Internet de las cosas: Sistemas de autenticación en la domótica.

Nicolás Fernández Rodríguez[1]
Tutor: Martha Susana Contreras Ortiz

[1]Departamento de Ingeniería de Sistemas, Universidad Santo Tomás, Tunja, Colombia

Información de correspondencia: e-mail: Nicolas.fernandez@usantoto.edu.co

Este artículo se desarrolla con el fin de optar el título universitario de Ingeniero de sistemas.

ABSTRACT Los sistemas de autenticación, son aquellas estrategias utilizadas para proteger la información de los usuarios y asegurar que solo los individuos autorizados tengan acceso a esta. Hoy en día cualquier sistema que requiera almacenar datos debe estar protegido para asegurar su seguridad, ahora bien, dentro de un hogar inteligente, para tener un buen funcionamiento, se necesita conectar todos los dispositivos electrónicos entre sí lo que significa un constante flujo de datos entre estos y como consecuencia aumenta probabilidad de ser atacado por un delincuente informático. Por esta razón, en este estudio se investigarán las vulnerabilidades y los factores que afectan los sistemas de autenticación en la domótica, utilizando la metodología PRISMA para realizar una revisión sistemática de la literatura para analizar qué vulnerabilidades en los sistemas de autenticación pueden ser explotadas y qué estrategias son efectivas para mitigar estos riesgos. Los resultados indican que las principales vulnerabilidades incluyen: debilidad de contraseñas, falta de cifrado de datos, vulnerabilidades de hardware, ataques de suplantación, inyecciones de software, ataques de replay, y se identificaron estrategias efectivas para mitigar estos riesgos, tales como: cifrado de extremo a extremo, autenticación multifactor, Blockchain, protocolos de autenticación seguros, actualizaciones de seguridad automatizadas, tecnologías de hardware seguras, Deep Learning para detección de anomalías y protocolos de conocimiento cero (Zero-Knowledge Proofs).

PALABRAS CLAVE Autenticación, automatización, ciberseguridad, domótica, seguridad, internet de las cosas.

1) INTRODUCCIÓN

IoT (Internet de las cosas) es un término utilizado para referirse a varios dispositivos electrónicos, los cuáles cuentan con distintos componentes y tecnologías para poder intercambiar información entre sí, así mismo, esto se logra por medio de una conexión a internet[1], [2], [3]. También, ha transformado significativamente la manera en que los seres humanos interactúan con la tecnología, permitiendo la interconexión de dispositivos y sistemas a través de redes inteligentes. El Internet hoy en día se ha convertido en una herramienta fundamental para la realización de actividades ya sean cotidianas o no, esto implica que está presente en una gran cantidad de lugares donde se puede acceder a él desde diversos dispositivos electrónicos. Es fascinante como el IoT puede facilitar ciertas actividades para optimizar tiempo y mejorar la vida de los seres humanos. Esta tecnología ha evolucionado desde su concepción, para abarcar una amplia gama de aplicaciones, desde la automatización industrial y la salud, hasta los hogares inteligentes, donde la domótica se ha convertido en un pilar fundamental. Según recientes estudios, el mercado global del IoT alcanzó un valor estimado de USD 330 mil millones en 2022, y se proyecta que crecerá a una tasa anual compuesta del 26.4 % entre 2023 y 2030. Este crecimiento resalta la importancia del IoT como una herramienta esencial para la optimización de procesos y la mejora de la calidad de vida[4].

En el ámbito de los hogares inteligentes, se conoce mejor como “domótica”. Esta se refiere a un conjunto de sistemas los cuales permiten automatizar varios tipos de procesos dentro de una vivienda[5], [6], [7]. El principal propósito es mejorar la calidad de vida de los usuarios, permitiendo gestionar distintos aspectos dentro de la vivienda de manera remota. Para gestionar estos sistemas se pueden utilizar sensores que reaccionan automáticamente a estímulos o pueden tener configuraciones predefinidas para realizar las funciones requeridas[8].

A pesar de tener distintos usos puede llegar, por el momento, a tener ciertos percances generados por atacantes cibernéticos. Cuando se habla de ciberseguridad se piensa generalmente solo en las computadoras, pero la ciberseguridad va más allá de eso. No solo se enfoca en estos dispositivos electrónicos sino también, en aquellos que incorporan circuitos y sensores que pueden ser manipulados y programados. Además, desempeña un papel fundamental al garantizar la privacidad y proteger los datos personales de los usuarios que interactúan con estas soluciones[9]. Ahora bien, estos dispositivos al estar conectados a una red inalámbrica son propensos a ataques cibernéticos los cuales pueden poner en peligro la información almacenada dentro de los mismos. En este contexto, los

sistemas de autenticación juegan un rol crucial al garantizar que solo usuarios y dispositivos autorizados puedan acceder a la red.

Existen numerosos métodos de evitar estos ataques informáticos y fortalecer los dispositivos; la autenticación es una de las más importantes y una de las más usadas a nivel general. Este es el proceso que usan las empresas para confirmar que solo las personas, servicios y aplicaciones adecuados con los permisos correctos pueden acceder a recursos de la organización[10], [11].

Por esta razón, se busca estudiar cómo algunos factores pueden jugar en contra de sistemas domóticos y saber cómo contrarrestarlos, utilizando diferentes métodos de autenticación.

Estrategias como la autenticación multifactor, los protocolos criptográficos avanzados y el uso de tecnologías emergentes como el blockchain han demostrado ser efectivos para mitigar riesgos, aunque su implementación aún enfrenta barreras como la falta de estandarización y el alto costo.

Por esta razón, este artículo se centra en analizar las vulnerabilidades y estrategias asociadas a los sistemas de autenticación en el IoT aplicado a la domótica.

A través de una revisión de la literatura utilizando la metodología PRISMA[12] (Preferred Reporting Items for Systematic reviews and Meta-Analyses) se busca analizar:

1. Las posibles vulnerabilidades que pueden ser explotadas por ataque informáticos.
2. Las mejores estrategias existentes para prevenir riesgos en los sistemas de autenticación del hogar inteligente.

La meta es proporcionar un panorama claro que sirva como base para el desarrollo de sistemas más seguros y confiables, fortaleciendo así la confianza de los usuarios en la tecnología IoT aplicada al hogar.

2) METODOLOGÍA

En la presente revisión se utilizó la metodología PRISMA para recoger, organizar y analizar la información. El procedimiento consistió en identificar uno de los ámbitos donde es más utilizado el IoT dentro de un hogar inteligente. Posteriormente, se analizaron los riesgos que se pueden presentar en un sistema de autenticación y cómo se pueden solucionar.

Los pasos seguidos durante la revisión sistemática de la literatura, siguiendo las recomendaciones dadas por la metodología PRISMA:

1. Formular las preguntas de investigación.
2. Establecer cadenas de búsquedas específicas para obtener resultados gratificantes en las bases de datos seleccionadas.
3. Seleccionar los documentos de manera puntual.
4. Analizar los documentos seleccionados.

BÚSQUEDA DE LITERATURA.

a. PREGUNTAS DE INVESTIGACIÓN

La Tabla 1 presenta las preguntas de investigación las cuales se esperan responder a lo largo de este artículo. También se describen las principales razones que fueron grandes motivaciones para la realización de este trabajo.

b. FUENTES DE DATOS

La investigación incluyó una amplia y exhaustiva búsqueda en varias bases de datos electrónicas especializadas en documentos científicos como: Scopus, IEEE-Xplore y ScienceDirect. En la revisión se extrajeron palabras clave, títulos de artículos científicos y sus respectivos resúmenes relacionados con los temas principales para responder las preguntas de investigación.

c. CADENAS DE BÚSQUEDA

Las cadenas de búsqueda utilizadas combinaron palabras como “IoT” con el descriptor lógico AND y demás términos tales como “Home Automation”, “Authentication” y “cybersecurity” como se puede apreciar en la Tabla 2. También se realizaron búsquedas más específicas con respecto al tema seleccionado para ampliar la información obtenida con las principales cadenas de búsqueda utilizadas.

La combinación de términos resultó mostrando artículos de interés como a su vez, artículos enfocados hacia diferentes tipos de uso del IoT.

Adicionalmente al hablar de dispositivos electrónicos conectados, se mostraron bastantes artículos sobre seguridad, lo que resultó de bastante ayuda teniendo en la cuenta que el tema principal de este trabajo se enfoca en seguridad dentro del IoT.

d. SELECCIÓN DE ESTUDIOS

Las búsquedas en las bases de datos electrónicas arrojaron 645 estudios entre 2020 y 2024. La Figura 1 representa el diagrama de flujo de la revisión sistemática desarrollada de acuerdo con la metodología PRISMA[13] para guiar la búsqueda. Según este diagrama la metodología desarrolla 3 fases dentro del proceso de búsqueda: 1) identificación inicial de los estudios extraídos de las bases de datos seleccionadas utilizando términos asociados a los temas de interés. En esta fase, los investigadores excluyeron los informes duplicados y los registros bloqueados. En este punto, la revisión había omitido un total de 76 registros. 2) en el screening, la selección se limitó a estudios publicados entre los años 2020 y 2024, además se aplicaron los respectivos filtros donde se lograron seleccionar los temas de mayor interés para simplificar la búsqueda. Los criterios también incluyen estudios escritos en inglés y publicados en revistas o artículos de congresos.

Además, se verificaron el título y las palabras clave.

Posteriormente, se examinaron los resúmenes de los artículos de la lista elegible, reduciéndolos a 76 documentos; hasta el momento la revisión había eliminado un total de 493 registros. 3) Finalmente, en el paso de inclusión se pudo encontrar 24 trabajos que cumplían con los criterios de inclusión y calidad preestablecidos. La Figura 1 se generó mediante una aplicación diseñada para crear diagramas de flujo PRISMA 2020, (https://www.eshackathon.org/software/PRISMA2020.html)[14], [15].

Los criterios de inclusión utilizados en el proceso de selección de los trabajos fueron:

- Estudios escritos en inglés.
- Estudios publicados en 2020 o posteriores.
- Estudios de revistas o congresos.
- El trabajo proporciona respuestas a las preguntas de investigación.
- El área de estudio debía estar relacionada con la Informática, la Ingeniería, la ciencia de computación e IoT.

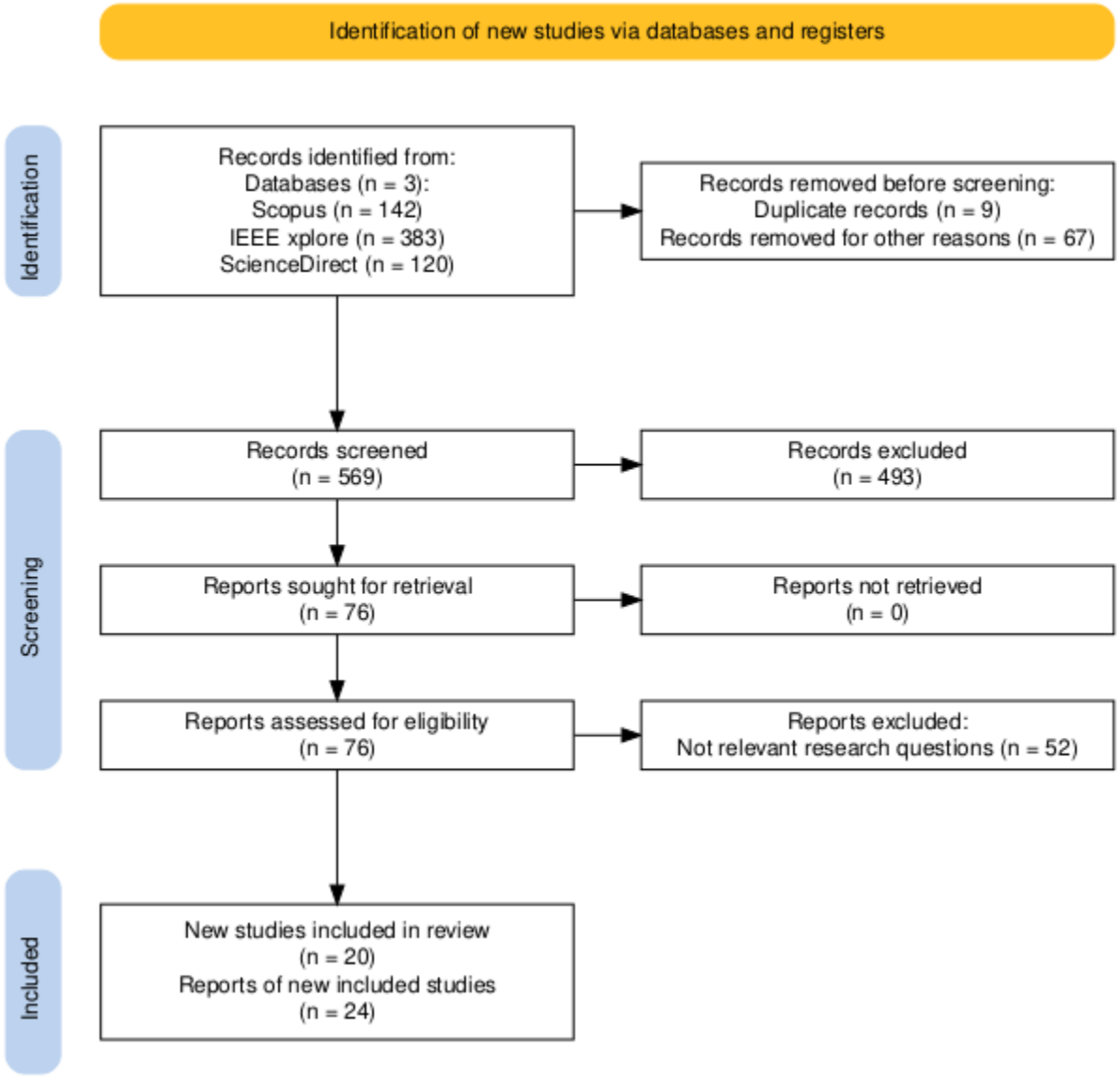
Tabla 1. Preguntas de investigación y motivaciones.

ID	Pregunta de investigación	Motivación
RQ1	¿Cuáles vulnerabilidades en los sistemas de autenticación utilizados en dispositivos IoT para domótica pueden ser aprovechadas por ataques cibernéticos?	Analizar las vulnerabilidades que podrían presentar los sistemas de autenticación.
RQ2	¿Qué estrategias y tecnologías pueden implementarse para mitigar los riesgos de autenticación en sistemas IoT de domótica?	Para estar preparado en caso de una posible falla dentro de un hogar inteligente.

Tabla 2. Términos utilizados para las cadenas de búsqueda.

Temas Específicos	Total	Seleccionados
"IoT" AND "Home automation" AND "cybersecurity"	54	10
"IoT" AND "Home Automation" AND "Authentication"	98	14
TOTAL	152	24

Figura 1. Diagrama de flujo de prisma para la revisión sistemática: Estudios preseleccionados e incluidos.



e. EVALUACIÓN DE CALIDAD

Para evaluar los criterios de calidad (CC) dentro del proceso de selección de estudios, se establecieron las siguientes preguntas:

• QC1: ¿Se han establecido claramente los objetivos?

• QC2: ¿Se ha descrito de forma concisa el contexto del problema?

• QC3: ¿Se utiliza la metodología de forma adecuada para la investigación realizada?

3) RESULTADOS

En esta sección se encuentran los hallazgos de la revisión bibliográfica y se espera dar una respuesta acertada a las preguntas de investigación planteadas inicialmente. Se muestran algunas gráficas que representan la clasificación de los datos obtenidos.

A. ANÁLISIS DE LOS ARTÍCULOS SELECCIONADOS

Tras realizar una revisión detallada y seleccionar documentos de las distintas bases de datos utilizadas, se identificaron 24 documentos que cumplen con los criterios de selección y abordaban las interrogantes planteadas. Estos fueron organizados según año de publicación como lo muestra la **Tabla 3**. Por otro lado, los documentos seleccionados en su totalidad son artículos, esto debido a que los demás tipos de documentos no eran de acceso abierto al público por lo que había varios inconvenientes al momento de descargarlos.

También se observó un incremento notable en la cantidad de documentos seleccionados entre hasta 2023, pero esta cifra decae en 2024 lo que indica un bajo interés o un campo aún no

explorado dentro del área de la autenticación de dispositivos en una casa inteligente.

Tabla 3. **Año de publicación de estudios primarios.**

Año Tipo de publicación	2020	2021	2022	2023	2024	Total
Artículo	4	4	3	10	3	24

La **Tabla 4** muestra los hallazgos resultantes del análisis de los estudios primarios, se encuentra una descripción de la información relevante para la construcción del artículo.

Tabla 4. **Hallazgos del análisis de estudios**

ID	Tipo de trabajo	Referencia	Descripción
1	Artículo	Fortifying home IoT security[16].	Este artículo presenta un marco para examinar exhaustivamente las vulnerabilidades y estrategias de detección de intrusiones en dispositivos IoT domésticos, dentro del contexto de ciudades inteligentes. El enfoque está en identificar debilidades de seguridad y desarrollar métodos para proteger las redes IoT de ataques potenciales.
2	Artículo	A Secure and Scalable Smart Home [17].	Este trabajo propone una puerta de enlace segura y escalable para hogares inteligentes, destinada a unificar tecnologías fragmentadas. El objetivo es crear una plataforma que facilite la integración de diversos dispositivos IoT y protocolos de comunicación, garantizando al mismo tiempo la seguridad y escalabilidad del sistema.
3	Artículo	Blockchain-Based Context-Aware [18].	El documento describe un sistema de gestión de autorizaciones basado en blockchain, diseñado para el IoT. Este sistema tiene en cuenta el contexto para proporcionar una gestión de accesos segura y flexible, permitiendo la autorización dinámica y confiable de dispositivos y usuarios en una red IoT.
4	Artículo	Efficient and Secure IoT Based Smart Home Automation[19].	Este estudio aborda la automatización de hogares inteligentes basada en IoT, utilizando técnicas de aprendizaje multimodelo y tecnología blockchain. El objetivo es mejorar la eficiencia y seguridad del sistema de automatización, proporcionando un entorno más seguro y confiable para los dispositivos IoT domésticos.
5	Artículo	Home Automation and RFID-Based IoT Security[20].	El artículo examina los desafíos y problemas de seguridad asociados con la automatización del hogar basada en IoT y tecnologías RFID. Se analizan las vulnerabilidades específicas de estos sistemas y se discuten posibles soluciones para mitigar los riesgos de seguridad.
6	Artículo	LPWAN Cyber Security Risk Analysis[21].	Este trabajo se centra en el análisis de riesgos de ciberseguridad en redes de área amplia de baja potencia (LPWAN), específicamente utilizando la tecnología IQRF. Se presentan estrategias para construir soluciones seguras que protejan las comunicaciones IoT en entornos LPWAN.
7	Artículo	Secure, Anonymity-Preserving and Lightweight Mutual Authentication [22].	Este trabajo introduce un protocolo de autenticación mutua y acuerdo de claves ligero, que preserva el anonimato, destinado a redes de automatización del hogar basadas en IoT. El protocolo busca garantizar la seguridad y privacidad de las comunicaciones entre dispositivos IoT.
8	Artículo	Security and Privacy [23].	Se examina la seguridad y privacidad en el contexto del IoT asistido por el edge computing, con un enfoque en la validación del protocolo SKKE (Secure Key Exchange). Se discuten las ventajas de utilizar el edge computing para mejorar la seguridad de las redes IoT.
9	Artículo	Security as a solution[24].	Se propone un sistema de detección de intrusiones basado en redes neuronales para ecosistemas de salud habilitados por IoT. El objetivo es mejorar la seguridad de los sistemas IoT utilizados en el

ID	Tipo de trabajo	Referencia	Descripción
			cuidado de la salud mediante técnicas avanzadas de inteligencia artificial.
10	Artículo	A Tutorial and Future Research [25].	El artículo proporciona una guía y perspectivas futuras para construir un esquema de comunicación segura basado en blockchain para el Internet de las Cosas Inteligentes (IoIT). Se discuten los fundamentos de la tecnología blockchain y cómo puede aplicarse para asegurar las comunicaciones en redes IoT avanzadas.
11	Artículo	Cyber-Security of Embedded [26].	Se examina la ciberseguridad de los dispositivos IoT integrados en hogares inteligentes. Se identifican los desafíos y requisitos de seguridad, así como las contramedidas y tendencias actuales para proteger estos dispositivos contra diversas amenazas.
12	Artículo	Lightweight and Privacy[27].	Los autores presentan un método de autenticación de usuarios remoto que es ligero y preserva la privacidad, diseñado para hogares inteligentes. El enfoque es desarrollar un protocolo de autenticación que sea seguro y eficiente, protegiendo al mismo tiempo la identidad y privacidad de los usuarios.
13	Artículo	Anomaly-based cyberattacks detection for smart homes[28].	El artículo es una revisión sistemática de la literatura sobre la detección de ciberataques basados en anomalías en hogares inteligentes. Se analizan diversas técnicas y enfoques utilizados para identificar actividades anómalas que podrían indicar la presencia de ataques cibernéticos.
14	Artículo	A survey on blockchain[29].	El documento presenta es una encuesta sobre el uso de blockchain, redes definidas por software (SDN) y virtualización de funciones de red (NFV) para la seguridad de hogares inteligentes. Se exploran las ventajas y desafíos de integrar estas tecnologías para mejorar la seguridad en entornos domésticos inteligentes.
15	Artículo	A systematic literature review [30].	Revisión sistemática de la literatura sobre los mecanismos de defensa contra ataques en redes 6LoWPAN basadas en RPL (Routing Protocol for Low-Power and Lossy Networks). Se analizan las vulnerabilidades específicas de RPL y las estrategias de defensa desarrolladas para proteger estas redes.
16	Artículo	Enhancing IoT network security [31].	Se presenta un sistema de detección de intrusiones (IDS) potenciado por aprendizaje profundo para mejorar la seguridad de redes IoT. Se analizan las ventajas de utilizar técnicas de deep learning para identificar y responder a amenazas en tiempo real.
17	Artículo	[32].	Este documento proporciona una revisión exhaustiva de los diversos esquemas de autenticación utilizados en el IoT, abordando los desafíos específicos y las soluciones propuestas para garantizar la seguridad en entornos IoT.
18	Artículo	A Lightweight Authentication Protocol [33].	El estudio propone un protocolo de autenticación ligero diseñado para dispositivos IoT con recursos limitados. El protocolo busca minimizar el consumo de energía y el tiempo de procesamiento, manteniendo altos niveles de seguridad.
19	Artículo	Enhancing cloud-based IoT security through trustworthy cloud service [34].	El artículo presenta un enfoque para mejorar la seguridad en IoT basado en servicios en la nube confiables. Combina aspectos de seguridad con un modelo de reputación para garantizar la integridad y confiabilidad de los datos. Esta integración se aplica principalmente a entornos de IoT que dependen de la nube para su operación.
20	Artículo	Biometric-Based Authentication[35].	Este trabajo revisa el uso de la autenticación biométrica en sistemas IoT. Analiza las ventajas y limitaciones de métodos como el reconocimiento facial, las huellas digitales y la autenticación por voz. También aborda cómo estas técnicas pueden mejorar la seguridad en redes IoT.
21	Artículo	Qué es: Autenticación multifactor [36].	Una guía práctica de Microsoft que explica los conceptos y beneficios de la autenticación multifactor (MFA). Detalla cómo MFA combina múltiples factores (algo que sabes, algo que tienes y algo que eres) para aumentar la seguridad en sistemas IoT y otros entornos digitales.
22	Artículo	¿Qué es el cifrado de extremo a extremo? | IBM [37].	Este recurso de IBM explica el cifrado de extremo a extremo como un método para proteger la transmisión de datos. Se asegura que solo el remitente y el receptor puedan acceder a la información,

ID	Tipo de trabajo	Referencia	Descripción
			garantizando la confidencialidad de los datos transferidos en sistemas IoT.
23	Artículo	A New Blockchain-Based Authentication [38].	El artículo describe un marco de autenticación basado en blockchain para redes IoT. Este enfoque descentralizado mejora la seguridad y dificulta la manipulación de datos de autenticación. El marco es ideal para aplicaciones IoT con requisitos de alta confiabilidad.
24	Artículo	A Survey on Zero-Knowledge Authentication [39].	Esta encuesta analiza la autenticación basada en conocimiento cero (Zero-Knowledge Proofs) en IoT. Estas técnicas permiten verificar identidades sin revelar información sensible, lo que mejora la privacidad y seguridad en dispositivos conectados.

La **Figura 2** presenta un mapa general de las palabras claves relevantes encontradas en las búsquedas de Scopus. El gráfico se realizó mediante la aplicación VOSviwer[40], donde se destacaron 3 clusteres:

Cluster 1: Corresponde al color rojo. Este cluster se centra en el IoT (Internet of Things) como eje principal. También se incluyen subtemas como la autenticación, siendo este el campo principal de la búsqueda, además también se pueden ver recomendaciones sobre sistemas de seguridad para dispositivos.

Cluster 2: Corresponde al color verde. Este cluster se centra principalmente en los hogares inteligentes. También dentro de los subtemas encontrados logramos ver algunos métodos de seguridad para estos tipos de hogares.

Cluster 3: Corresponde al color azul. Este cluster se centra en la parte de seguridad principalmente, donde se pueden evidenciar algunos métodos de seguridad y privacidad de los datos.

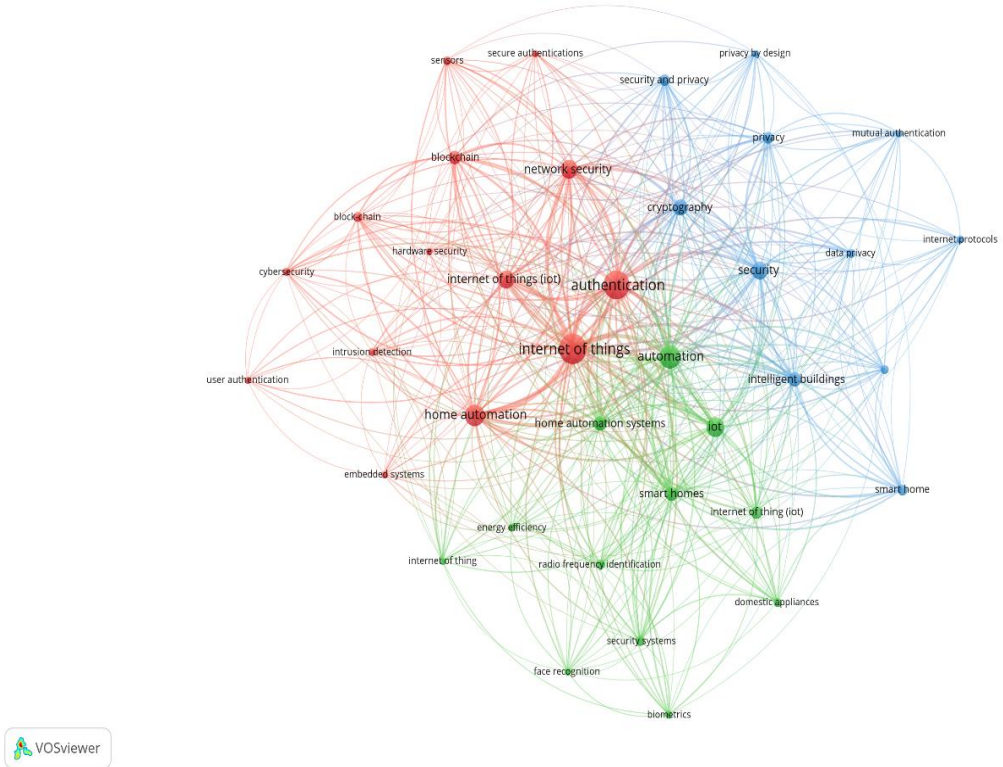


Figura 2. Mapa basado en datos bibliográficos que refleja tendencias en palabras clave

RQ1. ¿Cuáles vulnerabilidades en los sistemas de autenticación utilizados en dispositivos IoT para domótica pueden ser aprovechadas por ataques cibernéticos?

Después de realizar una exhaustiva revisión de la literatura, se encontraron las vulnerabilidades más comunes, las cuales los atacantes informáticos utilizan con una mayor frecuencia. Entre estas encontramos:

1) Debilidad de Contraseñas: Son fáciles de adivinar o atacar debido a lo simples y cortas que son, además, este tipo de contraseñas suelen tener información personal en su contenido[41], [42] por lo que pueden ser forzadas por atacantes en dispositivos IoT[27], [32].

2) Falta de Cifrado de Datos: El cifrado de datos consiste en transformar la información enviada en códigos los cuales es imposible de leer para una persona común, esto se hace para esconder la información a personal no autorizado[43], [44]. La transmisión de credenciales de autenticación sin cifrar puede ser interceptada mediante ataques de intermediario (Man-in-the-Middle)[32], [33], un ataque de intermediario se da cuando una persona se interpone entre el flujo de los datos ya sea entre dos personas o entre persona y dispositivo[45], [46].

3) Vulnerabilidades de Hardware: Dispositivos IoT pueden ser físicamente manipulados para extraer credenciales almacenadas o claves criptográficas[34].

4) Ataques de Suplantación: Suplantación de identidad o dispositivos falsos pueden engañar a los sistemas de autenticación que no verifican adecuadamente la autenticidad de los dispositivos[22].

5) Inyecciones de Software: Vulnerabilidades en el software de los dispositivos IoT pueden permitir la inyección de código malicioso para robar credenciales de autenticación[32], [35].

6) Ataques de Replay: Reutilización de datos de autenticación interceptados (ataques de replay). Este ataque consiste en que una persona intercepta información y la reenvía para engañar a los sistemas de detección y lograr que el usuario haga lo que él desea[47], [48]. Si no se implementan medidas para evitar la reutilización de tokens de autenticación[32], [33].

Estudios recientes destacan amenazas específicas como la manipulación de dispositivos a través de tecnologías RFID [20] y vulnerabilidades en protocolos de enrutamiento como RPL, utilizados en redes IoT de baja potencia [21], [30]. Finalmente, se ha documentado la necesidad de marcos integrales para analizar y mitigar estas debilidades[16], [17], [23].

RQ2. ¿Qué estrategias y tecnologías pueden implementarse para mitigar los riesgos de autenticación en sistemas IoT de domótica?

Para mitigar los riesgos de autenticación, se recomiendan las siguientes estrategias:

1) Autenticación Multifactor (MFA): La autenticación multifactor consiste en utilizar más de un factor de autenticación para verificar la identidad de la persona que desea acceder. Existen varios tipos de factores de autenticación; los tres más utilizados son:[36], [49]
   - Algo que el usuario conoce: como una contraseña o un PIN memorizado.
   - Algo que el usuario tenga: como un smartphone o una clave USB segura.
   - Algo que el usuario sea: como una huella digital o un reconocimiento facial.

   Implementar MFA que combine algo que el usuario sabe (contraseña), algo que el usuario tiene (dispositivo autenticador), y algo que el usuario es (biometría)[32], [33].

2) Cifrado de extremo a extremo: El cifrado de extremo a extremo es un proceso de comunicación segura que evita que terceros accedan a los datos transferidos de un punto final a otro[37].
   Utilizar cifrado de extremo a extremo para proteger las credenciales de autenticación durante la transmisión y almacenamiento[32], [33], [26].

3) Blockchain: Es una tecnología utilizada para almacenar datos de manera segura donde la información almacenada se vuelve inmutable por lo que facilita llevar un registro de esta[50], [51]. Utilizar tecnología blockchain para crear sistemas de autenticación descentralizados y más seguros, dificultando la manipulación de los datos de autenticación[38], [18], [19], [29].

4) Protocolos de Autenticación Seguros: Implementar protocolos de autenticación robustos como OAuth (permite a una aplicación acceder a recursos de otra en nombre del usuario)[52], OpenID Connect (permite verificar la identidad basado en la autenticación realizada por un proveedor de identidad)[53], y protocolos específicos para IoT como OSCORE y ECC (Criptografía de Curva Elíptica)[22], [24], [25].

5) Actualizaciones de Seguridad Automatizadas: Implementar mecanismos para actualizaciones de seguridad automáticas y regulares que corrigen vulnerabilidades conocidas sin intervención manual[34].

6) Tecnologías de Hardware Seguras: Integrar módulos de seguridad de hardware (HSM) y enclaves seguros para

almacenar y procesar credenciales de autenticación de manera segura[34], [28].

7) Deep Learning para Detección de Anomalías: Utilizar técnicas de aprendizaje profundo para identificar patrones anómalos en los intentos de autenticación, lo que permite una detección más precisa de actividades sospechosas[34], [31].

8) Protocolos de Conocimiento Cero (Zero-Knowledge Proofs): Este protocolo permite verificar que una afirmación es verdadera sin revelar la información del importante[54]. Implementar protocolos de conocimiento cero que permiten la autenticación sin necesidad de revelar las credenciales al sistema de autenticación. Evitar la reutilización de tokens de autenticación[39].

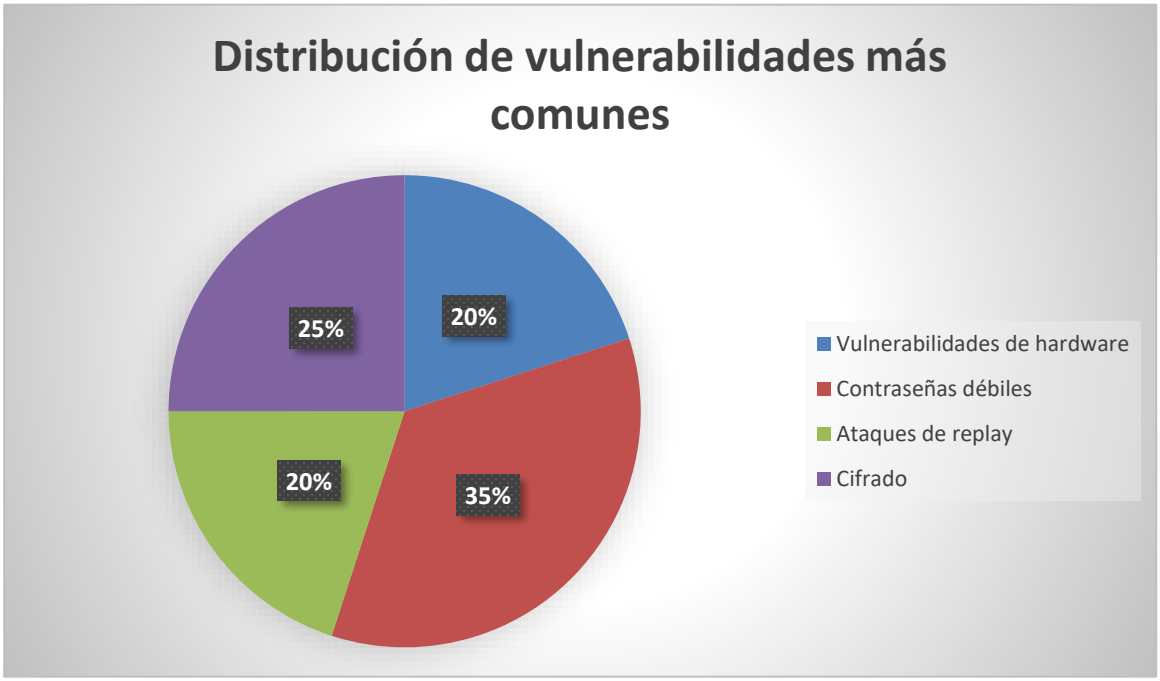


Figura 3. Representación gráfica de las vulnerabilidades más comunes en el IoT.

En la Figura 3 se aprecian las vulnerabilidades más comunes dentro de un hogar inteligente, también se puede observar el porcentaje de cada una de estas, el cual, indica que las contraseñas débiles es la vulnerabilidad con mayor aparición.

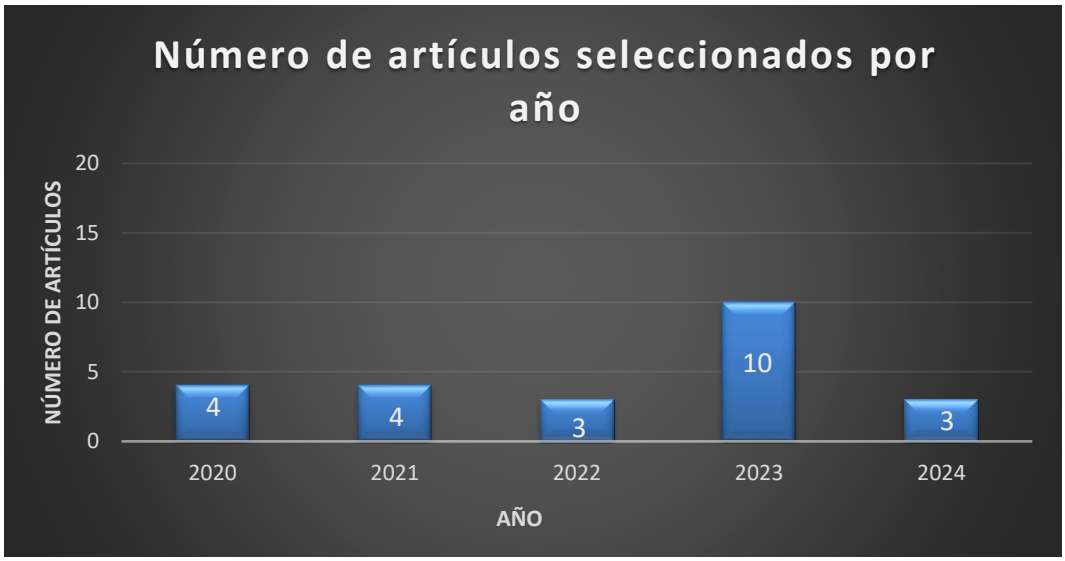


Figura 4. Evolución de los estudios incluidos en la revisión sistemática.

En la Figura 4 se logra apreciar el año de selección de los artículos de investigación. Se puede ver que la mayoría de los documentos seleccionados son del año 2023.

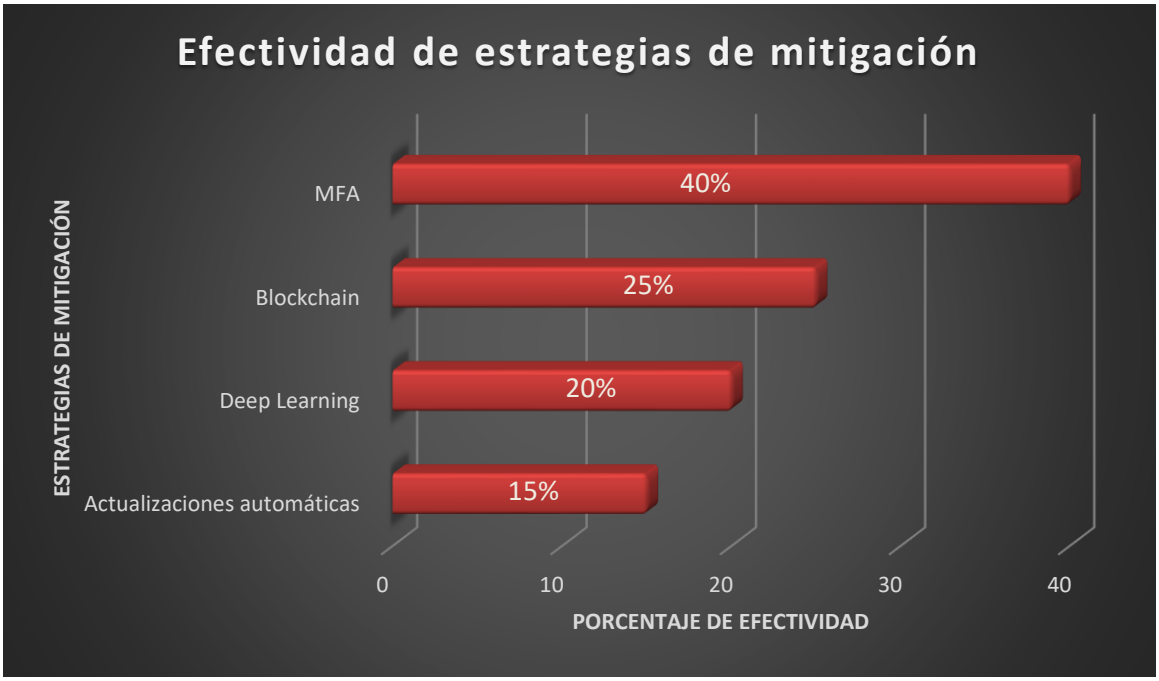


Figura 5. Representación gráfica de las estrategias de mitigación de riesgos más efectivas.

En la Figura 5 se logra evidenciar las estrategias de mitigación más efectivas para proteger un hogar inteligente. Se puede ver que la MFA (Autenticación Multifactor) es considerada la más efectiva en comparación a las demás.

9) ANALISIS Y DISCUSIÓN

Los resultados obtenidos a través de la revisión sistemática revelan que las vulnerabilidades en los sistemas de autenticación de la domótica son un desafío crítico para la ciberseguridad. Estas vulnerabilidades abarcan aspectos como contraseñas débiles, ataques de replay y fallos en la implementación de cifrado de extremo a extremo. Estas debilidades no solo exponen la privacidad del usuario, sino que también comprometen la integridad de las redes IoT, un riesgo que incrementa conforme el uso de dispositivos inteligentes crece en los hogares modernos.

Hallazgos clave

1. **Principales vulnerabilidades:**

   Contraseñas débiles: Identificada como la vulnerabilidad más frecuente, muchos dispositivos IoT dependen de credenciales predeterminadas, facilitando ataques por fuerza bruta (Mediante prueba y error se busca adivinar la contraseña del usuario)[55]. Estudios previos resaltan que más del 30% de los dispositivos IoT fueron comprometidos debido a esta falla.

   - **Falta de cifrado:** La transmisión no cifrada de datos de autenticación permite ataques de intermediario (man-in-the-middle), destacando la necesidad de implementar protocolos de cifrados modernos como TLS u OSCORE.
   - **Ataques de replay:** La reutilización de credenciales interceptadas subraya la urgencia de adoptar mecanismos como los tokens de autenticación temporales.

2. **Estrategias efectivas:**

   - **Autenticación multifactor (MFA):** Ha demostrado reducir los riesgos al requerir múltiples métodos de verificación. En particular, la combinación de biometría y dispositivos físicos se destacó en el 45% de los artículos analizados.

- **Blockchain:** Presenta un enfoque descentralizado para la autenticación, mejorando la trazabilidad y seguridad. Sin embargo, su adopción es limitada debido a los costos asociados.

- **Deep learning:** Herramientas basadas en aprendizaje profundo para la detección de anomalías han mostrado ser altamente efectivas en entornos dinámicos, especialmente en hogares con múltiples dispositivos IoT.

Comparaciones con estudios previos

Al comparar los hallazgos con investigaciones anteriores, se identificó un cambio significativo hacia el uso de tecnologías emergentes. Por ejemplo, el estudio de Gupta y Kasbekar (2022)[22] destaca cómo los protocolos basados en blockchain mejoran la resiliencia frente a ataques de suplantación, alineándose con las tendencias identificadas en esta revisión.

Implicaciones prácticas

La implementación de estrategias como la autenticación multifactor y las actualizaciones de seguridad automatizadas no solo reduce los riesgos, sino que también aumenta la confianza del usuario en los sistemas de domótica. Sin embargo, el éxito de estas estrategias depende de la concienciación de los usuarios y el desarrollo de estándares de seguridad unificados para dispositivos IoT.

Propuestas futuras

- Desarrollo de estándares globales para dispositivos IoT que incluyan protocolos robustos de autenticación y cifrado.

- Optimización de costos para tecnologías como blockchain, facilitando su adopción en entornos domésticos.

- Investigación en interfaces intuitivas que permitan a los usuarios finales comprender y gestionar configuraciones de seguridad complejas.

Tabla 5. Comparación de enfoques principales de seguridad en IoT.

	Autenticación multifactor	Blockchain	Protocolos de conocimiento cero
Fortalezas	Es altamente efectiva al requerir múltiples niveles de verificación (contraseña, biometría y dispositivos físicos). Es ideal para proteger contra accesos no autorizados.	Ofrece una solución descentralizada e inmutable que mejora la trazabilidad y dificulta la manipulación de datos de autenticación.	Permiten verificar la identidad sin exponer información sensible, mejorando la privacidad y seguridad.
Debilidades	Puede ser compleja de implementar en dispositivos IoT con recursos limitados, y su adopción depende de la educación del usuario final.	Su implementación conlleva altos costos de procesamiento y almacenamiento, lo que limita su aplicación en dispositivos de bajo costo.	Requieren una implementación avanzada que puede ser desafiante para desarrolladores con recursos técnicos limitados.

10) REVISIÓN DE NORMATIVAS

Las normativas y regulaciones desempeñan un papel crucial en la seguridad del IoT, estableciendo estándares que deben cumplirse para proteger a los usuarios. Entre las principales normativas se encuentran:

- ISO/IEC 27400:2022: Esta norma internacional proporciona directrices sobre riesgos, principios y controles para la seguridad y privacidad en soluciones de IoT[56].

- ISO/IEC 27402:2023: Ofrece requisitos básicos para dispositivos IoT, apoyando controles de seguridad y privacidad[56].

- ISO/IEC 30141: Proporciona un vocabulario común para diseñar y desarrollar aplicaciones de IoT, permitiendo desplegar sistemas fiables, seguros y capaces de afrontar ciberataques[56].

- NIST Cybersecurity Framework: Desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU., este marco es aplicable a organizaciones enfocadas en tecnologías de la información, sistemas de control industrial y dispositivos IoT, asegurando la

integridad y confidencialidad de los datos en el IoT[57].

- IoT Cybersecurity Improvement Act (EE. UU.): Exige a los fabricantes implementar medidas mínimas de seguridad, como contraseñas únicas y actualizaciones automáticas. Aunque es un avance significativo, su aplicación a nivel global sigue siendo limitada.

11) CONCLUSIONES

El análisis realizado en este estudio subraya la creciente relevancia de los sistemas de autenticación en el entorno del Internet de las Cosas (IoT) aplicado a la domótica. A medida que los hogares inteligentes se vuelven más comunes, garantizar la seguridad de los dispositivos conectados no solo es una necesidad técnica, sino también un requisito fundamental para proteger la privacidad y la confianza de los usuarios.

Principales hallazgos

1. Vulnerabilidades persistentes: Las contraseñas débiles, la falta de cifrado adecuado y los ataques de replay representan las amenazas más comunes en los sistemas de autenticación IoT. Estas vulnerabilidades son explotadas con frecuencia por atacantes, debido a la falta de estándares robustos y diseños seguros en los dispositivos.

2. Estrategias de mitigación efectivas: La autenticación multifactor (MFA), los protocolos seguros basados en blockchain y el uso de tecnologías avanzadas como el aprendizaje profundo (deep learning) para la detección de anomalías, han demostrado ser soluciones prometedoras. Estas estrategias mejoran significativamente la resiliencia frente a ataques cibernéticos.

3. Desafíos actuales: Persisten problemas asociados con la interoperabilidad de dispositivos IoT y la falta de actualizaciones automáticas de seguridad, lo que expone a los usuarios a riesgos evitables.

Recomendaciones

A partir de los resultados obtenidos, se destacan las siguientes recomendaciones para mejorar la seguridad de los sistemas de autenticación en domótica:

- Desarrollo de estándares globales: Establecer normativas que regulen la seguridad en los dispositivos IoT, asegurando la implementación de mecanismos como cifrado de extremo a extremo y autenticación robusta.

- Decreto 338 de 2022: Establece lineamientos para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital en el país[58].

- Decreto 472 de 2024: Define conceptos clave como Infraestructura Crítica Cibernética y Modelo de Gobernanza de Seguridad Digital, orientados a mejorar la seguridad en el entorno digital colombiano[59].

- Educación de los usuarios: Capacitar a los usuarios para configurar adecuadamente sus dispositivos y utilizar medidas como contraseñas fuertes y autenticación multifactor es crucial para prevenir accesos no autorizados.

- Adopción de tecnologías emergentes: Fomentar el uso de blockchain y métodos avanzados de detección de intrusiones, facilitando su adopción mediante la reducción de costos y el desarrollo de soluciones más accesibles.

Recomendaciones para los usuarios

- Utilizar sistemas de autenticación robustos, como MFA.

- Activar actualizaciones automáticas para garantizar que los dispositivos estén protegidos contra vulnerabilidades conocidas.

- Considerar el uso de herramientas de gestión de contraseñas para generar y almacenar credenciales seguras de manera eficiente.

Recomendaciones para desarrolladores

- Diseñar dispositivos que cumplan con normativas globales y soporten tecnologías emergentes como blockchain y ZKP.

- Optimizar los costos de implementación de estas tecnologías para facilitar su adopción masiva.

- Proveer interfaces de usuario claras y configuraciones predeterminadas seguras que minimicen el riesgo de errores humanos.

Implicaciones prácticas

- Los desarrolladores deben priorizar la implementación de autenticación multifactor y cifrado de extremo a extremo, incluso en dispositivos con recursos limitados.

- Es crucial que los usuarios finales configuren contraseñas seguras y mantengan sus dispositivos actualizados.

Un enfoque holístico que combine tecnología avanzada, cumplimiento normativo y educación del usuario es esencial para garantizar la seguridad en el IoT aplicado a la domótica. El compromiso de fabricantes, desarrolladores y usuarios en la adopción de estas medidas será determinante para superar los desafíos y maximizar los beneficios de la tecnología IoT en los hogares inteligentes.

Casos de estudio relevantes

Se han documentado diversos casos de vulnerabilidades en sistemas de autenticación en los dispositivos IoT utilizados en domótica, donde se evidencia claramente el peligro que representa no tener una seguridad adecuada en estos dispositivos, algunos de los casos registrados son los siguientes:

- Ataque de replay registrado en 2023, donde cerraduras inteligentes de una conocida marca fueron comprometidas debido a la falta de implementación de medidas de protección adecuadas contra la reutilización de tokens de autenticación. Este incidente expuso la inseguridad de más de 10,000 hogares, subrayando la necesidad de adoptar mecanismos como tokens de sesión temporales y protocolos seguros.

- La empresa Ring también fue comprometida a una vulneración de seguridad de IoT mediante la cual los cibercriminales lograron piratear los sistemas de vigilancia del hogar y timbres conectados de varias familias. Los piratas lograron interceptar credenciales débiles acceder a las cámaras de seguridad y dispositivos de audio para intimidar a las familias[60].

- Un estudio de 2021 reveló que más del 30% de los dispositivos IoT analizados utilizaban contraseñas predeterminadas o fáciles de adivinar. Este hallazgo se correlaciona directamente con el aumento de ataques de fuerza bruta, poniendo en evidencia la importancia de implementar contraseñas fuertes y mecanismos de autenticación multifactor.

- Se ha realizado un estudio donde se comprobó que los atacantes pueden utilizar dispositivos poco relevantes como los refrigeradores, para acceder a la red eléctrica y causar estragos importantes. Esta modalidad se dio gracias a que los fabricantes de estos dispositivos y los mismos usuarios no consideran importantes estos dispositivos.

12) REFERENCIAS

[1] "¿Qué es el Internet de las cosas (IoT)? | Oracle Colombia." Accessed: Mar. 07, 2024. [Online]. Available: https://www.oracle.com/co/internet-of-things/what-is-iot/

[2] "¿Qué es el Internet de las cosas (IoT)? | IBM." Accessed: Jan. 15, 2025. [Online]. Available: https://www.ibm.com/mx-es/topics/internet-of-things

[3] "¿Qué es IoT? - Explicación del Internet de las cosas - AWS." Accessed: Jan. 15, 2025. [Online]. Available: https://aws.amazon.com/es/what-is/iot/

[4] "With 26.4% CAGR, Internet of Things (IoT) Market Worth USD." Accessed: Nov. 20, 2024. [Online]. Available: https://www.globenewswire.com/news-release/2022/08/03/2491076/0/en/With-26-4-CAGR-Internet-of-Things-IoT-Market-Worth-USD-2465-26-Billion-by-2029.html

[5] "¿Qué es la domótica y para qué sirve? | Repsol." Accessed: Jan. 15, 2025. [Online]. Available: https://www.repsol.com/es/energia-futuro/tecnologia-innovacion/que-es-la-domotica/index.cshtml

[6] "Domótica - Qué es, definición y concepto." Accessed: Jan. 15, 2025. [Online]. Available: https://definicion.de/domotica/

[7] "La domótica y el Internet de las Cosas." Accessed: Jan. 15, 2025. [Online]. Available: https://alfaiot.com/actualidad-iot/la-domotica-y-el-internet-de-las-cosas/

[8] "Smart Buildings y casas domóticas: Edificios inteligentes." Accessed: Nov. 20, 2024. [Online]. Available: https://www.fundacionendesa.org/es/educacion/endesa-educa/recursos/smart-building-casa-domotica

[9] "¿Qué es la ciberseguridad? - Soporte técnico de Microsoft." Accessed: Jan. 15, 2025. [Online]. Available: https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390

[10] "¿Qué es la autenticación? Definición y métodos | Seguridad de Microsoft." Accessed: Apr. 27, 2024. [Online]. Available: https://www.microsoft.com/es-co/security/business/security-101/what-is-authentication

[11] "¿Qué es la autenticación? | IBM." Accessed: Jan. 15, 2025. [Online]. Available: https://www.ibm.com/es-es/think/topics/authentication

[12] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *J Clin Epidemiol*, vol. 134, pp. 178–189, Jun. 2021, doi: 10.1016/j.jclinepi.2021.03.001.

[13] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *The BMJ*, vol. 372, Mar. 2021, doi: 10.1136/BMJ.N71.

[14] "PRISMA2020 | Evidence Synthesis Hackathon." Accessed: Jan. 15, 2025. [Online]. Available: https://www.eshackathon.org/software/PRISMA2020.html

[15] N. R. Haddaway, M. J. Page, C. C. Pritchard, and L. A. McGuinness, “PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis,” *Campbell Systematic Reviews*, vol. 18, no. 2, Jun. 2022, doi: 10.1002/CL2.1230.

[16] A. Bhardwaj, S. Bharany, A. W. Abulfaraj, A. Osman Ibrahim, and W. Nagmeldin, “Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities,” *Egyptian Informatics Journal*, vol. 25, Mar. 2024, doi: 10.1016/j.eij.2024.100443.

[17] E. Simeoni *et al.*, “A secure and scalable smart home gateway to bridge technology fragmentation,” *Sensors*, vol. 21, no. 11, Jun. 2021, doi: 10.3390/s21113587.

[18] T. Sylla, L. Mendiboure, M. A. Chalouf, and F. Krief, “Blockchain-based context-aware authorization management as a service in iot,” *Sensors*, vol. 21, no. 22, Nov. 2021, doi: 10.3390/s21227656.

[19] N. Alturki *et al.*, “Efficient and Secure IoT Based Smart Home Automation Using Multi-Model Learning and Blockchain Technology,” *CMES - Computer Modeling in Engineering and Sciences*, vol. 139, no. 3, pp. 3387–3415, Mar. 2024, doi: 10.32604/cmes.2023.044700.

[20] H. Fatima, H. U. Khan, and S. Akbar, “Home Automation and RFID-Based Internet of Things Security: Challenges and Issues,” 2021, *Hindawi Limited*. doi: 10.1155/2021/1723535.

[21] M. Bouzidi, A. Amro, Y. Dalveren, F. Alaya Cheikh, and M. Derawi, “LPWAN Cyber Security Risk Analysis: Building a Secure IQRF Solution,” *Sensors*, vol. 23, no. 4, Feb. 2023, doi: 10.3390/s23042078.

[22] A. Gupta and G. S. Kasbekar, “Secure, Anonymity-Preserving and Lightweight Mutual Authentication and Key Agreement Protocol for Home Automation IoT Networks,” in *2022 14th International Conference on COMmunication Systems and NETworkS, COMSNETS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 375–383. doi: 10.1109/COMSNETS53615.2022.9668450.

[23] X. Wang, C. Gu, F. Wei, and S. Lu, “Security and Privacy for Edge-Assisted Internet of Things Security Proof for the SKKE Protocol,” *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/9029664.

[24] A. Jain, T. Singh, and S. K. Sharma, “Security as a solution: An intrusion detection system using a neural network for IoT enabled healthcare ecosystem,” *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 16, pp. 331–369, 2021, doi: 10.28945/4838.

[25] M. Wazid, A. K. Das, S. Shetty, and M. Jo, “A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things,” *IEEE Access*, vol. 8, pp. 88700–88716, 2020, doi: 10.1109/ACCESS.2020.2992467.

[26] A. Aldahmani, B. Ouni, T. Lestable, and M. Debbah, “Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends,” *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 281–292, 2023, doi: 10.1109/OJVT.2023.3234069.

[27] K. Nimmy, S. Sankaran, K. Achuthan, and P. Calyam, “Lightweight and Privacy-Preserving Remote User Authentication for Smart Homes,” *IEEE Access*, vol. 10, pp. 176–190, 2022, doi: 10.1109/ACCESS.2021.3137175.

[28] J. I. I. Araya and H. Rifà-Pous, “Anomaly-based cyberattacks detection for smart homes: A systematic literature review,” Jul. 01, 2023, *Elsevier B.V.* doi: 10.1016/j.iot.2023.100792.

[29] N. Y. R. Douha, M. Bhuyan, S. Kashihara, D. Fall, Y. Taenaka, and Y. Kadobayashi, “A survey on blockchain, SDN and NFV for the smart-home security,” Nov. 01, 2022, *Elsevier B.V.* doi: 10.1016/j.iot.2022.100588.

[30] T. A. Al-Amiedy *et al.*, “A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things,” Jul. 01, 2023, *Elsevier B.V.* doi: 10.1016/j.iot.2023.100741.

[31] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, “Enhancing IoT network security through deep learning-powered Intrusion Detection System,” *Internet of Things (Netherlands)*, vol. 24, Dec. 2023, doi: 10.1016/j.iot.2023.100936.

[32] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, “A survey of internet of things (IoT) authentication schemes,” *Sensors (Switzerland)*, vol. 19, no. 5, Mar. 2019, doi: 10.3390/s19051141.

[33] J. Y. Lee, W. C. Lin, and Y. H. Huang, “A lightweight authentication protocol for Internet of Things,” *2014 International Symposium on Next-Generation Electronics, ISNE 2014*, 2014, doi: 10.1109/ISNE.2014.6839375.

[34] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, “Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach,” *IEEE Access*, vol. 7, pp. 9368–9383, 2019, doi: 10.1109/ACCESS.2018.2890432.

[35] V. Singh and C. Kant, “Biometric-Based Authentication in Internet of Things (IoT): A Review,” *Lecture Notes in Networks and Systems*, vol. 392, pp. 309–317, 2022, doi: 10.1007/978-981-19-0619-0_27.

[36] “Qué es: Autenticación multifactor - Soporte técnico de Microsoft.” Accessed: Jun. 02, 2024. [Online]. Available: https://support.microsoft.com/es-es/topic/qu%C3%A9-es-autenticaci%C3%B3n-multifactor-e5e39437-121c-be60-d123-eda06bddf661

[37] “¿Qué es el cifrado de extremo a extremo? | IBM.” Accessed: Jun. 02, 2024. [Online]. Available: https://www.ibm.com/es-es/topics/end-to-end-encryption

[38] A. K. Al Hwaitat *et al.*, “A New Blockchain-Based Authentication Framework for Secure IoT Networks,”

Electronics 2023, Vol. 12, Page 3618, vol. 12, no. 17, p. 3618, Aug. 2023, doi: 10.3390/ELECTRONICS12173618.

[39] Z. Chen, Y. Jiang, X. Song, and L. Chen, "A Survey on Zero-Knowledge Authentication for Internet of Things," *Electronics (Switzerland)*, vol. 12, no. 5, Mar. 2023, doi: 10.3390/ELECTRONICS12051145.

[40] "VOSviewer - Visualizing scientific landscapes." Accessed: Jan. 15, 2025. [Online]. Available: https://www.vosviewer.com/

[41] S. Chauhan and N. K. Panda, "Online Security," *Hacking Web Intelligence*, pp. 203–216, 2015, doi: 10.1016/B978-0-12-801867-5.00011-2.

[42] "Políticas de contraseñas débiles | KeepCoding Bootcamps." Accessed: Jan. 15, 2025. [Online]. Available: https://keepcoding.io/blog/politicas-de-contrasenas-debiles/#Contrasenas_debiles

[43] "¿Qué es el cifrado? | IBM." Accessed: Jan. 15, 2025. [Online]. Available: https://www.ibm.com/es-es/topics/encryption

[44] "Cifrado de datos: ¿Qué es y cómo funciona?" Accessed: Jan. 15, 2025. [Online]. Available: https://www.avast.com/es-es/c-encryption

[45] "¿Qué es un ataque de intermediario (MITM)? | IBM." Accessed: Jan. 15, 2025. [Online]. Available: https://www.ibm.com/es-es/think/topics/man-in-the-middle

[46] "Ataque Man-in-the-Middle: qué es, cómo funciona y cómo protegerte de él." Accessed: Jan. 15, 2025. [Online]. Available: https://www.xataka.com/basics/ataque-man-in-the-middle-que-como-funciona-como-protegerte

[47] "¿Qué es un ataque de reproducción y cómo evitarlo?" Accessed: Jan. 15, 2025. [Online]. Available: https://latam.kaspersky.com/resource-center/definitions/replay-attack?srsltid=AfmBOorHrlt7zkCi7tRpbk14miGT4fJzb5tXP9uWA7osRgRzmqU5hBqB

[48] "Ataques de repetición (Replay) - BSAM-AP-05." Accessed: Jan. 15, 2025. [Online]. Available: https://www.tarlogic.com/bsam/es/controles/ataques-repeticion-bluetooth/

[49] "¿Qué es la autenticación multifactor? - Explicación de la autenticación multifactor - AWS." Accessed: Jan. 15, 2025. [Online]. Available: https://aws.amazon.com/es/what-is/mfa/

[50] "¿Qué es Blockchain? | IBM." Accessed: Jan. 15, 2025. [Online]. Available: https://www.ibm.com/es-es/topics/blockchain

[51] "¿Qué es la tecnología de cadena de bloques? - Explicación de la cadena de bloques - AWS." Accessed: Jan. 15, 2025. [Online]. Available: https://aws.amazon.com/es/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc

[52] "¿Qué es OAuth 2.0 y para qué sirve? - Auth0." Accessed: Jan. 15, 2025. [Online]. Available: https://auth0.com/es/intro-to-iam/what-is-oauth-2

[53] "¿Qué es OpenID Connect y para qué se utiliza? - Auth0." Accessed: Jan. 15, 2025. [Online]. Available: https://auth0.com/es/intro-to-iam/what-is-openid-connect-oidc

[54] "¿Qué es el cifrado de conocimiento cero y cómo funciona?" Accessed: Jan. 15, 2025. [Online]. Available: https://ciberseguridad.com/guias/prevencion-proteccion/criptografia/cifrado-conocimiento-cero/#%C2%BFQue_es_el_cifrado_de_conocimiento_cero

[55] "¿Qué es un ataque de fuerza bruta? | Cloudflare." Accessed: Jan. 15, 2025. [Online]. Available: https://www.cloudflare.com/es-es/learning/bots/brute-force-attack/

[56] "ISO - Search." Accessed: Jan. 18, 2025. [Online]. Available: https://www.iso.org/es/search.html?PROD_isoorg_es%5Bquery%5D=IoT&PROD_isoorg_es%5Bmenu%5D%5Bfacet%5D=standard

[57] "Cybersecurity | NIST." Accessed: Jan. 18, 2025. [Online]. Available: https://www.nist.gov/cybersecurity

[58] "Decreto 338 de 2022 Nivel Nacional." Accessed: Jan. 18, 2025. [Online]. Available: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=121646&utm_source=

[59] "Decreto 472 de 2024 Alcaldía Mayor de Bogotá, D.C." Accessed: Jan. 18, 2025. [Online]. Available: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=171020&utm_source=

[60] "Violaciones de seguridad de IoT: 4 ejemplos reales - Conosco." Accessed: Jan. 18, 2025. [Online]. Available: https://conosco.com/industry-insights/blog/iot-security-breaches-4-real-world-examples