Artificial Intelligence for IoT Network Security in Peru: A Systematic Analysis of Threat Detection Strategies

Helí Alejandro Córdova-Berona[1] Junior Delgado Flores[2]; Saul Villar Quin[3]; Jose Briones-Zuñiga[4]
[1,2,3,4]Universidad Tecnológica del Perú, *C16068@utp.edu.pe, U22243528@utp.edu.pe, U20230503@utp.edu.pe, C19980@utp.edu.pe*

Abstract*– This study presents a systematic literature review focused on threat detection strategies in Internet of Things (IoT) networks using artificial intelligence techniques, with a particular emphasis on their applicability to the Peruvian context. The PRISMA protocol was applied for the selection and analysis of studies published between 2020 and 2025, covering a range of topics from decision tree and random forest-based smart irrigation systems to advanced deep learning models (autoencoders, CNNs, LSTMs) and explainable artificial intelligence (XAI) approaches for botnet detection. The review identifies methods that achieve the highest detection rates (> 95%), evaluates their scalability on resource-constrained devices, and examines challenges arising from protocol heterogeneity and the lack of security standards. Furthermore, it describes emerging solutions such as blockchain, physical unclonable functions (PUFs), and federated learning to enhance privacy and resilience against both physical and logical attacks. The findings reveal critical gaps in regional adoption, such as the absence of regulatory frameworks and limited edge computing infrastructure, which hinder the implementation of AI-based detection systems. Based on this analysis, a set of recommendations is proposed to guide the development and integration of robust solutions tailored to the technological, economic, and regulatory characteristics of Peru, fostering a more resilient and reliable IoT cybersecurity architecture

Keywords*-- Internet of Things, Network Security, Artificial Intelligence, Intrusion Detection, Threat Detection

Inteligencia Artificial para la Seguridad de Redes IoT en el Perú: Un Análisis Sistemático de Estrategias de Detección de Amenazas

Helí Alejandro Córdova-Berona[1] Junior Delgado Flores[2]; Saul Villar Quin[3]; Jose Briones-Zuñiga[4]
[1,2,3,4]Universidad Tecnológica del Perú, *C16068@utp.edu.pe, U22243528@utp.edu.pe, U20230503@utp.edu.pe, C19980@utp.edu.pe*

Resumen*– Este trabajo presenta una revisión sistemática de la literatura centrada en las estrategias de detección de amenazas en redes de Internet de las Cosas (IoT) mediante técnicas de inteligencia artificial, con un énfasis particular en su aplicabilidad al contexto peruano. Se aplicó el protocolo PRISMA para la selección y análisis de estudios publicados entre 2020 y 2025, abarcando desde sistemas de riego inteligente basados en árboles de decisión y bosques aleatorios hasta modelos avanzados de deep learning (autoencoders, CNN, LSTM) y enfoques de inteligencia artificial explicable (XAI) para la detección de botnets. La revisión identifica los métodos que alcanzan las mayores tasas de detección (> 95 %), evalúa su escalabilidad en dispositivos con recursos limitados y examina los desafíos derivados de la heterogeneidad de protocolos y la falta de estándares de seguridad. Además, se describen soluciones emergentes como blockchain, funciones físicas inmutables cuánticas (PUFs) y aprendizaje federado para mejora de la privacidad y resistencia frente a ataques físicos y lógicos. Los hallazgos revelan brechas críticas en la adopción regional, tales como la carencia de marcos normativos y la limitada infraestructura de cómputo perimetral, que dificultan la implementación de sistemas de detección basados en IA. A partir de este análisis, se proponen un conjunto de recomendaciones para orientar el desarrollo e integración de soluciones robustas y adaptadas a las características tecnológicas, económicas y regulatorias del Perú, fomentando una arquitectura de ciberseguridad IoT más resiliente y confiable.

Palabras clave*— Internet de las Cosas, Seguridad de redes, Inteligencia Artificial, Detección de intrusiones, Detección de Amenazas.

I. Introducción

En los últimos años, el Internet de las Cosas (IoT) ha permitido optimizar procesos en ámbitos tan diversos como la agricultura, las ciudades inteligentes y la salud. Por ejemplo, en agricultura de precisión, la integración de sensores de humedad y temperatura con modelos de árboles de decisión y bosques aleatorios ha demostrado reducir hasta un 30 % el consumo de agua y aumentar el rendimiento de cultivos mediante riego inteligente [1]. Sin embargo, la adopción masiva de IoT enfrenta importantes barreras de infraestructura, financiación y confianza en tecnologías emergentes, como reveló un análisis que combinó PRISMA y DEMATEL para proyectos de ciudades inteligentes en China [2]. Aun así, tecnologías de vanguardia —blockchain, 5G y edge computing— se perfilan como elementos clave para reforzar la trazabilidad y resiliencia de la cadena de suministro urbana, siempre que se establezcan marcos de gobernanza que garanticen interoperabilidad [3]. En el ámbito sanitario, los dispositivos médicos conectados han incorporado modelos supervisados (SVM, K-NN) y redes neuronales convolucionales (CNN) para detectar accesos no autorizados con hasta un 98 % de precisión, aunque este avance requiere esquemas de privacidad diferencial para proteger datos sensibles de pacientes [4].

A pesar de estos progresos, la diversidad de protocolos y las limitaciones de cómputo y energía de los nodos IoT los exponen a ataques de denegación de servicio (DDoS), botnets, spoofing y manipulación de datos. En ese sentido, las investigaciones identifican más de un centenar de contramedidas, estas concluyen que los enfoques híbridos —criptografía ligera combinada con aprendizaje automático— ofrecen el mejor equilibrio entre seguridad y eficiencia energética [5]. Para incrementar la resistencia ante ataques físicos y lógicos, se han propuesto funciones físicas inmutables cuánticas (PUFs) y soluciones basadas en blockchain, si bien aumentan la complejidad de implementación [6]. En cuanto a detección, las técnicas de inteligencia artificial destacan por su capacidad de adaptarse a entornos dinámicos: autoencoders y LSTM, permiten vigilar anomalías en tiempo real, aunque integrarlos en dispositivos con recursos limitados sigue siendo un desafío abierto [7]. Un ejemplo de ello, es lo que se realiza en el campo de la salud conectada (IoMT), el jamming y los replay attacks en la capa de radiofrecuencia pueden ser contrarrestados mediante esquemas de correlación de señal, que han mostrado eficacia en la identificación temprana de estas amenazas [8].

Por otro lado, los sistemas de detección de intrusiones (IDS) basados en deep learning han superado el 99 % de precisión al combinar arquitecturas CNN-autoencoder para identificar tráfico malicioso sin necesidad de etiquetas manuales [9]. Por su parte, los métodos clásicos de machine learning, como Random Forest, mantienen velocidades de entrenamiento elevadas y alcanzan precisiones del orden del 96 %, lo que los hace atractivos en escenarios donde los recursos de cómputo son limitados [10]. En entornos urbanos,

modelos híbridos CNN-LSTM optimizados con algoritmos genéticos han logrado hasta un 99,7 % de precisión en la detección de patrones de ataque en sistemas de gestión de residuos inteligentes [11]. La tendencia actual apunta hacia técnicas de clustering jerárquico y ensamblados (ensembles), aunque la falta de benchmarks homogéneos dificulta la comparación de resultados entre estudios [12]. Estudios comparativos han confirmado que algoritmos como XGBoost y LightGBM ofrecen un compromiso óptimo entre alta precisión (> 95 %) y tiempos de inferencia adecuados para despliegues en edge y cloud [13]. Finalmente, la incorporación de inteligencia artificial explicable (XAI) —mediante herramientas como SHAP y LIME— permite desentrañar las decisiones de los modelos en la detección de botnets, fortaleciendo la confianza de los operadores de red [14].

En el Perú, donde los despliegues de IoT en sectores como la agricultura, el transporte y la salud crecen de forma acelerada, aún faltan análisis que adapten críticamente estas soluciones de detección basadas en IA a las particularidades tecnológicas y regulatorias locales.

II. Metodología

Para abordar de manera rigurosa la revisión sistemática de literatura sobre detección de ciber amenazas en redes IoT en Perú, la investigación se basó en dos métodos aceptados internacionalmente: el modelo PICO y el protocolo PRISMA. El protocolo PRISMA del 2020 se usó para guiar y documentar cada etapa de la revisión sistemática. Se utilizó el modelo PICO para estructurar las preguntas de investigación y facilitar la identificación de publicaciones relevantes. Los componentes PICO para esta RSL son los siguientes:

- P (Población): Redes IoT heterogéneas, incluyendo sistemas de salud conectados (IoMT) y proyectos de ciudades inteligentes.
- I (Intervención): Técnicas avanzadas de Inteligencia Artificial y Aprendizaje Automático, abarcando Machine Learning (ML), Deep Learning (DL), y la Inteligencia Artificial Explicable (XAI).
- C (Comparación): Métodos de detección tradicionales, como *firewalls*.
- O (Resultado): Las mejoras en métricas de rendimiento como precisión, *recall*, *F1-score*, así como la eficiencia operacional y el consumo de recursos de cómputo.

Se elaboró una estrategia de búsqueda centrada en referencias académicas de gran relevancia, empleando la base de datos Scopus como único repositorio principal por su confiabilidad y alcance multidisciplinario. A esto se le agregó una fuente adquirida de manera manual debido a su vinculación directa con el contexto local. La Tabla 1 muestra los criterios empleados para la búsqueda. Además e emplearon conjuntos de términos clave en español e inglés como: inteligencia artificial, detección, ciberseguridad, redes, IoT, técnicas, aprendizaje automático, entre otros vinculados. La ecuación de búsqueda se ajustó para asegurar resultados que cumplieran con el propósito del estudio. Los documentos seleccionados debían cumplir con los siguientes criterios: estar publicados entre los años 2019 y 2024, estar disponibles en acceso abierto, escritos en inglés o español, y clasificados como artículos científicos, papers de conferencia o revisiones. Para finalizar, los documentos que cumplieron con los requisitos tratados, fueron utilizados para el desarrollo e implementación de la presente SRL.

TABLA I
RESUMEN DE LA METODOLOGÍA USADA EN LA BÚSQUEDA

Parámetros de Búsqueda	Parámetros de Búsqueda de Información		
Pregunta de Investigación	¿Qué técnicas de inteligencia artificial y aprendizaje automático se aplican para detectar ciber amenazas en redes IoT?		
Palabras Clave usadas en la Búsqueda	Inteligencia artificial Ciberseguridad. Prevención. Detección de Amenazas. Redes. IoT. Técnicas.		
Repositorio de Datos	Scopus		
Intervalo de Selección	2019-2024		
Idioma	Español	Inglés	
Tipo de Documento	Revisión Sistemática	Conference Paper	Artículo Científico
Accesibilidad	Open Access		
Criterio de Selección	Proceso elaborado en 3 procesos principales, a su vez distribuido en 7 etapas (Figura 1)		
Ecuación General	(TITLE-ABS-KEY ("IoT security" or "network protection" or "Peruvian IoT") and ("machine learning" or "classification algorithms" or "deep learning models") and ("cyberattack detection" or "intrusion detection" or "detection accuracy"))		

Para estructurar y dar mayor claridad a las preguntas de investigación, se empleó el modelo PICO, que permitió definir los componentes clave: la población objetivo, las intervenciones, las comparaciones y los resultados esperados. Esta estructura facilitó la identificación y clasificación de las publicaciones más relevantes para el análisis. La Tabla 2 muestra el desglose de las cuatro preguntas abordadas a partir del modelo PICO.

TABLA II
ESQUEMA PICO

Esquema PICO	Parámetros de Búsqueda de Información
P	¿Cuáles son las principales vulnerabilidades de las redes IoT en Perú frente a ciberataques?
I	¿Qué técnicas de inteligencia artificial y aprendizaje automático se aplican para detectar ciber amenazas en redes IoT?
C	¿Qué diferencias existen entre las técnicas basadas en IA y los métodos tradicionales para la detección de amenazas en redes IoT?
O	¿Qué mejoras en precisión y capacidad de detección ofrecen los sistemas de IA frente a los tradicionales en redes IoT?

Después de haber realizado el proceso de búsqueda de información mediante las palabras claves resultantes de ambas metodologías aplicadas, se obtuvieron 120 registros en Scopus, adicionalmente de haber integrado uno manual de Scielo debido a la pertinencia correspondiente al tema. De los artículos totales, 81 fueron excluidos debido a una relación estrecha entre el objetivo de la RSL, adicionando uno más a la exclusión debido a la duplicidad, los cuales fueron recuperados 38 artículos de los 39 obtenidos, que se utilizaron para el desarrollo de esta RSL. La figura 1 muestra el diagrama de proceso de la metodología PRISMA.

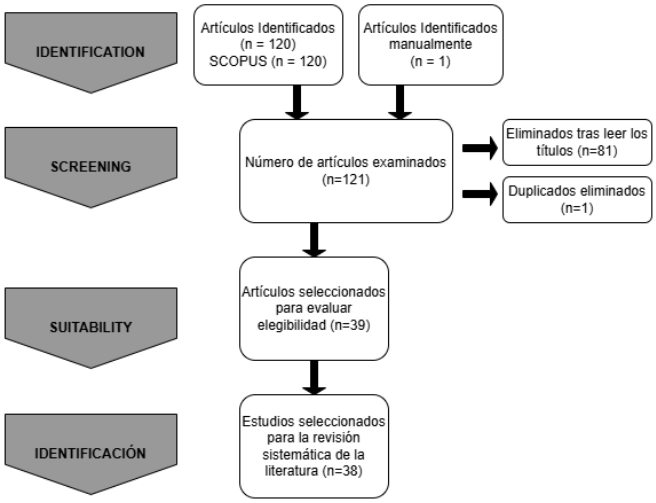

Fig. 1 Diagrama Prisma

III. RESULTADOS

La presente sesión de resultados se divide en dos partes, a partir de las cuales se van analizar los 38 artículos seleccionados.

A. Resultados Bibliométricos

En la presente investigación, los documentos científicos fueron organizados según su año de publicación. La Figura 2 identifica cómo la aplicación de técnicas de inteligencia artificial para la detección de ciber amenazas en redes IoT ha incrementado el interés académico desde 2021, donde en 2024 se registra el mayor número de publicaciones con 17 estudios, representando el 44.7% del total de documentos analizados.

Fig. 2 Artículos por año sobre Inteligencia Artificial en Detección de amenazas en redes IoT

Por otro lado, la Figura 3 muestra que el país India es el que tiene el mayor impacto y dominio sobre el tema, con un total de 19 artículos relacionados con esta RSL. Al mismo tiempo, seguido por los siguientes países: Arabia Saudita, China, Polonia, Estados Unidos, Irak y Perú, entre otros.

Fig. 3 Artículos por país de Origen

Asimismo, la Figura 4 presenta la distribución de los estudios según su enfoque de investigación metodológica, donde la investigación descriptiva predomina con 29 artículos (76.3% del total), mientras que la investigación cualitativa representa 9 artículos (23.7% del total).

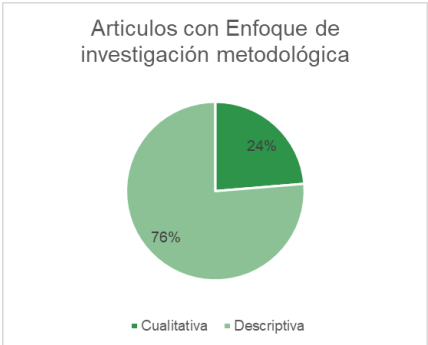

Fig. 4 Artículos dependiendo su enfoque metodológico

Los hallazgos expuestos previamente aportarán significativamente al perfeccionamiento de los procesos de análisis y detección de amenazas en redes IoT, contribuyendo de manera sustancial al cumplimiento tanto del objetivo general como de los objetivos específicos establecidos en esta revisión sistemática de la literatura.

.

B. Resultados de ingeniería

Al principio, se realizó una recopilación de la información analizada en los 38 artículos en base a las preguntas PICO.

P: ¿Cuáles son las principales vulnerabilidades de las redes IoT en Perú frente a ciberataques?

El análisis de los documentos seleccionados para la primera pregunta PICO revela un panorama complejo de vulnerabilidades que afectan múltiples dimensiones de la seguridad en redes IoT. Los ataques de Denegación de Servicio (DoS) emergen como la amenaza más prevalente, siendo identificados en más del 50% de los estudios revisados, lo que evidencia su impacto crítico sobre la disponibilidad de los sistemas [15][16].

Con frecuencia igualmente significativa se identifican la manipulación de datos y los ataques de spoofing, amenazas que aparecen de manera consistente en la literatura analizada y que reflejan una preocupación constante por la integridad y autenticidad de la información en entornos IoT [17][18]. Los ataques DDoS también presentan alta incidencia, acompañados de amenazas como escaneo de red, accesos no autorizados y violaciones de privacidad, configurando un espectro amplio y multifacético de riesgos [19][20].

Esta diversidad de amenazas permite categorizar las vulnerabilidades en cuatro dimensiones fundamentales: disponibilidad, integridad, confidencialidad y control de acceso. Esta clasificación sugiere que los entornos IoT enfrentan un espectro de amenazas en constante evolución, requiriendo estrategias de protección integrales que aborden todos los componentes de la seguridad de la información, trascendiendo enfoques limitados a la confidencialidad o autenticación de usuarios [21][22].

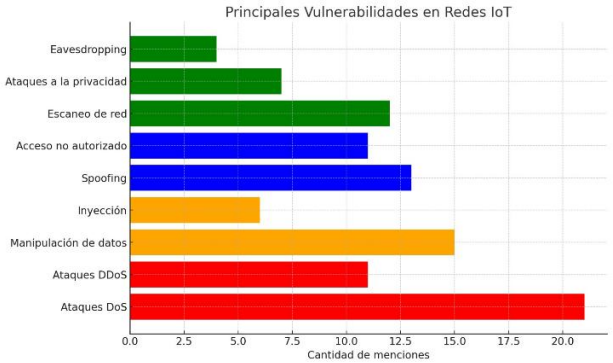

Fig. 5 Principales Vulnerabilidades Detectadas

I: ¿Qué técnicas de inteligencia artificial y aprendizaje automático se aplican para detectar ciber amenazas en redes IoT?

El análisis de la segunda pregunta PICO demuestra que los algoritmos de aprendizaje automático constituyen el núcleo de las estrategias contemporáneas de detección. Random Forest se posiciona como la técnica más utilizada, destacándose en estudios que valoran su equilibrio óptimo entre precisión y eficiencia computacional [23][24]. Support Vector Machine (SVM) mantiene una adopción extendida, particularmente en tareas de clasificación de tráfico malicioso en redes heterogéneas [25][26].

En el ámbito del aprendizaje profundo, se observa una integración creciente de modelos avanzados. Las redes neuronales convolucionales (CNN), las redes neuronales profundas (DNN) y los modelos LSTM demuestran particular eficacia en la detección de patrones anómalos en datos secuenciales y análisis en tiempo real [27][28]. Los enfoques híbridos, como CNN-LSTM, y las técnicas de ensemble learning que combinan múltiples arquitecturas, emergen como estrategias prometedoras para optimizar la precisión de detección [29][30].

Paralelamente, algunas investigaciones exploran el aprendizaje federado como alternativa para preservar la privacidad durante el entrenamiento distribuido, evitando el intercambio de datos sensibles entre nodos [31]. A pesar del avance hacia soluciones más complejas, los algoritmos tradicionales como K-NN, Naive Bayes y Decision Tree mantienen relevancia debido a sus bajos requerimientos computacionales y precisión adecuada para dispositivos IoT con recursos limitados [32][33].

La tendencia hacia la integración de múltiples paradigmas se evidencia en la incorporación de tecnologías complementarias como blockchain y algoritmos metaheurísticos para optimización de hiperparámetros [34][35].

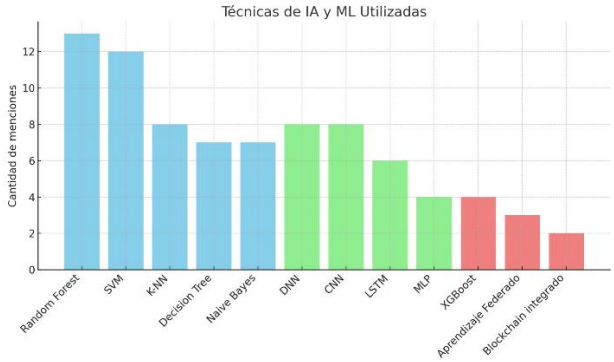

Fig. 6 Técnicas de IA y ML Utilizadas

C: ¿Qué diferencias existen entre las técnicas basadas en IA y los métodos tradicionales para la detección de amenazas en redes IoT?

El análisis de la tercera pregunta PICO revela diferencias sustanciales entre ambos enfoques en términos de capacidades de detección, adaptabilidad y eficiencia operativa. Los métodos tradicionales —firewalls, sistemas de detección de intrusos (IDS), listas negras, detección basada en firmas y reglas fijas— mantienen su importancia en la arquitectura de seguridad, aunque sus limitaciones frente a amenazas emergentes, sofisticadas o no catalogadas están ampliamente documentadas [36][37].

Los firewalls e IDS, aunque fundamentales según múltiples investigaciones, frecuentemente sirven como referencias comparativas que evidencian el rendimiento superior de los modelos basados en aprendizaje automático y profundo [15][38]. La detección basada en firmas y reglas predefinidas presenta limitaciones críticas, incluyendo baja capacidad de generalización y elevadas tasas de falsos negativos, comprometiendo la protección ante ataques novedosos.

En contraste, las técnicas de IA ofrecen capacidades diferenciales: detección de patrones anómalos sin requerir firmas previas, adaptación a condiciones dinámicas de red y reducción significativa de falsos positivos [20][25]. Esta diferencia trasciende lo meramente técnico, representando un cambio paradigmático donde la capacidad predictiva, la automatización del análisis y la escalabilidad adquieren roles decisivos en la protección de infraestructuras inteligentes.

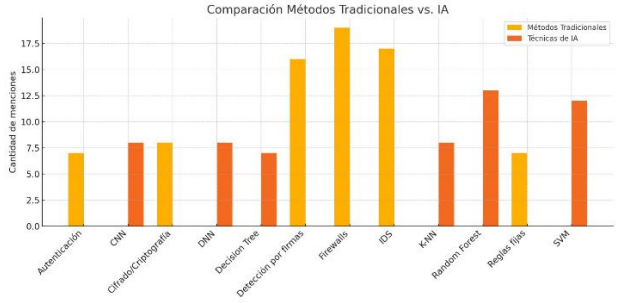

Fig. 7 Comparación entre Métodos tradicionales e IA

O: ¿Qué diferencias existen entre las técnicas basadas en IA y los métodos tradicionales para la detección de amenazas en redes IoT?

Los hallazgos relacionados con la cuarta pregunta PICO documentan beneficios notables en rendimiento, eficiencia y robustez de los modelos basados en IA. La mayoría de los estudios reporta precisiones superiores al 98%, representando mejoras significativas respecto a métodos convencionales [19][24].

Se documenta una reducción importante de falsos positivos, métrica crítica en sistemas de seguridad en tiempo real, ya que minimiza alertas innecesarias que pueden comprometer la operatividad de la red [29][36]. Múltiples investigaciones destacan la capacidad de estos modelos para detectar amenazas desconocidas o variantes de ataques sin entrenamiento previo específico [25][27].

Las métricas de evaluación confirman la solidez del enfoque basado en IA, con valores de F1-score y recall cercanos al 99% [23][33]. Adicionalmente, se reportan mejoras en tiempo de respuesta, escalabilidad y eficiencia en el uso de recursos, aspectos especialmente relevantes para dispositivos con restricciones de procesamiento o energía [28][31].

Finalmente, la incorporación de técnicas de inteligencia artificial explicable (XAI), como SHAP y LIME, permite interpretar las decisiones del modelo, facilitando su validación y aumentando la confianza en su implementación en entornos operativos reales [30][35].

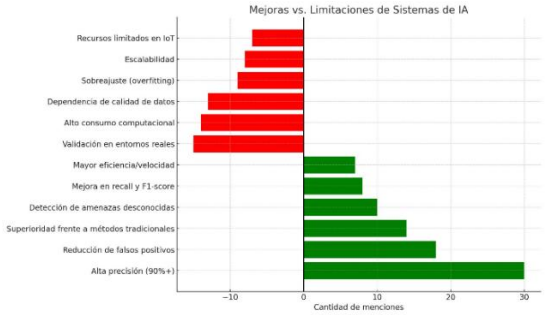

Fig. 8 Mejoras y Limitaciones de Sistemas IA

Finalmente, a modo de síntesis de los gráficos presentados, se presenta la siguiente tabla (TABLA III) donde se observa el rendimiento y eficiencia de las técnicas de detección de amenazas en redes IoT

TABLA III
COMPARATIVA CONSOLIDADA DE TÉCNICAS DE DETECCIÓN DE AMENAZAS EN REDES IOT

Técnica Principal	Precisión Típica (%)	Recall Típico (%)	F1-Score Típico (%)	Consumo de Recursos (Inferencia)
Random Forest (RF)	96-98	95-98	96-98	Bajo a Modera-do
Support Vector Machine (SVM)	95-97	94-96	94 96	Bajo
XGBoost / LightGBM	> 95	Alto	Alto	Bajo/Moderado (Opt.)
Redes Neuronales Profundas (DNN)	98-99	97-99	98-99	Alto
LSTM Redes Recurrentes	98-99.5	98-99	98-99	Muy Alto

Enfoques Híbridos CNN-LSTM	> 99.5	> 99	> 99	Muy Alto
Aprendizaje Federado FL	Variable	Variable	Variable	Moderado (Com.)

La Tabla III ofrece datos cuantitativos clave para evaluar el rendimiento y la eficiencia de las técnicas de inteligencia artificial en la detección de amenazas en redes IoT. Muestra que los algoritmos de Deep Learning, especialmente los híbridos y LSTM, logran precisiones superiores al 99% en la detección de amenazas sofisticadas o desconocidas, pero, su inferencia requiere muchos recursos, por lo que solo puede instalarse en nodos *Fog/Edge L2* de alta capacidad.

En contraste, las técnicas de Machine Learning como Random Forest y XGBoost logran alta precisión (95-98%) y requieren pocos recursos, por lo que son aptas para uso directo en dispositivos de borde con capacidad limitada. Además de la Precisión, tanto el *Recall* como el *F1-Score* tienen relevancia para evaluar la operatividad de los sistemas. El Aprendizaje Federado (FL) se caracteriza principalmente por su capacidad de preservar la privacidad durante el entrenamiento, lo cual resulta especialmente importante en entornos con regulaciones estrictas sobre datos sensibles.

V. Discusión

Los resultados del análisis sistemático revelan un panorama técnico comprehensivo sobre la aplicación de inteligencia artificial para la detección de amenazas en redes IoT, al tiempo que evidencian desafíos significativos para su implementación práctica en contextos como el peruano.

La presencia de ataques DoS y DDoS como amenazas predominantes en las redes IoT pone de manifiesto la necesidad apremiante de establecer mecanismos eficaces para la detección y mitigación de anomalías en el tráfico [15]. El uso de técnicas de aprendizaje automático posibilita la identificación de comportamientos anómalos en tiempo real, lo que contribuye a optimizar la disponibilidad de los sistemas [15]. No obstante, en el caso de Perú, la infraestructura de ciberseguridad limitada obliga a priorizar alternativas que sean factibles y escalables, en especial para servicios críticos que dependen de redes IoT. Por ello, es indispensable adoptar estrategias que permitan una detección temprana y que sean de bajo costo.

En este contexto, se recomienda la implementación de sistemas híbridos de detección de intrusos (IDS) con arquitecturas distribuidas, donde la carga de procesamiento se reparte entre nodos IoT y servidores locales [20]. Este modelo ayuda a disminuir la latencia en la respuesta ante incidentes y garantiza la continuidad operativa [20]. Además, facilita la integración con infraestructuras existentes sin requerir grandes inversiones, fortaleciendo así la disponibilidad y resiliencia de los sistemas IoT en entornos con recursos limitados. Este enfoque es adaptable a las condiciones operativas de Perú.

Respecto a las amenazas que afectan la integridad y autenticidad de los datos, como el spoofing y la manipulación, se sugiere la integración de IDS embebidos en los dispositivos IoT [17]. Asimismo, la utilización de federated learning junto con differential privacy permite proteger información sensible y entrenar modelos de detección sin exponer datos críticos [21]. Estas soluciones refuerzan la confidencialidad y el control de acceso, resultandos indispensables en entornos IoT peruanos cada vez más diversos y vulnerables a ataques, además de contribuir al cumplimiento de las crecientes normativas de privacidad de datos.

El empleo frecuente de Random Forest y Support Vector Machine en la detección de intrusiones en IoT evidencia su capacidad para equilibrar precisión y eficiencia computacional [23][24]. No obstante, en el contexto peruano, resulta fundamental favorecer algoritmos que requieran pocos recursos, permitiendo así su adaptación a dispositivos con capacidades limitadas [26]. Esta estrategia facilita su despliegue en infraestructuras locales sin afectar la operatividad.

Por otra parte, la incorporación de modelos de aprendizaje profundo como CNN, DNN y LSTM posibilita la identificación en tiempo real de patrones complejos y anómalos en datos secuenciales [25][28]. El uso de arquitecturas híbridas, tales como CNN-LSTM o ResNet-GRU, representa una alternativa prometedora para incrementar la precisión ante ataques sofisticados [30]. Sin embargo, su implementación requiere una infraestructura robusta o la aplicación de técnicas de optimización de parámetros debido a su elevado costo computacional.

Así, el aprendizaje federado se posiciona como una opción eficaz para resguardar la privacidad durante el entrenamiento distribuido, evitando la transferencia de datos sensibles [24]. Además, la integración de inteligencia artificial con tecnologías como blockchain y metaheurísticas para la optimización de hiperparámetros refuerza tanto la capacidad de detección como la confianza en el sistema [32][34]. Estas soluciones integradas resultan esenciales para entornos IoT en Perú que buscan una seguridad escalable y sostenible.

Los métodos convencionales, como los firewalls y los sistemas de detección de intrusos (IDS) basados en firmas, continúan siendo pilares fundamentales en la seguridad de IoT, ya que permiten filtrar el tráfico y detectar amenazas previamente identificadas [36]. No obstante, estos enfoques presentan limitaciones significativas frente a ataques novedosos o sofisticados que no se encuentran registrados en sus bases de datos, lo que provoca una elevada tasa de falsos negativos [37]. Esto afecta la capacidad de defensa contra amenazas emergentes.

Por un lado, los modelos de inteligencia artificial y aprendizaje automático ofrecen la ventaja de identificar patrones anómalos sin depender de firmas predefinidas, mejorando así la respuesta ante ciberataques desconocidos [20]. Su habilidad para adaptarse a las condiciones cambiantes de la

red es crucial en entornos IoT heterogéneos, lo que incrementa su eficacia frente a nuevas variantes de amenazas. [25].

Por otro lado, la integración de técnicas tradicionales con inteligencia artificial puede constituir una solución integral para las redes IoT en Perú, combinando la detección basada en firmas para amenazas conocidas con el aprendizaje automático para ataques más avanzados [15]. Este enfoque híbrido permite optimizar los recursos, disminuir los falsos positivos y asegurar una protección continua en infraestructuras inteligentes, además de facilitar una transición gradual hacia modelos de ciberseguridad predictiva.

Además, los modelos de inteligencia artificial superan ampliamente a los métodos tradicionales al alcanzar precisiones superiores al 98%, garantizando una detección eficaz de amenazas en redes IoT [24]. Además, su capacidad para identificar amenazas desconocidas o variaciones de ataques sin necesidad de entrenamiento específico fortalece su utilidad frente a ciberataques avanzados [25][27]. Estas características representan un avance fundamental hacia sistemas de seguridad IoT predictivos y adaptativos.

De ese modo, los enfoques basados en IA disminuyen los falsos positivos y mejoran indicadores como el F1-score y el recall, alcanzando valores cercanos al 99%, lo que aumenta la confiabilidad operativa [23][33]. La incorporación de técnicas explicativas como SHAP y LIME facilita la interpretación de las decisiones del modelo, permitiendo su validación y generando confianza para su aplicación en entornos reales [35]. Estas soluciones consolidan un enfoque integral, robusto y escalable para la seguridad en IoT.

Finalmente, en línea con las recomendaciones que se han ido presentado a lo largo de esta investigación, es importante mencionar que, el Estado peruano debe establecer leyes claras que asignen responsabilidades en la protección de redes IoT ante ciberataques. La Estrategia Nacional de Ciberseguridad 2026-2028 (ESNACIB) [53] redefine las políticas públicas al fijar un marco estatal para proteger infraestructuras críticas y reforzar el ciberespacio, evidenciado en compras gubernamentales como la adquisición de equipamiento de ciberseguridad para EGASA a través de PERÚ COMPRAS. Sin embargo, ESNACIB necesita pasar de un enfoque general a exigir la adopción de modelos de detección de anomalías basados en IA, superando los sistemas tradicionales con firmas, para enfrentar eficazmente las amenazas cambiantes [12]

VI. CONCLUSIÓN

La presente revisión sistemática confirma la relevancia de la inteligencia artificial como herramienta clave para fortalecer la detección de amenazas en redes IoT, destacando su capacidad para identificar ataques desconocidos y reducir falsos positivos. Sin embargo, en el contexto peruano se evidencia la necesidad de adoptar estrategias híbridas que integren métodos tradicionales y modelos de aprendizaje automático optimizados para dispositivos con recursos limitados. Asimismo, la incorporación de enfoques como el aprendizaje federado y blockchain puede contribuir a mejorar la privacidad y la confianza en los sistemas. Finalmente, es esencial orientar el desarrollo de estas soluciones hacia arquitecturas escalables y accesibles, adaptadas a las condiciones tecnológicas y regulatorias locales, para garantizar una ciberseguridad IoT más sólida y sostenible en el país.

REFERENCIAS

[1] N. P. Kalpana, N. L. Smitha, N. D. Madhavi, N. S. A. Nabi, N. G. Kalpana, and S. Kodati, “A smart irrigation system using the IoT and advanced machine learning model,” International Journal of Computational and Experimental Science and Engineering, vol. 10, no. 4, Nov. 2024, doi: 10.22399/ijcesen.526.

[2] K. Wang, Y. Zhao, R. K. Gangadhari, and Z. Li, “Analyzing the adoption challenges of the internet of things (IoT) and artificial intelligence (AI) for smart cities in China,” Sustainability, vol. 13, no. 19, p. 10983, Oct. 2021, doi: 10.3390/su131910983.

[3] B. Najafi, A. Najafi, F. Madanchi, H. Maghroor, and H. Taherdoost, “The Impact of Cutting-Edge Technologies on Smart City Supply Chain: A Systematic Literature Review of the evidence and implications,” IEEE Engineering Management Review, vol. 52, no. 3, pp. 148–171, Mar. 2024, doi: 10.1109/emr.2024.3373502.

[4] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, “Security analysis of IoT Devices by using Mobile Computing: A Systematic Literature Review,” IEEE Access, vol. 8, pp. 120331–120350, Jan. 2020, doi: 10.1109/access.2020.3006358.

[5] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches,” Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, Oct. 2020, doi: 10.1002/ett.4150.

[6] R. Shah and A. Chircu, “IOT AND AI IN HEALTHCARE: A SYSTEMATIC LITERATURE REVIEW,” Issues in Information Systems, Jan. 2018, doi: 10.48009/3_iis_2018_33-41.

[7] M. S. Farooq, S. Riaz, A. Abid, T. Umer, and Y. B. Zikria, “Role of IoT Technology in Agriculture: A Systematic Literature review,” Electronics, vol. 9, no. 2, p. 319, Feb. 2020, doi: 10.3390/electronics9020319.

[8] I. A. Jayaraj et al., “A Systematic Review of Radio Frequency Threats in IoMT,” J. Sens. Actuator Networks, vol. 11, no. 4, p. 62, Sep. 2022. doi: 10.3390/jsan11040062

[9] M. A. Alsoufi et al., “Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic literature review,” Applied Sciences, vol. 11, no. 18, p. 8383, Sep. 2021, doi: 10.3390/app11188383.

[10] A. D. Saleem y A. A. Abdulrahman, “Attacks Detection in Internet of Things Using Machine Learning Techniques: A Review,” JAETS, vol. 6, no. 1, pp. 684–703, Dec. 2024. doi: 10.37385/jaets.v6i1.4878

[11][11] M. M. Aborokbah, “A Novel Intrusion Detection Model for Enhancing Security in Smart City,” IEEE Access, vol. 12, pp. 107431–107444, Jan. 2024. doi: 10.1109/ACCESS.2024.3438619

[12] M. Berhili et al., “Intrusion Detection Systems in IoT Based on Machine Learning: A State of the Art,” Procedia Comput. Sci., vol. 251, pp. 99–107, 2024. doi: 10.1016/j.procs.2024.11.089

[13] T. Saranya et al., “Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review,” Procedia Comput. Sci., vol. 171, pp. 1251–1260, 2020. doi: 10.1016/j.procs.2020.04.133

[14] M. Saied y S. Guirguis, “Explainable Artificial Intelligence for Botnet Detection in Internet of Things,” Sci. Rep., vol. 15, no. 1, Mar. 2025. doi: 10.1038/s41598-025-90420-6

[15] H. Hakami, M. Faheem, and M. B. Ahmad, “Machine learning techniques for enhanced intrusion detection in IoT security,” IEEE Access, p. 1, Jan. 2025, doi: 10.1109/access.2025.3542227.

[16] S. Verma and C. Prakash, “IOT Security Against Network Anomalies through Ensemble of Classifiers Approach,” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 7s, pp. 54–63, Jul. 2023, doi: 10.17762/ijritcc.v11i7s.6976.

[17] A. Javed, M. N. Awais, A.-U.-H. Qureshi, M. Jawad, J. Arshad, and H. Larijani, “Embedding Tree-Based intrusion Detection System in smart thermostats for enhanced IoT security,” Sensors, vol. 24, no. 22, p. 7320, Nov. 2024, doi: 10.3390/s24227320.

[18] N. A. Shaik, N. B. Unhelkar, and N. P. Chakrabarti, “Exploring Artificial Intelligence and Data Science-Based Security and its Scope in IoT Use Cases,” International Journal of Computational and Experimental Science and Engineering, vol. 11, no. 1, Feb. 2025, doi: 10.22399/ijcesen.869.
[19] “Hybrid IDS architecture for IoT security enhancing threat detection with CPBNN and CNN models,” International Journal of Advanced Technology and Engineering Exploration, vol. 11, no. 120, Nov. 2024, doi: 10.19101/ijatee.2024.111100172.
[20] H. A. Tarish, R. Hassan, K. A. Z. Ariffin, and M. M. Jaber, “Network security framework for Internet of medical things applications: A survey,” Journal of Intelligent Systems, vol. 33, no. 1, Jan. 2024, doi: 10.1515/jisys-2023-0220.
[21] A. U. Karimy and P. C. Reddy, “Enhancing IoT Security: A Novel Approach with Federated Learning and Differential Privacy Integration,” International Journal of Computer Networks & Communications, vol. 16, no. 4, pp. 01–17, Jul. 2024, doi: 10.5121/ijcnc.2024.16401.
[22] A. Houkan et al., “Enhancing security in industrial IoT networks: machine learning solutions for feature selection and reduction,” IEEE Access, p. 1, Jan. 2024, doi: 10.1109/access.2024.3481459.
[23] M. Mohy-Eddine, A. Guezzaz, S. Benkirane, M. Azrour, and Y. Farhaoui, “An ensemble learning based intrusion detection model for industrial IoT security,” Big Data Mining and Analytics, vol. 6, no. 3, pp. 273–287, Apr. 2023, doi: 10.26599/bdma.2022.9020032.
[24] J. P. Singh and R. Kazmi, “FusionSEC-IOT: a federated Learning-Based intrusion detection system for enhancing security in IoT networks,” International Journal of Advanced Computer Science and Applications, vol. 15, no. 11, Jan. 2024, doi: 10.14569/ijacsa.2024.0151116.
[25] A. Odeh and A. A. Taleb, “Robust Network Security: A deep learning approach to intrusion detection in IoT,” Computers, Materials & Continua/Computers, Materials & Continua (Print), vol. 0, no. 0, pp. 1–10, Jan. 2024, doi: 10.32604/cmc.2024.058052.
[26] D. F. Doghramachi and S. Y. Ameen, “Internet of Things (IoT) security enhancement using XGBoost Machine learning techniques,” Computers, Materials & Continua/Computers, Materials & Continua (Print), vol. 77, no. 1, pp. 717–732, Jan. 2023, doi: 10.32604/cmc.2023.041186.
[27] L. K. R, D. K. V. K, and P. P, “Advancing IoT Security with an Innovative Machine Learning Paradigm for Botnet Attack Detection,” EAI Endorsed Transactions on Internet of Things, vol. 11, Feb. 2025, doi: 10.4108/eetiot.4521.
[28] M. Almohaimeed and F. Albalwy, “Enhancing IoT network security using feature selection for intrusion detection systems,” Applied Sciences, vol. 14, no. 24, p. 11966, Dec. 2024, doi: 10.3390/app142411966.
[29] T. Althiyabi, I. Ahmad, and M. O. Alassafi, “Enhancing IoT Security: A Few-Shot learning approach for intrusion detection,” Mathematics, vol. 12, no. 7, p. 1055, Mar. 2024, doi: 10.3390/math12071055.
[30] J. A and M. A. E. A, “A novel paradigm for IoT security: ResNet-GRU model revolutionizes botnet attack detection,” International Journal of Advanced Computer Science and Applications, vol. 14, no. 12, Jan. 2023, doi: 10.14569/ijacsa.2023.0141231.
[31] D.-M. Ngo et al., “HH-NIDS: Heterogeneous Hardware-Based Network Intrusion Detection Framework for IoT Security,” Future Internet, vol. 15, no. 1, p. 9, Dec. 2022, doi: 10.3390/fi15010009.
[32] W. Villegas-Ch, J. Govea, R. Gurierrez, and A. Mera-Navarrete, “Optimizing security in IoT ecosystems using hybrid artificial intelligence and blockchain models: a scalable and efficient approach for threat detection,” IEEE Access, p. 1, Jan. 2025, doi: 10.1109/access.2025.3532800.
[33] 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, Sep. 2023, doi: 10.19101/ijatee.2023.10101465.
[34] J. Jose and J. JE, “Deep Learning Model with Normalized Bayesian Optimizer for Anomaly Classification in IoT Security,” International Journal of Electronics and Communication Engineering, vol. 11, no. 8, pp. 185–199, Aug. 2024, doi: 10.14445/23488549/ijece-v11i8p119.
[35] B. Mopuru and Y. Pachipala, “Advancing IoT Security: Integrative machine learning models for enhanced intrusion detection in wireless sensor networks,” Engineering Technology & Applied Science Research, vol. 14, no. 4, pp. 14840–14847, Aug. 2024, doi: 10.48084/etasr.7641.
[36] K. Bella et al., “An efficient intrusion detection system for IoT security using CNN decision forest,” PeerJ Computer Science, vol. 10, p. e2290, Sep. 2024, doi: 10.7717/peerj-cs.2290.
[37] Z. Chen et al., “Machine Learning-Enabled IoT Security: Open issues and challenges under Advanced Persistent Threats,” ACM Computing Surveys, vol. 55, no. 5, pp. 1–37, Apr. 2022, doi: 10.1145/3530812.
[38] D. Alsalman, “A comparative study of anomaly detection Techniques for IoT Security using Adaptive Machine Learning for IoT threats,” IEEE Access, vol. 12, pp. 14719–14730, Jan. 2024, doi: 10.1109/access.2024.3359033.
[39] J. Li, H. Chen, M. O. Shahizan, and L. M. Yusuf, “Enhancing IoT security: A comparative study of feature reduction techniques for intrusion detection system,” Intelligent Systems With Applications, vol. 23, p. 200407, Jun. 2024, doi: 10.1016/j.iswa.2024.200407.
[40] M. Dobrojevic, M. Zivkovic, A. Chhabra, N. S. Sani, N. Bacanin, and M. M. Amin, “Addressing Internet of Things security by enhanced sine cosine metaheuristics tuned hybrid machine learning model and results interpretation based on SHAP approach,” PeerJ Computer Science, vol. 9, p. e1405, Jun. 2023, doi: 10.7717/peerj-cs.1405.
[41] H. Assmi et al., “A robust security detection strategy for next generation IoT networks,” Computers, Materials & Continua/Computers, Materials & Continua (Print), vol. 82, no. 1, pp. 443–466, Jan. 2025, doi: 10.32604/cmc.2024.059047.
[42] A. Yang et al., “Application of meta-learning in cyberspace security: a survey,” Digital Communications and Networks, vol. 9, no. 1, pp. 67–78, Mar. 2022, doi: 10.1016/j.dcan.2022.03.007.
[43] T. Nagaraj and R. K. Channarayappa, “An efficient security framework for intrusion detection and prevention in internet-of-things using machine learning technique,” International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering, vol. 14, no. 2, p. 2313, Jan. 2024, doi: 10.11591/ijece.v14i2.pp2313-2321.
[44] K. M. Harahsheh and C.-H. Chen, “A survey of using machine learning in IoT security and the challenges faced by researchers,” Informatica, vol. 47, no. 6, May 2023, doi: 10.31449/inf.v47i6.4635.
[45] N. Sunanda, K. Shailaja, P. Kandukuri, Krishnamoorthy, V. S. Rao, and S. R. Godla, “Enhancing IoT network security: ML and blockchain for intrusion detection,” International Journal of Advanced Computer Science and Applications, vol. 15, no. 4, Jan. 2024, doi: 10.14569/ijacsa.2024.0150497.
[46] I. Mutambik, “An efficient Flow-Based anomaly detection system for enhanced security in IoT networks,” Sensors, vol. 24, no. 22, p. 7408, Nov. 2024, doi: 10.3390/s24227408.
[47] S. Rahman, S. Pal, S. Mittal, T. Chawla, and C. Karmakar, “SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security,” Internet of Things, vol. 26, p. 101212, May 2024, doi: 10.1016/j.iot.2024.101212.
[48] A. Jain, T. Singh, and S. K. Sharma, “Security as a solution: An intrusion detection system using a neural network for IoT enabled healthcare ecosystem,” Interdisciplinary Journal of Information Knowledge and Management, vol. 16, pp. 331–369, Jan. 2021, doi: 10.28945/4838.
[49] N. Mazhar, R. Saleh, R. Zaba, M. Zeeshan, M. M. Hameed, and N. Khan, “R-IDPS: real time SDN-Based IDPS system for IoT security,” Computers, Materials & Continua/Computers, Materials & Continua (Print), vol. 73, no. 2, pp. 3099–3118, Jan. 2022, doi: 10.32604/cmc.2022.028285.
[50] R. J. Alzahrani and A. Alzahrani, “Security analysis of DDOS attacks using machine learning algorithms in networks traffic,” Electronics, vol. 10, no. 23, p. 2919, Nov. 2021, doi: 10.3390/electronics10232919.
[51] B. S. Khater et al., “Classifier Performance Evaluation for Lightweight IDS using FOG computing in IoT Security,” Electronics, vol. 10, no. 14, p. 1633, Jul. 2021, doi: 10.3390/electronics10141633.
[52] G. Kornaros, “Hardware-Assisted Machine Learning in Resource-Constrained IoT Environments for Security: review and future Prospective,” IEEE Access, vol. 10, pp. 58603–58622, Jan. 2022, doi: 10.1109/access.2022.3179047.
[53]Presidencia del Consejo de Ministros, “Estrategia Nacional de Ciberseguridad del Perú 2026-2028 (ESNACIB)”. Lima, Perú: PCM, Ago. 15, 2025. https://www.gob.pe/institucion/pcm/informes-

publicaciones/7046161-estrategia-nacional-de-ciberseguridad-del-peru-2026-2028-esnacib