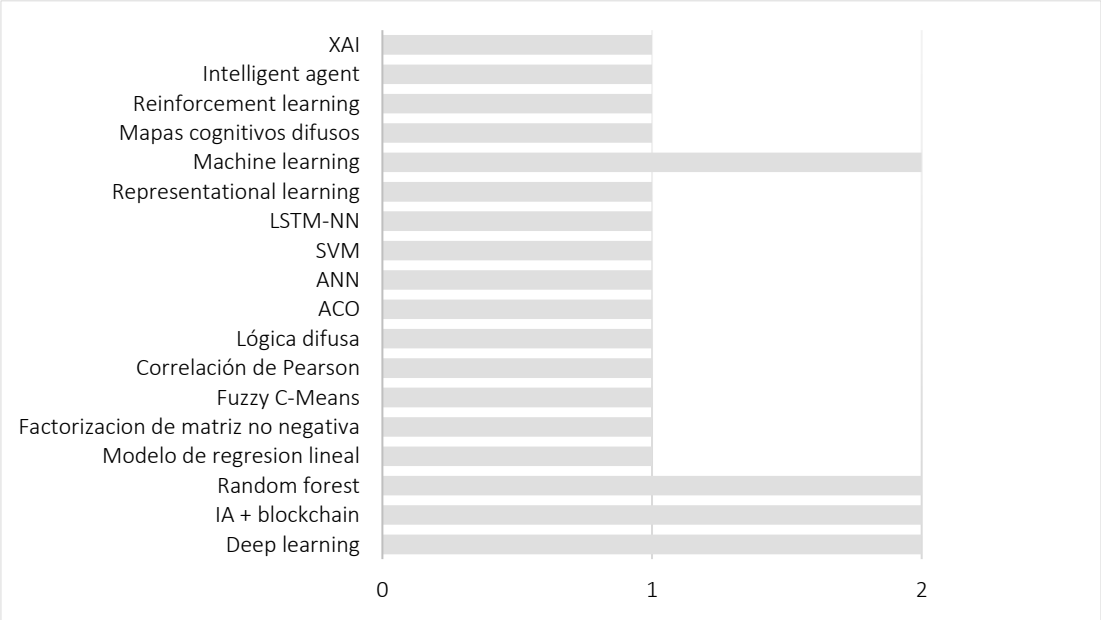
Tabla 3 (Continuación/2)

ID	Autor/Año Herramienta IA	Uso
10	Attar (2023) Machine learning (ML), Deep learning (DL)	Las tecnologías de machine learning (ML) y deep learning (DL) pueden emplearse para ofrecer soluciones de seguridad avanzadas para dispositivos IoT.
11	Mar et al. (2024) Mapas cognitivos difusos	El modelo creado con técnicas de inteligencia artificial, basado en la representación del conocimiento causal a través de Mapas Cognitivos Difusos para el diagnóstico de habilidades, aseguró la toma de decisiones en el control de acceso a las prácticas del laboratorio de Ingeniería de Control II.
12	Khan et al. (2020) Reinforcement learning	Aprender automáticamente el nivel de confianza de los usuarios y otorgar acceso a una red de blockchain privada.
13	Yao et al. (2019) Intelligent agent	Combinación de detección, aprendizaje y optimización para facilitar el desarrollo y la implementación de sistemas 5G.
14	Alotaibi y Yadav (2022) Inteligencia Artificial Explicable (XAI)	En una estrategia para establecer el límite superior de la probabilidad de un estado de fuga de nodo sin necesidad de utilizar el enfoque de Monte Carlo, que es muy laborioso, aplicando inteligencia artificial explicable (XAI) en el conjunto de datos rastreados de Sina Weibo.
15	Choi et al. (2023) Machine learning	Se usa para mejorar los modelos que generan tráfico 5G, lo cual es relevante para el control de acceso en redes inalámbricas, ya que ayuda a optimizar el manejo del tráfico y garantizar un rendimiento adecuado en la comunicación.

Por último, la Figura 5 presenta la cantidad de menciones de diferentes herramientas de inteligencia artificial (IA) en los artículos analizados. Entre las tecnologías destacadas, se observan menciones de herramientas avanzadas como *Machine Learning*, Deep Learning, y enfoques como Random Forest y Modelos de regresión lineal. Sin embargo, es notable que algunas técnicas, como XAI (inteligencia artificial explicable), *Reinforcement Learning*, SVM, y Agentes inteligentes, también aparecen, pero con menor frecuencia. Esto sugiere que, aunque hay una amplia variedad de herramientas IA, las más tradicionales, como el aprendizaje profundo y supervisado, siguen dominando en la investigación actual sobre control de acceso.

Figura 5

Frecuencia de mención de las herramientas IA



4. Discusión

Niel y Bastard (2019) menciona que la inteligencia artificial (IA) consiste en un conjunto de algoritmos que establecen de manera precisa una serie de operaciones para realizar cálculos que permiten percibir, razonar y actuar. Aunque se utiliza para ejecutar diversas tareas, también puede ser aplicada para potenciar la inteligencia humana. Mientras que Rahmat et al. (2020) expresan que el control de acceso se utiliza como un mecanismo de seguridad para restringir el acceso a un conjunto específico de usuarios autorizados que pueden acceder a cierta información o función. Por ende, el sistema de control de acceso inteligente, es un dispositivo que, tras validar la identidad del usuario, permite el acceso a un recurso determinado. Para esto existen diferentes métodos para implementar el control de acceso. Como enfoques de software que requieren la entrada de una contraseña, así como sistemas que utilizan huellas dactilares y reconocimiento facial, entre otras alternativas (Villegas, s.f.).

El reconocimiento facial representa solo una de las múltiples aplicaciones de la inteligencia artificial en el control de acceso. Otras herramientas de IA también permiten el análisis de patrones de comportamiento, lo cual facilita que los sistemas identifiquen intentos sospechosos de acceso en función de la conducta de los usuarios. Por ejemplo, si un usuario autorizado exhibe una conducta inusual, como intentar acceder desde una ubicación no habitual o en horarios atípicos, el sistema activa protocolos de seguridad adicionales. Este enfoque, basado en el comportamiento, ofrece la ventaja de adaptarse a situaciones cambiantes, haciendo que los sistemas de control de acceso resulten menos predecibles y, por ende, más difíciles de vulnerar (Ayub et al., 2023).

Además, mejoras significativas se han observado en los sistemas de control de acceso predictivo, donde la inteligencia artificial permite no solo reaccionar ante eventos, sino también anticiparse a posibles amenazas mediante el análisis de datos históricos y patrones emergentes. En grandes infraestructuras, como aeropuertos o edificios gubernamentales, la IA

permite analizar flujos de personas y conductas sospechosas para prever posibles riesgos antes de que ocurran. Estas capacidades predictivas no solo refuerzan la seguridad, sino que también optimizan la eficiencia operativa, ya que permiten a los administradores de seguridad concentrarse en situaciones de riesgo potencial en lugar de monitorear manualmente todos los accesos (Liu et al., 2024).

Otro campo en el que la inteligencia artificial marca una diferencia significativa es el control de acceso mediante dispositivos inteligentes y sensores. En los sistemas de control de acceso de edificios inteligentes, por ejemplo, se utilizan tecnologías como la identificación por radiofrecuencia (RFID) y sensores, los cuales, al combinarse con la IA, permiten un monitoreo continuo y una autorización de acceso en tiempo real. Estos sistemas pueden integrarse con otros dispositivos de seguridad, como cámaras y alarmas, para ofrecer un entorno más seguro y automatizado. La inteligencia artificial facilita que estos dispositivos interactúen de manera eficiente, analizando grandes volúmenes de datos en tiempo real y gestionando las decisiones de acceso sin intervención humana (Song y Wu, 2024).

Britti (2021) implementaron la IA a través del aprendizaje profundo (*Deep Learning*) con el objetivo de gestionar el acceso de manera efectiva. En esa línea Gutiérrez (2021) desarrollaron la Videovigilancia IA donde se encarga de marcar a las personas que acceden al edificio mediante cámaras, con el objetivo de darle un identificador único, para que se realice un seguimiento en el lugar donde fue implementado el sistema. En ambos casos la IA está siendo aplicada al campo de control de acceso para brindar mayor seguridad.

En comparación, Lan et al. (2024) destacan tanto las fortalezas como las limitaciones de estos sistemas avanzados frente a los métodos tradicionales. Respecto a las fortalezas, los sistemas de IA pueden alcanzar tasas de precisión superiores al 95 % en autenticación biométrica, superando a las soluciones tradicionales en términos de tiempo de respuesta y confiabilidad. Sin embargo, estos sistemas requieren grandes volúmenes de datos y dependen de algoritmos complejos, lo que plantea desafíos en cuanto a la privacidad y la seguridad de la información almacenada. La falta de transparencia en los algoritmos y el riesgo de sesgos representan problemas significativos, ya que errores en la identificación pueden derivar en accesos no autorizados o bloqueos indebidos, comprometiendo así la seguridad de los sistemas.

En cuanto a la implementación, Rashed et al. (2024) manifiestan que el costo es uno de los principales obstáculos para adoptar tecnologías avanzadas de IA en el control de acceso, especialmente en infraestructuras existentes donde la actualización tecnológica requiere una reestructuración considerable. Además, la IA aplicada al control de acceso enfrenta problemas relacionados con la regulación de datos personales, ya que la recopilación y procesamiento de información sensible, como características faciales y patrones de movimiento, puede vulnerar derechos de privacidad si no se gestiona adecuadamente

Para enfrentar estos desafíos, Rubio-Medrano et al. (2024) sugieren integrar IA con tecnologías emergentes como blockchain para fortalecer la seguridad en la gestión de acceso. Su naturaleza descentralizada puede aportar transparencia y confianza, permitiendo un registro inmutable de eventos de acceso y facilitando auditorías de seguridad en tiempo real. Además, podría ayudar a mitigar problemas de seguridad en el almacenamiento de datos, dado que los registros se distribuyen en nodos, lo cual reduce el riesgo de manipulación y pérdida de datos.

A futuro, las investigaciones deberían enfocarse en desarrollar algoritmos más eficientes y menos dependientes de datos para reducir costos y mejorar la accesibilidad. También sería valioso investigar metodologías híbridas que combinen inteligencia humana y artificial en entornos de seguridad, permitiendo una supervisión continua que podría ajustar los algoritmos de IA para evitar sesgos y errores en tiempo real. Igualmente, se deberían explorar enfoques que maximicen la privacidad, como el uso de técnicas de anonimización y *federated learning*, que permiten el aprendizaje sin que los datos personales salgan del dispositivo.

5. Conclusiones

El análisis bibliométrico identificó que la IA es clave en la evolución de los sistemas de control de acceso, con un creciente interés global. China, India, Estados Unidos y Corea del Sur lideran la investigación en esta área. Las palabras claves destacaron conceptos como *machine learning*, *deep learning*, criptografía y biometría. Además, muestra una integración de tecnologías emergentes como '*blockchain*' e 'internet de las cosas', lo que podría transformar las soluciones de seguridad. Respecto al análisis sistemático, de manera similar muestra que las herramientas más citadas en la literatura son subtemas de *machine learning* y *deep learning*, con un enfoque destacado en lógica difusa y redes neuronales. Estas tecnologías se consideran las más efectivas para el control de acceso, proporcionando soluciones sofisticadas y confiables. Además, el uso de blockchain inteligente emerge como una opción innovadora para mejorar la transparencia y confiabilidad en estos sistemas.

6. Referencias Bibliográficas

Alotaibi, S. D., y Yadav, K. (2022). Explainable artificial-intelligence-based privacy preservation approach for information dissemination on social networks: An incremental technique. *IEEE Systems Man and Cybernetics Magazine*, *8*(4), 44–47. https://doi.org/10.1109/msmc.2022.3188406

Arguelles, E., y Amaro, M. (2022). Preocupaciones éticas en el uso de inteligencia artificial, transparencia y derecho de acceso a la información. El caso de los chatbots en el gobierno de México, en el contexto de la COVID-19. *Estudios en derecho a la información*, 85–111. https://doi.org/10.22201/iij.25940082e.2023.15.17472

Attar, H. (2023). Joint IoT/ML platforms for smart societies and environments: A review on multimodal information-based learning for safety and security. *ACM Journal of Data and Information Quality*, *15*(3), 1–26. https://doi.org/10.1145/3603713

Ayub, A. M., Kolandaisamy, R., y Keoy, K. H. (2023, del 21 al 23 de mayo). Getting smarter with fatrix: A facial recognition access control system [conferencia]. *2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, 149–153. Benghazi, Libia. 10.1109/MI-STA57575.2023.10169208

Bera, B., Das, A. K., Obaidat, M. S., Vijayakumar, P., Hsiao, K.-F., y Park, Y. (2021). AI-enabled blockchain-based access control for malicious attacks detection and mitigation in

IoE. *IEEE consumer electronics magazine*, *10*(5), 82–92. https://doi.org/10.1109/mce.2020.3040541

Bouramdane, A.-A. (2023). Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *Journal of Cybersecurity and Privacy*, *3*(4), 662–705. https://doi.org/10.3390/jcp3040031

Britti, G. (2021). *Servicios de video vigilancia hogareño con soporte de inteligencia artificial* [Tesis de maestría, Universidad de San Andrés]. https://repositorio.udesa.edu.ar/items/71d00735-2aef-41bc-b408-8cc88cf01c36

Cajal, B., Jiménez, R., Gervilla, E., y Montaño, J. J. (2020). Doing a systematic review in health sciences. *Clinica y Salud*, *31*(2), 77–83. https://doi.org/10.5093/clysa2020a15

Choi, Y.-H., Kim, D., Ko, M., Cheon, K.-Y., Park, S., Kim, Y., y Yoon, H. (2023). ML-based 5G traffic generation for practical simulations using open datasets. *IEEE communications magazine*, *61*(9), 130–136. https://doi.org/10.1109/mcom.001.2200679

Dong, L., Wu, T., Jia, W., Jiang, B., y Li, X. (2023). Computable access control: Embedding access control rules into euclidean space. *IEEE transactions on systems, man, and cybernetics. Systems*, *53*(10), 6530–6541. https://doi.org/10.1109/tsmc.2023.3283527

El-Banby, G. M., Elazm, L. A. A., El-Shafai, W., El-Bahnasawy, N. A., El-Samie, F. E. A., Elazm, A. A., y Siam, A. I. (2024). Security enhancement of the access control scheme in IoMT applications based on fuzzy logic processing and lightweight encryption. *Complex & Intelligent Systems*, *10*(1), 435–454. https://doi.org/10.1007/s40747-023-01149-6

Gutiérrez, D. (2021). *Videovigilancia IA.* [Proyecto de fin de grado, Universidad Politécnica de Madrid]. https://oa.upm.es/68128

Kadam, M. V., Mahajan, H. B., Uke, N. J., y Futane, P. R. (2023). Cybersecurity threats mitigation in Internet of Vehicles communication system using reliable clustering and routing. *Microprocessors and Microsystems*, *102*(104926), 104926. https://doi.org/10.1016/j.micpro.2023.104926

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *An International Journal on Information Fusion*, *97*(101804), 101804. https://doi.org/10.1016/j.inffus.2023.101804

Khan, A. S., Zhang, X., Lambotharan, S., Zheng, G., AsSadhan, B., y Hanzo, L. (2020). Machine learning aided blockchain assisted framework for wireless networks. *IEEE network*, *34*(5), 262–268. https://doi.org/10.1109/mnet.011.1900643

Khan, B. M., y Kadri, M. B. (2023). Seamless connections: Harnessing machine learning for MAC optimization in home area networks. *Electronics*, *12*(19), 4082. https://doi.org/10.3390/electronics12194082

Lan, D., Xu, P., Nong, J., Song, J., y Zhao, J. (2024). Application of Artificial Intelligence technology in Vulnerability Analysis of intelligent ship network. *International Journal of Computational Intelligence Systems*, *17*(1). https://doi.org/10.1007/s44196-024-00539-z

Liu, L.-J., Si, H., y Karimi, H. R. (2024). Intelligent emergency traffic signal control system with pedestrian access. *Information Sciences*, *679*(120805), 120805. https://doi.org/10.1016/j.ins.2024.120805

Liu, Z., Lv, Y., Bi, M., y Zhai, Y. (2023). A novel artificial intelligence based wireless local area network channel access control scheme for low latency e-health applications. *IET Communications*, *17*(17), 1974–1983. https://doi.org/10.1049/cmu2.12668

Lucero, B. A., Saracini, C., Mora, M., y Muñoz-Quezada, M. T. (2020). Aspectos éticos del uso de identificadores biométricos. *Acta Bioethica*, *26*(1), 43–50. https://doi.org/10.4067/s1726-569x2020000100043

Mar, O., Gulín, J., y Santana, I. (2024). Modelo computacional para la toma de decisiones sobre el control de acceso a las prácticas de laboratorios. *Revista Cubana de Ciencias Informáticas, 18*(1), 83-99. https://goo.su/tWuVYQ

Marwan, M., AlShahwan, F., Afoudi, Y., Ait Temghart, A., y Lazaar, M. (2023). Leveraging artificial intelligence and mutual authentication to optimize content caching in edge data centers. *Journal of King Saud University - Computer and Information Sciences*, *35*(9), 101742. https://doi.org/10.1016/j.jksuci.2023.101742

Motinho, L., y Cavique, L. (2023). Impact of artificial intelligence in Industry 4.0 and 5.0. En *Advances in Human and Social Aspects of Technology* (pp. 358–376). IGI Global.

Motroni, A., Pino, M. R., Cecchi, G., y Nepa, P. (2023). A near-field focused array antenna empowered by deep learning for UHF-RFID smart gates. *IEEE transactions on antennas and propagation*, *71*(10), 7946–7957. https://doi.org/10.1109/tap.2023.3302434

Niel, O., y Bastard, P. (2019). Artificial intelligence in nephrology: Core concepts, clinical applications, and perspectives. *American Journal of Kidney Diseases: The Official Journal of the National Kidney Foundation*, *74*(6), 803–810. https://doi.org/10.1053/j.ajkd.2019.05.020

Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support Systems*, *106*, 1–14. https://doi.org/10.1016/j.dss.2017.11.003

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *International Journal of Surgery (London, England)*, *88*(105906), 105906. https://doi.org/10.1016/j.ijsu.2021.105906

Psarra, E., Apostolou, D., Verginadis, Y., Patiniotakis, I., y Mentzas, G. (2024). Permissioned blockchain network for proactive access control to electronic health records. *BMC Medical Informatics and Decision Making*, *24*(1). https://doi.org/10.1186/s12911-024-02708-8

Rahmat, R. F., Zai, E., Fawwaz, I., y Aulia, I. (2020). Facial Recognition-Based Automatic Door Access System Using Extreme Learning Machine. *IOP Conference Series: Materials Science and Engineering, 851*(012065). https://doi.org/10.1088/1757-899X/851/1/012065

Rashed, A. N. Z., Yarrarapu, M., Prabu, R. T., Raj Antony, G. S., Edeswaran, L., Kumar, E. S., Aswitha, K., Snehith, N., y Ahammad, S. H. (2024). Connected smart elevator systems for smart power and time saving. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-69173-1

Rubio-Medrano, C. E., Kotak, A., Wang, W., y Sohr, K. (2024, 15 al 17 de mayo). Pairing human and artificial intelligence: Enforcing access control policies with LLMs and formal specifications [conferencia]. *Proceedings of the 29th ACM Symposium on Access Control Models and Technologies*, 105–116. San Antonio, Texas, New York, Estados Unidos. https://doi.org/10.1145/3649158.3657032

Song, C., y Wu, Z. (2024). Artificial intelligence-assisted RFID tag-integrated multi-sensor for quality assessment and sensing. *Sensors (Basel, Switzerland)*, *24*(6), 1813. https://doi.org/10.3390/s24061813

van Eck, N. J., y Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Villegas, J. (s.f.). *¿Qué es un Sistema de Control de Acceso?* En *TECNOSeguro*. Recuperado el 28 de septiembre de 2024. https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso

Wang, F., Hu, Z., Wang, H., Chen, X., y Feng, W. (2023). Cross-domain dynamic access control based on "blockchain + artificial intelligence". *Neural Computing & Applications*, *35*(35), 24575–24585. https://doi.org/10.1007/s00521-023-08360-z

Yao, M., Sohul, M., Marojevic, V., y Reed, J. H. (2019). Artificial intelligence defined 5G radio access networks. *IEEE communications magazine*, *57*(3), 14–20. https://doi.org/10.1109/mcom.2019.1800629