UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE COMPUTACIÓN

TEMA:
ESTADO DEL ARTE UTILIZANDO MAPEO SISTEMÁTICO DE LA SEGURIDAD DEL INTERNET DE LAS COSAS PARA INFRAESTRUCTURAS EN HOGARES INTELIGENTES

Trabajo de titulación previo a la obtención del título de:
Ingeniero en Ciencias de la Computación

AUTORES:
JONATHAN SEBASTIAN PASTAS PASTAZ
JONATHAN FERNANDO PUJOS TUALOMBO

TUTOR:
JOSÉ LUIS AGUAYO MORALES

Quito - Ecuador
2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Jonathan Sebastian Pastas Pastaz con documento de identificación N° 0401787528 y Jonathan Fernando Pujos Tualombo con documento de identificación N° 1725520389; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 11 de Marzo del 2022

Atentamente,

Jonathan Sebastian Pastas Pastaz
0401787528

Jonathan Fernando Pujos Tualombo
1725520389

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, Jonathan Sebastian Pastas Pastaz con documento de identificación No. 0401787528 y Jonathan Fernando Pujos Tualombo con documento de identificación No. 1725520389, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Articulo Académico: " Estado del arte utilizando mapeo sistemático de la seguridad del internet de las cosas para infraestructuras en hogares inteligentes ", el cual ha sido desarrollado para optar por el título de: Ingeniero en Ciencias de la Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 11 de Marzo del 2022

Atentamente,

Jonathan Sebastian Pastas Pastaz
0401787528

Jonathan Fernando Pujos Tualombo
1725520389

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, José Luis Aguayo Morales con documento de identificación N° 1709562597, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ESTADO DEL ARTE UTILIZANDO MAPEO SISTEMÁTICO DE LA SEGURIDAD DEL INTERNET DE LAS COSAS PARA INFRAESTRUCTURAS EN HOGARES INTELIGENTES, realizado por Jonathan Sebastian Pastas Pastaz con documento de identificación N° 0401787528 y por Jonathan Fernando Pujos Tualombo con documento de identificación N°1725520389 , obteniendo como resultado final el trabajo de titulación bajo la opción Articulo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 11 de Marzo del 2022

Atentamente,

.....

Ing. José Luis Aguayo Morales, MSc

1709562597

Estado del Arte utilizando mapeo sistematico de la seguridad del internet de las cosas para infraestructuras en hogares inteligentes

1st Jonathan Sebastian Pastas
jpastas@est.ups.edu.ec

2nd Jonathan Fernando Pujos
jpujos@est.ups.edu.ec

3rd José Luis Aguayo
jaguayo@ups.edu.ec

***Resumen*—A medida que aumenta la tecnología, los servicios de internet de las cosas (IoT) avanzan y se han convertido en un tema muy conocido en todo el mundo, son ampliamente utilizados tanto en el lugar de trabajo como en el hogar. Los dispositivos IoT utilizados dentro de un hogar inteligente van desde cámaras, sensores, lámparas inteligentes, parlantes hasta implantes de monitoreo cardíaco. Esto ha producido una gran cantidad de dispositivos que se conectan entre sí, por lo que se debe revisar la seguridad de los sistemas sobre sus vulnerabilidades y cómo protegerlas. En este proyecto se desarrolló un estado del arte utilizando mapeo sistemático, para la obtención de datos, de las revistas y congresos relevantes entre 2017 y 2021. Una vez realizada la revisión sistemática de la literatura, se elaboró un esquema de clasificación de los ataques que afectan la confidencialidad, integridad y disponibilidad (CIA). Como resultado de la investigación, los ataques más estudiados son: el ataque a la confidencialidad más habitual es el phishing con un 11,90%, el ataque a la integridad más frecuente es la inyección con un 37,29% y el ataque a la disponibilidad más habitual es la denegación de servicios con un 28,57%. Asimismo, la vulnerabilidad más destacada fue Actualización de software, que representa un 14,29% del interés de investigación. Además, se han encontrado técnicas como: Blockchain, Cloud Computing, Machine Learning, Test Banks, Attack Simulation y Fuzzing, que servirán para prevenir posibles ataques.**

***Palabras Clave*—seguridad IoT, hogar inteligente, ataques IoT, vulnerabilidades, técnicas**

***Abstract*—As technology increases, internet of things (IoT) services progresses and has become a well-known topic worldwide, they are widely used both in the workplace and in the home. IoT devices used within a smart home range from cameras, sensors, smart lamps, speakers to heart monitoring implants. This has produced a large number of devices that are connected to each other,so the security of the systems must be reviewed about their vulnerabilities and how to protect them. In this project, a state of the art was developed using systematic mapping, to got data, from the journals and the relevant conferences between 2017 to 2021.Once the systematic literature review is done, a classification scheme of attacks that affecting confidentiality, integrity and availability (CIA). As a result of the research, the most frequently studied attacks are: the most usual attack to confidentiality is phishing with 11.90%, the most frequent attack to integrity is injection with 37.29% ,and the most common attack to availability is denial of services with 28.57%.Similarly,the most prominent vulnerability was Software update which represents 14.29% of research interest. In addition, techniques such as: Blockchain, Cloud Computing, Machine Learning, Test Banks, Attack Simulation and Fuzzing, have been found which will serve to prevent possible attacks.**

***Keywords*—IoT security, smart home, IoT attacks, vulnerabilities, techniques**

I. Introducción

El internet de las cosas (del inglés IoT, Internet of Things) es una red de objetos interconectados que intercambian información a través de internet. Una red IoT está conformada de varios artefactos inteligentes como: sensores, asistentes de voz, electrodomésticos, entre otros. El IoT gracias a su tecnología ha incursionado en varios campos laborales como: industria, agricultura, hogares, medicina, entre otros [1]. Los hogares inteligentes (del inglés SH, SmartHome) es uno de los campos más importantes dentro del IoT, una SH es una residencia que está equipada con uno o varios objetos inteligentes conectados a una red de comunicación con el objetivo de ser monitoreados y controlados sin necesidad de presencia física [2]. Los dispositivos que integran una SH actualmente se han visto vulnerables a múltiples ataques que afecta a la seguridad de los habitantes del hogar, por dos razones: i) los fabricantes ignoran los aspectos de seguridad que deben tener los productos IoT, ii) los usuarios finales no tienen la debida información acerca de los posibles problemas que pueda ocasionar el mal uso del producto IoT dentro del hogar [3]. Para obtener un estado de arte actualizado sobre la seguridad IoT en Infraestructuras de hogares inteligentes se recopilaron estudios realizados durante los últimos cinco años. Seguido se aplicaron dos metodologías de investigación: Mapeo Sistemático (SM, Systematic Mapping) y revisión sistemática de la literatura (SLR, Systematic Literature Revision). El objetivo del uso del SM y SLR es encontrar una taxonomía que represente la seguridad IoT en infraestructuras de hogares inteligentes, del mismo modo encontrar las vulnerabilidades y ataques de los dispositivos IoT que son usados comúnmente en una SH.

II. Metodología

Para la realización de la investigación se emplearon dos metodologías: SM y SLR. El SM aporta a la identificación y clasificación de la seguridad IoT en infraestructuras de hogares inteligentes [4], la SLR proporciona una planificación y ejecución para obtener una mejor referencia de las principales vulnerabilidades y ataques más comunes que afectan a los dispositivos IoT en una SH durante los años 2017 al 2021. Dentro de IoT, un hogar inteligente se lo define como:

"hogares automatizados que facilitan las actividades del ser humano satisfaciendo las necesidades de cada miembro que integra el hogar, promoviendo la comodidad y facilidad de uso de cada dispositivo inteligente" [5]. Para el desarrollo del estado del arte se establecieron 3 etapas para la investigación: La Etapa 1 define los objetivos, alcance y los criterios de selección para cada uno de los estudios. La etapa 2 ejecuta la revisión y extracción de los principales contenidos encontrados en cada estudio. La etapa 3 clasifica en diferentes categorías a los estudios reportados por la revisión para lograr el SM y SLR.

A. Etapa 1

Para obtener los estudios pertinentes sobre el tema de seguridad IoT para infraestructuras de hogares inteligentes se aplicó el método de PICOC, el cual estructura las preguntas de investigación en base a sus cuatro componentes como se muestra en la tabla I.

TABLE I
MÉTODO P I C O C

Population (P): ¿Quiénes son?	Hogares Inteligentes
Intervention (I): ¿Qué es?, ¿Como es?	Seguridad en IoT
Comparison (C): ¿Con que comparar?	Estudios que analicen la seguridad IoT en ambientes domésticos
Outcomes (O): ¿Qué se busca conseguir /mejorar?	Identificar ataques y vulnerabilidades que afectan a los hogares inteligentes
Context (C) : ¿En cual organización esta y bajo que circunstancia?	Revisar las investigaciones existentes en repositorios científicos digitales

Después se establecieron los términos que generaron una cadena de búsqueda (ver tabla II). Con la ayuda de conectores booleanos tales como "AND" u "OR", se definió la cadena así: "(IoT Security OR IoT Vulnerabilities OR IoT methods OR IoT technique OR IoT devices) AND (Smart home OR Smart Building OR domotics)"

B. Criterios de selección de estudios

Para la selección de los artículos de investigación, se aplicaron los criterios para incluir y excluir, lo que ayuda a delimitar los estudios más relevantes para el desarrollo de la investigación, a continuación, se detallan los criterios:

- Criterios de exclusión: Se descartaron los artículos de investigación que no estén redactados en inglés, con seis hojas o menos, duplicados en varias revistas científicas y los que no estén netamente relacionados con las SH y el IoT.
- Criterios de Inclusión: Se definieron ciertos criterios como: la selección de términos de búsqueda en títulos y resúmenes (ver tabla II), de igual forma se buscaron investigaciones que describan las vulnerabilidades y ataques dentro de una SH. Todo este proceso se aplicó en el proceso de búsqueda de cada artículo en tres repositorios electrónicos.

TABLE II
TÉRMINOS PARA ELABORACIÓN DE LA CADENA DE BÚSQUEDA

Términos Generales	Términos Similares
IoT Security	IoT Vulnerabilities, IoT Architecture
SmartHome	Smart Building, Home Automation
Vulnerability Assessment	Test benches,attacks simulation methods,vulnerability assesment techniques

C. Etapa 2

1) Preguntas de investigación: La investigación realizada tuvo por objetivo actualizar el estado del arte de la seguridad IoT de infraestructuras en hogares inteligentes, por tal motivo se plantearon preguntas de investigación tanto para SM (QSM) y SLR (QSLR) las cuales se enlistan a continuación:

- *QSM 1: ¿Cuál es la distribución de los estudios investigativos acerca de seguridad en el Internet de las Cosas en los últimos cinco años?*
- *QSLR 1: ¿Existe una taxonomía para la Seguridad en el Internet de las Cosas en Hogares Inteligentes?*
- *QSLR 2: ¿Cuáles son las principales vulnerabilidades que ponen en riesgo a las infraestructuras IoT para Hogares Inteligentes?*
- *QSLR 3: ¿Cuáles son los principales ataques que ponen en riesgo a las infraestructuras IoT para Hogares Inteligentes?*
- *QSLR 4: ¿Cuáles son las técnicas de seguridad que se implementan en las Infraestructuras IoT para Hogares Inteligentes?*

2) Estrategias de búsqueda: La cadena de búsqueda se aplicó en cinco repositorios digitales, ver tabla III, previamente establecidos los cuales garantizan que existan un número suficiente de artículos para realizar los estudios de SM y SLR. Para la realización de las búsquedas se aplicaron dos filtros, en el primero filtro se recopilaron 1250 estudios. Los repositorios digitales seleccionados fueron IEEE, Scopus, Science Direct, ACM para estos se aplicó una búsqueda de estudios desde los años 2017 al 2021 (cinco años). Para el segundo filtro se descargaron los estudios que dentro de su resumen y titulo aportaban a nuestro tema de investigación, de igual manera se aplicaron los criterios de inclusión y exclusión para finalmente tener un total de 40 estudios.

D. Etapa 3

En esta etapa se realizó la extracción de datos de los diferentes estudios ya seleccionados previamente, seguido se

TABLE III
CADENAS DE BÚSQUEDA PARA CADA REPOSITORIO

Repositorio	Cadena de Búsqueda	Tipo Artículo	Filtro 1	Filtro 2
IEEE	Título:" IoT Security Home OR IoT Vulnerabilities OR IoT attacks" AND Resumen: "Smart Home OR domotics OR Home automation" AND Texto: "Vulnerability assessment AND Test benches"	Revistas y Conferencia	626	18
Scopus	(IoT Security Home OR IoT Vulnerabilities OR IoT attacks) AND (Smart Home OR domotics OR Home automation)	Revistas	31	4
Science Direct	IoT Security Home OR IoT Vulnerabilities OR IoT attacks AND Smart Home OR domotics OR Home automation AND Vulnerability assessment AND Test benches	Revistas	361	7
ACM	Título:" IoT Security Home, IoT Vulnerabilities, IoT attacks" AND "Smart Home, domotics, Home automation"	Revistas	232	11
		TOTAL	1250	40

sintetizó la información dando como resultado una taxonomía que describe la seguridad en infraestructuras de hogares inteligentes ver figura 1.

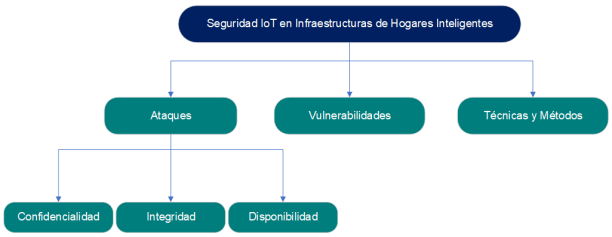

Fig. 1. Taxonomía de la seguridad IoT en Infraestructuras de Hogares Inteligentes

1) Seguridad IoT SH : En los últimos años, con el auge de los equipos IoT conectados, muchos analistas han comenzado a predecir cómo será el futuro con estos dispositivos, en [6] una cifra que mencionan sobre dispositivos conectados es de 29 mil millones para el 2020, de los cuales 18 mil millones estarán relacionados con IoT.

Si bien los números sobre los dispositivos conectados cambiarán, lo cierto es que muchos de estos dispositivos serán dispositivos de consumo que ofrecerán muchos beneficios al hogar, pero también pueden amenazar la privacidad y seguridad de los usuarios.

2) Ataques en SH: Los dispositivos IoT utilizados en el hogar como cámaras, interruptores, sensores, entre otros; son dispositivos que los ciberdelincuentes han utilizado para vulnerar la seguridad y llegar a conseguir información delicada de los usuarios.

Para salvaguardar la información del usuario, se deben considerar la Confidencialidad, Integridad y Disponibilidad (CIA), porque estos son los aspectos principales de la seguridad ya que, si alguno de estos se ve afectado, la seguridad de la información está en peligro y el sistema es mucho más vulnerable. Teniendo en cuenta CIA, se realizó una clasificación de los ataques que afectan a los dispositivos IoT en un SH.

3) Ataques que afectan a la confidencialidad: En [7], [8] se describe a la confidencialidad como la capacidad para conservar la información solo con las personas o sistemas autorizados. Este tipo de ataque está dirigido al robo de información personal de un individuo del cual obtienen datos de cuentas bancarias, usuarios y contraseñas. Una vez que se ve afectado por un ataque de este tipo, la información se puede vender o incluso intercambiar en la web oscura para que otros la compren y la usen.

Un ejemplo de cómo el ciberdelincuente puede acceder a la información personal de los usuarios es con la ayuda de los asistentes de voz, el atacante genera un sonido inaudible para el ser humano pero el asistente de voz puede captarlo como un comando.

Los ataques a la confidencialidad con respecto a los SH se presentan en la tabla IV. Se han representado a cada uno con una etiqueta para facilitar su identificación. La recurrencia de algunos ataques a la confidencialidad en los estudios es muy relevante. Para observar cómo se distribuyen (ver figura 2), donde se muestra una alta recurrencia en los ataques de Phishing (AC21), Man in the Middle (AC19), Ataque de suplantación de identidad (AC06) y Ataques de Escaneo (AC08).

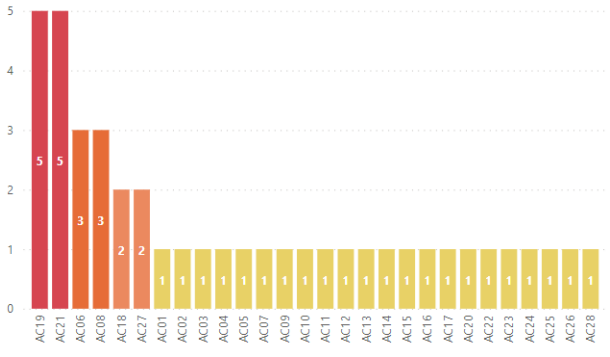

Fig. 2. Recurrencia de Ataques a la Confidencialidad

4) Ataques que afectan a la Integridad: En [7], [8] menciona que los datos deben permanecer intactos y no ser modificados o cambiados por terceros, cuando la base de datos se modifica se considera una violación, ya sea accidental o intencionalmente, se pierde la integridad y el proceso falla.

TABLE IV
ATAQUES A LA CONFIDENCIALIDAD

N	Nombre Ataque	Referencia
AC01	Acceso no autorizado de RFID	[9]
AC02	Adware	[9]
AC03	Algoritmo criptográfico y ataques de gestión de claves	[10]
AC04	Análisis de tráfico	[9]
AC05	Ataque de sonidos Skill Squatting (Asistente de Amazon)	[11]
AC06	Ataque de suplantación de identidad	[9], [12], [12], [10]
AC07	Ataques de control de acceso	[10]
AC08	Ataques de escaneo	[12], [13], [10]
AC09	Ataques de escucha clandestina	[10]
AC10	Ataques de escucha del Tráfico(pasivo)	[14]
AC11	Ataques de prueba (Robo en Casa - Orden Falsa)	[15]
AC12	Ataques de reflexión	[16]
AC13	Clickjacking	[17]
AC14	Espionaje	[14]
AC15	Fuerza bruta	[12]
AC16	Ingeniería social	[9]
AC17	Interferencia de nodos en redes de sensores inalámbricos	[9]
AC18	Interferencia de Radiofrecuencia (RF)	[9]
AC19	Man in the Middle	[14], [18], [13], [10], [19]
AC20	Mapeo por cable e inalámbrico	[10]
AC21	Phishing	[9], [20], [21], [22]
AC22	Privación del sueño	[9]
AC23	Secuestro	[14]
AC24	Sonido inaudible	[23]
AC25	Spoofing y enmascaramiento	[10]
AC26	Spyware	[9]
AC27	Suplantación y clonación	[9], [24]
AC28	Url maliciosos	[21]

Este ataque ocurre cuando un ciberdelincuente accede a información personal y la divulga con el objetivo de exponer datos del usuario tales como cuándo el usuario está en casa, o saber la información privada sobre sus hábitos o costumbres.

Los ataques que afectan a la integridad están descritos en la tabla V. En la figura3 se puede observar que se destacan los ataques de Inyección (AI04), Ataques de interferencia (AI03) y Ataques de seguridad Física (AI05).

5) Ataques que afectan a la Disponibilidad: Es un pilar esencial de la seguridad de la información, y si la información

TABLE V
ATAQUES A LA INTEGRIDAD

N	Nombre Ataque	Referencia
AI01	Ataque de manipulación de nodo	[9]
AI02	Ataques a la integridad del sistema operativo y las aplicaciones	[10]
AI03	Ataques de interferencia	[13], [10]
AI04	Ataques de Inyección	[25], [26], [12], [13], [10], [27]
AI05	Ataques de seguridad física	[9], [10], [27]
AI06	Caballo de troya	[9]
AI07	Scripts maliciosos	[9], [16]
AI08	XSS	[17]

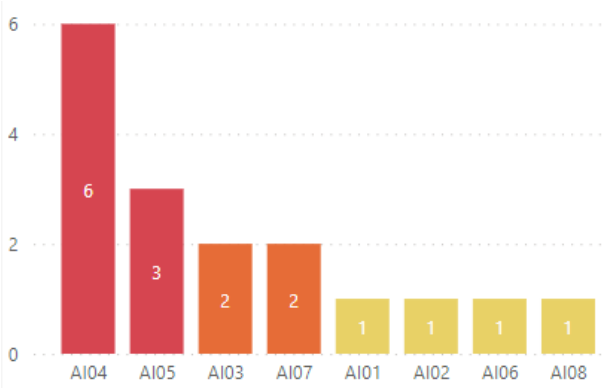

Fig. 3. Recurrencia de Ataques a la Integridad

no está disponible cuando un usuario o sistema necesite consultarla, los datos no están seguros si uno de los pilares fundamentales no funciona. [7], [8]

En el ataque a la disponiblidad se busca que el usuario no pueda acceder a sus propios datos, para esto los ciberdelincuentes no permiten el acceso a los usuarios autorizados como por ejemplo no les permiten el ingreso a sus dispositivos y crean un conflicto.

Los ataques que afectan a la disponibilidad están descritos en la Tabla VI. Para tener una mejor perspectiva de cómo se distribuyen estos, en la figura 4 se puede observar que destacan los ataques de Denegación de servicios distribuidos (AD07) y Ataque de denegación de servicios (AD09).

6) Vulnerabilidades en una SH: Una vulnerabilidad según el NIST (del ingles,National Institute of Standards and Tecnology) la define como: debilidades de seguridad en los sistemas, procedimientos y controles internos o externos, que pueden representar una amplia gama de amenazas potenciales [1]. En las SH se pueden encontrar una gran cantidad de vulnerabilidades en varios dispositivos, en la tabla VII se enlistan las vulnerabilidades que los investigadores están poniendo mayor énfasis en sus estudios.

TABLE VI
ATAQUES A LA DISPONIBILIDAD

N	Nombre Ataque	Referencia
AD01	Ataques de canal lateral	[25]
AD02	Ataques de desbordamiento	[25]
AD03	Ataques de protocolo	[10]
AD04	Ataques volumétricos	[13]
AD05	Botnet	[21], [28]
AD06	Captura de nodos	[25]
AD07	DDoS	[25], [29], [14], [12], [22], [30], [31], [10], [25]
AD08	DoLS	[12]
AD09	DoS	[25], [9], [29], [21], [31], [10], [24], [28], [32], [33]
AD10	Firmware	[12]
AD11	MIRAI atack	[31], [24], [24], [34], [10]
AD12	Ramsomware	[21]
AD13	Secuestro de dispositivos	[10]
AD14	Spam	[21]

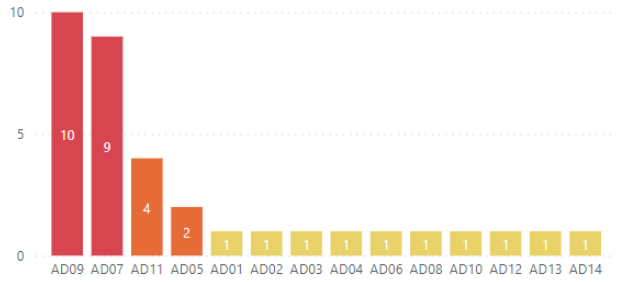

Fig. 4. Recurrencia de Ataques a la Disponibilidad

En la figura 5 se puede visualizar a cada una de las vulnerabilidades encontradas en los estudios, la vulnerabilidad V03 (Autenticación Insuficiente) es la más destacada ya que un atacante puede aprovechar varios enfoques de autenticación para poder añadir nodos maliciosos dentro de la SH y así poder interferir en las comunicaciones habituales de cada dispositivo [26]. Del mismo modo la vulnerabilidad V01 (Actualizaciones de Software) representa un gran problema actualmente, ya que la mayoría de dispositivos IoT no cuentan con los recursos necesarios para poder actualizarlo es por ello que los investigadores también han centrado sus estudios en esta vulnerabilidad.

7) Técnicas de seguridad: Son un conjunto de herramientas que los investigadores han propuesto para mejor la seguridad

TABLE VII
TABLA DE VULNERABILIDADES

ID	Vulnerabilidad	Referencia
V01	Actualizaciones de Software	[25], [26], [20], [35], [36]
V02	Seguridad Física Ineficiente	[26], [15], [37]
V03	Autenticación Ineficiente	[26], [14], [37], [15]
V04	Puertos Abiertos Innecesarios	[26]
V05	Control de Acceso Insuficiente	[15], [26], [38]
V06	Piratería de productos	[2], [39]
V07	Privacidad del Usuario	[2], [29], [14], [24]
V08	Contraseñas débiles o por defecto	[12]
V09	Falta de cifrado	[14], [37], [40]
V10	Recursos de hardware limitados	[41], [13]
V11	Puertos de enlace	[22] , [42]
V12	Vulnerabilidad en bases de datos	[13]
V13	Configuración predeterminada	[13], [37]
V14	Protocolos vulnerables	[43], [31]

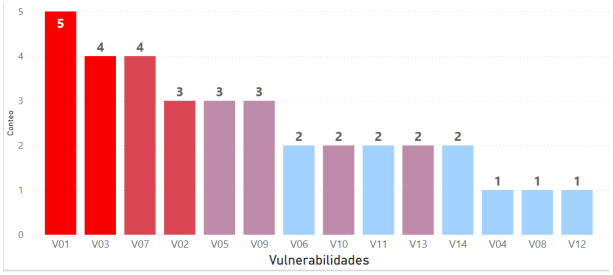

Fig. 5. Recurrencia de Vulnerabilidades

IoT dentro de una SH, ya que como se pudo evidenciar anteriormente existen una serie de vulnerabilidades y ataques que ponen en riesgo a varios frentes de seguridad en una SH. En los estudios analizados se han detectado cinco posibles técnicas, ver tabla 6, donde se proponen algunas técnicas para un correcto manejo de la seguridad en IoT.

TABLE VIII
TABLA DE TÉCNICAS DE SEGURIDAD

ID	Técnica de seguridad	Referencia
TM01	Blockchain	[25], [29], [43]
TM02	Computación en nube	[25] , [43]
TM03	Machine learning	[25]
TM04	Bancos de prueba	[26]
TM05	Simulación de ataques	[26]
TM06	Técnicas de fuzzing	[26]

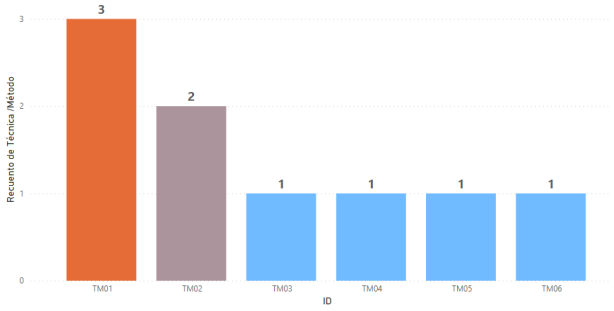

Fig. 6. Recurrencia de técnicas de seguridad

En la tabla VIII se pueden observar las técnicas obtenidas de los diferentes estudios analizados. En la figura 6 se puede observar que la técnica más recurrente en las investigaciones es Blockchain (TM01) y Computación en Nube (TM02). El blockchain y la computación en nube son usadas como una técnica de seguridad que aprovecha toda su tecnología e infraestructura con el objetivo brindar más seguridad a los dispositivos IoT domésticos.

III. RESULTADOS Y DISCUSIÓN

A. QSM 1: ¿Cuál es la distribución de los estudios investigativos acerca de seguridad en el Internet de las Cosas en los últimos cinco años?

La distribución de estudios tanto en revistas como en conferencias se distribuyen de la siguiente manera: desde el 2017 al 2021 se identificaron una mayoría de publicaciones solamente en revistas, en conferencias se encontró una minoría de publicaciones de todo el conjunto de datos usados (ver figura 7).

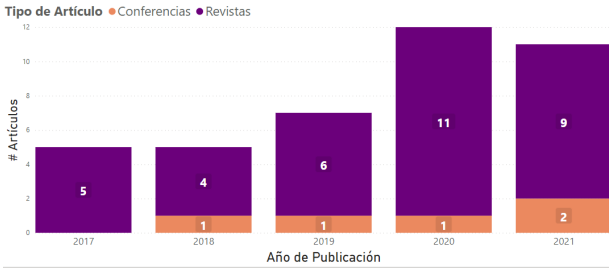

Fig. 7. Distribución de estudios

B. QSLR 1: ¿Existe una taxonomía para la Seguridad en el Internet de las Cosas en Hogares Inteligentes?

La taxonomía es la encargada de establecer una clasificación estructurada y organizada de la seguridad en internet de las cosas en hogares inteligentes. En la figura 1 se puede observar la clasificación de la seguridad IoT en SH que son: ataques, vulnerabilidades, técnicas de seguridad. Dentro de IoT existen múltiples ataques que afectan a toda la infraestructura de una SH, por lo que estos se pueden clasificar en: confidencialidad, integridad y disponibilidad. Las vulnerabilidades también son consideradas dentro de la clasificación ya que existen una gran cantidad que día tras día llaman la atención de los investigadores. Finalmente, las técnicas de seguridad son métodos usados para mejorar la seguridad de las infraestructuras de IoT con el fin de minimizar y solucionar los problemas de seguridad.

C. QSLR 2: ¿Cuáles son las principales vulnerabilidades que ponen en riesgo a las infraestructuras IoT para Hogares Inteligentes?

En la revisión de los estudios se puede evidenciar (ver figura 5 cuatro vulnerabilidades que los autores han prestado más interés en sus investigaciones, las cuales son:

- Autenticación Insuficiente (V03) : En [26] menciona que la autenticación es un gran problema que afecta a los dispositivos IoT, porque estos usaban credenciales de seguridad predeterminadas lo que hacía que los algoritmos de autenticación robustos se vuelvan insuficientes. En [20] hacen referencia a los asistentes de voz (del inglés VA, Voice Assistants) virtuales los cuales manejan una autenticación de un solo factor, refiriéndose a que estos objetos no controlan la presencia física del usuario con el dispositivo. En [23] mencionan tres cuestiones sobre la falta de autenticación de los asistentes de voz:i) Los VA no pueden autentificar de manera correcta quien es la persona que está activando el dispositivo mediante la voz, ii) Los VA están todo el tiempo escuchando lo que sucede a su alrededor con el objetivo de reconocer el comando para despertarlos y actuar, lo que conlleva a importantes problemas de privacidad. iii) Los VA son vulnerables al sonido inaudible producido por frecuencias ultrasónicas.
- Actualizaciones de Software (V01): En [25] mencionan que la mayoría de los dispositivos IoT cuentan con recursos limitados como almacenamiento, también estos objetos no cuentan con una interfaz de usuario y tampoco cuentan con una capacidad de cálculo necesaria para descargar nuevas firmas. En [26] dice que los fabricantes de dispositivos IoT home no mantienen una constante actualización de sus productos ya que no cuentan con los mecanismos suficientes para realizar una gestión de parches, lo que hace que estos objetos inteligentes puedan ser modificados con fines maliciosos.
- Seguridad Física Ineficiente (V02): En [26] explica que un dispositivo IoT funciona de forma autónoma en entornos desatendidos, como por ejemplo un hogar. El atacante puede invadir el hogar con el objetivo de tomar control del dispositivo físicamente o incluso podría cargar firmwares maliciosos para corromper su control y robar datos en tiempo real.
- Privacidad del Usuario (V08): En [14] menciona que dentro de las SH hay muchas amenazas para el usuario como: las aplicaciones de monitoreo de IoT. Estas aplicaciones registran una gran cantidad de datos de los usuarios lo que puede conllevar a que esta información sea vulnerada y expuesta.

D. QSLR 3: ¿Cuáles son los principales ataques que ponen en riesgo a las infraestructuras IoT para Hogares Inteligentes?

En el análisis de la confidencialidad existen varios ataques como se pueden observar en la tabla IV, se muestra también en la Figura 2 que los ataques más investigados por la comunidad científica son:

- Phishing (AC21): En [26] lo considera como un ataque de software y que puede atacar a diferentes capas de una arquitectura de SH. En la figura 2 se puede observar que este ataque obtiene un 11.90% del total de los ataques a la confidencialidad. En [9], [20] mencionan que se deben investigar sobre cómo evitar estos tipos de ataques e implementar protocolos más seguros.
- Man in the Middle (AC19): En [12] menciona que es un tipo de ataque en el cual el atacante se introduce en medio de las comunicaciones y hace parecer que la comunicación es normal. En la figura 2 se observa que tiene un 11.90% del total de los ataques a la confidencialidad.
- Ataque de suplantación de identidad (AC06): En [12] menciona que para que ocurra este ataque deben utilizar otras herramientas como el escaneo de puertos, un ataque de fuerza bruta para que pueda ingresar a los datos de un SH. En la figura 2 se observa que tiene un 7.14% del total de los ataques a la confidencialidad.
- Ataques de Escaneo (AC08): En [12] menciona que el atacante puede encontrar dispositivos relacionados a un SH mediante un escaneo de las direcciones Mac y también puede identificar si los usuarios utilizan contraseñas predeterminadas. En la figura 2 se observa que tiene un 7.14% del total de los ataques a la confidencialidad.

En el análisis de la Integridad existen varios ataques como se puede observar en la tabla V, se muestra también en la figura 3 que los ataques más investigados por la comunidad científica son:

- Ataques de Inyección (AI04): En [25] menciona que este tipo de ataque hace que el atacante inyecte algún tipo de código malicioso y hacer que el sistema realice funciones no deseadas. También puede inyectar datos erróneos lo que hace que el sistema produzca datos falsos y hace que el sistema no funcione correctamente. En la figura 3 se observa que tiene un 37.29% del total de los ataques a la integridad.
- Ataques de seguridad Física (AI05): En [10] menciona que este tipo de ataque se produce cuando un atacante ingresa físicamente a un dispositivo integrado y accede a datos sensibles como configuraciones y hace que el dispositivo falle cambiando o eliminando datos. En la figura 3 se observa que tiene un 17.65% del total de los ataques a la integridad.
- Ataques de interferencia (AI03): En [25], [22] mencionan que los atacantes pueden espiar a los usuarios y a su vez capturar datos personales durante la transmisión o autenticación. En la figura 3 se observa que tiene un 11.76% del total de los ataques a la integridad.

En el análisis de la Disponibilidad existen varios ataques como se puede observar en la tabla VI, se muestra también en la figura 4 que los ataques más investigados por la comunidad científica son:

- Denegación de servicios distribuidos (AD07): En [25] dice que este tipo de ataque está basado en múltiples fuentes para inundar de peticiones no deseadas al servidor, este ataque no es específico de las aplicaciones IoT,pero debido a que la capa de red no tiene mucha seguridad. En [10] dice que la sobrecarga de peticiones no es la única causa, menciona que se debe también a la multitud de usuarios, multitud de atacantes e inundación por usuarios legítimos agresivos. En la figura 4 se observa que tiene un 25.71% del total de los ataques a la Disponibilidad.
- Ataque de denegación de servicios (AD09): Este tipo de ataque se parece mucho ADO7 debido a que comparten algunas similitudes, en [10] menciona que este tipo de ataque se usa para suspender el funcionamiento de un dispositivo de forma temporal o indefinida. En la figura 4 se observa que tiene un 28.57% del total de los ataques a la Disponibilidad.

E. QSLR 4: ¿Cuáles son las técnicas de seguridad que se implementan en las Infraestructuras IoT para Hogares Inteligentes?

Las técnicas que más se han investigado por parte de la comunidad científica se pueden observar en la tabla VIII y se puede observar también en la figura 6 la frecuencia con la que son investigadas y son las siguientes:

- Blockchain (TM01), En [25] menciona que esta tecnología ayudará a mejorar el nivel de comodidad y el nivel de confianza en los usuarios. Esta técnica consiste en recibir datos de sensores y almacenarlos en una especie de libro de contabilidad en el cual cada dispositivo tendrá claves, si un dispositivo sufre algún cambio se registrará como una transacción, esto mejorará la seguridad debido a que cada cadena de datos se encriptará con tablas hash. En [43] se muestra una forma de implementar esta técnica.
- Computación en Nube (TM02): En [25] menciona que a medida que la tecnología avanza los usuarios utilizan un gran número de dispositivos y con eso genera una gran cantidad de datos, con la integración de la nube se pueden gestionar y almacenar los datos de manera eficaz.
- Machine Learning (TM03): En [25] menciona que esta es una nueva técnica en la cual se utiliza el aprendizaje automático para identificar vulnerabilidades y una vez aprendido sobre estas, el sistema pueda actuar sobre ellas y generar seguridad.
- Bancos de Prueba (TM04): En [26] menciona que esta técnica ayuda con la simulación de ataques y a encontrar vulnerabilidades. Esta técnica utiliza herramientas como Kali Linux y con esto generar una base de datos para identificar vulnerabilidades.

- Simulación de Ataques (TM05): Esta técnica consiste en generar un ataque a dispositivos en un ambiente controlado para identificar vulnerabilidades y así poder corregir dichas amenazas.
- Técnicas de Fuzzing (TM06): esta técnica consiste en encontrar errores en el código y con ello evitar que ciberdelincuentes se aprovechen de estos y con ello generar seguridad.

IV. CONCLUSIONES

El SM en esta investigación aportó en la extracción y sintetización de los estudios más relevantes de la seguridad IoT en SH, ya que facilitó en el reconocimiento de los intereses que tienen los autores acerca del tema. Durante el proceso de SM se implantaron tres etapas: i) Definir la cadena de búsqueda, criterios de inclusión y exclusión, ii) definir las preguntas de investigación, iii) Extracción y sintetización de los estudios, que ayudaron a obtener los artículos que más aportaban en nuestra investigación. Con la ayuda del SLR se pudo tener un panorama más claro sobre la seguridad IoT en infraestructuras de SH entre los años 2017 a 2021 de los diferentes repositorios digitales más destacados. En los estudios se han identificado una gran cantidad de ataques que afectan a las SH, para identificar los ataques se realizó una clasificación según su confidencialidad, integridad y disponibilidad. Para los ataques contra la confidencialidad los más frecuentes fueron AC21 y AC19, ambos comparten el 11.90% de interés investigativo. En cuanto a la disponibilidad los ataques más recurrentes son AD09 con un 28.57% y AD07 con un 25.71% de interés investigativo. Finalmente, para la integridad el ataque más recurrente es AI04 con un 37.29% de interés investigativo.

De igual manera en la investigación se encontraron un total de catorce vulnerabilidades que los autores las destacaban. La vulnerabilidad V01 es la relevante de todo el conjunto de estudios recopilado con un 14.29% de interés investigativo. A continuación,le sigue las vulnerabilidades V03 y V02 que comparten un 11.43% de interés en los estudios analizados.

Las técnicas de seguridad dentro del IoT están en un proceso prematuro de investigación ya que se han identificado una poca afluencia investigativa de dichas técnicas. Para lo cual en la investigación solo se han detectado seis técnicas que aún están en proceso de estudio e implementación, como por ejemplo entre la que más destaca es TM01 ya que gracias a su tecnología ayuda al IoT a autenticar y proteger la información que van generando los dispositivos inteligentes.
La seguridad IoT en SH es un tema de mucha importancia ya que actualmente las nuevas tecnologías se están introduciendo en múltiples campos donde años atrás eran poco indispensables, por ello esta investigación aporta evidenciando una gran cantidad de brechas de seguridad que actualmente existen y están siendo de mucho interés en la ciencia.

REFERENCES

[1] "What is the Internet of Things (IoT)? - TWI." [Online]. Available: https://www.twi-global.com/technical-knowledge/faqs/what-is-the-internet-of-things-iot

[2] H. Lee, "Home IoT resistance: Extended privacy and vulnerability perspective," *Telematics and Informatics*, vol. 49, p. 101377, Jun. 2020.

[3] B. Tushir, Y. Dalal, B. Dezfouli, and Y. Liu, "A Quantitative Study of DDoS and E-DDoS Attacks on WiFi Smart Home Devices," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6282–6292, Apr. 2021.

[4] C. N. Corona and M. S. R. Montoya, "Mapeo sistemático de la literatura sobre evaluación docente (2013-2017)," *Educação e Pesquisa*, vol. 44, no. 0, Nov. 2018.

[5] R. B. Auliar and G. Bekaroo, "Security in IoT-based Smart Homes: A Taxonomy Study of Detection Methods of Mirai Malware and Countermeasures," in *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*. Mauritius, Mauritius: IEEE, Oct. 2021, pp. 1–6.

[6] "Search results for: "PROTECCIÓN COMPLETA PARA UN HOGAR INTELIGENTE"." [Online]. Available: https://www.welivesecurity.com/la-es/search/PROTECCI%C3%93N+COMPLETA+PARA+UN+HOGAR+INTELIGENTE/

[7] "Seguridad de la Información CIA (Confidencialidad, Integridad, Disponibilidad)," Jul. 2017. [Online]. Available: https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

[8] "Ciberseguridad y ataques cibernéticos." [Online]. Available: https://www.onyxsystems.es/ciberseguridad-ataques-ciberneticos.html

[9] B. D. Davis, J. C. Mason, and M. Anwar, "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 102–10 110, Oct. 2020.

[10] V. A. Ferman and M. Ali Tawfeeq, "Machine Learning Challenges for IoT Device Fingerprints Identification," *Journal of Physics: Conference Series*, vol. 1963, no. 1, p. 012046, Jul. 2021. [Online]. Available: https://iopscience.iop.org/article/10.1088/1742-6596/1963/1/012046

[11] H. Hu, L. Yang, S. Lin, and G. Wang, "A Case Study of the Security Vetting Process of Smart-home Assistant Applications," in *2020 IEEE Security and Privacy Workshops (SPW)*. San Francisco, CA, USA: IEEE, May 2020, pp. 76–81.

[12] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1899–1909, Dec. 2017.

[13] M. Lyu, D. Sherratt, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Quantifying the reflective DDoS attack capability of household IoT devices," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. Boston Massachusetts: ACM, Jul. 2017, pp. 46–51.

[14] M. Khawla and M. Tomader, "A Survey on the Security of Smart Homes: Issues and Solutions," p. 7.

[15] X. Lei, G.-H. Tu, A. X. Liu, C.-Y. Li, and T. Xie, "The Insecurity of Home Digital Voice Assistants - Vulnerabilities, Attacks and Countermeasures," in *2018 IEEE Conference on Communications and Network Security (CNS)*. Beijing: IEEE, May 2018, pp. 1–9.

[16] U. Zia, B. Scotney, M. McCartney, J. Martinez, M. AbuTair, and A. Sajjad, "A scalable and secure model for surveillance cameras in resource constrained IoT systems," in *Proceedings of the 2020 4th International Conference on Cloud and Big Data Computing*. Virtual United Kingdom: ACM, Aug. 2020, pp. 92–96.

[17] A. Mohanty and M. Sridhar, "HybriDiagnostics: Evaluating Security Issues in Hybrid SmartHome Companion Apps," in *2021 IEEE Security and Privacy Workshops (SPW)*. San Francisco, CA, USA: IEEE, May 2021, pp. 228–234.

[18] "Scopus - Document details - Architecture internet of things based on cluster housing security system using fog computing," Jan. 2022. [Online]. Available: https://bibliotecas.ups.edu.ec:2226/record/display.uri?eid=2-s2.0-85077627201&origin=resultslist&sort=plf-f&src=s&st1=Architecture+Internet+of+Things+Based+on+Cluster+Housing+Security+System+Using+Fog+Computing&sid=c6d44ce1654614beb9561472e318508a&sot=b&sdt=b&sl=107&s=TITLE-ABS-KEY%28Architecture+Internet+of+Things+Based+on+Cluster+Housing+Security+System+Using+Fog+Computing%29&relpos=0&citeCnt=3&searchTerm=

[19] A. Giaretta, N. Dragoni, and F. Massacci, "SxC4IoT: A Security-by-contract Framework for Dynamic Evolving IoT Devices," *ACM Transactions on Sensor Networks*, vol. 18, no. 1, pp. 1–51, Feb. 2022, number: 1.

[20] X. Lei, G.-H. Tu, C.-Y. Li, T. Xie, and M. Zhang, "SecWIR: securing smart home IoT communications via wi-fi routers with embedded intelligence," in *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*. Toronto Ontario Canada: ACM, Jun. 2020, pp. 260–272.

[21] F. Schmeidl, B. Nazzal, and M. H. Alalfi, "Security Analysis for SmartThings IoT Applications," in *2019 IEEE/ACM 6th International Conference on Mobile Software Engineering and Systems (MOBILESoft)*. Montreal, QC, Canada: IEEE, May 2019, pp. 25–29.

[22] V. Simadiputra and N. Surantha, "Rasefiberry: Secure and efficient Raspberry-Pi based gateway for smarthome IoT architecture," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 2, pp. 1035–1045, Apr. 2021, number: 2.

[23] J. S. Edu, J. M. Such, and G. Suarez-Tangil, "Smart Home Personal Assistants: A Security and Privacy Review," *ACM Computing Surveys*, vol. 53, no. 6, pp. 1–36, Feb. 2021.

[24] N. Abdi, X. Zhan, K. M. Ramokapane, and J. Such, "Privacy Norms for Smart Home Personal Assistants," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Yokohama Japan: ACM, May 2021, pp. 1–14.

[25] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[26] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[27] A. Singh, A. Payal, and S. Bharti, "A walkthrough of the emerging IoT paradigm: Visualizing inside functionalities, key features, and open issues," *Journal of Network and Computer Applications*, vol. 143, pp. 111–151, Oct. 2019.

[28] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," *IEEE Access*, vol. 9, pp. 121 975–121 995, 2021.

[29] J. F. DeFranco and M. Kassab, "Smart Home Research Themes: An Analysis and Taxonomy," *Procedia Computer Science*, vol. 185, pp. 91–100, 2021.

[30] R. O. Andrade, I. Ortiz-Garces, and M. Cazares, "Cybersecurity Attacks on Smart Home During Covid-19 Pandemic," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. London, United Kingdom: IEEE, Jul. 2020, pp. 398–404.

[31] E. Jhordany Serna Valdivia and J. Mejia Miranda, "Proposal of a Intelligent Agent for Management and Mitigation in Cibersecurity Risk for IoT Environments," in *2020 9th International Conference On Software Process Improvement (CIMPS)*. Mazatlan, Sinaloa, Mexico: IEEE, Oct. 2020, pp. 148–154.

[32] ——, "Propuesta de un Agente Inteligente para el Manejo y Mitigación de Riesgos de Ciberseguridad en Entornos IoT," in *2020 9th International Conference On Software Process Improvement (CIMPS)*. Mazatlan, Sinaloa, Mexico: IEEE, Oct. 2020, pp. 158–158.

[33] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: Evolution and technologies from a security perspective," *Sustainable Cities and Society*, vol. 54, p. 101728, Mar. 2020.

[34] J. Roux, E. Alata, G. Auriol, V. Nicomette, and M. Kaaniche, "Toward an Intrusion Detection Approach for IoT Based on Radio Communications Profiling," in *2017 13th European Dependable Computing Conference (EDCC)*. Geneva: IEEE, Sep. 2017, pp. 147–150.

[35] R. Yu, X. Zhang, and M. Zhang, "Smart Home Security Analysis System Based on The Internet of Things," in *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*. Nanchang, China: IEEE, Mar. 2021, pp. 596–599.

[36] A. K. Simpson, F. Roesner, and T. Kohno, "Securing vulnerable home IoT devices with an in-hub security manager," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. Kona, HI: IEEE, Mar. 2017, pp. 551–556.

[37] S. ur Rehman and V. Gruhn, "An approach to secure smart homes in cyber-physical systems/Internet-of-Things," in *2018 Fifth International Conference on Software Defined Systems (SDS)*, Apr. 2018, pp. 126–129.

[38] G. Salzillo and M. Rak, "A (in)Secure-by-Design IoT Protocol: the ESP Touch Protocol and a Case Study Analysis from the Real Market," in *Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy*. Virtual Event USA: ACM, Nov. 2020, pp. 37–48.

[39] B. Ali and A. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," *Sensors*, vol. 18, no. 3, p. 817, Mar. 2018.

[40] L. Yang, H. Deng, and X. Dang, "Preference Preserved Privacy Protection Scheme for Smart Home Network System Based on Information Hiding," *IEEE Access*, vol. 8, pp. 40 767–40 776, 2020.

[41] S. Gendita Bunawan, D. I. Setiani, and M. Aldenny, "Architecture Internet of Things Based on Cluster Housing Security System Using Fog Computing," Apr. 2020.

[42] G. Postolache, P. S. Girao, O. A. Postolache, J. M. Dias Pereira, and V. Viegas, "IoT based model of healthcare for physiotherapy," in *2019 13th International Conference on Sensing Technology (ICST)*. Sydney, Australia: IEEE, Dec. 2019, pp. 1–6.

[43] J. Ali, T. Ali, Y. Alsaawy, A. S. Khalid, and S. Musa, "Blockchain-based Smart-IoT Trust Zone Measurement Architecture," in *Proceedings of the International Conference on Omni-Layer Intelligent Systems*. Crete Greece: ACM, May 2019, pp. 152–157.