ISBN: 978-628-96613-1-6. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2025.1.1.2106

Systematic review on risk assessment and protective measures for automation systems with Z-Wave technology

Carbajal Cabanillas, José Luis[1], Carbajal Cabanillas, José Antonio[1], Guzman Aquije, Elvis Henry[1]
[1,3] *Universidad Tecnológica del Perú, Perú, U21203710@utp.edu.pe, U21203712@utp.edu.pe, c20203@utp.edu.pe*

Abstract– Z-Wave technology is widely used in smart home and building automation systems, especially in IoT equipment. However, it presents several security vulnerabilities that could jeopardize the integrity and privacy entrusted to us by users. Therefore, this systematic literature review (SLR) explores the main security risks associated with Z-Wave, as well as the protection measures proposed in the literature to mitigate these vulnerabilities. The review included 74 studies on Z-Wave implementation, security comparisons with other similar technologies (such as Zigbee and Wi-Fi), and evaluations of protection methods such as encryption, intrusion detection, and anonymous authentication. The findings highlight the need to strengthen Z-Wave security by developing advanced protection measures and constantly monitoring the network for intrusions in real time.

Keywords-- Domotic, Automation, Computer applications, Automatic control, Machine learning

Revisión sistemática sobre la evaluación de riesgos y medidas de protección para sistemas de automatización con tecnología Z-Wave

Carbajal Cabanillas, José Luis[1], Carbajal Cabanillas, José Antonio[1], Guzman Aquije, Elvis Henry[1]
[1,3] *Universidad Tecnológica del Perú, Perú, U21203710@utp.edu.pe, U21203712@utp.edu.pe, c20203@utp.edu.pe*

Resumen– La tecnología Z-Wave es ampliamente utilizada en sistemas de automatización del hogar y edificios inteligentes, especialmente en equipos de Internet de las Cosas (IoT). Sin embargo, presenta diversas vulnerabilidades de seguridad que podrían poner en peligro la integridad y privacidad que los usuarios confían. Por ello, esta revisión sistemática de literatura (RSL), explora los principales riesgos de seguridad asociados con Z-Wave, así como las medidas de protección propuestas en la literatura para mitigar estas vulnerabilidades. La revisión incluyó 74 estudios sobre la implementación de Z-Wave, comparaciones de seguridad con otras tecnologías similares (como Zigbee y Wi-Fi) y evaluaciones de métodos de protección como cifrado, detección de intrusiones, y autenticación anónima. Los hallazgos destacan la necesidad de fortalecer la seguridad en Z-Wave mediante el desarrollo de medidas de protección avanzadas y el monitoreo constante de la red para detectar intrusiones en tiempo real.

Palabras clave-- ***Domótica, Automatización, Aplicación informática, Control automático, Aprendizaje automático.***

I. INTRODUCCIÓN

En la última década, el IoT ha transformado radicalmente el panorama de la automatización, integrándose en hogares, empresas e infraestructuras críticas. Dentro de este ámbito, la tecnología Z-Wave se ha consolidado como una de las principales soluciones para la automatización del hogar debido a su bajo consumo de energía, facilidad de implementación y compatibilidad con múltiples dispositivos IoT [1]-[5]. Este protocolo opera en bandas de frecuencia específicas para evitar interferencias, lo que lo hace ideal para entornos domésticos y comerciales. Sin embargo, el aumento en la adopción de dispositivos Z-Wave ha revelado una serie de vulnerabilidades de seguridad, desde fallos en el cifrado hasta ataques de suplantación y denegación de servicio, generando preocupaciones significativas en cuanto a la protección de datos y la privacidad [6]-[10]. A pesar de los avances en tecnologías relacionadas como Zigbee y Wi-Fi, Z-Wave continúa enfrentándose a desafíos específicos en seguridad, posicionándose en el centro de las investigaciones actuales sobre automatización y seguridad IoT.

En la actualidad, la tecnología Z-Wave presenta limitaciones importantes en la protección de redes y dispositivos IoT. Entre los problemas más destacados se encuentran los ataques de repetición, la debilidad en ciertos métodos de autenticación y la falta de un cifrado robusto en muchas implementaciones. Estas deficiencias no solo comprometen la privacidad y la seguridad de los usuarios, sino que también afectan la confianza en su implementación en infraestructuras críticas como edificios inteligentes y sistemas de salud [11]-[16]. Si bien se han realizado investigaciones aisladas sobre estos temas, falta una visión integral que identifique, analice y sintetice los riesgos de seguridad y las medidas de protección específicas para Z-Wave. Esto resulta especialmente crítico dado el rápido crecimiento en su uso y el potencial impacto de estas vulnerabilidades en aplicaciones de alta sensibilidad [17]-[20].

La realización de una revisión sistemática de literatura (RSL) sobre Z-Wave es fundamental, ya que hasta la fecha no existe una recopilación exhaustiva y actualizada que analice los riesgos de seguridad y las soluciones disponibles para esta tecnología en el contexto de IoT. Aunque se han desarrollado revisiones parciales centradas en tecnologías similares como Zigbee o Wi-Fi, ninguna aborda específicamente las peculiaridades y vulnerabilidades de Z-Wave en profundidad [21]-[25]. Además, la creciente dependencia de sistemas de automatización en entornos domésticos y comerciales exige un análisis riguroso que informe tanto a los investigadores como a los desarrolladores sobre las mejores prácticas y estrategias de mitigación. Esta RSL no solo llenará un vacío en la literatura existente, sino que también proporcionará una base sólida para futuras investigaciones y desarrollos tecnológicos en el campo.

Este estudio tiene como objetivo principal investigar los riesgos de seguridad asociados con la tecnología Z-Wave y analizar las medidas de protección disponibles, proporcionando una síntesis estructurada de las investigaciones recientes para guiar futuras estrategias en la mejora de su seguridad en aplicaciones IoT.

El presente documento se organiza en varias secciones. Primero, se presenta el enfoque metodológico utilizado para llevar a cabo esta RSL, describiendo los criterios de selección y las bases de datos consultadas. Posteriormente, se analizan los resultados obtenidos, clasificando los riesgos de seguridad identificados y las medidas de protección propuestas en la literatura. La sección de discusión compara estas medidas con otras tecnologías similares, como Zigbee y Wi-Fi, destacando las fortalezas y debilidades de Z-Wave. Finalmente, se ofrecen conclusiones y recomendaciones prácticas para mejorar la seguridad de esta tecnología, junto con sugerencias para futuras investigaciones en el área.

II. METODOLOGÍA

Para este estudio se empleó un enfoque basado en el análisis exhaustivo de la evidencia científica disponible, utilizando las dos herramientas más eficientes para esta RSL: PICO que

permitió determinar los temas de estudio y PRISMA que nos ayudó en la elección de artículos incluidos en este análisis.

A. Planteamiento PICO

Siguiendo las recomendaciones que nos dieron nuestros tutores, la formulación de las preguntas se realizó considerando dos puntos claves: primero, que la interrogante está completamente vinculada al tema de estudio, y segundo, que esté formulada de tal manera que su respuesta sea precisa. Nuestros tutores nos recomendaron fragmentar la pregunta en cuatro aportes fundamentales (P) población de estudio, (I) intervención a considerar, (C) comparación que se plantea y (O) resultados de interés. Aplicando este enfoque en la investigación, se identificaron estos componentes en las diferentes fases del proceso.

1) Clasificación de los elementos PICO: para iniciar con la primera fase, se clasificaron los valores fundamentales para la indagación: primero empezamos con población de interés; como segundo sería intervención a considerar; como tercero tenemos comparación planteada y, por último, tenemos resultados relevantes y el contexto del estudio [ver Tabla I].

TABLA I
IDENTIFICACIÓN DE LOS COMPONENTES PICO

P	Problema/Población	Dispositivos de automatización del hogar, sistemas inteligentes, dispositivos z-wave, IoT(Internet of Things).
I	Intervención	Medidas de protección, evaluación de riesgos, detección de vulnerabilidades, protocolos de seguridad.
C	Comparación	Tecnologías similares, como Zigbee, Bluetooth, Wi-Fi, u otros protocolos de comunicación en sistemas de automatización del hogar.
O	Resultados	Reducción del nivel de vulnerabilidad.

2) Formulación de preguntas: En la segunda fase, se formuló una pregunta de investigación usando los resultados de la metodología PICO, dando lugar a ¿cómo se lleva a cabo la aplicación de medidas de protección en los dispositivos Z-Wave influye en la reducción de vulnerabilidades en comparación con otros protocolos de comunicación como tecnología BAS en sistemas de automatización del hogar? Luego, se desglosó la pregunta en interrogantes específicas basadas en los componentes PICO [ver Tabla II].

TABLA II
PREGUNTAS PICO

P	Problema/ Población	Dispositivos de automatización del hogar, sistemas inteligentes, dispositivos z.wave, IoT(Internet of Things).	¿Cuáles fueron las vulnerabilidades encontradas en los dispositivos Z-Wave utilizados en la automatización del hogar?
I	Intervención	Medidas de protección, evaluación de riesgos, detección de vulnerabilidades, protocolos de seguridad.	¿Qué protocolos de seguridad se han implementado para mitigar las vulnerabilidades en Z-Wave?
C	Comparación	Tecnologías similares, como Zigbee, Bluetooth, Wi-Fi, u otros protocolos de comunicación en sistemas de automatización del hogar.	¿Cómo se comparan las medidas de seguridad en Z-Wave con las de otras tecnologías de automatización como Zigbee, Bluetooth o Wi-Fi?
O	Resultados	Reducción del nivel de vulnerabilidad	¿Cuáles son las medidas de protección para reducir las vulnerabilidades en dispositivos Z-Wave?

3) Selección de términos relevantes: continuando con la tercera fase, logramos identificar los términos más relevantes para cada sección que compone una incógnita [ver Tabla III]

TABLA III
PALABRAS CLAVE

P	Problema/ Población	Dispositivos de automatización del hogar, sistemas inteligentes, dispositivos z-wave, IoT(Internet of Things).	“Z-Wave”,”Z Wave”, ”home automation”, “smart home systems”, “IoT”, “Internet of Things”, “Automation”, “smart home automation”, “AI”, “Artificial Intelligence”, “Machine Learning”, “Automatic control”, “smart homes”, “IoT devices”, “smart cities”
I	Intervención	Medidas de protección, evaluación de riesgos, detección de vulnerabilidades, protocolos de seguridad.	“security, “”blockchain”, “blockchains”, “Intrusion Detection Systems”, “IDS”, “data safety”, “privacy issues”, “vulnerabilidades”, “secure IoT”
C	Comparación	Tecnologías similares, como Zigbee, Bluetooth, Wi-Fi, u otros protocolos de comunicación en sistemas de automatización del hogar.	“Zigbee”, “Bluetooth”, “Wi-Fi”, “BAs”, “Building automation system”, “li-fi”, “EnOcean”, “BACnet”, “KNX”, “LonWorks”, “Modbus”
O	Resultados	Reducción del nivel de vulnerabilidad.	“Cybersecurity”, “BAs protocol”, “Wireless protocols”, “Cyber-attacks”, “Machine Learning”, “ML”, “Expert System”, “ICS Security”, “Datasets”, “Deep Learning”, “Smart Buildings”, “Analytics”, “Sensors”

4) Formulación de preguntas: En la cuarta fase, se definió la estructura de búsqueda, empleando el conector lógico “OR” y

comillas (“”) para las palabras claves compuestas [ver Tabla IV].

TABLA IV
PALABRAS CLAVE

P	Problema/ Población	Dispositivos de automatización del hogar, sistemas inteligentes, dispositivos z-wave, IoT(Internet of Things).	“Z-Wave” OR ”Z Wave” OR ”home automation” OR “smart home systems” OR “IoT” OR “Internet of Things” OR “Automation” OR “smart home automation” OR “AI” OR “Artificial Intelligence” OR “Machine Learning” OR “Automatic control” OR “smart homes” OR “IoT devices” OR “smart cities”
I	Intervención	Medidas de protección, evaluación de riesgos, detección de vulnerabilidades, protocolos de seguridad.	“security” OR “blockchain” OR “blockchains” OR “Intrusion Detection Systems” OR “IDS” OR “data safety” OR “privacy issues” OR “vulnerabilidades” OR “secure IoT”
C	Comparación	Tecnologías similares, como Zigbee, Bluetooth, Wi-Fi, u otros protocolos de comunicación en sistemas de automatización del hogar.	“Zigbee” OR “Bluetooth” OR “Wi-Fi” OR “BAs” OR “Building” automation system”, “li-fi”, “EnOcean”, “BACnet”, “KNX”, “LonWorks”, “Modbus”
O	Resultados	Reducción del nivel de vulnerabilidad.	"Cybersecurity" OR "BAs protocols" OR "Wireless protocols" OR "Cyber-attacks" OR "Machine learning" OR "ML" OR "Expert System" OR "ICS Security" OR "Datasets" OR "Deep learning" OR "Smart buildings" OR "Analytics" OR "Sensors"

5) Sintaxis de la fórmula PICO: En la última fase, se establece una conexión entre los componentes PICO utilizando el operador lógico “AND” [ver Tabla V].

TABLA V
FÓRMULAS DE BÚSQUEDA

(TITLE-ABS-KEY ("Z-Wave" OR "Z Wave" OR "home automation" OR "smart home systems" OR "IoT" OR "Internet of Things" OR "Automation" OR "smart home automation" OR "AI" OR "Artificial Intelligence" OR "Machine learning" OR " Automatic control" OR "smart homes" OR "IoT devices" OR "smart cities") AND TITLE-ABS-KEY ("security" OR "blockchain" OR "blockchains" OR "Intrusion Detection Systems" OR "IDS" OR "data safety" OR "privacy issues" OR "vulnerabilities" OR "secure IoT") AND TITLE-ABS-KEY ("Zigbee" OR "Bluetooth" OR "Wi-Fi" OR "BAs" OR "Building automation system" OR "li-fi" OR "EnOcean" OR "BACnet" OR "KNX" OR "LonWorks" OR "Modbus") AND TITLE-ABS-KEY ("Cybersecurity" OR "BAs protocols" OR "Wireless protocols" OR "Cyber-attacks" OR "Machine learning" OR "ML" OR "Expert System" OR "ICS Security" OR "Datasets" OR "Deep learning" OR "Smart buildings" OR "Analytics" OR "Sensors"))

Se obtuvieron 2,039 documentos encontrados en el repertorio de artículos de Scopus. Fueron analizados, evaluados y seleccionados para así elegir las fuentes usadas en la revisión sistemática.

6) Establecimientos de los parámetros de Inclusión y Exclusión

a) Criterios para la Inclusión (CI):

CI1: Artículos que usaron metodologías de automatización de hogares

CI2: Artículos que se enfocaron en el funcionamiento de dispositivos Z-Wave;

CI3: Artículos originales;

CI4: Artículos pertenecientes al área de ciencias computacionales.

b) Criterios para la Exclusión (CE):

CE1: Publicaciones sin acceso abierto;

CE2: Idiomas distintos al inglés o español;

CE3: Documentos con más de 4 años de antigüedad;

CE4: Fuentes que no estén relacionadas con el tema.

B. Proceso de selección: PRISMA

En la selección de artículos; se aplicó la metodología PRISMA, la cual mejoró la calidad y fiabilidad de las fuentes. Este proceso se dividió en dos partes: una para identificar los artículos a incluir y otra para excluir aquellos que no cumplían con los criterios, buscando obtener resultados de mayor calidad.

1) Proceso de identificación; la selección de artículos tuvo 5 fases: Primero la “Identificación”, como segunda la “Duplicación”, como tercera la “Elegibilidad”, como cuarta la “selección” y, por ultima, el “Sesgo”. Siendo primera la fase de identificación, se indagó exhaustivamente en el repositorio de Scopus -seleccionada por su amplia cobertura y calidad de publicaciones-. Se identificaron un total de 1,039 registros.

2) Proceso de elegibilidad; se eliminaron registros no especializados en ingeniería, quedando 839, y después se excluyeron los que no estaban relacionados con sistemas de automatización con tecnología z-wave, resultando en 244 registros.

3) Proceso de selección; primero se eliminaron 1 documento por idioma, luego, 30 por no estar en el rango 2021-2025, 73 cuyo resumen no estaba relacionado con el tema y finalmente 66 que resultaron en fallas al obtener el documento, dejando 74.

4) Proceso de sesgo; finalmente, quedaron 74 artículos para la revisión sistemática, como podemos apreciar en la Fig. 1

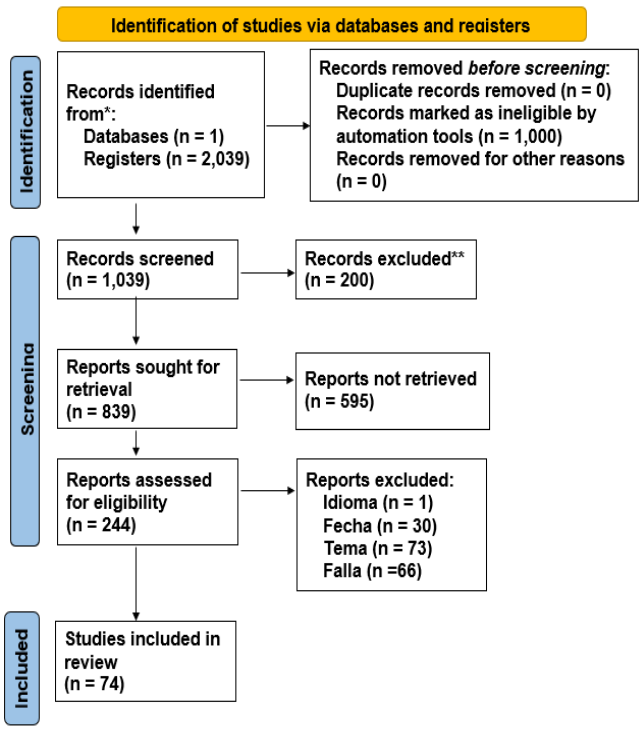

Fig. 1. Diagrama flujo PRISMA

III. Resultados

Se confeccionó una tabla que abarca un total de 74 artículos, asignando un código único a cada uno para garantizar una referencia ágil y eficiente recopilación de información. Posteriormente, se diseñó un esquema con preguntas específicas, las cuales fueron respondidas mediante el análisis detallado de los artículos.

En primer lugar, se identificaron los tipos de ataques en redes Z-Wave que los autores abordaron en sus investigaciones, los cuales se resumieron en la Fig. 2.

Fig. 2. Tipos de ataques en Z-Wave

Se observó un predominio de ataques de interferencia, *jamming* y denegación de servicio (DoS/DDoS), con 12 artículos revisados [3]–[14]. Le siguieron los Ataques en redes específicas de IoT (Zigbee, Z-Wave, Wi-Fi, BLE) con 9 artículos [15]–[23] y los ataques de suplantación y acceso no autorizado con 8 artículos cada uno [24]–[31]. Las vulnerabilidades en comunicación y seguridad se abordaron en 7 artículos [32]–[38], mientras que los ataques de privacidad y la detección de intrusiones se analizaron en 6 artículos cada uno [39]–[44]. Los ataques de inyección de datos contaron con 5 artículos [45]–[49], y los ataques en redes de automatización y energía con 2 [50], [51].

Los ataques más investigados, interferencia y redes específicas de IoT, reflejan su alto impacto en la disponibilidad y seguridad de redes Z-Wave.

En la Fig. 3 es posible observar cómo se distribuyen los diferentes artículos publicados en los años 2020-2024. Se llega apreciar un gran aumento en la cantidad de publicaciones, particularmente en los años 2023 y 2024, que concentran la mayor cantidad de artículos. Este incremento puede atribuirse al crecimiento de investigaciones y avances recientes en la temática de estudio, los cuales han impulsado la producción académica en los últimos dos años.

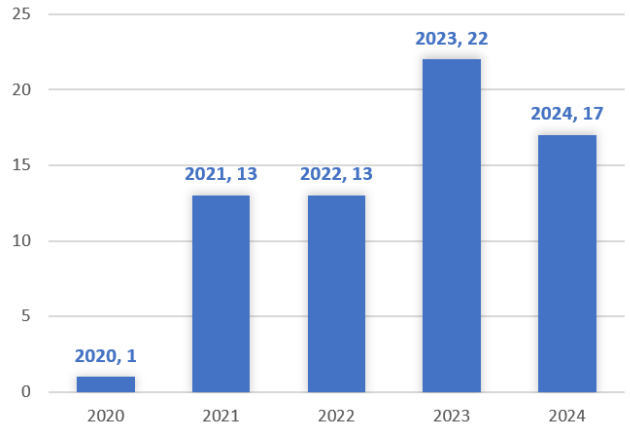

Fig. 3. Años de publicación de los artículos

En la Fig. 4, se logra visualizar el número relacionado con las publicaciones distribuidas entre las editoriales más relevantes, destacando IEEE con 24 artículos, seguido de MDPI con 13 y Elsevier con 10. Este predominio de publicaciones en estas editoriales sugiere una notable curiosidad por parte de muchos científicos siguiendo este tema de estudio, aprovechando las plataformas de difusión más influyentes para alcanzar una mayor audiencia académica.

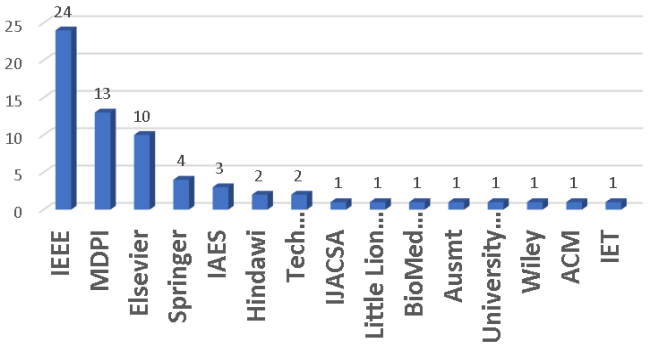

Fig. 4. Editoriales de los artículos

En la Fig. 5, se muestran los artículos publicados por el país de origen del estudio. Del total de 74 artículos, la mayoría de los países contribuyen con 1 o 2 artículos. Sin embargo, India y EE.UU. destacaron con 16 y 11 artículos respectivamente, lo que evidencia un interés significativo en estos países por desarrollar investigaciones en torno a la temática de estudio, apoyando el avance y aplicación de nuevos conocimientos en el área.

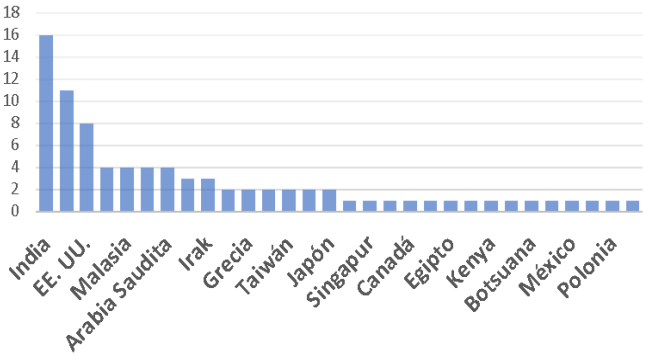

Fig. 5. País de origen del estudio

En la Fig. 6, la cantidad de artículos que tratan sobre los dispositivos más vulnerables en sistemas Z-Wave. Del total de 74 artículos, se identificaron principalmente vulnerabilidades en dispositivos de seguridad y acceso, con 9 artículos, seguidos de dispositivos IoT generales, dispositivos con conectividad Wi-Fi y Bluetooth (BLE), y sensores en redes IoT, cada uno con 8 artículos. Estos resultados reflejan una preocupación creciente por la seguridad en dispositivos ampliamente utilizados en entornos domésticos e industriales, donde el acceso no autorizado podría comprometer la integridad de los sistemas conectados.

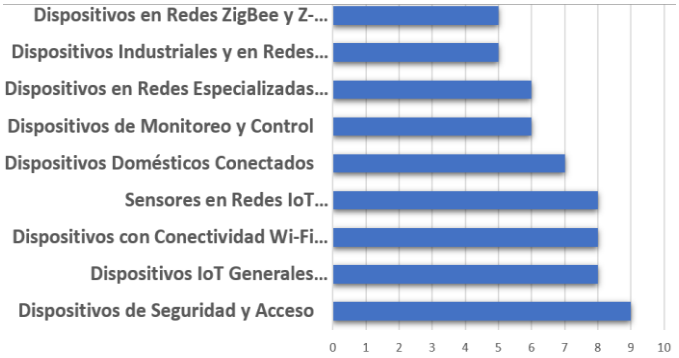

Fig. 6. Dispositivos más vulnerables en sistemas Z-Wave

En la Fig. 7 se ilustran las tecnologías utilizadas para la detección y prevención de ataques en sistemas Z-Wave. De un total de 74 artículos, destacan muchas tecnologías inspiradas en machine learning (ML) e inteligencia artificial con 17 artículos, seguidas de métodos de detección de intrusiones y seguridad con 10, y de sensores y tecnología híbrida con 9. Estos resultados indican una fuerte tendencia hacia el uso de tecnologías avanzadas de IA y ML para mejorar la protección en redes Z-Wave, destacando la importancia de soluciones automatizadas para mitigar y detectar las amenazas en tiempo real.

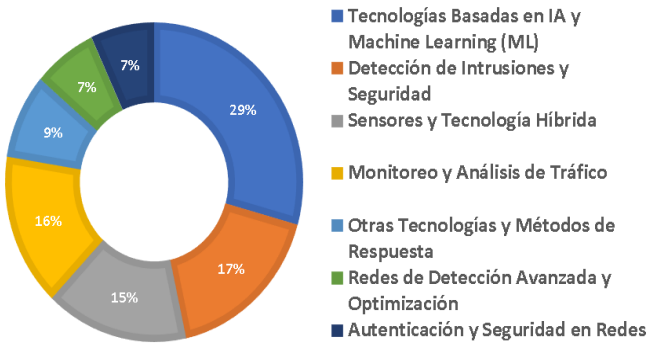

Fig. 7. Tecnologías utilizadas para la detección y prevención de ataques en Z-Wave

En la Fig. 8 es posible observar cómo se compara la seguridad de Z-Wave con tecnología BAS en distintos aspectos. De un total de 74 artículos, se destaca el análisis de vulnerabilidades y seguridad general, con 13 artículos, seguido de la seguridad en autenticación y control de acceso, con 9 artículos, y enfoques en aplicaciones específicas y otros protocolos, con 8 artículos. Estos resultados evidencian un interés significativo durante el análisis comparativo sobre la seguridad en Z-Wave, resaltando áreas clave como la autenticación y la eficiencia de la red, esenciales para fortalecer la protección en aplicaciones de IoT.

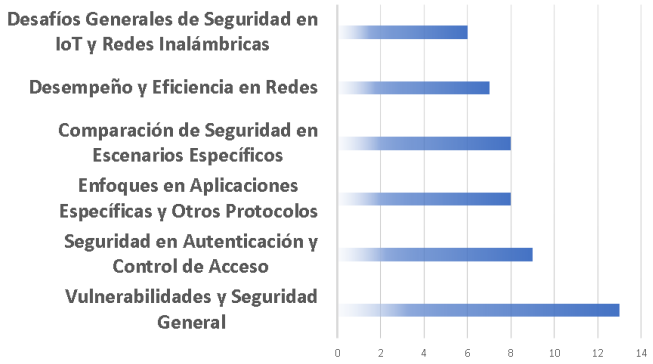

Fig. 8. Comparación entre la seguridad de Z-Wave con tecnología BAS

En la Fig. 9, se presenta la comparación de la seguridad entre Z-Wave y Wi-Fi en diversas áreas. Del total de 74 artículos, se observa que la seguridad general y las vulnerabilidades fueron los temas más abordados, con 13 artículos, seguidos del desempeño y la eficiencia de la red, con 10 artículos. La autenticación y el control de acceso también fueron destacados, con 9 artículos, lo que resalta la preocupación por fortalecer la seguridad en estos aspectos clave. Estos resultados reflejan un enfoque importante en la evaluación comparativa de la seguridad entre ambas tecnologías, particularmente en cuanto a la protección frente a vulnerabilidades y la eficiencia de las redes.

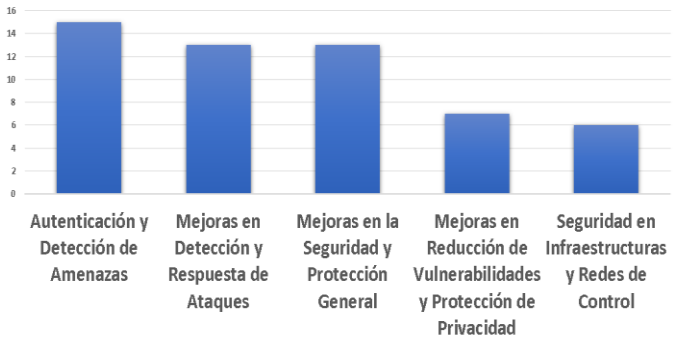

Fig. 9. Comparación entre la seguridad de Z-Wave con Wi-Fi

En la Fig. 10 se detallan las medidas de protección implementadas en Z-Wave según los artículos revisados. Del total de 74 artículos, la autenticación y la detección de amenazas fueron los temas más recurrentes, con 15 artículos, seguidos de las mejoras en la detección y respuesta a ataques, así como en la seguridad y protección general, ambos con 13 artículos. Estas medidas reflejan un enfoque significativo en la mejora de la seguridad en Z-Wave, priorizando la protección frente a amenazas externas y la optimización de las respuestas ante ataques. Los resultados también indican esfuerzos importantes en la reducción de vulnerabilidades y la protección de la privacidad, elementos clave para fortalecer las infraestructuras y redes de control en estos sistemas.

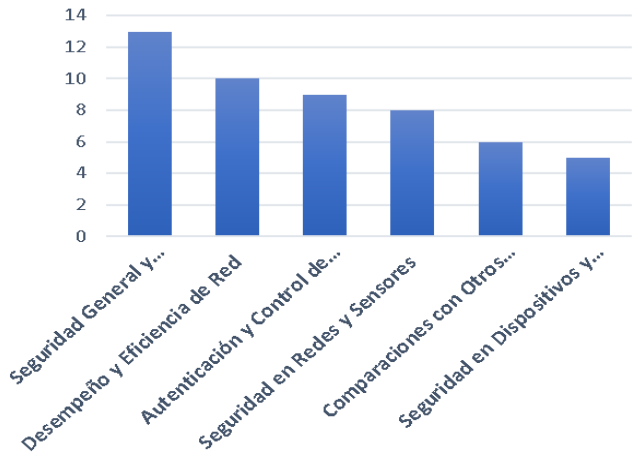

Fig. 10. Las medidas de protección implementadas en Z-Wave

En la Fig. 11 se muestra los resultados relacionadas con la reducción del éxito de los ataques en Z-Wave tras implementar medidas de protección. Del total de 74 artículos, la mayor cantidad se centró en la reducción general de ataques y el éxito de los mismos, con 20 artículos, lo que indica un enfoque predominante en mitigar los efectos de los ataques. Además, se observan mejoras en la autenticación y las técnicas de defensa, así como en la detección y respuesta a amenazas, con 10 artículos en cada área. Estos hallazgos destacan la efectividad de las medidas implementadas para reforzar la seguridad en Z-Wave, particularmente con respecto a las medidas de protección frente ante amenazas y mejoras de la respuesta ante incidentes de seguridad.

Fig. 11. Reducción del éxito de los ataques en Z-Wave tras implementar medidas de protección

IV. Discusión

A medida que los dispositivos Z-Wave se desplegaba en hogares y empresas, sus vulnerabilidades en seguridad comenzaron a destacar como un problema crucial. Los

estudios más recientes han detallado que las principales amenazas a los dispositivos Z-Wave incluyen ataques de suplantación, denegación de servicio (DoS) y de acceso no autorizado. Estas amenazas, además, son facilitadas por deficiencias en el cifrado, debido a que muchas implementaciones de Z-Wave no cuentan con un sistema de encriptación fuerte y confiable, lo que permite que los atacantes intercepten y manipulen la información transmitida en la red sin obstáculos significativos [7], [24], [58].

Un análisis comparativo entre Z-Wave y tecnologías similares, como Zigbee y Wi-Fi, muestra diferencias clave en la forma en que estos protocolos abordan la seguridad. Por ejemplo, Zigbee se ha consolidado como un estándar con una sólida base de encriptación AES-128, que se aplica de extremo a extremo para cada transmisión de datos. Esta implementación ha demostrado ser eficaz contra accesos no autorizados y ataques de suplantación, aspectos en los que Z-Wave aún muestra vulnerabilidades críticas, especialmente en dispositivos que usan versiones antiguas o poco seguras del protocolo [19], [20]. El uso de cifrado más avanzado y de protocolos de autenticación también se ha vuelto esencial para impedir los ataques de "downgrade", en los cuales el atacante fuerza al dispositivo a utilizar una versión menos segura del protocolo, facilitando así la explotación de sus vulnerabilidades [10]-[15].

Como respuesta, los estudios revisados han explorado distintas soluciones de protección para Z-Wave. Las propuestas más comunes incluyen la implementación de encriptación avanzada, como AES y TLS, para garantizar que los datos en tránsito permanezcan seguros, así como la introducción de mecanismos de autenticación anónima, que aseguran que solo los dispositivos autorizados puedan conectarse a la red. Estos métodos representan avances significativos, ya que mejoran el aspecto de privacidad junto con la solidez en las comunicaciones de redes Z-Wave [22]-[25]. Además, tecnologías de detección en tiempo real, como los métodos basados en el RSS (Received Signal Strength), permiten identificar patrones de ataque y localizar la fuente de la intrusión, reduciendo así el impacto de los ataques y fortaleciendo la respuesta de seguridad en tiempo real [29].

Otro enfoque innovador para fortalecer la seguridad en Z-Wave es el uso de algoritmos de aprendizaje profundo. Estos algoritmos permiten que el sistema aprenda de los patrones de tráfico y detecte anomalías que puedan estar relacionadas con actividades maliciosas. Esta estrategia ha mostrado resultados prometedores en términos de precisión y adaptabilidad, especialmente en un contexto en el que los atacantes constantemente desarrollan nuevas técnicas para evadir las medidas de seguridad [37], [40]. A pesar de los avances, la discusión en la literatura sugiere que las implementaciones de seguridad en Z-Wave aún están lejos de alcanzar un nivel óptimo de confiabilidad, sobre todo cuando se considera su uso en aplicaciones críticas, como la seguridad y la salud [64]-[75].

V. Conclusión

La evolución de Z-Wave y su creciente adopción en sistemas de automatización en hogares y empresas presentan una paradoja: mientras más dispositivos conectados y automatización inteligente se despliegan en la vida cotidiana, más aumenta la exposición a riesgos de seguridad. Los resultados de esta revisión subrayan que, aunque Z-Wave ha implementado medidas de seguridad básicas, estas no son suficientes para garantizar una protección robusta contra ataques sofisticados. La comparación con tecnologías como Zigbee revela una discrepancia significativa en los niveles de protección, lo que hace evidente que Z-Wave necesita mejorar en áreas clave, como la encriptación, la autenticación y la detección de intrusiones en tiempo real [3], [12], [27].

Para abordar las deficiencias de Z-Wave, se requieren desarrollos continuos que incluyan soluciones avanzadas, tales como el uso de algoritmos de aprendizaje profundo y métodos de detección en tiempo real. Estas herramientas no solo permitirán una detección más rápida y precisa de posibles intrusiones, sino que también ayudarán a adaptar las defensas de Z-Wave frente a nuevos tipos de ataques que los hackers desarrollan constantemente [38], [45]. A nivel de políticas, es crucial que la industria establezca estándares de seguridad que obliguen a los fabricantes a implementar configuraciones de seguridad consistentes y robustas, eliminando así las brechas de seguridad generadas por configuraciones variables entre dispositivos [50], [70].

Por lo tanto, esta revisión concluye que para que Z-Wave siga siendo una opción viable y segura en el mercado de la automatización, es imprescindible que los desarrolladores y fabricantes adopten enfoques de seguridad integrales y estandarizados. Con el incremento del uso de dispositivos IoT en infraestructuras críticas, la seguridad en Z-Wave debe fortalecerse al fin de asegurar la seguridad de información y la integridad en los sistemas. Así, al reforzar la seguridad en Z-Wave, se contribuirá no solo a un entorno más seguro para los usuarios, sino también al aspecto de confiabilidad al utilizar tecnologías con automatización para sectores críticos de la sociedad [1]-[74].

Referencias

[1] C. Morales-Gonzalez et al., "On Building Automation System security", High-Confidence Comput., p. 100236, mayo de 2024. https://doi.org/10.1016/j.hcc.2024.100236

[2] K. Taghizad-Tavana, M. Ghanbari-Ghalehjoughi, N. Razzaghi-Asl, S. Nojavan y A. Alizadeh, "An Overview of the Architecture of Home Energy Management System as Microgrids, Automation Systems, Communication Protocols, Security, and Cyber Challenges", Sustainability, vol. 14, n.º 23, p. 15938, noviembre de 2022. https://doi.org/10.3390/su142315938

[3] B. N. S. Yii, N. Ahmad, M. H. A. Wahab, W. M. Jubadi, C. Uttraphan y S. Z. S. Idrus, "Integration of Home Automation and Security System Controller with FPGA Implementation", Ann. Emerg. Technol. Comput., vol. 7, n.º 5, pp. 1–10, octubre de 2023. https://doi.org/10.33166/aetic.2023.05.001

[4] M. A. Nassiri Abrishamchi, A. Zainal, F. A. Ghaleb, S. N. Qasem y A. M. Albarrak, "Smart Home Privacy Protection Methods against a Passive Wireless Snooping Side-Channel Attack", Sensors, vol. 22, n.º 21, p. 8564, noviembre de 2022. https://doi.org/10.3390/s22218564

[5] H. Fatima, H. U. Khan y S. Akbar, "Home Automation and RFID-Based Internet of Things Security: Challenges and Issues", Secur. Communication Netw., vol. 2021, pp. 1–21, noviembre de 2021. https://doi.org/10.1155/2021/1723535
[6] M. Islam, H. Jamil, S. Pranto, R. Das, A. Amin y A. Khan, "Future Industrial Applications: Exploring LPWAN-Driven IoT Protocols", Sensors, vol. 24, n.º 8, p. 2509, abril de 2024. https://doi.org/10.3390/s24082509
[7] C. K. Nkuba, S. Woo, H. Lee y S. Dietrich, "ZMAD: Lightweight Model-based Anomaly Detection for the Structured Z-Wave Protocol", IEEE Access, p. 1, 2023. https://doi.org/10.1109/access.2023.3285476
[8] C. K. Nkuba, S. Kim, S. Dietrich y H. Lee, "Riding the IoT Wave With VFuzz: Discovering Security Flaws in Smart Homes", IEEE Access, vol. 10, pp. 1775–1789, 2022. https://doi.org/10.1109/access.2021.3138768
[9] C. Braghin, M. Lilli y E. Riccobene, "A Model-based approach for Vulnerability Analysis of IoT Security Protocols: the Z-Wave case study", Comput. & Secur., p. 103037, diciembre de 2022. https://doi.org/10.1016/j.cose.2022.103037
[10] A. Adhikary et al., "Design and Implementation of an IOT-based Smart Home Automation System in Real World Scenario", EAI Endorsed Trans. Internet Things, vol. 10, junio de 2024. https://doi.org/10.4108/eetiot.6201
[11] A. A. Razzaq y K. N. Rao, "Improving the performance of IoT devices that use Wi-Fi", Int. J. Reconfigurable Embedded Syst. (IJRES), vol. 13, n.º 3, p. 748, noviembre de 2024. https://doi.org/10.11591/ijres.v13.i3.pp748-757
[12] G. Karacayılmaz y H. Artuner, "A novel approach detection for IoT attacks via artificial intelligence", Cluster Comput., mayo de 2024. https://doi.org/10.1007/s10586-024-04529-w
[13] C. Caballero-Gil, R. Álvarez, C. Hernández-Goya y J. Molina-Gil, "Research on smart-locks cybersecurity and vulnerabilities", Wireless Netw., mayo de 2023.https://doi.org/10.1007/s11276-023-03376-8
[14] C.-I. Nicola, M. Nicola, D. Sacerdoțianu y I. Pătru, "Real-Time Monitoring of Cable Sag and Overhead Power Line Parameters Based on a Distributed Sensor Network and Implementation in a Web Server and IoT", Sensors, vol. 24, n.º 13, p. 4283, julio de 2024. https://doi.org/10.3390/s24134283
[15] E. Anthi, L. Williams, V. Ieropoulos y T. Spyridopoulos, "Investigating Radio Frequency Vulnerabilities in the Internet of Things (IoT)", IoT, vol. 5, n.º 2, pp. 356–380, junio de 2024. https://doi.org/10.3390/iot5020018
[16] H. Safi, A. I. Jehangiri, Z. Ahmad, M. A. Ala'anzy, O. I. Alramli y A. Algarni, "Design and Evaluation of a Low-Power Wide-Area Network (LPWAN)-Based Emergency Response System for Individuals with Special Needs in Smart Buildings", Sensors, vol. 24, n.º 11, p. 3433, mayo de 2024. https://doi.org/10.3390/s24113433
[17] E. Iturbe, O. Llorente-Vazquez, A. Rego, E. Rios y N. Toledo, "Unleashing offensive artificial intelligence: Automated attack technique code generation", Comput. & Secur., p. 104077, agosto de 2024. https://doi.org/10.1016/j.cose.2024.104077
[18] C.-L. Wu et al., "Novel AMI in Zigbee Satellite Network Based on Heterogeneous Wireless Sensor Network for Global Machine-to-Machine Connectivity", Electronics, vol. 13, n.º 8, p. 1421, abril de 2024. https://doi.org/10.3390/electronics13081421
[19] A. Allen, A. Mylonas, S. Vidalis y D. Gritzalis, "Smart homes under siege: Assessing the robustness of physical security against wireless network attacks", Comput. & Secur., p. 103687, diciembre de 2023. https://doi.org/10.1016/j.cose.2023.103687
[20] P. Netinant, T. Utsanok, M. Rukhiran y S. Klongdee, "Development and Assessment of Internet of Things-Driven Smart Home Security and Automation with Voice Commands", IoT, vol. 5, n.º 1, pp. 79–99, febrero de 2024. Accedido el 11 de noviembre de 2024. [En línea]. Disponible: https://doi.org/10.3390/iot5010005
[21] P. Phalaagae, A. M. Zungeru, B. Sigweni y S. Rajalakshmi, "Authentication schemes in wireless internet of things sensor networks: a survey and comparison", Indonesian J. Elect. Eng. Comput. Sci., vol. 33, n.º 3, p. 1876, marzo de 2024. https://doi.org/10.11591/ijeecs.v33.i3.pp1876-1888
[22] H. J. Jin, F. R. Ghashghaei, N. Elmrabit, Y. Ahmed y M. Yousefi, "Enhancing Sniffing Detection in IoT Home Wi-Fi Networks: An Ensemble Learning Approach with Network Monitoring System (NMS)", IEEE Access, p. 1, 2024. https://doi.org/10.1109/access.2024.3416095
[23] M. L. Hoang, "Smart Drone Surveillance System Based on AI and on IoT Communication in Case of Intrusion and Fire Accident", Drones, vol. 7, n.º 12, p. 694, diciembre de 2023. https://doi.org/10.3390/drones7120694
[24] A. A. S. AlQahtani, T. Alshayeb, M. Nabil y A. Patooghy, "Leveraging Machine Learning for Wi-Fi-based Environmental Continuous Two-Factor Authentication", IEEE Access, p. 1, 2024. https://doi.org/10.1109/access.2024.3356351
[25] V. Gavra, O. A. Pop y I. Dobra, "A Comprehensive Analysis: Evaluating Security Characteristics of Xbee Devices against Zigbee Protocol", Sensors, vol. 23, n.º 21, p. 8736, octubre de 2023. https://doi.org/10.3390/s23218736
[26] İ. Avcı y M. Koca, "Predicting DDoS Attacks Using Machine Learning Algorithms in Building Management Systems", Electronics, vol. 12, n.º 19, p. 4142, octubre de 2023. https://doi.org/10.3390/electronics12194142
[27] G. Routis y I. Roussaki, "Low Power IoT Electronics in Precision Irrigation", Smart Agricultural Technol., p. 100310, agosto de 2023. https://doi.org/10.1016/j.atech.2023.100310
[28] A. Allakany, A. Saber, S. M. Mostafa, M. Alsabaan, M. I. Ibrahem y H. Elwahsh, "Enhancing Security in ZigBee Wireless Sensor Networks: A New Approach and Mutual Authentication Scheme for D2D Communication", Sensors, vol. 23, n.º 12, p. 5703, junio de 2023. https://doi.org/10.3390/s23125703
[29] P. Kumari y B. Mondal, "An Encryption Scheme Based on Grain Stream Cipher and Chaos for Privacy Protection of Image Data on IoT Network", Wireless Pers. Commun., abril de 2023. https://doi.org/10.1007/s11277-023-10382-8
[30] Y. Himeur et al., "AI-big data analytics for building automation and management systems: a survey, actual challenges and future perspectives", Artif. Intell. Rev., octubre de 2022. https://doi.org/10.1007/s10462-022-10286-2
[31] K. Uszko, M. Kasprzyk, M. Natkaniec y P. Chołda, "Rule-Based System with Machine Learning Support for Detecting Anomalies in 5G WLANs", Electronics, vol. 12, n.º 11, p. 2355, mayo de 2023. https://doi.org/10.3390/electronics12112355
[32] S.-J. Lee, Y.-r. Lee, S.-E. Jeon y I.-G. Lee, "Machine Learning-based Jamming Attack Classification and Effective Defense Technique", Comput. & Secur., p. 103169, marzo de 2023. https://doi.org/10.1016/j.cose.2023.103169
[33] X. Zhang, S. Yu, H. Zhou, P. Huang, L. Guo y M. Li, "Signal Emulation Attack and Defense for Smart Home IoT", IEEE Trans. Dependable Secure Comput., p. 1, 2022. https://doi.org/10.1109/tdsc.2022.3169705
[34] M. Ren, X. Ren, H. Feng, J. Ming y Y. Lei, "Security Analysis of Zigbee Protocol Implementation via Device-agnostic Fuzzing", Digit. Threats: Res. Pract., septiembre de 2022. https://doi.org/10.1145/3551894
[35] O. Shvartzman et al., "Characterization and Detection of Cross-Router Covert Channels", Comput. & Secur., vol. 127, p. 103125, abril de 2023. https://doi.org/10.1016/j.cose.2023.103125
[36] P. Locatelli, M. Perri, D. M. J. Gutierrez, A. Lacava y F. Cuomo, "Device discovery and tracing in the Bluetooth Low Energy domain", Comput. Commun., febrero de 2023. https://doi.org/10.1016/j.comcom.2023.02.008
[37] D. R. Philips, E. Salami, H. Ramiah y J. Kanesan, "Location Accuracy Optimization in Bluetooth Low Energy (BLE) 5.1 Based Indoor Positioning System (IPS) - A Machine Learning Approach", IEEE Access, p. 1, 2023. https://doi.org/10.1109/access.2023.3338358
[38] C.-J. Huang, C.-J. Chi y W.-T. Hung, "Hybrid-AI-Based iBeacon Indoor Positioning Cybersecurity: Attacks and Defenses", Sensors, vol. 23, n.º 4, p. 2159, febrero de 2023. https://doi.org/10.3390/s23042159
[39] S. R. Movahhed Ghodsinya, E. Azimirad y R. Mohamadnia H.A, "Implementing Multi-Channel Technology in Node Sleeping Mode of ZigBee Wireless Sensor Networks", Int. J. Automat. Smart Technol., vol. 13, n.º 1, p. 2398, 2023. https://doi.org/10.5875/ausmt.v13i1.2398
[40] F. t. Zahra, Y. S. Bostanci y M. Soyturk, "Real-Time Jamming Detection in Wireless IoT Networks", IEEE Access, p. 1, 2023. https://doi.org/10.1109/access.2023.3293404
[41] S. Priya y K. Pradeep Mohan Kumar, "Feature Selection with Deep Reinforcement Learning for Intrusion Detection System", Comput. Syst. Sci. Eng., pp. 1–15, 2023. https://doi.org/10.32604/csse.2023.030630
[42] D. S. Deris Stiawan, D. W. Deris Stiawan, T. W. S. Dimas Wahyudi, M. Y. I. Tri Wanda Septian y R. B. Mohd Yazid

Idris, "The Development of an Internet of Things (IoT) Network Traffic Dataset with Simulated Attack Data", 網際網路技術學刊, vol. 24, n.º 2, pp. 345– 356, marzo de 2023. https://doi.org/10.53106/160792642023032402013
[43] A. A. Mustofa, Y. A. Dagnew, P. Gantela y M. J. Idrisi, "SECHA: A Smart Energy-Efficient and Cost-Effective Home Automation System for Developing Countries", J. Comput. Netw. Commun., vol. 2023, pp. 1–12, marzo de 2023. https://doi.org/10.1155/2023/8571506
[44] R. Li, W. Zhang, L. Wu, Y. Tang y X. Xie, "ZPA: A Smart Home Privacy Analysis System Based on ZigBee Encrypted Traffic", Wireless Commun. Mobile Comput., vol. 2023, pp. 1–16, enero de 2023. https://doi.org/10.1155/2023/6731783
[45] V. Graveto, T. Cruz y P. Simoes, "A Network Intrusion Detection System for Building Automation and Control Systems", IEEE Access, vol. 11, pp. 7968–7983, 2023. https://doi.org/10.1109/access.2023.3238874
[46] F. L. Færøy, M. M. Yamin, A. Shukla y B. Katt, "Automatic Verification and Execution of Cyber Attack on IoT Devices", Sensors, vol. 23, n.º 2, p. 733, enero de 2023. https://doi.org/10.3390/s23020733
[47] N. Hussein y A. Nhlabatsi, "Living in the Dark: MQTT-Based Exploitation of IoT Security Vulnerabilities in ZigBee Networks for Smart Lighting Control", IoT, vol. 3, n.º 4, pp. 450–472, noviembre de 2022. https://doi.org/10.3390/iot3040024
[48] A. S. AlShuhail, S. Bhatia, A. Kumar y B. Bhushan, "Zigbee-Based Low Power Consumption Wearables Device for Voice Data Transmission", Sustainability, vol. 14, n.º 17, p. 10847, agosto de 2022. https://doi.org/10.3390/su141710847
[49] O. Setayeshfar et al., "Privacy invasion via smart-home hub in personal area networks", Pervasive Mobile Comput., p. 101675, julio de 2022. https://doi.org/10.1016/j.pmcj.2022.101675
[50] Y. Wu y T. Feng, "An Anonymous Authentication and Key Update Mechanism for IoT Devices Based on EnOcean Protocol", Sensors, vol. 22, n.º 17, p. 6713, septiembre de 2022. https://doi.org/10.3390/s22176713
[51] S. Saxena, A. Pandey y S. Kumar, "RSS based multistage statistical method for attack detection and localization in IoT networks", Pervasive Mobile Comput., p. 101648, julio de 2022. https://doi.org/10.1016/j.pmcj.2022.101648
[52] A. A. Sahrab y H. M. Marhoon, "Design and Fabrication of a Low-Cost System for Smart Home Applications", J. Robot. Control (JRC), vol. 3, n.º 4, pp. 409–414, julio de 2022. https://doi.org/10.18196/jrc.v3i4.15413
[53] A. M. Albalawi y M. Amin Almaiah. "Assessing and reviewing of cyber-security threats, attacks, litigation techniques in IoT environment". Journal of Theoretical and Applied Information TechnologyVolume 100, Issue 9, Pages 2988 - 301115 May 2022 https://doi.org/19928645
[54] B. H. Hameed, A. Y. Taher, R. K. Ibrahim, A. H. Ali y Y. A. Hussein, "Based on mesh sensor network: design and implementation of security monitoring system with Bluetooth technology", Indonesian J. Elect. Eng. Comput. Sci., vol. 26, n.º 3, p. 1781, junio de 2022. https://doi.org/10.11591/ijeecs.v26.i3.pp1781-1790
[55] S. Sarkar, Y. M. Teo y E.-C. Chang, "A cybersecurity assessment framework for virtual operational technology in power system automation", Simul. Modelling Pract. Theory, vol. 117, p. 102453, mayo de 2022. https://doi.org/10.1016/j.simpat.2021.102453
[56] Atef Abdrabou, Monika Prakash and Weihua Zhuang "Application-Oriented Traffic Modeling of WiFi-Based Internet of Things Gateways", IEEE Internet of Things JournalVolume 9, Issue 2, Pages 1159 - 117015 January 2022 https://doi.org/10.1109/JIOT.2021.3079115
[57] B. Wang y F. Yan, "Application of Internet of Things Real-Time Monitoring Technology in Community Security Prevention and Control", Mobile Inf. Syst., vol. 2022, pp. 1–10, junio de 2022. https://doi.org/10.1155/2022/8194442
[58] A. Das y P. -, "Design and Development of an Efficient Network Intrusion Detection System using Ensemble Machine Learning Techniques for Wifi Environments", Int. J. Adv. Comput. Sci. Appl., vol. 13, n.º 4, 2022. https://doi.org/10.14569/ijacsa.2022.0130499
[59] M. Anuradha1, G. Mani, T. Shanthi, N. R. Nagarajan, P. Suresh5 and C. Bharatiraja, "Intrusion Detection System for Big Data Analytics in IoT Environment", Computer Systems Science and EngineeringOpen AccessVolume 43, Issue 1, Pages 381 – 3962022 https://doi.org/10.32604/csse.2022.023321
[60] V. Graveto, T. Cruz y P. Simões, "Security of Building Automation and Control Systems: Survey and future research directions", Comput. & Secur., vol. 112, p. 102527, enero de 2022. https://doi.org/10.1016/j.cose.2021.102527
[61] E. Kalinin, D. Belyakov, D. Bragin y A. Konev, "IoT Security Mechanisms in the Example of BLE", Computers, vol. 10, n.º 12, p. 162, noviembre de 2021. https://doi.org/10.3390/computers10120162
[62] .Z. Chen, L. Peng, A. Hu y H. Fu, "Generative adversarial network-based rogue device identification using differential constellation trace figure", EURASIP J. Wireless Commun. Netw., vol. 2021, n.º 1, abril de 2021. https://doi.org/10.1186/s13638-021-01950-2
[63] G. D. O'Mahony, K. G. McCarthy, P. J. Harris y C. C. Murphy, "Developing a Low-Order Statistical Feature Set Based on Received Samples for Signal Classification in Wireless Sensor Networks and Edge Devices", IoT, vol. 2, n.º 3, pp. 449–475, agosto de 2021. https://doi.org/10.3390/iot2030023
[64] V. Ponnusamy, A. Yichiet, N. Jhanjhi, M. humayun y M. Fahhad Almufareh, "IoT Wireless Intrusion Detection and Network Traffic Analysis", Comput. Syst. Sci. Eng., vol. 40, n.º 3, pp. 865–879, 2022. https://doi.org/10.32604/csse.2022.018801
[65] M. M. Sultan, A. T. Saeed y A. M. Sana, "Design and implementation of an adaptive multilevel wireless security system using IoT", Indonesian J. Elect. Eng. Comput. Sci., vol. 23, n.º 3, p. 1804, septiembre de 2021. https://doi.org/10.11591/ijeecs.v23.i3.pp1804-1813
[66] C.-W. Tien, T.-Y. Huang, P.-C. Chen y J.-H. Wang, "Using Autoencoders for Anomaly Detection and Transfer Learning in IoT", Computers, vol. 10, n.º 7, p. 88, julio de 2021. https://doi.org/10.3390/computers10070088
[67] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras y P. Sarigiannidis, "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments", IEEE Trans. Netw. Service Manage., vol. 18, n.º 2, pp. 1137–1151, junio de 2021. https://doi.org/10.1109/tnsm.2021.3078381
[68] S. Nagendram, P. Kanakaraja, M. S. R. KiranNag y K. Akhil, "Design and Implementation of Low-Cost Smart Home System with Sensor Multiplexing", SN Comput. Sci., vol. 2, n.º 3, abril de 2021. https://doi.org/10.1007/s42979-021-00602-y
[69] M. Nivaashini y P. Thangaraj, "Computational intelligence techniques for automatic detection of Wi-Fi attacks in wireless IoT networks", Wireless Netw., vol. 27, n.º 4, pp. 2761–2784, abril de 2021. https://doi.org/10.1007/s11276-021-02594-2
[70] Radhanand, K. N. B. Kumar, S. Namburu y P. Sampathkrishna Reddy, "Implementation of a Distributed Home Automation Scheme with Custom Hardware Nodes Using ZigBee and MQTT Protocols", IETE J. Res., pp. 1–7, mayo de 2021. https://doi.org/10.1080/03772063.2021.1923078
[71] M. Murad, O. Bayat y H. M. Marhoon, "Design and implementation of a smart home system with two levels of security based on IoT technology", Indonesian J. Elect. Eng. Comput. Sci., vol. 21, n.º 1, p. 546, enero de 2021. https://doi.org/10.11591/ijeecs.v21.i1.pp546-557
[72] M. O. A. Helo, A. Shaker y L. A. Abdul-Rahaim, "Design and Implementation a Cloud Computing System for Smart Home Automation", Webology, vol. 18, SI05, pp. 879–893, octubre de 2021. https://doi.org/10.14704/web/v18si05/web18269
[73] D. R. dos Santos, M. Dagrada y E. Costante, "Leveraging operational technology and the Internet of things to attack smart buildings", J. Comput. Virol. Hacking Techn., junio de 2020. https://doi.org/10.1007/s11416-020-00358-8
[74] Nivaashini M.; Nivaashini M.; Thangaraj P.; Sountharrajan S.; Suganya E.; Soundariya R.S, "Effective feature selection for hybrid wireless iot network intrusion detection systems using machine learning techniques", Ad-Hoc and Sensor Wireless NetworksVolume 49, Issue 3-4, Pages 175 - 206. https://surl.li/ovqwdu