ISBN: 978-628-96613-1-6. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2025.1.1.2032

Systematic Review of Machine Learning and Deep Learning Applications in the Development of Smart Homes Using IoT

Castro-García, José Heiner[1], Mg.; Miranda-Saldaña, Rodolfo Junior[2], Mg; Ocaña-Velásquez, Jesús Daniel[3], Dr.
[1,3]Universidad Tecnológica del Perú, Chimbote, Perú, *c20312@utp.edu.pe, e20206@utp.edu.pe, c25777@utp.edu.pe*

Abstract– ***The advancement of technology has led to a remarkable development in smart homes, where remote and automated management of connected devices transforms the user experience. This article systematically reviews the applications of Machine Learning and Deep Learning in the development of smart homes through the Internet of Things (IoT) technology. The objective of this research is to carry out a systematic review on the application of Machine Learning and Deep Learning in smart homes connected to IoT, focusing on energy efficiency, security and comfort, as well as identifying trends, challenges and opportunities for improvement to serve as a guide for researchers and developers. The PRISMA method was used to gather 68 relevant articles. The results show that Machine Learning and Deep Learning play a fundamental role in this field, with a greater number of investigations carried out in China and India. The most common methods in Machine Learning are Random Forest and Decision Trees, while in Deep Learning LSTM and CNN stand out. It is concluded that Machine Learning and Deep Learning are essential to improve security and Quality of Service by identifying and solving problems in advance. Deep Learning, in particular, improves surveillance and motion detection, and its combination with Machine Learning promises to transform monitoring, creating more integrated and efficient management systems.***

Keywords-- ***Machine Learning, Deep Learning, Smart Homes, Internet of Things (IoT).***

Revisión Sistemática de las Aplicaciones de Machine Learning y Deep Learning en el Desarrollo de Hogares Inteligentes Mediante IoT

Castro-García, José Heiner[1], Mg.; Miranda-Saldaña, Rodolfo Junior[2], Mg; Ocaña-Velásquez, Jesús Daniel[3], Dr.
[1,3]Universidad Tecnológica del Perú, Chimbote, Perú, *c20312@utp.edu.pe, e20206@utp.edu.pe, c25777@utp.edu.pe*

Resumen- El avance de la tecnología ha propiciado un notable desarrollo en hogares inteligentes., donde la gestión remota y automatizada de dispositivos conectados transforma la experiencia del usuario. Este artículo revisa sistemáticamente las aplicaciones de Machine Learning y Deep Learning en el desarrollo de hogares inteligentes a través de la tecnología del Internet de las Cosas (IoT). El objetivo de esta investigación es realizar una revisión sistemática sobre la aplicación de Machine Learning y Deep Learning en hogares inteligentes conectados a IoT, enfocándose en la eficiencia energética, seguridad y comodidad, así como identificar tendencias, desafíos y oportunidades de mejora para servir de guía a investigadores y desarrolladores. Se utilizó el método PRISMA para reunir 68 artículos pertinentes. Los resultados muestran que el Machine Learning y el Deep Learning desempeñan un papel fundamental en este campo, con un mayor número de investigaciones llevadas a cabo en China e India. Los métodos más comunes en Machine Learning son Bosque aleatorio y árboles de decisión, mientras que en Deep Learning destacan LSTM y CNN. Se concluye que Machine Learning y Deep Learning son fundamentales para mejorar la seguridad y la Calidad del Servicio al identificar y resolver problemas de manera anticipada. El Deep Learning, en particular, mejora la vigilancia y detección de movimiento, y su combinación con Machine Learning promete transformar el monitoreo, creando sistemas de gestión más integrados y eficientes.

Palabras clave-- Machine Learning, Deep Learning, Hogares Inteligentes, Internet de las Cosas (IoT).

I. Introducción

El uso de tecnologías innovadoras ha impulsado la creación de hogares inteligentes, donde los dispositivos conectados se gestionan de forma remota y automatizada. Este fenómeno, ha cobrado relevancia en los últimos años, mejora la calidad de vida, aumenta la eficiencia energética y refuerza la seguridad en el hogar [1], [2], [3] .

Los hogares inteligentes, gracias a la tecnología del Internet de las Cosas (IoT), mejoran nuestra interacción con el hogar al conectar dispositivos electrónicos y ofrecer servicios inteligentes que enriquecen la calidad de vida [4], [5].

La inteligencia artificial y Machine Learning están revolucionando en los hogares inteligentes, al automatizar la interacción con dispositivos, anticipar hábitos de los usuarios y mejorar la eficiencia energética y la seguridad [6], [7].

Los algoritmos de Machine Learning son fundamentales para su desarrollo, destacando entre los más comunes: regresión lineal, clasificador Bayesiano ingenuo, máquinas de soporte vectorial (SVM), redes neuronales, árboles de decisión, bosque aleatorio y K vecinos más cercanos (KNN). Cada uno tiene características únicas que los hacen adecuados para diferentes problemas [8], [9].

Las CNN, RNN y LSTM son algoritmos de Deep Learning especializados: las CNN son ideales para el procesamiento de imágenes, las RNN se utilizan para datos secuenciales, y las LSTM son clave para gestionar dependencias a largo plazo. Estas redes han revolucionado áreas como la visión por computadora y el procesamiento del lenguaje natural [10].

La investigación busca entender la aplicación efectiva de técnicas de Machine Learning y Deep Learning en hogares inteligentes mediante IoT, abordando limitaciones y desafíos actuales, y ofreciendo una revisión sistemática para guiar futuras investigaciones y desarrollos.

El objetivo de esta investigación es llevar a cabo una revisión sistemática sobre el uso de Machine Learning y Deep Learning en hogares inteligentes mediante IoT, centrada en la eficiencia energética, seguridad y comodidad, así como identificar tendencias, desafíos y oportunidades de mejora, para ofrecer un marco de referencia útil para investigadores y desarrolladores.

Este documento está estructurado en cinco partes: la primera examina investigaciones anteriores, la segunda expone la metodología empleada, la tercera muestra los resultados, la cuarta analiza estos resultados y, por último, se exponen las conclusiones.

II. Trabajo relacionado

El estudio [11] indica que la seguridad en línea ha cobrado relevancia al proporcionar soluciones que fortalecen la protección de dispositivos IoT y hogares inteligentes. Este estudio ofrece un análisis exhaustivo de diversas arquitecturas y tecnologías diseñadas para prevenir y detectar ataques cibernéticos. Entre las estrategias abordadas se encuentran las técnicas de detección de anomalías, el uso de firmas y la aplicación de aprendizaje automático. Además, se lleva a cabo una comparación detallada del rendimiento de estas técnicas, así como de las herramientas utilizadas, sus beneficios y sus limitaciones.

De acuerdo al [12] indica que este trabajo contribuye al campo de la localización en interiores para la vida asistida en hogares inteligentes mediante un estudio comparativo de diversos métodos de aprendizaje automático, como bosque aleatorio, redes neuronales, y otros. Concluye en identificar el enfoque óptimo para la localización en interiores. Además, integra avances en Big Data, aprendizaje automático, Internet de las cosas y tecnologías de vida asistida, abordando múltiples desafíos de investigación en este ámbito.

El estudio de [13] presenta una técnica innovadora para predecir la ocupación en hogares inteligentes, basada en variables ambientales, que optimiza la gestión energética del sistema de calefacción eléctrica. Se destaca el uso de una red neuronal de memoria a largo plazo (LSTM), una metodología de aprendizaje profundo eficaz para series de tiempo, que ha mostrado resultados prometedores. Los hallazgos indican que un LSTM optimizado puede reducir el consumo energético y mejorar la seguridad y el confort de los ocupantes. Se sugiere que futuras investigaciones podrían centrarse en la predicción de parámetros térmicos en distintos tipos de edificaciones, como hospitales y hoteles.

La investigación [14] menciona que el hogar inteligente, parte del ámbito de las redes IoT, enfrenta riesgos de seguridad debido a la interconexión de electrodomésticos. Para abordar este problema, se han desarrollado sistemas de detección que utilizan técnicas de aprendizaje automático y profundo. Se propone una solución innovadora para detectar intrusiones mediante la identificación de anomalías en estas redes. El modelo híbrido presentado muestra un rendimiento óptimo, con mejoras significativas en la clasificación y reducción de errores en comparación con soluciones actuales.

III. Metodología

En este estudio, se utiliza el método PRISMA, que permite una documentación clara y precisa de los datos obtenidos de artículos importantes relacionados con este tema.

A. Preguntas de Investigación

Se realizaron cuatro preguntas de investigación utilizando el modelo PICO.

RQ1: ¿Cuáles son las principales aplicaciones de Machine Learning y Deep Learning utilizados en hogares inteligentes mediante IoT?

RQ2: ¿Cuáles son los algoritmos más utilizados de Machine Learning y Deep Learning en las aplicaciones de Hogares Inteligentes?

RQ3: ¿Cuáles son las principales limitaciones de Machine Learning y Deep Learning en las aplicaciones de Hogares Inteligentes Mediante IoT?

RQ4: ¿Como la integración de técnicas de Machine Learning y Deep Learning contribuye al desarrollo de hogares inteligentes?

B. Estrategia de búsqueda

La investigación se realiza a través de una cuidadosa estrategia de búsqueda y la utilización de filtros en bases de datos reconocidas, como Scopus, ScienceDirect, Web of Science, IEEE Xplore y EBSCOhost, con el propósito de localizar artículos pertinentes. A continuación, se aplican criterios de inclusión y exclusión, según la Tabla 1 y la guía PRISMA, para seleccionar artículos para el análisis del estudio. La estrategia de búsqueda se enfoca en localizar artículos que incluyan tanto el título como las palabras clave relacionadas con el estudio de la siguiente manera:

("smart homes" OR "smart home" OR "Home Automation" OR "Home Security") AND ("Artificial Intelligence" OR "Machine Learning" OR "Deep Learning") AND (IoT OR "internet of things" OR "Quality of Service" OR Applications OR Integration OR Limitations OR Security OR Sensors OR "Alarm systems" OR Comfort)

C. Criterios de inclusión y exclusión

Los criterios de inclusión y exclusión empleados en esta revisión sistemática se detallan minuciosamente en la Tabla 1.

TABLA I
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Criterios		
Inclusión	I01	Artículos relacionados con Machine Learning o Deep Learning en el desarrollo de casa inteligentes.
	I02	Artículos que exploran el desarrollo de hogares inteligentes mediante la implementación de técnicas de Machine Learning y Deep Learning a través de Internet de las Cosas (IoT).
	I03	Artículos en inglés
	I04	Artículos de los últimos 4 años (2021 -2024).
Exclusión	E01	Artículos que no guardan relación con el tema de investigación
	E02	Artículos que no tengan Open Access
	E03	Artículos que no están relacionados con Machine Learning o Deep Learning aplicados a los hogares inteligentes.

En la figura 1 se aplicó el método PRISMA en tres fases para seleccionar artículos de cinco bases de datos, comenzando con 8149 artículos. Después de eliminar 218 duplicados, se encontraron 7931 artículos. Al filtrar por acceso abierto, quedaron 1756, de los cuales se revisaron exhaustivamente y se descartaron 1130 por no cumplir con los criterios de inclusión, resultando en 626 para evaluación. Finalmente, se eliminaron 558 por irrelevancia, seleccionando 68 artículos para el estudio.

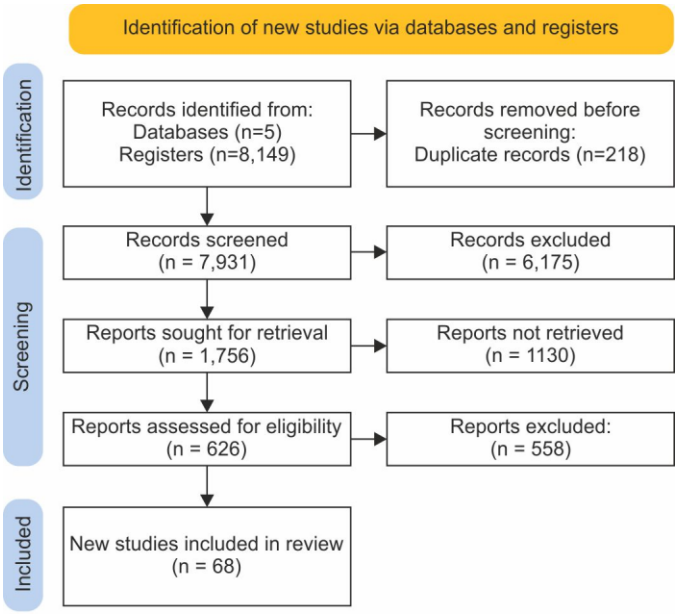

Fig. 1 Selección de artículos científicos según método PRISMA

IV. Resultados

Se realiza un análisis bibliométrico de 68 artículos que cumplen con los criterios de inclusión definidos.

A. *Análisis bibliométrico*

A través de VOSViewer, se llevó a cabo un análisis de investigaciones que generó redes de palabras clave y mapas visuales, lo que ayuda a interpretar los datos. Se analizaron 195 palabras clave, lo que resultó en la identificación de 21 términos fundamentales.

Al analizar el mapa de la red mostrado en la Figura 2, se pueden identificar 21 términos clave que muestran conexiones significativas. Por ejemplo, el nodo "smart homes" se relaciona estrechamente con "Machine Learning", "Deep Learning" y “artificial intelligence”. Por su parte, "Machine Learning" presenta conexiones con "artificial intelligence", "internet of things (IoT)", "smart city", "cloud computing", "energy management", "energy utilization" y "energy efficiency". Asimismo, el nodo "smart homes" se relaciona con "domestic appliances", "home automation", “sensor”, "home security", "cyber security", "network security", "home networks" y "security". Finalmente, el nodo "deep learning" está conectado con "blockchain", "intrusion-detection" y "smart devices".

El nodo "Smart homes" se sitúa en el centro de la red, lo que resalta la relevancia de implementar estas tecnologías en el desarrollo de hogares inteligentes.

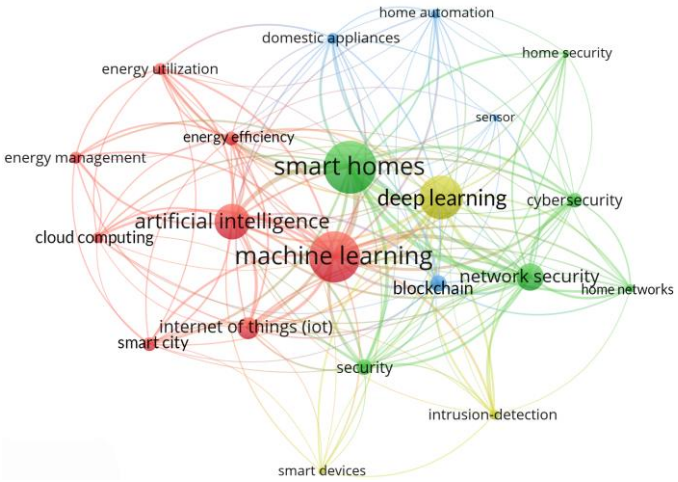

Fig. 2 Mapa bibliométrico de las relaciones entre palabras clave

B. *Análisis de manuscritos*

Se llevó a cabo un análisis de artículos en cinco bases de datos: Scopus, ScienceDirect, Web of Science, EBSCO Host e IEEE Xplore. Inicialmente, se identificaron 8,149 investigaciones, de las cuales se descartaron 218 duplicados. Después de aplicar los criterios de inclusión y exclusión, se eligieron 68 estudios, como se presenta en la Figura 3.

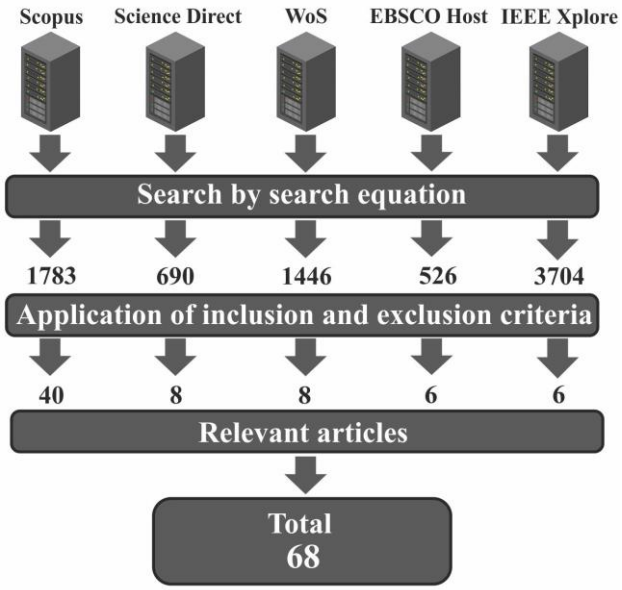

Fig. 3 Resultados obtenidos en la búsqueda.

La Figura 4 ofrece una representación detallada del porcentaje de contribución informativa de diversas bases de datos, destacando a Scopus como la principal fuente, con un impresionante 58.8% de la contribución total. A continuación, Science Direct y Web of Science comparten un 11.8% cada una, mientras que IEEE Xplore y EBSCO Host aportan un 8.8% cada una. Esta distribución porcentual no solo resalta la

influencia de cada base de datos, sino que también refleja las preferencias y tendencias actuales en la investigación sobre hogares inteligentes.

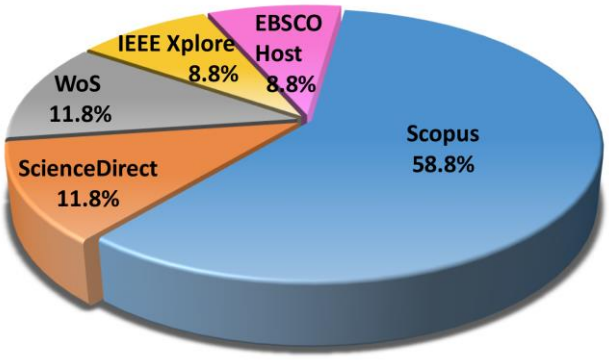

Fig. 4 Gráfico de resultados obtenidos en la búsqueda

Este estudio se enfoca en la contabilización anual de artículos publicados, elegidos de acuerdo con criterios de inclusión, desde 2021 hasta 2024. La Figura 5 presenta un gráfico de barras que ilustra la cantidad y el porcentaje de artículos considerados en la revisión sistemática, organizados por su año de publicación. Este incremento pone de manifiesto un crecimiento significativo en la producción literaria relacionada con el tema, indicando una atención y relevancia creciente en esta área de investigación en los últimos años. En particular, se observa un aumento notable en el número de publicaciones en 2024, que alcanzó su punto más alto con 25 artículos, lo que equivale al 36.8% del total.

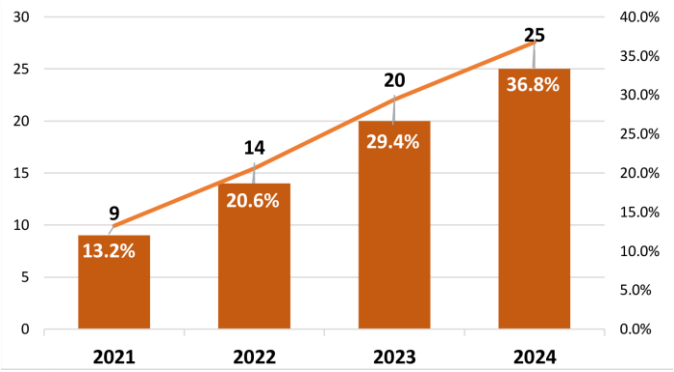

Fig. 5 Porcentajes de cantidad de artículos por año

La Figura 6 muestra el número de manuscritos publicados anualmente en las diferentes bases de datos analizadas. En 2024, se observó un aumento significativo en la cantidad de publicaciones en las cinco plataformas. Scopus lideró el grupo con un total de 15 manuscritos, seguido por ScienceDirect y Web of Science, que contabilizaron 3 artículos cada uno. Por otro lado, tanto IEEE Xplore como EBSCO Host registraron 2 publicaciones cada una.

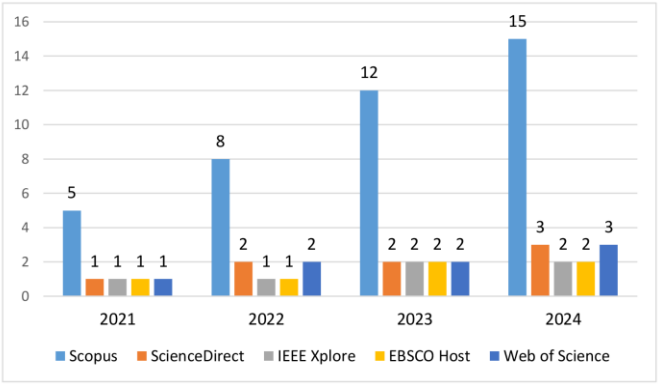

Fig. 6 Artículos por año y base de datos

La Figura 7 presenta la distribución de artículos publicados por país, destacando a China como el principal contribuyente a la investigación, con un total de 10 publicaciones. Este liderazgo resalta su creciente influencia en el desarrollo de hogares inteligentes. En segundo lugar se encuentra India, con 9 artículos, lo que demuestra un notable compromiso con la investigación en este ámbito, seguida de Arabia Saudita, Pakistán y Estados Unidos, cada uno con 7 contribuciones. Malasia aporta 6 artículos, mientras que Francia e Irak contribuyen con 3 cada uno. Por su parte, Inglaterra, Egipto, Corea del Sur y Australia publican 2 artículos cada uno. Finalmente, Canadá, México, España, Alemania, Italia, Túnez, Sudáfrica y Japón registran una sola publicación cada uno.

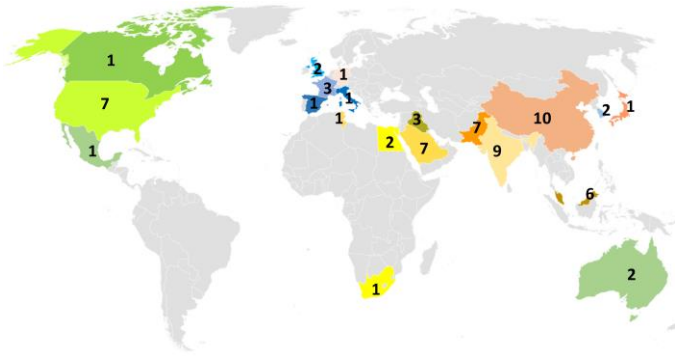

Fig. 7 Número de artículos publicados por país

V. Discusión

Se llevó a cabo un exhaustivo proceso de selección y revisión de literatura para evaluar cuántos estudios han integrado técnicas de Machine Learning o Deep Learning en el desarrollo de hogares inteligentes. Este enfoque meticuloso no solo facilitó la identificación de tendencias y lagunas en la investigación actual, sino que también permitió abordar de manera efectiva las preguntas de investigación planteadas en nuestro estudio.

RQ1: ¿Cuáles son las principales aplicaciones de Machine Learning y Deep Learning utilizados en hogares inteligentes mediante IoT?

La Tabla 2 ofrece un resumen de las principales aplicaciones de Machine Learning y Deep Learning, poniendo de relieve que Machine Learning se destaca en áreas como la seguridad y el monitoreo [15], seguido por la mejora de la Calidad del Servicio (QoS). En contraste, Deep Learning se orienta más hacia la seguridad y el control [14], siendo particularmente eficaz en el monitoreo y la detección de movimiento. El Machine Learning se muestra particularmente adecuado para tareas relacionadas con la seguridad y la mejora de la Calidad del Servicio (QoS). Por su parte, el Deep Learning se enfoca en aspectos de seguridad y control, siendo especialmente eficaz en el monitoreo y la detección de movimiento. Se propone que la evolución conjunta de estas dos tecnologías podría dar lugar al desarrollo de sistemas de gestión de seguridad y monitoreo más integrados y eficientes.

TABLA II
APLICACIONES MACHINE LEARNING Y DEEP LEARNING

Campos de la IA	Aplicaciones	Referencia
Machine Learning	Seguridad y Monitoreo	[11], [12], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29].
	Reconocimiento de la actividad humana	[12], [30], [31], [32], [33].
	Gestión de Energía	[17], [29], [34], [35], [36], [37].
	Automatización y Control Remoto	[17], [25], [33], [34], [37], [38].
	Mejora de la Calidad del Servicio (QoS)	[17], [26], [37], [38], [39], [40], [41].
	Asistentes de Salud y Bienestar	[28], [37], [39], [40].
	Predicción	[23], [34], [37], [41], [42], [43], [44].
Deep Learning	Seguridad y control	[13], [14], [24], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58].
	Reconocimiento de la actividad humana	[24], [32], [47], [53], [55], [56], [57], [59], [60], [61].
	Monitoreo y Detección de Movimiento	[13], [24], [32], [47], [49], [50], [51], [53], [54], [56], [57], [60], [62].
	Salud y bienestar	[24], [54], [56], [57].
	Automatización y Control de Dispositivos	[13], [24], [41], [49], [50], [51], [52], [53], [55], [63].
	Gestión de energía	[41], [49], [50], [54], [58], [63].
	Reconocimiento de Imágenes y Vídeos	[49], [53], [56], [64], [65].
	Reconocimiento facial	[48], [65].
	Predicción	[24], [41], [48], [49], [50], [52], [62], [63].
	Reconocimiento de voz	[54], [55], [59], [60], [66], [67].

RQ2: ¿Cuáles son los algoritmos más utilizados de Machine Learning y Deep Learning en las aplicaciones de Hogares Inteligentes?

La Tabla 3 muestra la utilización de algoritmos en función de los resultados deseados en el contexto de los hogares inteligentes. En el ámbito del Machine Learning, el algoritmo más popular es el Bosque Aleatorio, seguido de árboles de decisión. Por otro lado, en el campo del Deep Learning, el algoritmo más utilizado es el Long Short-Term Memory (LSTM), seguido de las Redes Neuronales Convolucionales (CNN). La elección de algoritmos para sistemas de hogares inteligentes se basa en su alineación con necesidades específicas. El Bosque Aleatorio previene el sobreajuste en datos ruidosos, mientras que el LSTM es clave para la gestión del tiempo y predicción de comportamientos. La combinación de Machine Learning y Deep Learning mejora la eficiencia energética y la seguridad, y su evolución sugiere un gran potencial para innovaciones en automatización y personalización del hogar.

TABLA III
TIPO DE ALGORITMOS DE MACHINE LEARNING Y DEEP LEARNING

Campos de la IA	Algoritmos	Referencia
Machine Learning	Regresión Lineal	[12], [15], [22], [55], [68], [69].
	Bayesiano ingenuo	[51], [55], [70].
	SVM	[15], [25], [26], [30], [51], [55], [69].
	Árboles de decisión	[12], [14], [21], [22], [23], [24], [28], [30], [39], [42], [43], [51], [55], [68], [71].
	Bosque aleatorio (RF)	[11], [12], [14], [23], [24], [25], [26], [27], [28], [29], [30], [39], [51], [52], [55], [68], [69], [71].
	K-Vecino más cercano (KNN)	[12], [14], [22], [26], [28], [32], [39], [51], [55], [68], [69], [71].
	Red neuronal artificial (ANN)	[12], [19], [21], [22], [23], [24], [26], [34], [41], [44], [52], [64].
	Clustering K-Means	[25].
	C4.5	[17].
	RTS-DELM	[19].
	XGBoost	[12], [23], [27], [28], [29], [33], [51], [68].
Deep Learning	Redes neuronales convolucionales (CNN)	[14], [13], [32], [40], [46], [47], [48], [50], [51], [53], [59], [63], [67], [72].
	DNN	[36], [51], [59], [71].
	Gated Recurrent Unit (GRU)	[14], [52], [58], [67].
	Memoria a corto plazo y largo plazo (LSTM)	[14], [45], [47], [51], [52], [54], [55], [58], [59], [60], [61], [62], [66], [67], [71].
	KNN-LSTM	[14].
	ResNet18	[57].
	BiLSTM	[52], [63].
	RNN	[32], [51], [52], [58], [60].

RQ3: ¿Cuáles son las principales limitaciones de Machine Learning y Deep Learning en las aplicaciones de Hogares Inteligentes Mediante IoT?

La Tabla 4 muestra que Machine Learning son vulnerables a ataques de seguridad. Por otro lado, las limitaciones del Deep Learning radican principalmente en su dependencia de grandes volúmenes de datos para su entrenamiento efectivo. De estos hallazgos, es crucial considerar cómo estas limitaciones impactan la implementación real de sistemas de Hogares Inteligentes. La vulnerabilidad del Machine Learning a ataques de seguridad, lo que plantea serias preocupaciones sobre la privacidad y la integridad de los datos en entornos residenciales conectados. Por otro lado, la exigencia de grandes conjuntos de datos por parte del Deep Learning podría limitar su aplicabilidad en entornos donde la recopilación de datos es escasa o difícil, como en situaciones rurales o en comunidades con acceso limitado a tecnologías avanzadas. En conjunto, estas limitaciones resaltan la necesidad de enfoques más robustos y seguros, así como de estrategias que permitan la recolección ética y efectiva de datos, para que las aplicaciones de Hogares Inteligentes puedan prosperar y ofrecer realmente el valor prometido a los consumidores

TABLA IV
LIMITACIONES DE MACHINE LEARNING Y DEEP LEARNING

Campos de la IA	Limitaciones	Referencia
Machine Learning	Calidad de datos	[20], [21], [23], [25], [52], [53], [68], [70], [71], [73], [74].
	Requerimientos Computacionales	[16], [20], [22], [23], [25], [68], [69], [70], [73].
	Consumo de Energía y Recursos	[16], [22], [23], [36], [70].
	Costos de Implementación	[16], [25], [36], [41], [42], [72].
	Tráfico de la Red	[18], [19], [25], [31], [35], [68], [72], [74].
	Ataques de seguridad	[20], [21], [22], [23], [25], [28], [35], [44], [68], [69], [71], [74].
	Vulnerabilidades de Seguridad	[20], [73].
	Error cuadrático medio	[12], [24], [74].
Deep Learning	Cantidad de datos	[14], [13], [24], [45], [46], [48], [49], [50], [51], [52], [53], [55], [58], [62], [63], [66].
	ciberataques	[14], [50], [51], [52], [63], [69].
	Reentrenamiento	[14], [13], [45], [49], [50], [51], [52], [53], [54], [62].
	Recursos computacionales	[13], [24], [46], [48], [49], [50], [51], [54], [62].
	Ruido	[60].
	Costos de Implementación	[41], [48], [49], [50], [62].

RQ4: ¿Como la integración de técnicas de Machine Learning y Deep Learning contribuye al desarrollo de hogares inteligentes?

La Tabla 5 muestra el impacto significativo de las técnicas de Machine Learning y Deep Learning en el desarrollo de hogares inteligentes. Se realizaron diversas pruebas y evaluaciones de diferentes enfoques, subrayando que la selección del método más adecuado varía según la aplicación. Entre los métodos estudiados, las LSTM destacan por su eficacia en la predicción de demanda de energía, detección de ataques en dispositivos IoT y reconocimiento de comandos de voz. Las LSTM son fundamentales para predecir patrones de consumo energético, aumentando la eficiencia y sostenibilidad. También desempeñan un papel crucial en la detección de ataques en dispositivos IoT, asegurando la seguridad en entornos conectados. Su aplicación en el reconocimiento de comandos de voz mejora la interacción con dispositivos inteligentes, prometiendo mayor precisión en el procesamiento del lenguaje. La integración de Machine Learning y Deep Learning en hogares inteligentes optimiza su funcionalidad y seguridad, transformando la interacción humana con el entorno hacia un futuro más conectado y eficiente.

TABLA V
LA INTEGRACIÓN DE TÉCNICAS DE MACHINE LEARNING Y DEEP LEARNING

Métodos		Método más eficiente	Aplicación	Referencia
Machine Learning	Deep Learning			
KNN, Árboles de decisión, Bosque aleatorio, Adaboost	LSTM, RNN, GRU,	KNN+DT+ LSTM	Detección de ataques en la red	[14]
KNN, GBDT	CNN, RNN, HAR	HAR	Reconocer actividades de usuarios	[32]
KNN, Bosque aleatorio, Bayesiano ingenuo, SVM, XGBoost,	LSTM, DNN, CNN, MLP	LSTM	Detectar ataques IoT	[51]
Bosque aleatorio, ANN, GA-RL	LSTM, BiLSTM, GRU, ELM, RNN.	BiLSTM, GRU, ELM.	Detección de ciberataques	[52]
Regresión Lineal, Bayesiano ingenuo, Árboles de decisión, SVM, XGBoost	LSTM, MLP	LSTM	Identificar con precisión los comandos de voz	[55]
ARIMA	LSTM	LSTM	Predicción de la demanda de energía	[75]

VI. CONCLUSIONES

El Machine Learning y el Deep Learning son herramientas clave para optimizar la seguridad y la Calidad del Servicio, permitiendo identificar y resolver problemas activamente. El Deep Learning destaca en la vigilancia y detección de movimiento, mejorando los sistemas de

seguridad. La combinación de ambas tecnologías promete revolucionar el monitoreo, ofreciendo sistemas de gestión más integrados y eficientes que mejoran la seguridad y la Calidad del Servicio.

La utilización de algoritmos como el Bosque Aleatorio en hogares inteligentes es esencial para garantizar un rendimiento eficiente y confiable en estos entornos. El uso de LSTM en la gestión del tiempo y la predicción de comportamientos resalta el papel crucial de las redes neuronales en la automatización del hogar, permitiendo una adaptación dinámica a las necesidades de los usuarios y mejorando la experiencia del hogar inteligente. La integración de Machine Learning y Deep Learning en hogares inteligentes mejora la eficiencia energética y la seguridad, además de permitir innovaciones en automatización y personalización, lo que sugiere un futuro prometedor para la tecnología doméstica.

Las limitaciones en la seguridad del Machine Learning destacan la necesidad urgente de desarrollar sistemas más resilientes que protejan la privacidad y la integridad de los datos en Hogares Inteligentes, lo cual es crucial para ganar la confianza del consumidor y asegurar el futuro de estas tecnologías. La necesidad de grandes volúmenes de datos en Deep Learning plantea un desafío en contextos con recopilación limitada, lo que puede reducir su efectividad en comunidades con menos recursos. Es fundamental crear métodos más seguros y éticos para la recolección de datos, asegurando que los Hogares Inteligentes brinden un valor real a los consumidores y salvaguarden su información.

Las LSTM son clave para optimizar el consumo energético, mejorar la seguridad de dispositivos IoT y facilitar la interacción entre usuarios y dispositivos inteligentes. Su habilidad para predecir patrones y detectar amenazas, junto con los avances en procesamiento del lenguaje, sugiere un futuro en el que la integración de Machine Learning y Deep Learning en hogares aumentará funcionalidad y seguridad, transformando la interacción humana con el entorno hacia un estilo de vida más eficiente y sostenible.

REFERENCIAS

[1] M. Chan, E. Campo, D. Estève, and J. Y. Fourniols, "Smart homes - current features and future perspectives.," *Maturitas*, vol. 64 2, no. 2, pp. 90–7, Oct. 2009, doi: 10.1016/J.MATURITAS.2009.07.014.

[2] A. Shuhaiber and I. Mashal, "Understanding users' acceptance of smart homes," *Technol. Soc.*, vol. 58, Aug. 2019, doi: 10.1016/J.TECHSOC.2019.01.003.

[3] W. A. Jabbar *et al.*, "Design and Fabrication of Smart Home With Internet of Things Enabled Automation System," *IEEE Access*, vol. 7, pp. 144059–144074, 2019, doi: 10.1109/ACCESS.2019.2942846.

[4] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *J. Clean. Prod.*, vol. 140, pp. 1454–1464, Jan. 2017, doi: 10.1016/J.JCLEPRO.2016.10.006.

[5] A. Iqbal *et al.*, "Interoperable Internet-of-Things platform for smart home system using Web-of-Objects and cloud," *Sustain. Cities Soc.*, vol. 38, pp. 636–646, Apr. 2018, doi: 10.1016/J.SCS.2018.01.044.

[6] J. Jaihar, N. Lingayat, P. S. Vijaybhai, G. Venkatesh, and K. P. Upla, "Smart Home Automation Using Machine Learning Algorithms," *2020 Int. Conf. Emerg. Technol.*, pp. 1–4, Jun. 2020, doi: 10.1109/INCET49848.2020.9154007.

[7] A. A. Saleem, M. M. Hassan, and I. A. Ali, "INTELLIGENT HOME: EMPOWERING SMART HOME WITH MACHINE LEARNING FOR USER ACTION PREDICTION," *Sci. J. Univ. Zakho*, vol. 11, no. 3, pp. 403–420, Aug. 2023, doi: 10.25271/SJUOZ.2023.11.3.1145.

[8] Q. Ling, "Machine learning algorithms review," *Appl. Comput. Eng.*, vol. 4, no. 1, pp. 91–98, May 2023, doi: 10.54254/2755-2721/4/20230355.

[9] B. Yu and Y. Zheng, "Research on algorithms of machine learning," *Appl. Comput. Eng.*, vol. 39, no. 1, pp. 277–281, Feb. 2024, doi: 10.54254/2755-2721/39/20230614.

[10] M. Ma *et al.*, "Multi-features fusion for short-term photovoltaic power prediction," *Intell. Converg. Networks*, vol. 3, no. 4, pp. 311–324, Dec. 2022, doi: 10.23919/ICN.2022.0025.

[11] J. Keerthi, K. Bhanu Naveen Teja, V. Rama Seshu, A. Phani Sridhar, and B. S. Kiruthika Devi, "A Survey on IoT Based Intrusion Detection System and Its Security for Smart Homes," in *Advances in Transdisciplinary Engineering*, M. K.V.S.R., K. S., and S. M.K., Eds., India: IOS Press BV, 2023, pp. 400 – 405. doi: 10.3233/ATDE221288.

[12] N. Thakur, C. Y. Han, and S. Panagiotakis, "Multimodal Approaches for Indoor Localization for Ambient Assisted Living in Smart Homes.," *Inf.*, vol. 12, no. 3, p. 114, 2021, [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=149454741&lang=es&site=ehost-live&authtype=sso&custid=ns256095

[13] S. Mari, G. Bucci, F. Ciancetta, E. Fiorucci, and A. Fioravanti, "An Embedded Deep Learning NILM System: A Year-Long Field Study in Real Houses," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–15, 2023, doi: 10.1109/TIM.2023.3328085.

[14] N. Butt *et al.*, "Intelligent Deep Learning for Anomaly-Based Intrusion Detection in IoT Smart Home Networks," *Mathematics*, vol. 10, no. 23, 2022, doi: 10.3390/math10234598.

[15] O. Taiwo and A. E. Ezugwu, "Internet of Things-Based Intelligent Smart Home Control System," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/9928254.

[16] M. A. Khan *et al.*, "A Machine Learning Approach for Blockchain-Based Smart Home Networks Security," *IEEE Netw.*, vol. 35, no. 3, pp. 223 – 229, 2021, doi: 10.1109/MNET.011.2000514.

[17] J. Reyes-Campos, G. Alor-Hernández, I. Machorro-Cano, J. O. Olmedo-Aguirre, J. L. Sánchez-Cervantes, and L. Rodríguez-Mazahua, "Discovery of resident behavior patterns using machine learning techniques and IoT paradigm," *Mathematics*, vol. 9, no. 3, pp. 1–25, Jan. 2021, doi: 10.3390/MATH9030219.

[18] M. Mainuddin, Z. Duan, and Y. Dong, "Network Traffic Characteristics of IoT Devices in Smart Homes," in *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, USA, 2021. doi: 10.1109/ICCCN52240.2021.9522168.

[19] M. S. Farooq, S. Khan, A. Rehman, S. Abbas, M. A. Khan, and S. O. Hwang, "Blockchain-Based Smart Home Networks Security Empowered with Fused Machine Learning," *Sensors*, vol. 22, no. 12, 2022, doi: 10.3390/s22124522.

[20] M. Albany, E. Alsahafi, I. Alruwili, and S. Elkhediri, "A review: Secure

Internet of thing System for Smart Houses," *Procedia Comput. Sci.*, vol. 201, pp. 437–444, 2022, doi: https://doi.org/10.1016/j.procs.2022.03.057.

[21] N. Sarwar, I. S. Bajwa, M. Z. Hussain, M. Ibrahim, and K. Saleem, "IoT Network Anomaly Detection in Smart Homes Using Machine Learning," *IEEE Access*, vol. 11, pp. 119462 – 119480, 2023, doi: 10.1109/ACCESS.2023.3325929.

[22] N. Tekin, A. Acar, A. Aris, A. S. Uluagac, and V. C. Gungor, "Energy consumption of on-device machine learning models for IoT intrusion detection," *Internet of Things*, vol. 21, p. 100670, 2023, doi: https://doi.org/10.1016/j.iot.2022.100670.

[23] A. Javed, A. Ehtsham, M. Jawad, M. N. Awais, A.-U.-H. Qureshi, and H. Larijani, "Implementation of Lightweight Machine Learning-Based Intrusion Detection System on IoT Devices of Smart Homes," *Futur. Internet*, vol. 16, no. 6, 2024, doi: 10.3390/fi16060200.

[24] H. Gao, Q. Wang, J. Zhou, and C. Yu, "Human Vital Signs Signal Monitoring and Repairment with an Optical Fiber Sensor Based on Deep Learning," *Photonics*, vol. 11, no. 8, Aug. 2024, doi: 10.3390/PHOTONICS11080707.

[25] S. M. Abdulrahman *et al*., "INTELLIGENT HOME IOT DEVICES: AN EXPLORATION OF MACHINE LEARNING-BASED NETWORKED TRAFFIC INVESTIGATION," *J. Ilm. Ilmu Terap. Univ. Jambi*, vol. 8, no. 1, pp. 1 – 10, 2024, doi: 10.22437/jiituj.v8i1.32767.

[26] S. Khan *et al.*, "Hybrid computing framework security in dynamic offloading for IoT-enabled smart home system," *PeerJ Comput. Sci.*, vol. 10, p. e2211, Aug. 2024, doi: 10.7717/PEERJ-CS.2211.

[27] H. Attaullah, S. Sanaullah, and T. Jungeblut, "Analyzing Machine Learning Models for Activity Recognition Using Homomorphically Encrypted Real-World Smart Home Datasets: A Case Study," *Appl. Sci.*, vol. 14, no. 19, Oct. 2024, doi: 10.3390/APP14199047.

[28] N. Karmous, M. O.-E. Aoueileyine, M. Abdelkader, L. Romdhani, and N. Youssef, "Software-Defined-Networking-Based One-versus-Rest Strategy for Detecting and Mitigating Distributed Denial-of-Service Attacks in Smart Home Internet of Things Devices," *Sensors*, vol. 24, no. 15, 2024, doi: 10.3390/s24155022.

[29] O. A. Abraham, H. Ochiai, M. D. Hossain, Y. Taenaka, and Y. Kadobayashi, "Electricity Theft Detection for Smart Homes: Harnessing the Power of Machine Learning With Real and Synthetic Attacks," *IEEE Access*, vol. 12, pp. 26023–26045, 2024, doi: 10.1109/ACCESS.2024.3366493.

[30] M. K, A. Ramesh, R. G, S. Prem, R. A A, and D. M. P. Gopinath, "1D Convolution approach to human activity recognition using sensor data and comparison with machine learning algorithms," *Int. J. Cogn. Comput. Eng.*, vol. 2, pp. 130–143, 2021, doi: https://doi.org/10.1016/j.ijcce.2021.09.001.

[31] G. Xue, Y. Wan, X. Lin, K. Xu, and F. Wang, "An Effective Machine Learning Based Algorithm for Inferring User Activities From IoT Device Events," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 9, pp. 2733 – 2745, 2022, doi: 10.1109/JSAC.2022.3191123.

[32] X. Huang and S. Zhang, "Human Activity Recognition based on Transformer in Smart Home," *ACM Int. Conf. Proceeding Ser.*, pp. 520–525, Mar. 2023, doi: 10.1145/3590003.3590100.

[33] L. Gramoli, J. Cumin, J. Lacoche, A. Foulonneau, B. Arnaldi, and V. Gouranton, "Generating and Evaluating Data of Daily Activities with an Autonomous Agent in a Virtual Smart Home," *ACM Trans. Multimed. Comput. Commun. Appl.*, Jan. 2024, doi: 10.1145/3665331.

[34] X. Feng, E. Ahvar, and G. M. Lee, "Evaluation of Machine Leaning Algorithms for Streets Traffic Prediction: A Smart Home Use Case," *Sensors*, vol. 23, no. 4, Feb. 2023, doi: 10.3390/S23042174.

[35] M. Almutairi, "Smart Home IoT Privacy and Security Preservation via Machine Learning Techniques," *Comput. Mater. Contin.*, vol. 74, no. 1, pp. 1959 – 1983, 2023, doi: 10.32604/cmc.2023.031155.

[36] M. Devi, S. Muralidharan, R. Elakiya, and M. Monica, "Design and Implementation of a Smart Home Energy Management System Using IoT and Machine Learning," in *E3S Web of Conferences*, M. B.V., Ed., India, 2023. doi: 10.1051/e3sconf/202338704005.

[37] T. Alshammari, "Using Artificial Neural Networks with GridSearchCV for Predicting Indoor Temperature in a Smart Home," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 2, pp. 13437 – 13443, 2024, doi: 10.48084/etasr.7008.

[38] Q. Waseem, W. I. S. Wan Din, A. Bin Ab Rahman, and K. Nisar, "Exploring Machine Learning in IoT Smart Home Automation," *8th Int. Conf. Softw. Eng. Comput. Syst. ICSECS 2023*, pp. 252–257, 2023, doi: 10.1109/ICSECS58457.2023.10256283.

[39] S. H. Alsamhi *et al.*, "Machine Learning for Smart Environments in B5G Networks: Connectivity and QoS," *Comput. Intell. Neurosci.*, vol. 2021, 2021, doi: 10.1155/2021/6805151.

[40] G. Bhavanasi, L. Werthen-Brabants, T. Dhaene, and I. Couckuyt, "Patient activity recognition using radar sensors and machine learning," *Neural Comput. Appl.*, vol. 34, no. 18, pp. 16033–16048, Sep. 2022, doi: 10.1007/S00521-022-07229-X/TABLES/11.

[41] R. K. Vemuri, C. B. V. Durga, S. A. S. Ibrahim, N. Arumalla, S. Subramanian, and L. Bhukya, "Intelligent-of-things multiagent system for smart home energy monitoring," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 34, no. 3, pp. 1858 – 1867, 2024, doi: 10.11591/ijeecs.v34.i3.pp1858-1867.

[42] M. Marufuzzaman, T. Tumbraegel, L. F. Rahman, and L. M. Sidek, "A machine learning approach to predict the activity of smart home inhabitant," *J. Ambient Intell. Smart Environ.*, vol. 13, no. 4, pp. 271–283, 2021, doi: 10.3233/AIS-210604.

[43] M. K. I. Shafi, M. R. Sultan, S. M. M. Rahman, and M. M. Hoque, "IoT Based Smart Home: A Machine Learning Approach," in *24th International Conference on Computer and Information Technology, ICCIT 2021*, USA: Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/ICCIT54785.2021.9689786.

[44] S. Sohail, Z. Fan, X. Gu, and F. Sabrina, "Multi-tiered Artificial Neural Networks model for intrusion detection in smart homes," *Intell. Syst. with Appl.*, vol. 16, p. 200152, 2022, doi: https://doi.org/10.1016/j.iswa.2022.200152.

[45] S. Mahjoub, S. Labdai, L. Chrifi-Alaoui, B. Marhic, and L. Delahoche, "Short-Term Occupancy Forecasting for a Smart Home Using Optimized Weight Updates Based on GA and PSO Algorithms for an LSTM Network," *Energies*, vol. 16, no. 4, Feb. 2023, doi: 10.3390/EN16041641.

[46] A. Rahim, Y. Zhong, T. Ahmad, S. Ahmad, P. Pławiak, and M. Hammad, "Enhancing Smart Home Security: Anomaly Detection and Face Recognition in Smart Home IoT Devices Using Logit-Boosted CNN Models," *Sensors*, vol. 23, no. 15, Aug. 2023, doi: 10.3390/S23156979.

[47] V. Sarveshwaran, I. T. Joseph, M. Maravarman, and P. Karthikeyan, "Investigation on Human Activity Recognition using Deep Learning," *Procedia Comput. Sci.*, vol. 204, pp. 73–80, Jan. 2022, doi: 10.1016/J.PROCS.2022.08.009.

[48] V. Padmapriya and M. Srivenkatesh, "Digital Twins for Smart Home Gadget Threat Prediction using Deep Convolution Neural Network," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 2, pp. 587 – 594, 2023, doi: 10.14569/IJACSA.2023.0140270.

[49] Z. Wang and D. Wang, "Deep Learning-based Automatic Optimization of Design Smart Home," *Comput. Aided. Des. Appl.*, vol. 21, no. S18, pp. 96–113, 2024, doi: 10.14733/CADAPS.2024.S18.96-113.

[50] F. F. Alruwaili, "Blockchain-Powered Deep Learning for Internet of Things with Cloud-Assisted Secure Smart Home Networks," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3450796.

[51] S. N. B. S. A. Sham, K. K. Ishak, N. A. M. Razali, N. M. Noor, and N. A. Hasbullah, "IoT Attack Detection Using Machine Learning and Deep Learning in Smart Home," *Int. J. Informatics Vis.*, vol. 8, no. 1, pp. 510 – 519, 2024, doi: 10.62527/joiv.8.1.2174.

[52] R. Allafi and I. R. Alzahrani, "Enhancing Cybersecurity in the Internet of Things Environment Using Artificial Orca Algorithm and Ensemble Learning Model," *IEEE Access*, vol. 12, pp. 63282 – 63291, 2024, doi: 10.1109/ACCESS.2024.3390093.

[53] C. Sanjay, K. Jahnavi, and S. Karanth, "A secured deep learning based smart home automation system," *Int. J. Inf. Technol.*, pp. 1–7, Aug. 2024, doi: 10.1007/S41870-024-02097-1/FIGURES/4.

[54] J. Li, Y. Shi, J. Chen, Q. Huang, M. Ye, and W. Guo, "Flexible Self-Powered Low-Decibel Voice Recognition Mask," *Sensors*, vol. 24, no. 10, May 2024, doi: 10.3390/S24103007.

[55] X. Guo, K. Yu, Q. Li, and D. Chen, "VoiceA!ack: Fingerprinting Voice Command on VPN-protected Smart Home Speakers," *BuildSys 2024 - Proc. 2024 11th ACM Int. Conf. Syst. Energy-Efficient Build. Cities, Transp.*, pp. 55–65, Oct. 2024, doi: 10.1145/3671127.3698171.

[56] Y. Lu, L. Zhou, A. Zhang, S. Zha, X. Zhuo, and S. Ge, "Application of Deep Learning and Intelligent Sensing Analysis in Smart Home," *Sensors*, vol. 24, no. 3, Feb. 2024, doi: 10.3390/S24030953.

[57] D. H. Heo, S. H. Park, and S. J. Kang, "Resource-constrained edge-based deep learning for real-time person-identification using foot-pad," *Eng. Appl. Artif. Intell.*, vol. 138, p. 109290, Dec. 2024, doi: 10.1016/J.ENGAPPAI.2024.109290.

[58] Q. W. Khan, R. Ahmad, A. Rizwan, A. N. Khan, K. T. Lee, and D. H. Kim, "Optimizing energy efficiency and comfort in smart homes through predictive optimization: A case study with indoor environmental parameter consideration," *Energy Reports*, vol. 11, pp. 5619–5637, Jun. 2024, doi: 10.1016/J.EGYR.2024.05.038.

[59] J. Yu, A. de Antonio, and E. Villalba-Mora, "Deep Learning (CNN, RNN) Applications for Smart Homes: A Systematic Review," *Computers*, vol. 11, no. 2, Feb. 2022, doi: 10.3390/COMPUTERS11020026.

[60] Q. Deng, D. Wang, T. Luan, and B. Hao, "Tiny Deep Convolution Recurrent Network for Online Speech Enhancement with Various Noise Types," *Front. Artif. Intell. Appl.*, vol. 363, pp. 364–374, Dec. 2022, doi: 10.3233/FAIA220555.

[61] M. J. Hossen, J. M. Z. Hoque, N. A. binti A. Aziz, T. T. Ramanathan, and J. E. Raja, "Unsupervised novelty detection for time series using a deep learning approach," *Heliyon*, vol. 10, no. 3, p. e25394, Feb. 2024, doi: 10.1016/J.HELIYON.2024.E25394.

[62] B. Galeb, H. Saad, H. Bashar, K. Al-Majdi, and A. Al-Hilali, "ANOMALY DETECTION IN SMART HOME ELECTRICAL APPLIANCES USING MACHINE LEARNING WITH STATISTICAL ALGORITHMS AND OPTIMIZED TIME SERIES ALGORITHMS," *J. Mech. Contin. Math. Sci.*, vol. 19, no. 5, pp. 116 – 135, 2024, doi: 10.26782/jmcms.2024.05.00008.

[63] S. Vidhya, M. Balaji, and V. Kamaraj, "An Optimized Hybrid Deep Learning Model for Appliance Energy Prediction in Smart Homes.," *J. Eng. Sci. Technol. Rev.*, vol. 17, no. 3, pp. 151–158, 2024, doi: 10.25103/JESTR.173.18.

[64] T.-W. Sung, C.-Y. Lee, T. Gaber, and H. Nassar, "Innovative Artificial Intelligence-Based Internet of Things for Smart Cities and Smart Homes.," *Wirel. Commun. & Mob. Comput.*, pp. 1–3, 2023, [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true&db=egs&AN=164183778&lang=es&site=ehost-live&authtype=sso&custid=ns256095

[65] X. Jiang, Y. Zhang, G. Lin, and L. Yu, "Music Emotion Recognition Based on Deep Learning: A Review," *IEEE Access*, vol. 12, pp. 157716–157745, 2024, doi: 10.1109/ACCESS.2024.3484470.

[66] G. H. Alshammri, "IoT-Based Voice-Controlled Smart Homes with Source Separation Based on Deep Learning," *J. Sensors*, vol. 2023, 2023, doi: 10.1155/2023/1911385.

[67] J. Boyd, M. Fahim, and O. Olukoya, "Voice spoofing detection for multiclass attack classification using deep learning," *Mach. Learn. with Appl.*, vol. 14, p. 100503, 2023, doi: https://doi.org/10.1016/j.mlwa.2023.100503.

[68] X. Li, H. Ghodosi, C. Chen, M. Sankupellay, and I. Lee, "Improving Network-Based Anomaly Detection in Smart Home Environment," *Sensors*, vol. 22, no. 15, 2022, doi: 10.3390/s22155626.

[69] M. S. Abdalzaher, M. M. Fouda, H. A. Elsayed, and M. M. Salim, "Toward Secured IoT-Based Smart Systems Using Machine Learning," *IEEE Access*, vol. 11, pp. 20827–20841, Jan. 2023, doi: 10.1109/ACCESS.2023.3250235.

[70] M. A. Torad, B. Bouallegue, and A. M. Ahmed, "A voice controlled smart home automation system using artificial intelligent and internet of things," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 20, no. 4, pp. 808 – 816, 2022, doi: 10.12928/TELKOMNIKA.v20i4.23763.

[71] P. Anand, Y. Singh, H. Singh, M. D. Alshehri, and S. Tanwar, "SALT: transfer learning-based threat model for attack detection in smart home," *Sci. Rep.*, vol. 12, no. 1, 2022, doi: 10.1038/s41598-022-16261-9.

[72] H. Jmila, G. Blanc, M. R. Shahid, and M. Lazrag, "A Survey of Smart Home IoT Device Classification Using Machine Learning-Based Network Traffic Analysis," *IEEE Access*, vol. 10, pp. 97117 – 97141, 2022, doi: 10.1109/ACCESS.2022.3205023.

[73] A. A. Abdlrazaq, S. N. Azzez, M. A. Anwer, and S. I. Hassen, "Proposed Solutions for the Main Challenges and Security Issues in IoT Smart Home Technology," *Zanco J. Pure Appl. Sci.*, vol. 35, no. 4, pp. 84 – 96, 2023, doi: 10.21271/ZJPAS.35.4.08.

[74] X. Liu, X. Fu, X. Du, B. Luo, and M. Guizani, "Machine Learning-Based Non-Intrusive Digital Forensic Service for Smart Homes," *IEEE Trans. Netw. Serv. Manag.*, vol. 20, no. 2, pp. 945 – 960, 2023, doi: 10.1109/TNSM.2022.3224863.

[75] F. Iqbal *et al.*, "Blockchain-Modeled Edge-Computing-Based Smart Home Monitoring System with Energy Usage Prediction," *Sensors*, vol. 23, no. 11, 2023, doi: 10.3390/s23115263.