ISBN: 978-628-96613-1-6. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2025.1.1.997

Effectiveness of Artificial Intelligence Models to Counter Cybersecurity Threats in IoT Devices with Blockchain. A Systematic Review

David Alejandro Miranda-Torres[1]; Nestor Abel Sánchez-Goycochea[2]
[1,2]Universidad Tecnológica del Perú, Perú,
[1]U21216338@utp.edu.pe, [2]nsanchezg@utp.edu.pe

Abstract*– Artificial intelligence models have significantly transformed the Internet of Things (IoT) sector, but they have also increased the risks associated with cybersecurity. This research aims to determine which of these models are most effective in countering cybersecurity threats in IoT devices integrated into a Blockchain ecosystem. A systematic literature review was developed, structured around three specific questions derived from the main research question: What are the most reliable artificial intelligence models when integrated into a Blockchain ecosystem to counter cybersecurity threats in IoT devices? The analysis was performed using the PRISMA protocol and information sourced from the Scopus and Web of Science databases. The findings indicate a high level of effectiveness of Machine Learning and Deep Learning-based models in enhancing the security of IoT devices within Blockchain-integrated environments. Notably, Convolutional Neural Networks, Long Short-Term Memory networks, and Federated Learning models demonstrated over 95% effectiveness in early threat detection. Nevertheless, their performance remains contingent upon factors such as dataset variability and computational resource constraints. Accordingly, it is concluded that these techniques provide robust and reliable solutions for mitigating risks in IoT, significantly contributing to the implementation of advanced cybersecurity strategies in organizations and technological sectors.

Keywords*-- Cybersecurity, Blockchain, Internet of Things, Network Security, Artificial intelligence.

Efectividad de Modelos de Inteligencia Artificial para Contrarrestar Amenazas de Ciberseguridad en Dispositivos IoT con Blockchain. Una Revisión Sistemática

David Alejandro Miranda-Torres[1]; Nestor Abel Sánchez-Goycochea[2]
[1,2]Universidad Tecnológica del Perú, Perú,
[1]U21216338@utp.edu.pe, [2]nsanchezg@utp.edu.pe

Resumen– ***Los modelos de inteligencia artificial han transformado significativamente el sector del Internet de las Cosas (IoT), pero también han incrementado los riesgos asociados a la ciberseguridad. Esta investigación tiene como objetivo determinar cuáles de estos modelos son más efectivos para contrarrestar amenazas de ciberseguridad en dispositivos IoT integrados en un ecosistema Blockchain. Se desarrolló una revisión sistemática de literatura, estructurada a partir de tres preguntas específicas derivadas de la pregunta principal: ¿Cuáles son los modelos de inteligencia artificial más fiables al integrarlos en un ecosistema Blockchain para contrarrestar amenazas de Ciberseguridad en Dispositivos IoT? El análisis se realizó utilizando el procedimiento PRISMA y fuentes de información obtenidas de las bases de datos Scopus y Web of Science. Los resultados demuestran una alta efectividad de los modelos basados en Machine Learning y Deep Learning para fortalecer la seguridad de dispositivos IoT integrados en entornos Blockchain. En particular, los modelos Convolutional Neural Network, Long Short Term Memory y Federated Learning superaron el 95% de efectividad en la detección temprana de amenazas. Sin embargo, su desempeño está condicionado por factores como la variabilidad en los conjuntos de datos y las limitaciones computacionales. En consecuencia, se concluye que estas técnicas ofrecen soluciones robustas y confiables para mitigar riesgos en IoT, contribuyendo significativamente a la implementación de estrategias avanzadas de ciberseguridad en organizaciones y sectores tecnológicos.***

Palabras clave-- Cybersecurity, Blockchain, Internet of Things, Network Security, Artificial intelligence.

I. Introducción

En la era moderna, el Internet de las Cosas (IoT) ha transformado profundamente la vida cotidiana, desde la creación de hogares inteligentes hasta la optimización de infraestructuras empresariales y servicios públicos [1]. Esta interconexión masiva ofrece comodidad y optimización de procesos, pero también plantea importantes desafíos en términos de seguridad cibernética [2]. Debido a sus limitaciones de procesamiento y almacenamiento, los dispositivos IoT están expuestos a diversas vulnerabilidades que pueden ser explotadas, comprometiendo la privacidad y la seguridad de sus usuarios [3]. Para abordar estos problemas, han surgido prometedoras innovaciones en los campos de la inteligencia artificial y la tecnología blockchain, que ofrecen enfoques avanzados de seguridad, permitiendo detectar y gestionar amenazas de manera más eficaz [4]. Estas tecnologías, aplicadas al IoT, representan una oportunidad significativa para enfrentar de manera integral los riesgos asociados a la hiperconectividad [5]. Diversas investigaciones se han centrado en desarrollar modelos de inteligencia artificial que puedan prevenir y mitigar ataques de seguridad en dispositivos IoT [6]. Estos estudios han explorado cómo los modelos de aprendizaje automático pueden detectar patrones anómalos en el comportamiento de los dispositivos y cómo el blockchain puede asegurar la integridad y transparencia de los datos generados. Un ejemplo concreto de esto es el uso de Long Short Term Memory en el módulo de detección de anomalías, donde su aplicación práctica en el análisis de conjuntos de datos públicos demostró su capacidad para identificar comportamientos inusuales, contribuyendo a una infraestructura más segura y confiable [7]. A pesar de estos avances, sigue existiendo una brecha en términos de determinar cuál de estos modelos es el más adecuado para integrarse en un ecosistema blockchain y maximizar la seguridad de los dispositivos IoT. En adición, la alta carga computacional y la interoperabilidad entre diversos modelos y redes blockchain representan desafíos técnicos relevantes [8]. La complejidad de estos entornos, sumada a la constante evolución de las amenazas, genera un panorama de desconocimiento que agrava aún más la problemática [9]. Esta situación ha motivado un interés creciente en identificar modelos de inteligencia artificial que no solo ofrezcan altos niveles de efectividad, sino que también se encuentren integrados adecuadamente en un ecosistema blockchain [10]. La finalidad de esta investigación es determinar los modelos de inteligencia artificial más confiables para contrarrestar amenazas de ciberseguridad en dispositivos IoT dentro de un ecosistema Blockchain. Este análisis se centrará en evaluar la eficacia de distintos modelos de aprendizaje automático en un entorno de blockchain, con el fin de identificar aquel que garantice una mayor seguridad y confiabilidad en la detección y mitigación de amenazas. La efectividad de estos modelos será evaluada mediante la recopilación y agrupación de las métricas de desempeño, analizando su rendimiento en escenarios reales. A su vez, permitirá comprender qué características y métricas son más críticas para garantizar una respuesta efectiva frente a amenazas de ciberseguridad en un entorno de IoT. La justificación de esta investigación radica en la creciente necesidad de contrarrestar las amenazas de ciberseguridad en dispositivos IoT, ya que los dispositivos conectados representan puntos de acceso vulnerables que pueden ser explotados por atacantes [11]. Cada modelo de inteligencia artificial tiene fortalezas y limitaciones únicas; por lo tanto, en un entorno tan crítico como el IoT, es fundamental conocer cuál de estos ofrece los mejores resultados y garantiza

mayor confiabilidad frente a las amenazas emergentes [12]. Esta investigación aborda estas carencias, ofreciendo una revisión exhaustiva de las estrategias actuales y manifestando aquellos modelos confiables. Los resultados del presente estudio buscan sintetizar los conocimientos existentes que serán de gran valor para la comunidad científica y tecnológica. Los hallazgos permitirán a los investigadores contar con un recurso estructurado y exhaustivo sobre los modelos más eficaces en la protección de dispositivos IoT, y ofrecerán a las organizaciones tecnológicas una base sólida para la toma de decisiones en la integración de seguridad avanzada en sus ecosistemas IoT. Esta comprensión, por lo tanto, no solo contribuirá a un entendimiento más profundo del tema, sino que también impulsará innovaciones y mejoras en la seguridad cibernética aplicada a IoT [13].

II. METODOLOGÍA

Este estudio se llevó a cabo mediante una revisión sistemática de literatura, empleando un enfoque basado en tres preguntas clave mostradas en la Tabla I, que guían el análisis de la necesidad abordada previamente y engloban la siguiente pregunta principal: ¿Cuáles son los modelos de inteligencia artificial más fiables al integrarlos en un ecosistema Blockchain para contrarrestar amenazas de Ciberseguridad en Dispositivos IoT? La primera pregunta específica se centra en la identificación y medición de la variable en estudio, proporcionando criterios claros para evaluar el problema. La segunda pregunta se orienta hacia el análisis de las características y métodos de solución, detallando los enfoques que ofrecen una posible resolución del problema. Finalmente, la tercera pregunta se enfoca en evaluar los resultados del modelo aplicado al problema, examinando su efectividad y precisión. Este enfoque metodológico se detalla en la Tabla I, la cual muestra las preguntas específicas y las palabras claves utilizadas.

TABLA I
PREGUNTAS ESPECÍFICAS Y KEYWORDS

ITEM	PREGUNTA	PALABRAS CLAVE
1	¿Cuáles son los criterios que brindan el porcentaje de evaluación más alto al contrarrestar amenazas de Ciberseguridad en Dispositivos IoT?	Cybersecurity, Security, Threat, Identify
2	¿Qué modelos integrados en un ecosistema Blockchain se utilizan para contrarrestar amenazas en dispositivos IoT?	Blockchain, IoT
3	¿Cuál es el nivel de efectividad de los modelos integrados en un ecosistema Blockchain para contrarrestar amenazas de Ciberseguridad en IoT?	Accuracy, Machine Learning, Deep Learning

Esta investigación se sustenta en una exhaustiva revisión bibliográfica realizada a través de las bases de datos Scopus y Web of Science. La ecuación de búsqueda empleada para esta investigación fue: (TITLE-ABS-KEY ("identify" OR "security" AND "threat" OR "cybersecurity") AND TITLE-ABS-KEY ("blockchain" AND "IoT") AND TITLE-ABS-KEY ("accuracy" OR ("machine learning" OR "deep learning"))) AND PUBYEAR > 2021 AND PUBYEAR < 2025 AND (LIMIT-TO (OA , "all")) AND LIMIT-TO (DOCTYPE , "ar")

La ecuación presentada anteriormente se compone de tres cadenas interconectadas por el operador lógico "AND". Cada cadena corresponde a las palabras clave identificadas en las preguntas específicas de la Tabla I. La primera cadena incluye una combinación de operadores "OR" y "AND", organizados de tal manera que optimicen los resultados obtenidos en las bases de datos. La segunda cadena, la más breve de las tres, utiliza exclusivamente el operador "AND", ya que las palabras clave aquí son fundamentales para el enfoque de esta investigación. Por último, la tercera cadena agrupa los niveles de aprendizaje de la inteligencia artificial, incluyendo el término *accuracy*, que en esta revisión se utiliza como indicador central para identificar estudios que midan la precisión de dichos modelos, con el objetivo de generar resultados diversos que ofrezcan una perspectiva amplia y coherente sobre el tema en cuestión. En la Tabla II, se describen los filtros que componen esta cadena.

TABLA II
FILTROS APLICADOS EN CADENA DE BÚSQUEDA

FILTRO	DESCRIPCIÓN
F1: PUBYEAR > 2021 AND PUBYEAR < 2025	D1: Limitar búsqueda a documentos publicados en un rango de fechas específico.
F2: LIMIT-TO (OA , "all")	D2: Restringir resultados a documentos de acceso abierto (Open Access).
F4: LIMIT-TO (DOCTYPE , "ar")	D3: Restringir resultados a artículos originales.

Después de una búsqueda exhaustiva en las bases de datos SCOPUS y Web of Science, realizada en la fecha 20/09/2024 a las 16:24 horas, se recuperó un total de 140 documentos. Con el fin de garantizar la calidad y relevancia de los estudios incluidos en esta revisión, se aplicó el protocolo PRISMA (Preferred Reporting Items for Systemic reviews and Meta-Analyses). Esta metodología, ampliamente reconocida en la comunidad científica [14], permitió llevar a cabo un proceso de selección. En primera instancia, se evaluaron de manera detallada los títulos y resúmenes de cada documento, descartando aquellos duplicados o que no se alineaban al tema

de investigación. Posteriormente, se procedió a un análisis detallado del texto completo de los artículos seleccionados, aplicando los criterios de inclusión y exclusión presentados en la Tabla III.

TABLA III
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

CRITERIOS DE INCLUSIÓN	CRITERIOS DE EXCLUSIÓN
CI1: Los estudios incluidos deben abordar el tema de Ciberseguridad, IoT y Blockchain.	CE3: Artículos que no estén disponibles de manera completa o no se puedan descargar.
CI2: Los estudios deben aplicar métricas y técnicas de Aprendizaje automático en relación con la Ciberseguridad.	CE1: Publicaciones que no estén relacionadas con las áreas temáticas de Ciencias de la Computación.
CI3: Los estudios deben estar disponibles en formato PDF y ser de acceso abierto.	CE2: Publicaciones cuya metodología de evaluación no esté acorde al objetivo de la investigación.

Siguiendo las fases del protocolo PRISMA para la selección de estudios, se identificaron 140 artículos y se procedió a una etapa de filtrado. En primer lugar, se eliminaron 33 duplicados. Posteriormente, se excluyeron 40 artículos por no ser relevantes para el tema de investigación, y 3 publicaciones que no pudieron ser recuperadas en su totalidad (PDF). Tras este proceso de filtrado, se obtuvieron 64 artículos seleccionados para evaluar su idoneidad. Finalmente, con base en los criterios de inclusión y exclusión mostrados en la Tabla III, se descartaron 18 documentos. De esta manera, se seleccionaron un total de 46 artículos para la revisión sistemática.

La metodología empleada en esta revisión se basa en la declaración PRISMA 2020, un estándar de referencia en la elaboración de revisiones sistemáticas [15]. Esta guía, que ha evolucionado a partir de la versión de 2009, proporciona un marco estructurado y detallado para garantizar la transparencia, la exhaustividad y la precisión de los informes. Los elementos que componen la declaración PRISMA 2020, junto con los diagramas de flujo (Ver Fig. 1) y las recomendaciones específicas, facilitan la realización y la evaluación de revisiones sistemáticas, contribuyendo a mejorar la calidad de la investigación en este campo [15]. El uso de Prisma no solo asegura la transparencia y exhaustividad en la selección de estudios, sino que también se ajusta a los estándares actualizados en presentación de informes en revisiones sistemáticas, beneficiando a la comunidad científica en general [16].

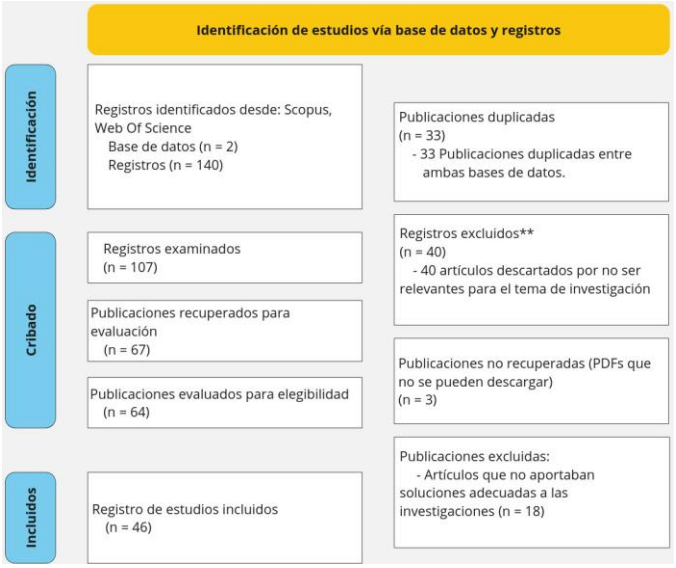

Fig. 1 Diagrama PRISMA

La hoja de trabajo se encuentra en el siguiente enlace: https://doi.org/10.5281/zenodo.14289259

III. RESULTADOS Y DISCUSIONES

La presente investigación ha recopilado y analizado sistemáticamente publicaciones científicas, los cuales han sido clasificados de acuerdo a su fecha de publicación, lugar de origen y aplicación en el contexto del IoT. Al examinar la Fig. 2, se observa un análisis de los datos que abarca el período comprendido entre 2021 y 2024, permitiendo identificar una clara tendencia de crecimiento en la cantidad de publicaciones en los últimos años. Este análisis revela un incremento significativo del 2022 al 2023, con un aumento superior al 300%, lo que refleja un interés creciente en el campo. Se destaca el punto más alto en la producción científica durante el año 2023, con un total de 29 publicaciones. Por otro lado, el año 2024 mantiene un volumen considerable de investigaciones, con 9 publicaciones, lo que sugiere una estabilización en el interés científico sobre este tema, debido a que el campo está alcanzando una fase de consolidación.

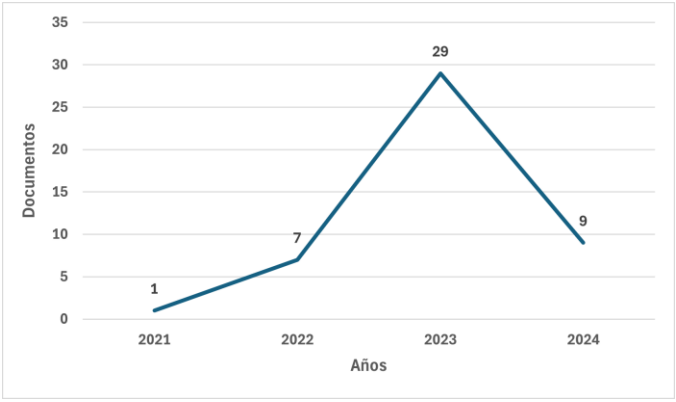

Fig. 2 Artículos organizados por año de publicación.

La distribución geográfica de los artículos analizados tal como se muestra en la Fig. 3, destaca una diversidad significativa en la contribución científica de distintos países al campo de la seguridad en IoT utilizando inteligencia artificial con blockchain. Los resultados indican que el 21.74% de los artículos provienen de India y Arabia Saudita, posicionándose en el primer lugar como los mayores contribuyentes a esta área de investigación. Este empate refleja el fuerte interés y la inversión que estas regiones están dedicando al desarrollo de soluciones tecnológicas innovadoras [17], [18]; impulsados por la necesidad de abordar desafíos propios de sus crecientes infraestructuras tecnológicas y su participación activa en el ámbito global de la innovación [19], [20].

Pais	Porcentaje
India	21.74%
Saudi Arabia	21.74%
China	10.87%
Australia	4.35%
Canada	4.35%
England	4.35%
Finland	4.35%
Pakistan	4.35%
Tunisia	4.35%
Italia	2.17%
Jordan	2.17%
Korea	2.17%
Malaysia	2.17%
Nigeria	2.17%
Poland	2.17%
Romania	2.17%
Serbia	2.17%
United States	2.17%
Total	**100.00%**

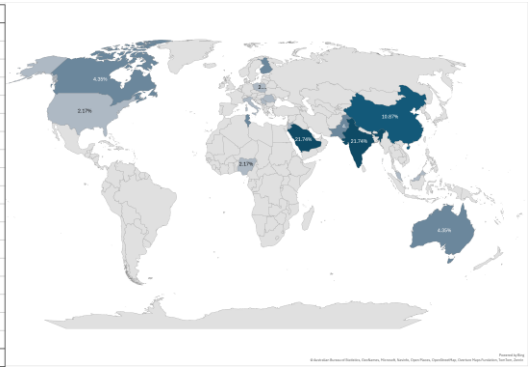

Fig. 3 Artículos organizados por país de publicación

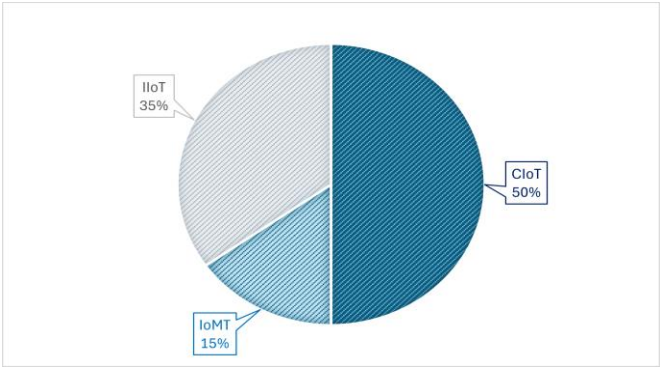

Fig. 4 Artículos organizados por aplicación IoT

La aplicación de los artículos analizados en el contexto del IoT tal como se muestra en la Fig. 4, se distribuye en tres principales categorías: Consumer Internet of Things (CIoT), Industrial Internet of Things (IIoT) y Internet of Medical Things (IoMT). Esta clasificación, realizada mediante la identificación del enfoque principal y el contexto de aplicación descrito por los autores, permite identificar las áreas de mayor interés y desarrollo dentro del campo de la seguridad cibernética en IoT mediante el uso de inteligencia artifical con blockchain. El Consumer IoT abarca dispositivos y aplicaciones diseñados para uso personal o doméstico, tales como hogares inteligentes, asistentes virtuales, sensores locales, y cámaras de vigilancia conectadas [21]. Con un 50% de los artículos analizados enfocados en esta categoría, se posiciona como la principal área de aplicación investigada. Esto refleja el crecimiento exponencial de los dispositivos CIoT en los últimos años, impulsado por la demanda de soluciones tecnológicas accesibles y la expansión de mercados emergentes. La investigación en este ámbito se centra en la protección de datos sensibles, la prevención de accesos no autorizados y la detección de anomalías en el comportamiento de los dispositivos, garantizando la privacidad y seguridad de los usuarios [22]. El Industrial IoT se enfoca en la conexión de dispositivos y sistemas dentro de entornos industriales, como satélites inteligentes, gestión vehicular y sistemas de comunicación avanzados [23]. La investigación en este campo se centra en prevenir ataques dirigidos a infraestructuras críticas, garantizar la integridad de los datos en tiempo real y optimizar la interoperabilidad entre dispositivos [24]. El Internet of Medical Things abarca dispositivos médicos conectados que recopilan y transmiten datos para mejorar la atención sanitaria, como monitores de pacientes, wearables médicos y dispositivos de diagnóstico remoto [25]. La principal preocupación y uso del Blockchain en este contexto es garantizar la privacidad de los datos médicos, evitar manipulaciones maliciosas en dispositivos críticos y asegurar la confiabilidad en la comunicación entre sistemas médicos [26]. Aunque su representación es menor en comparación con CIoT e IIoT, la investigación en IoMT es fundamental debido al impacto directo en la vida de los pacientes y la creciente adopción de tecnologías de telemedicina.

Mediante el software VOSviewer, se analizaron los keywords utilizados en los artículos, los cuales se aprecian de manera detallada en la Tabla IV y reflejan las 7 tendencias terminológicas predominantes en la literatura especializada sobre IoT, Blockchain y Ciberseguridad. Los resultados destacan no solo la frecuencia de aparición de ciertos términos en los artículos analizados, sino también su fuerza de enlace total, lo que indica tanto la conectividad de cada término con otros keywords de las bases de datos seleccionadas, como el trabajo complementario y aplicabilidad con otras terminologías. Por ejemplo, la palabra clave Blockchain presentó una frecuencia del 84.15% en los artículos seleccionados, lo que refleja su presencia dominante en la literatura. Además, obtuvo una fuerza de enlace total de 440, lo que evidencia que este término se encuentra fuertemente relacionado con otros conceptos clave. En la Tabla IV, se observa que términos como blockchain, IoT y network security son fundamentales para describir el núcleo de las investigaciones actuales, mientras que términos como cybersecurity y machine learning complementan estas temáticas desde perspectivas específicas. La mayor fuerza de enlace de cybersecurity respecto a machine learning, a pesar de su misma ocurrencia, indica que cybersecurity es un término más ampliamente relacionado con los diversos aspectos de la literatura. Esto sugiere que, al redactar documentos o publicaciones, es importante priorizar el uso de estos keywords para maximizar la visibilidad y citación en el campo académico.

TABLA IV
TERMINOLOGÍA UTILIZADA

KEYWORDS	FRECUENCIA	FUERZA DE ENLACE
Blockchain	84.15%	440
Internet of things	64.63%	390
Block-chain	57.32%	379
Network security	42.68%	279
Cybersecurity	32.93%	207
Machine Learning	32.93%	184
Deep Learning	25.61%	144

La primera pregunta específica planteada en esta investigación fue: ¿Cuáles son los criterios que brindan el porcentaje de evaluación más alto al contrarrestar amenazas de Ciberseguridad en Dispositivos IoT? (Ver Tabla I) Los resultados de la Tabla V muestran una clara preferencia por ciertos criterios de evaluación que prioritariamente se usan en los artículos, ya sea de manera conjunta o individual, destacándose Accuracy como el criterio más utilizado y valorado, seguido de la Precision, el F1-score, el Recall y F-measure. Accuracy se posiciona como el criterio predominante dado que el 65.22% de los artículos lo sitúan como el criterio con el porcentaje de evaluación más alto. Este resultado concuerda con la mayoría de los autores, quienes evidencian la importancia de este criterio, dado que mide el porcentaje total de predicciones correctas realizadas por el modelo y proporciona una evaluación general del rendimiento [27]. Con un 32.61%, Precision ocupa el segundo lugar. A diferencia de Accuracy, Precision se enfoca en la confiabilidad de las predicciones positivas, por lo cual es especialmente valorado en aplicaciones donde los falsos positivos pueden tener consecuencias graves [28]. F1-score registró un 21.74% de usos, destacándose como un balance entre Precision y Recall, lo que lo convierte en un criterio relevante cuando es necesario optimizar ambos aspectos simultáneamente [29]. Recall representa el 17.39% de los artículos analizados, mostrando su importancia en escenarios donde es crucial minimizar los falsos negativos, como en la detección de amenazas críticas que no deben ser ignoradas [30]. F-measure, con el 4.35%, se encuentra como el menos utilizado entre los criterios principales.

TABLA V
FRECUENCIA DE CRITERIOS

CRITERIOS	FRECUENCIA	ID REFERENCIA
ACCURACY	65.22%	[27],[29],[32],[33],[34],[35], [36],[37],[38],[41],[43],[45], [46],[47],[49],[51],[53],[55], [56],[57],[58],[60],[61],[63], [65],[66],[67],[70],[71],[72]
PRECISION	32.61%	[28],[29],[39],[40],[42], [44],[45],[48],[49],[54], [57],[59],[64],[66],[69]
F1-SCORE	21.74%	[29],[45],[49],[52],[54], [57],[64],[65],[66],[68]
RECALL	17.39%	[29],[30],[45],[49],[50], [54],[62],[66]
F-MEASURE	4.35%	[31],[42]

Para explorar relaciones entre los criterios, se aplicó el coeficiente de relación de Pearson, obteniendo como resultado una fuerte correlación positiva (0.9) entre Precision y Recall, indicando que en los artículos donde se emplea el criterio Precision, el Recall tiende a ser aplicado también. Además, se encontró una fuerte correlación positiva (0.6) entre Precision y F1-score, lo que implica que ambos se utilizan frecuentemente como una métrica integral para calcular la efectividad de los modelos. Finalmente, entre Recall y F1-score, se observó una fuerte correlación positiva (0.5), lo que confirma la interdependencia entre ambos criterios, dado que el F1-score es una métrica derivada directamente de la relación entre Precision y Recall. En el contexto de la seguridad en IoT, donde tanto la detección de todas las amenazas (Recall) como la minimización de falsas alarmas (Precision) son cruciales, el F1-score se convierte en una métrica valiosa para evaluar el rendimiento general de los modelos de detección de intrusiones.

En el análisis del tipo de blockchain utilizado en los artículos revisados, se consideraron cuatro categorías principales: blockchain pública, privada, híbrida y de consorcio. La distribución porcentual de estos tipos mostrados en la Tabla VI refleja la preferencia y la adecuación de cada uno según las necesidades específicas de las aplicaciones de

IoT en el ámbito de la ciberseguridad. Los resultados indican que la elección del tipo de blockchain está fuertemente influenciada por las necesidades específicas de cada aplicación IoT. Se tienen blockchain privadas, que dominan debido a su capacidad para ofrecer control y seguridad en entornos restringidos [31], mientras que las públicas, se utilizan en aplicaciones donde la descentralización es clave [32]. Los blockchain de consorcio e híbridas, aunque menos representadas, muestran potencial en casos donde se requiere colaboración entre múltiples partes o un equilibrio entre transparencia y control [28]. Esta distribución destaca la versatilidad del blockchain como tecnología base para mejorar la seguridad y confiabilidad en dispositivos IoT. En la Tabla VI se muestran las referencias por tipo de blockchain.

TABLA VI
TIPO DE BLOCKCHAIN

TIPO	FRECUENCIA	ID REFERENCIA
PRIVADA	43.48%	[31],[33],[34],[36],[40],[42],[44],[45],[46],[49],[51],[52],[53],[54],[57],[62],[63],[66],[70],[72]
PÚBLICA	26.09%	[29],[32],[37],[50],[55],[56],[60],[61],[67],[68],[69],[71]
CONSORCIO	17.39%	[30],[35],[38],[43],[58],[59],[64],[65]
HIBRIDA	13.04%	[27],[28],[39],[41],[47],[48]

Respecto al análisis del ecosistema en el que se implementa el Blockchain en los artículos revisados resaltan el enfoque de la implementación local e implementación en la nube. En la Tabla VII, el predominio de la implementación en la nube con el 67.39% refleja la creciente adopción de modelos basados en servicios remotos, que ofrecen flexibilidad, escalabilidad y acceso global. Esto, según los autores que utilizaron el ecosistema, resulta especialmente relevante en aplicaciones de IoT que requieren manejar grandes cantidades de datos generados por dispositivos distribuidos [32]. Por otro lado, la implementación local obtiene el 32.61%, el cual sigue siendo una opción válida en entornos más controlados o cuando las políticas de seguridad y privacidad limitan el uso de infraestructura externa. Por lo tanto, el criterio Accuracy ha demostrado ser el más utilizado para contrarrestar amenazas de ciberseguridad, especialmente en entornos de blockchain privadas y en la nube, evidenciando una estrecha relación entre este indicador y la adopción de estas tecnologías.

TABLA VII
ECOSISTEMA DE IMPLEMENTACIÓN

ECOSISTEMA	FRECUENCIA	ID REFERENCIA
NUBE	67.39%	[28],[30],[31],[32],[34],[36],[37],[38],[40],[41],[42],[43],[45],[46],[48],[50],[52],[55],[56],[58],[59],[60],[61],[64],[65],[66],[67],[68],[69],[70],[71]
LOCAL	32.61%	[27],[29],[33],[35],[39],[44],[47],[49],[51],[53],[54],[57],[62],[63],[70]

La segunda pregunta específica de esta investigación es: ¿Que modelos integrados en un ecosistema Blockchain se utilizan para contrarrestar amenazas en dispositivos IoT? Los modelos integrados en un ecosistema Blockchain para contrarrestar las amenazas en IoT se muestran en la Tabla VIII y revelan una clara preferencia por los enfoques basados en Machine Learning y Deep Learning, que en conjunto representan casi el 90% de los artículos analizados, mientras que un porcentaje menor utiliza otros modelos, principalmente criptográficos. El modelo más representado en los artículos revisados es el Deep Learning, con un 45.65% del total. De acuerdo con los autores, este enfoque se caracteriza por su capacidad para analizar grandes volúmenes de datos generados por dispositivos IoT, detectando patrones complejos que podrían pasar desapercibidos para métodos más tradicionales [34]. Los modelos de Machine Learning representan el 43.48% de los artículos, mostrando su continua relevancia en el campo de la ciberseguridad para IoT. Aunque menos sofisticados que los modelos de Deep Learning, los enfoques de Machine Learning son altamente efectivos para tareas de clasificación y predicción en entornos con recursos limitados. Sin embargo, algunos estudios cuestionan esta característica sugiriendo considerar diversos factores intrínsecos en contextos con menor demanda computacional [63]. Un menor porcentaje de los artículos, el 10.87%, utiliza otros modelos, en su mayoría criptográficos para abordar las amenazas en dispositivos IoT. Si bien, algunos autores mencionan que no son tan adaptables como los modelos de aprendizaje automático, los enfoques criptográficos ofrecen una solución robusta y confiable para proteger la comunicación y el almacenamiento de datos [30].

El análisis de la Tabla VIII revela que en los modelos de Deep Learning, CNN (Convolutional Neural Network) lidera con un 19.57%, utilizado para clasificar ataques con alta eficiencia y bajo costo computacional [40]. Le siguen LSTM (Long Short-Term Memory), con un 17.39%, eficaz en detección de APT en dispositivos edge [34]. En Machine Learning, domina con un 21.74% el modelo Federated Learning, gracias a su enfoque de aprendizaje distribuido que preserva la privacidad, incluso en contextos como el Metaverso [38], [39]. En la categoría *Otros*, se identificaron

enfoques específicos que, aunque menos representados en comparación con los anteriores, destacan por su aplicación en contextos especializados de ciberseguridad en dispositivos IoT [30]. De esta manera, podemos indicar que los modelos más relevantes son Machine Learning y Deep Learning, los cuales han demostrado ser fundamentales para garantizar la seguridad de los dispositivos IoT en un entorno de blockchain, al permitir la temprana detección de amenazas sin descuidar la privacidad de los datos.

TABLA VIII
MODELOS INTEGRADOS EN BLOCKCHAIN

MODELO	NOMBRE	ID REFERENCIA
DEEP LEARNING	CNN	[31], [33], [40], [44], [48], [58], [62], [66], [69]
	LSTM	[33], [34], [46], [53], [60], [66], [69], [71]
	Bi-GRU	[35],[46],[64],[72]
	Cloud-RNN	[43], [61]
	XAI, HybridChain, DragonFly, TNN	[42],[47],[49],[68]
MACHINE LEARNING	FEDERATED LEARNING	[30], [32], [38], [39], [45], [50], [58], [63], [65], [67]
	RANDOM FOREST	[28], [29], [36]
	MLP	[32],[56],[57]
	DECISION TREE	[59],[70]
	REGRESSION	[55],[56]
	ANN, LightGBM	[54], [37]
OTROS	HOMOMORPHIC ENCRYPTATION	[30], [52]
	DBN	[51]
	BAFWO-MLID	[41]
	BLOCKFOG	[27]

Respecto a la tercera pregunta específica: ¿Cuál es el nivel de efectividad de los modelos integrados en un ecosistema Blockchain para contrarrestar amenazas de Ciberseguridad en IoT? se ha considerado el uso del criterio Accuracy, identificado previamente en la Tabla V como el más representativo en los artículos analizados. Sin embargo, en aquellos modelos donde este criterio no estaba disponible, se optó por el criterio Precision para obtener una estimación comparable del desempeño. La clasificación se ha basado en rangos de efectividad, destacando los modelos más eficaces según el porcentaje de artículos en los que se implementaron, aquellas celdas marcadas como 'No Aplica', indican la ausencia de modelos en ese rango específico. Los resultados para los modelos de Deep Learning mostrados en la Tabla IX, logran altos niveles de efectividad en la detección de amenazas en IoT, especialmente en un rango de 95% a 100%, donde modelos como CNN y LSTM lideran con una presencia del 10.87% y 8.70% en los artículos respectivamente. Este desempeño se debe a su capacidad para procesar grandes cantidades de datos y extraer características relevantes. De acuerdo con diversos autores, esta funcionalidad es esencial en entornos IoT donde las amenazas son dinámicas y complejas [34]. El Bi-GRU, aunque tiene una representación menor en el rango intermedio (90% a 95%) con el 2.17% de veces, aumenta significativamente su efectividad en el rango superior (95% a 100%) alcanzado en el 6.52% de los artículos. Este resultado coincide con lo reportado en los estudios, quienes atribuyen este incremento a su diseño bidireccional, lo que permite un gran potencial y efectividad para adaptarse a tareas más complicadas [35]. Modelos emergentes como DragonFly y TNN también muestran una efectividad significativa, aunque su representación es limitada.

En el análisis de los niveles de efectividad de los modelos de Machine Learning, se evidencia una diversidad de rendimientos, destacando la frecuencia de Federated Learning en el rango superior. Este modelo se posiciona como el modelo más destacado en los cuatro rangos de efectividad presentados en la Tabla IX, pero es en el rango de efectividad superior al 95% donde alcanza un 13.04% de representación. Federated Learning, integrado con Blockchain, permite un aprendizaje distribuido y privado al entrenar modelos sin acceso a los datos originales [38]. Un ejemplo de su aplicación se encuentra en el contexto del Metaverso, el cual utiliza Federated Learning para la detección de intrusos, reduciendo los riesgos de seguridad asociados al traslado de datos sensibles [39]. Esto resalta su capacidad para combinar precisión con privacidad y eficiencia, características cruciales en aplicaciones IoT. Sin embargo, en un estudio en particular, se argumenta que los factores como la calidad, cantidad de datos, retrasos, desconexiones en dispositivos IoT y un entorno con recursos limitados pueden afectar la efectividad de este modelo [63]. Random Forest y MLP también destacan en el rango más alto, debido a su capacidad para manejar grandes volúmenes de datos, predicción de contratos inteligentes y adaptarse a diferentes escenarios tales como la agricultura [29, 57]. Los modelos clásicos como Regression y Decision Tree mantienen una presencia relevante en los rangos intermedio y superior, esto indica que su efectividad refuerza la capacidad de proveer un ambiente seguro en las ciudades inteligentes [55], además, los autores aseguran que son útiles contra amenazas de tipo ransomware APT [59]. Modelos avanzados como LightGBM demuestran potencial para manejar datos con alta dimensionalidad y estructuras complejas para detectar nodos maliciosos [37].

En la categoría denominada *Otros*, visualizados en la última columna de la Tabla IX, todos los enfoques analizados alcanzan un nivel de efectividad en el rango del 95% al 100%, según el criterio de Accuracy. Cada modelo tiene aplicaciones

específicas en el ámbito del IoT y blockchain, pero su adopción es limitada al tratarse de modelos modelos únicos y propios que los autores han desarrollado utilizando en su mayoría características criptográficas [41], por lo que su impacto a gran escala aún requiere mayor validación. En síntesis, los modelos CNN, LSTM y Federated Learning destacan, demostrando una efectividad excepcional en la detección de amenazas en IoT, alcanzando niveles de precisión superiores al 95% en diversos casos.

TABLA IX
EFECTIVIDAD DE MODELOS

EFECTIVIDAD	MACHINE LEARNING	DEEP LEARNING	OTROS
[95% - 100%]	Federated Learning, Random Forest, MLP, Decision Tree, LightGBM, Regression, ANN	CNN, LSTM, Bi-GRU, ClouD-RNN, DragonFly, TNN	BAFWO-MLID, Blockfog, DBN, HE
[90% - 95%[	Federated Learning, MLP	LSTM, CNN, HybridChain, Bi-GRU, XAI	No Aplica
[80% - 90%[	Federated Learning, Decision Tree, Random Forest	No Aplica	No Aplica
[70% - 80%[	Federated Learning	No Aplica	No Aplica
ID REFERENCIA	[32], [39], [45],[50], [65], [67], [29],[36], [57], [70], [37],[55], [54], [56], [58],[30], [38], [59], [28], [63]	[31],[48],[62],[66], [40],[34],[53],[60], [69],[35],[46],[72], [43],[61],[42],[49], [33],[71],[44],[47], [64], [68]	[41], [27], [51], [52]

IV. CONCLUSIONES

Tras el análisis se observó que los modelos más confiables y efectivos para contrarrestar amenazas de ciberseguridad en dispositivos IoT dentro de un ecosistema Blockchain son los basados en Deep Learning y Machine Learning. En la categoría de Deep Learning, los modelos CNN y LSTM lideran con niveles de efectividad superiores al 95%, mientras que en Machine Learning, el enfoque más destacado debido a su capacidad para preservar la privacidad y procesar datos distribuidos con alta precisión es el modelo Federated Learning. Además, se identificó que Accuracy es el criterio predominante en la evaluación de estos modelos, reflejando su relevancia como métrica clave para medir el rendimiento general. La correlación positiva observada entre Precision, Recall y F1-score subraya la interdependencia de estas métricas, lo que resalta la importancia de mantener un equilibrio entre ellas para garantizar una evaluación integral, especialmente en escenarios críticos de ciberseguridad. Asimismo, se determinó que el blockchain privado es el tipo más utilizado, mientras que, en términos de ecosistema, predomina el enfoque basado en la nube. Esto indica que las organizaciones priorizan entornos controlados y escalables para garantizar la seguridad de los datos, aprovechando la infraestructura distribuida y flexible que ofrece la tecnología blockchain en combinación con IoT. Una de las principales limitaciones del estudio radica en la necesidad de futuras investigaciones para corroborar los datos obtenidos en diversos escenarios. Como recomendaciones futuras, se sugiere analizar el impacto económico de implementar estos modelos, comparar la efectividad de distintos tipos de blockchain según el entorno IoT, y evaluar cómo las características de los datasets influyen en el desempeño de los modelos de IA.

AGRADECIMIENTO

Los autores expresan su sincero agradecimiento al Dr. Christian Dios Castillo, Doctor en Administración de la Educación, por su valiosa orientación académica durante el desarrollo de esta revisión sistemática de la literatura. Sus aportes y acompañamiento fueron fundamentales para llevarla a cabo con éxito. De igual forma, se agradece a la Universidad Tecnológica del Perú por brindar el respaldo institucional y académico necesario para la realización de esta investigación.

REFERENCIAS

[1] D. Witkowski, Bridging the Gap - 21st Century Wireless Telecommunications Handbook (2nd Edition, 2019). 2019.
[2] M. Danladi and M. Baykara, “Low Power Wide Area Network Technologies: Open Problems, Challenges, and Potential Applications,” Review of Computer Engineering Studies, vol. 9, pp. 71–78, Jan. 2022, doi: 10.18280/rces.090205.
[3] V. Adat Vasudevan and B. B. Gupta, “Security in Internet of Things: issues, challenges, taxonomy, and architecture,” Telecommunication Systems, vol. 67, pp. 1–19, Jan. 2018, doi: 10.1007/s11235-017-0345-9.
[4] B. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on IoT Security:Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology,” Internet of Things, vol. 11, p. 100227, May 2020, doi: 10.1016/j.iot.2020.100227.
[5] N. Mohamed, A. Oubelaid, and S. Almazrouei, “Staying Ahead of Threats: A Review of AI and Cyber Security in Power Generation and Distribution,” International Journal of Electrical and Electronics Research, vol. 11, Mar. 2023, doi: 10.37391/ijeer.110120.
[6] A. Buczak and E. Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” IEEE Communications Surveys & Tutorials, vol. 18, p. 1, Jan. 2015, doi: 10.1109/COMST.2015.2494502.
[7] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K.-K. R. Choo, “A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks,” IEEE Transactions on Industrial Informatics, vol. PP, p. 1, Dec. 2019, doi: 10.1109/TII.2019.2957140.
[8] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K. K. R. Choo, and A. Y. Zomaya, “Blockchain for smart communities: Applications, challenges and opportunities,” Journal of Network and Computer Applications, vol. 144, pp. 13–48, Oct. 2019, doi: 10.1016/J.JNCA.2019.06.018.
[9] W. Zhou, Y. Zhang, and P. Liu, “The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved,” IEEE Internet of Things Journal, vol. PP, Feb. 2018, doi: 10.1109/JIOT.2018.2847733.
[10] M. Banerjee, J. Lee, and K. K. R. Choo, “A blockchain future for internet of things security: a position paper,” Digital Communications and

Networks, vol. 4, no. 3, pp. 149–160, Aug. 2018, doi: 10.1016/j.dcan.2017.10.006.
[11] A. Jurcut, P. Ranaweera, and L. Xu, "Introduction to IoT Security," 2019, pp. 1–39. doi: 10.1002/9781119471509.w5GRef260.
[12] M. Kuzlu, C. Fair, and Ö. Güler, "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," Discover Internet of Things, vol. 1, Feb. 2021, doi: 10.1007/s43926-020-00001-4.
[13] M. Rele and D. Patil, "Examining the Impact of Artificial Intelligence on Cybersecurity within the Internet of Things," Sep. 2023. doi: 10.1016/j.dim.2023.100063.
[14] M. J. Page and D. Moher, "Evaluations of the uptake and impact of the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) Statement and extensions: a scoping review," Systematic Reviews, vol. 6, no. 1, p. 263, Dec. 2017, doi: 10.1186/s13643-017-0663-8.
[15] C. Sohrabi et al., "PRISMA 2020 statement: What's new and the importance of reporting guidelines," International Journal of Surgery, vol. 88, p. 105918, Apr. 2021, doi: 10.1016/j.ijsu.2021.105918.
[16] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," Syst Rev, vol. 10, no. 1, Dec. 2021, doi: 10.1186/s13643-021-01626-4.
[17] P. Gupta and S. Hanagandi, "A study of demographics and investment preference among entrepreneurs of Karnataka, India," International Journal of Technology Transfer and Commercialisation, vol. 19, p. 354, Jan. 2022, doi: 10.1504/IJTTC.2022.126309.
[18] M. Elsayed et al., "BOT Contracts of Saudi Arabia and Barriers of International Investment: Answer From Law and Economic Perspectives," Indian Journal of Science and Technology, vol. 9, no. 48, Dec. 2016, doi: 10.17485/ijst/2016/v9i48/101519.
[19] Y. Guo, "Study on the Impact of the Service Economy in China's First-Tier Cities on the Employment Structure," Technology and Investment, vol. 15, pp. 28–38, Jan. 2024, doi: 10.4236/ti.2024.151003.
[20] C. Saba and M. Pretorius, "The impact of artificial intelligence (AI) investment on human well-being in G-7 countries: Does the moderating role of governance matter?," Sustainable Futures, vol. 7, p. 100156, Jan. 2024, doi: 10.1016/j.sftr.2024.100156.
[21] C. Norval and J. Singh, "A Room With an Overview: Toward Meaningful Transparency for the Consumer Internet of Things," IEEE Internet of Things Journal, vol. 11, no. 5, pp. 7583–7603, Mar. 2024, doi: 10.1109/JIOT.2023.3318369.
[22] A. A. Tudoran, "Rethinking privacy in the Internet of Things: a comprehensive review of consumer studies and theories," Internet Research, Jun. 2024, doi: 10.1108/INTR-01-2023-0029.
[23] Z. Wei et al., "Guest Editorial Special Issue on Current Research Trends and Open Challenges for Industrial Internet of Things," IEEE Internet of Things Journal, vol. 11, no. 16, pp. 26548–26551, Aug. 2024, doi: 10.1109/JIOT.2024.3428109.
[24] S. Ugwuanyi and J. Irvine, "Industrial and Consumer Internet of Things: Cyber Security Considerations, Threat Landscape, and Countermeasure Opportunities," in 2021 International Conference on Smart Applications, Communications and Networking (SmartNets), IEEE, Sep. 2021, pp. 1–8. doi: 10.1109/SmartNets50376.2021.9555410.
[25] IS. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies," IETE Technical Review, vol. 39, no. 4, pp. 775–788, Jul. 2022, doi: 10.1080/02564602.2021.1927863.
[26] R. Wani, F. Thabit, and O. Can, "Security and privacy challenges, issues, and enhancing techniques for Internet of Medical Things: A systematic review," Security and Privacy, vol. 7, no. 5, Sep. 2024, doi: 10.1002/spy2.409.
[27] V. G. Prasuna, B. R. Babu, and B. Pydala, "Blockfog: A Blockchain-Based Framework For Intrusion Defense In Iot Fog Computing," Scalable Computing, vol. 25, no. 3, pp. 1950–1962, 2024, doi: 10.12694/scpe.v25I3.2686.
[28] N. F. Abdullah, A. R. Kairaldeen, A. Abu-Samah, and R. Nordin, "Machine Learning-Based Transactions Anomaly Prediction for Enhanced IoT Blockchain Network Security and Performance," KSII Transactions on Internet and Information Systems, vol. 18, no. 7, pp. 1986–2009, Jul. 2024, doi: 10.3837/tiis.2024.07.014.
[29] H. Shah et al., "Deep Learning-Based Malicious Smart Contract and Intrusion Detection System for IoT Environment," Mathematics, vol. 11, no. 2, Jan. 2023, doi: 10.3390/math11020418.
[30] M. Arazzi, S. Nicolazzo, and A. Nocera, "A Fully Privacy-Preserving Solution for Anomaly Detection in IoT using Federated Learning and Homomorphic Encryption," Information Systems Frontiers, 2023, doi: 10.1007/s10796-023-10443-0.
[31] F. M. Alserhani, "Integrating deep learning and metaheuristics algorithms for blockchain-based reassurance data management in the detection of malicious IoT nodes," Peer-to-Peer Networking and Applications, Nov. 2024, doi: 10.1007/s12083-024-01786-9.
[32] W. Almutairi and T. Moulahi, "Joining Federated Learning to Blockchain for Digital Forensics in IoT," Computers, vol. 12, no. 8, Aug. 2023, doi: 10.3390/computers12080157.
[33] A. Nazir et al., "Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration," Journal of King Saud University - Computer and Information Sciences, vol. 36, no. 2, Feb. 2024, doi: 10.1016/j.jksuci.2024.101939.
[34] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei, and A. K. M. Najmul Islam, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," Journal of Parallel and Distributed Computing, vol. 172, pp. 69–83, Feb. 2023, doi: 10.1016/j.jpdc.2022.10.002.
[35] P. Kumar, R. Kumar, A. Aljuhani, D. Javeed, A. Jolfaei, and A. K. M. N. Islam, "Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity," Solar Energy, vol. 263, Oct. 2023, doi: 10.1016/j.solener.2023.111921.
[36] B. M. Alshammari, "AIBPSF-IoMT: Artificial Intelligence and Blockchain-Based Predictive Security Framework for IoMT Technologies," Electronics (Switzerland), vol. 12, no. 23, Dec. 2023, doi: 10.3390/electronics12234806.
[37] S. Ismail, M. Nouman, D. W. Dawoud, and H. Reza, "Towards a lightweight security framework using blockchain and machine learning," Blockchain: Research and Applications, vol. 5, no. 1, Mar. 2024, doi: 10.1016/j.bcra.2023.100174.
[38] Z. Wang et al., "An Optimized and Scalable Blockchain-Based Distributed Learning Platform for Consumer IoT," Mathematics, vol. 11, no. 23, Dec. 2023, doi: 10.3390/math11234844.
[39] V. T. Truong and L. B. Le, "MetaCIDS: Privacy-Preserving Collaborative Intrusion Detection for Metaverse based on Blockchain and Online Federated Learning," IEEE Open Journal of the Computer Society, vol. 4, pp. 253–266, 2023, doi: 10.1109/OJCS.2023.3312299.
[40] S. Badri, "HO-CER: Hybrid-optimization-based convolutional ensemble random forest for data security in healthcare applications using blockchain technology," Electronic Research Archive, vol. 31, no. 9, pp. 5466–5484, 2023, doi: 10.3934/ERA.2023278.
[41] S. Thiruvenkatasamy, R. Sivaraj, and M. Vijayakumar, "Blockchain Assisted Fireworks Optimization with Machine Learning based Intrusion Detection System (IDS)," Tehnicki Vjesnik, vol. 31, no. 2, pp. 596–603, 2024, doi: 10.17559/TV-20230712000798.
[42] S. Menon et al., "Blockchain and Machine Learning Inspired Secure Smart Home Communication Network," Sensors, vol. 23, no. 13, Jul. 2023, doi: 10.3390/s23136132.
[43] J. K. Samriya, S. Kumar, M. Kumar, M. Xu, H. Wu, and S. S. Gill, "Blockchain and Reinforcement Neural Network for Trusted Cloud-Enabled IoT Network," IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 2311–2322, Feb. 2024, doi: 10.1109/TCE.2023.3347690.
[44] S. K. Poorazad, C. Benzaıd, and T. Taleb, "Blockchain and Deep Learning-Based IDS for Securing SDN-Enabled Industrial IoT Environments," Dec. 2023, [Online]. Available: http://arxiv.org/abs/2401.00468
[45] G. G. Gebremariam, J. Panda, and S. Indu, "Blockchain-Based Secure Localization against Malicious Nodes in IoT-Based Wireless Sensor Networks Using Federated Learning," Wireless Communications and Mobile Computing, vol. 2023, 2023, doi: 10.1155/2023/8068038.
[46] P. Kumar, R. Kumar, A. Kumar, A. A. Franklin, S. Garg, and S. Singh, "Blockchain and Deep Learning for Secure Communication in Digital Twin Empowered Industrial IoT Network," IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2802–2813, Sep. 2023, doi: 10.1109/TNSE.2022.3191601.

[47] A. A. Sharadqh, H. Hatamleh, A. M. Alnaser, and T. Alawneh, "Hybrid Chain: Blockchain Enabled Framework for Bi-Level Intrusion Detection and Graph-Based Mitigation for Security Provisioning in Edge Assisted IoT Environment," 2023, doi: 10.1109/ACCESS.2017.
[48] J. B. Awotunde, T. Gaber, L. V. N. Prasad, S. O. Folorunso, and V. L. Lalitha, "Privacy And Security Enhancement Of Smart Cities Using Hybrid Deep Learning-Enabled Blockchain," Scalable Computing, vol. 24, no. 3, pp. 561–584, 2023, doi: 10.12694/scpe.v24i3.2272.
[49] R. A. Alsemmeari, M. Y. Dahab, A. A. Alsulami, B. Alturki, and S. Algarni, "Resilient Security Framework Using TNN and Blockchain for IoMT," Electronics (Switzerland), vol. 12, no. 10, May 2023, doi: 10.3390/electronics12102252.
[50] A. A. Wardana, G. Kołaczek, and P. Sukarno, "Lightweight, Trust-Managing, and Privacy-Preserving Collaborative Intrusion Detection for Internet of Things," Applied Sciences (Switzerland), vol. 14, no. 10, May 2024, doi: 10.3390/app14104109.
[51] F. Y. Assiri and M. Ragab, "Optimal Deep-Learning-Based Cyberattack Detection in a Blockchain-Assisted IoT Environment," Mathematics, vol. 11, no. 19, Oct. 2023, doi: 10.3390/math11194080.
[52] D. Ingle and D. Ingle, "An Enhanced Blockchain Based Security and Attack Detection Using Transformer In IOT-Cloud Network," Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 31, no. 2, pp. 142–156, Jul. 2023, doi: 10.37934/araset.31.2.142156.
[53] N. Sunanda, K. Shailaja, P. Kandukuri, V. Sreenivasa Rao, and S. Rao Godla, "Enhancing IoT Network Security: ML and Blockchain for Intrusion Detection". International Journal of Advanced Computer Science and Applications: IJACSA, vol. 15, no. 4, 2024, doi:10.14569/ijacsa.2024.0150497.
[54] R. Jmal et al., "Distributed Blockchain-SDN Secure IoT System Based on ANN to Mitigate DDoS Attacks," Applied Sciences (Switzerland), vol. 13, no. 8, Apr. 2023, doi: 10.3390/app13084953.
[55] D. S. Reddy and K. v Srinivasarao, "A blockchain-based architecture and framework for cybersecure smart cities". IEEE access: practical innovations, open solutions, vol. 11, 2023, pp. 76359–76370, doi:10.1109/access.2023.3296482.
[56] W. Dhifallah, T. Moulahi, M. Tarhouni, and S. Zidi, "Intellig_block: enhancing IoT security with blockchain-based adversarial machine learning protection," International Journal of Advanced Technology and Engineering Exploration, vol. 10, no. 106, pp. 1167–1183, Sep. 2023, doi: 10.19101/ijatee.2023.10101465.
[57] J. Mehare and A. Gaikwad, "Secured Framework for Smart Farming in Hydroponics with Intelligent and Precise Management based on IoT with Blockchain Technology," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, pp. 244–254, 2023, doi: 10.17762/ijritcc.v11i9s.7418.
[58] L. Zhu, S. Hu, X. Zhu, C. Meng, and M. Huang, "Enhancing the Security and Privacy in the IoT Supply Chain Using Blockchain and Federated Learning with Trusted Execution Environment," Mathematics, vol. 11, no. 17, Sep. 2023, doi: 10.3390/math11173759.
[59] Z. Rahman, X. Yi, and I. Khalil, "Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat," p. 1, 2022, doi: 10.48550/arXiv.2201.12727.
[60] IF. Iqbal et al., "Blockchain-Modeled Edge-Computing-Based Smart Home Monitoring System with Energy Usage Prediction," Sensors, vol. 23, no. 11, Jun. 2023, doi: 10.3390/s23115263.
[61] A. Albakri, B. Alabdullah, and F. Alhayan, "Blockchain-Assisted Machine Learning with Hybrid Metaheuristics-Empowered Cyber Attack Detection and Classification Model," Sustainability (Switzerland), vol. 15, no. 18, Sep. 2023, doi: 10.3390/su151813887.
[62] M. Umer et al, "IoT based smart home automation using blockchain and deep learning models," PeerJ Computer Science, vol. 9, 2023, doi: 10.7717/peerj-cs.1332.
[63] W. E. Mbonu, C. Maple, and G. Epiphaniou, "An End-Process Blockchain-Based Secure Aggregation Mechanism Using Federated Machine Learning," Electronics (Switzerland), vol. 12, no. 21, Nov. 2023, doi: 10.3390/electronics12214543.
[64] G. Bravos et al., "Cybersecurity for industrial internet of things: Architecture, models and lessons learned". IEEE access: practical innovations, open solutions, vol. 10, 2022, pp. 124747–124765, doi:10.1109/access.2022.3225074.
[65] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "HBFL: A Hierarchical Blockchain-based Federated Learning Framework for a Collaborative IoT Intrusion Detection," Apr. 2022, [Online]. Available: http://arxiv.org/abs/2204.04254
[66] Alamro, Hayam, et al., "Modelling of blockchain assisted intrusion detection on IoT healthcare system using ant lion optimizer with hybrid deep learning". IEEE access: practical innovations, open solutions, vol. 11, 2023, pp. 82199–82207, doi:10.1109/access.2023.3299589.
[67] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. Srivastava, "Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-based IIoT Networks," Apr. 2022, doi: 10.1109/TII.2022.3168011.
[68] Y. Kang, W. Kim, H. Kim, M. Lee, M. Song, and H. Seo, "Malicious Contract Detection for Blockchain Network Using Lightweight Deep Learning Implemented through Explainable AI," Electronics (Switzerland), vol. 12, no. 18, Sep. 2023, doi: 10.3390/electronics12183893.
[69] Almuqren, Latifah, et al. "Blockchain-assisted secure smart home network using gradient-based optimizer with hybrid deep learning model". IEEE access: practical innovations, open solutions, vol. 11, 2023, pp. 86999–87008, doi:10.1109/access.2023.3303087.
[70] A. M. Hilal et al., "Malware Detection Using Decision Tree Based SVM Classifier for IoT," Computers, Materials and Continua, vol. 72, no. 1, pp. 713–726, 2022, doi: 10.32604/cmc.2022.024501.
[71] L. Xia, Y. Sun, R. Swash, L. Mohjazi, L. Zhang, and M. A. Imran, "Smart and Secure CAV Networks Empowered by AI-Enabled Blockchain: The Next Frontier for Intelligent Safe Driving Assessment," Apr. 2021, doi: 10.1109/MNET.101.2100387.
[72] A. O. N. Sindi, P. Si, and Q. Li, "Secure Task Offloading and Resource Allocation Strategies in Mobile Applications Using Probit Mish-Gated Recurrent Unit and an Enhanced-Searching-Based Serval Optimization Algorithm," Electronics (Switzerland), vol. 13, no. 13, Jul. 2024, doi: 10.3390/electronics13132462.