UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA DE INGENIERÍA DE SISTEMAS

ESTADO DEL ARTE DE LOS ESTUDIOS SOBRE LA SEGURIDAD QUE POSEEN LOS ASISTENTES DE VOZ DOMÓTICOS COMO SON ALEXA O GOOGLE HOME

Trabajo de titulación previo a la obtención del
Título de Ingenieros de Sistemas

AUTORES: JUAN CARLOS DE LA TORRE GARCÍA
WALTER DANILO NINACURI ROJANO

TUTOR: JOSÉ LUIS AGUAYO MORALES

Quito - Ecuador
2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Juan Carlos de la Torre García con documento de identificación N° 1400420863 y Walter Danilo Ninacuri Rojano con documento de identificación N°1726899485; 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, 01 de Agosto de 2022

Atentamente,

Juan Carlos de la Torre García
1400420863

Walter Danilo Ninacuri Rojano
1726899485

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

Nosotros, Juan Carlos de la Torre García con documento de identificación N° 1400420863 y Walter Danilo Ninacuri Rojano con documento de identificación N° 172689948, 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 Artículo Académico: "Estado del Arte de los Estudios sobre la Seguridad que poseen los Asistentes de Voz Domóticos como son Alexa o Google Home", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, 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, 01 de Agosto de 2022

Atentamente,

Juan Carlos de la Torre García
1400420863

Walter Danilo Ninacuri Rojano
1726899485

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 DE LOS ESTUDIOS SOBRE LA SEGURIDAD QUE POSEEN LOS ASISTENTES DE VOZ DOMÓTICOS COMO SON ALEXA O GOOGLE HOME, realizado por Juan Carlos de la Torre García con documento de identificación N° 1400420863 y Walter Danilo Ninacuri Rojano con documento de identificación N° 172689948, 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, 01 de Agosto de 2022

Atentamente,

Ing. José Luis Aguayo Morales, MSc.
1709562597

ESTADO DEL ARTE DE LOS ESTUDIOS SOBRE LA SEGURIDAD QUE POSEEN LOS ASISTENTES DE VOZ DOMÓTICOS COMO SON ALEXA O GOOGLE HOME

1st Juan Carlos de la Torre García
Egresado de Ingeniería de Sistemas
Universidad Politécnica Salesiana
Quito, Ecuador
jde@est.ups.edu.ec

2th Walter Danilo Ninacuri Rojano
Egresado de Ingeniería de Sistemas
Universidad Politécnica Salesiana
Quito, Ecuador
wninacuri@est.ups.edu.ec

3th José Luis Aguayo Morales
Docente de Ingeniería de Sistemas
Universidad Politécnica Salesiana
Quito, Ecuador
jaguayo@ups.edu.ec

***Resumen*—En la actualidad el manejo de los asistentes de voz domóticos Alexa o google home han tenido un incremento por su versatilidad para realizar tareas, además de interactuar con los usuarios y otros dispositivos del hogar, esto puede generar problemas que afecten a la seguridad. Este documento desarrolla un estado del arte sobre seguridad de los asistentes de voz, mediante las metodologías de mapeo sistemático y revisión sistemática de la literatura, para la recopilación de estudios relevantes en varios repositorios digitales entre los años 2017 al 2021, que se encuentren focalizados en ataques, vulnerabilidades y contramedidas que presentan estos dispositivos. Dentro de la clasificación de ataques, los aspectos como: confidencialidad, integridad y disponibilidad son los más afectados. Los ataques como: voice squatting, voice masquerading, eavesdropping, tampering entre otros. Se presentan como las agresiones con más concurrencia en la revisión de estudios realizados. Por el lado de las vulnerabilidades se encontró que las perspectivas a tomar en cuenta son: hardware, usuarios, autentificaciones, actualizaciones de software y market application; como los posibles caminos para quebrar las seguridades de los asistentes de voz domóticos. De la misma forma se halló métodos como: machine learning con un (15%), simulación de ataques con un (12%), soporte de hardware con un (19%), Autentificación/software con un (23%), control de acceso con un (8%), cifrado y protocolos con un (23%), que ayudarán a tratar con posibles ataques.**

***Palabras Claves*—Seguridad VA, ataques VA, riesgo de seguridad, vulnerabilidades, contramedidas.**

***Abstract*—currently, the management of home automation voice assistants Alexa or Google Home have had an increase due to their versatility to perform tasks, in addition to interacting with users and other devices in the home, this can generate problems that affect security. This document develops a state of the art on the security of voice assistants, through the methodologies of systematic mapping and systematic review of the literature, for the compilation of relevant studies in various digital repositories between the years 2017 and 2021, which are focused on attacks, vulnerabilities and countermeasures presented by these devices. Within the classification of attacks, aspects such as: confidentiality, integrity and availability are the most affected. Attacks such as: voice squatting, voice masquerading, eavesdropping, tampering among others. It is presented as the aggression with the most concurrence in the review of studies carried out. On the vulnerability side, it was found that the perspectives to be taken into account are: hardware, users, authentications, software updates and market application; as the possible ways to break the security of home automation voice assistants. In the same way, methods were found such as: machine learning with (15%), attack simulation with (12%), hardware support with (19%), authentication/software with (23%), access control with (8%), recorded and protocols with (23%), which help to deal with possible attacks.**

***Palabras Claves*—VA Security, VA attacks, security risk, vulnerabilities, countermeasures.**

I. Introducción

Los asistentes de voz (del inglés VA,*Voice Assistant*) domóticos son dispositivos con la capacidad de comprender comandos de voz y ejecutar acciones, por lo cual su hardware y software se especializa en grabar, procesar y analizar el sonido. Son denominados altavoces inteligentes, por ejemplo: Amazon alexa o Google home, actualmente son muy comunes y han generado un cambio en la relación de las personas con los entornos digitalizados, como hogares inteligentes (del inglés SH,*Smart home*) o automóviles inteligentes. Los VA se implementan como dispositivos independientes o se integran en los teléfonos, tabletas, PC y algunos electrodomésticos [1], además los VA poseen inteligencia artificial, esto favorece el dialogo del dispositivo con el usuario generando una experiencia que se vuelve más familiar con el continuo uso [2]. Dada la utilidad de los VA, su consistente desarrollo está aumentando rápidamente. Por lo tanto, es muy probable que las personas estén siempre en un rango de alcance de al menos un VA y no se den cuenta de su presencia, además de no poder desactivarlos o influir con las acciones que realizan estos equipos. Los dispositivos VA domóticos son capaces de monitorear y comprender el habla, generando que los usuarios presenten preocupaciones con respecto a su privacidad y seguridad. En el 2019, las empresas Amazon y Google admitieron escuchar con regularidad las grabaciones de voz obtenidas por los equipos

de VA con la justificación de mejorar el servicio para los usuarios, lo que provocó un malestar generalizado con estos dispositivos. Amazon rápidamente incorporó un comando de voz: "Alexa, elimina todo lo que dije hoy" para resolver esa incomodidad y ofrecer mayor control de la privacidad, otras empresas como Google siguieron ese ejemplo incorporando mecanismos para realizar el mismo proceso de eliminación de información. Los VA domóticos recibieron un fuerte golpe con las acciones que realizaban estas dos empresas, generando intranquilidad en la seguridad, inquietudes como posibles vulnerabilidades que pueden ser explotadas, los tipos de ataques de los cuales pueden ser víctimas tanto los equipos como los usuarios [3] y medidas para contrarrestar que podrían ejecutarse mejorando la seguridad de los VA domóticos. Para desarrollar un estado del arte vigente sobre la seguridad de los asistentes de voz domóticos se compilaron estudios que se han elaborado en un periodo de cinco años anteriores al actual. Se empleará dos metodologías para la investigación, el primero es: Mapeo Sistemático (del inglés SM, *Systematic Mapping*) y la segunda metodología es: Revisión Sistemática de la Literatura (del inglés SLR,*Systematic Literature Revision*). El propósito de aplicar estos métodos es descubrir una clasificación que establezca la seguridad que poseen los asistentes de voz domóticos Alexa o Google Home, de manera similar encontrar ataques realizados y vulnerabilidades en asistentes de voz.

II. Método de Invesigación

En la investigación que se efectuará con las metodologías antes mencionadas. Para aportar una forma de clasificación e identificación de la seguridad en asistentes de voz domóticos, el método usado será el SM, mientras SLR brindará una forma de organización de los ataques y vulnerabilidades más frecuentes que perturban a los asistentes de voz. Se estableció un periodo de años entre 2017 y 2021. Un VA domótico es un sistema informático conectado a la red y, como tal, está sujeto a amenazas como sustraerse datos específicos del usuario o se podrían usar como un nodo en una red de bots, por dar unos ejemplos, estos desafíos de seguridad deben abordarse dentro de los VA y las infraestructuras de servicios asociados. Sin embargo, estos están fuera del alcance de este documento. Este trabajo analiza específicamente los problemas que se relacionan con la seguridad [3]. El proceso se efectuará en 3 etapas: La primera etapa (Etapa 1) delimitará los objetivos y las pautas de elección de estudios. La segunda etapa (Etapa 2) es la exploración y recopilación de contenido relevante de cada investigación, para la tercera etapa (Etapa 3) se plasmará el SM y SLR.

A. Etapa 1: Delimitaciones y pautas de selección

Se conseguirán los estudios respectivos que aborden la seguridad de los VA domóticos, para lo cual se recurrió al sistema PICO, preparando las interrogantes a investigar correspondientes a sus cuatro módulos (ver Tabla I).

Tabla I Desarrollo sistema PICO

PICO - Preguntas	Respuestas
Población(P): ¿Quién?	Asistentes de voz domóticos Alexa o Google Home.
Intervención(I): ¿Qué?,¿Cómo?	Seguridad VA.
Comparación(C): ¿Con qué se diferenciará?	Estudios relacionados a la seguridad VA domóticos de los repositorios digitales.
Resultado(O): ¿Qué se desea lograr?	Identificar ataques, vulnerabilidades y contramedidas.

A continuación se delimitaron las expresiones para la creación de cadenas de búsqueda (ver Tabla II). Los operadores booleanos **"OR"** y **"AND"** serán agregados, se definió la secuencia de exploración de la siguiente forma: (**Security risks OR security gap OR attacks OR threats OR vulnerability) AND (Personal voice assistant OR home digital voice assistants OR amazon echo OR alexa OR google home**).

Tabla II Términos de búsqueda

Términos	Términos Semejantes
Security - Vulnerability	Security risks, security gap, attacks, threats, vulnerability
Voice assistant	Personal voice assistant, home digital voice assistants, amazon echo, Alexa, google home

1) Criterios de selección de estudios: : Los artículos e investigaciones a ser escogidos para su revisión, se establecieron en base a criterios para incluir y excluir, esto delimitará que estudios son valiosos para realizar este documento.

- Criterios de inclusión: Los criterios para el desarrollo de búsqueda se ejecutó en cuatro bibliotecas digitales, manejando las expresiones que se pueden apreciar en la Tabla II, además se empleó en los títulos y los resúmenes de las investigaciones relacionadas con ataques, vulnerabilidad y la seguridad de VA domóticos.

- Criterios de exclusión: Para descartar los artículos se estableció de preferencia un mínimo de número de hojas que no sea menor a cuatro, que esté duplicado en la búsqueda de los repositorios, también los que no se encuentren relacionados con los VA domóticos alexa o google, y para finalizar se dará preferencia a investigaciones que estén redactadas en el inglés.

B. Etapa 2: Recopilación de contenido.

1) Preguntas de investigación: Este documento tiene como objetivo principal la actualización del estado del arte de los estudios sobre la seguridad que poseen los asistentes de voz domóticos alexa o google home, por tal motivo se plantearon interrogantes para la investigación con el mapeo sistemático

Tabla III Cadenas de búsquedas

Bibliotecas Digitales	Búsqueda	Tipo de Articulo	F1	F2
IEEE	Título: "Personal voice assistant OR home digital voice assistants" AND Resumen: "amazon echo OR Alexa OR google home" AND texto: "Security risks OR security gap OR attacks OR threats OR vulnerability"	Revistas y Conferencias	324	8
ProQuest	"Personal voice assistant" OR "home digital voice assistants" AND "amazon echo" OR "Alexa" OR "google home" AND "Security risks" OR "security gap" AND "attacks" OR "threats" OR "vulnerability"	Revistas y Conferencias	373	10
Scopus	("Personal voice assistant" OR "home digital voice assistants" OR "amazon echo" OR "Alexa" OR "google home") AND ("Security risks" OR "security gap" OR "attacks" OR "threats" OR "vulnerability")	Revistas y Conferencias	152	8
Science Direct	Personal voice assistant OR home digital voice assistants AND amazon echo OR alexa OR google home AND Security risks OR security gap AND attacks OR threats OR vulnerability	Revistas y Conferencias	326	4
		Total	**1175**	**30**

y revisión de la literatura sistemática que se detallará de la siguiente forma:

- SMP1: ¿Cuáles son los tipos de investigaciones sobre seguridad de asistentes de voz domóticos en los últimos cinco años?
- SLRP1: ¿Se cuenta con una clasificación sobre seguridad de asistentes de voz domóticos?
- SLRP2: ¿Qué vulnerabilidades se muestran como un riesgo para la seguridad de los asistentes de voz domóticos?
- SLRP3: ¿Cuáles son los ataques que se exhiben con mayor regularidad en los asistentes de voz domóticos?
- SLRP4: ¿Cuáles son las contramedidas o formas de mitigación que se implementan para los asistentes de voz domóticos?

2) Planificación de Búsqueda: Las cadenas para la búsqueda, se emplearon como se puede visualizar en la Tabla III, en las cuatro bibliotecas digitales preliminarmente elegidas, que poseían la existencia de artículos o investigaciones suficientes para el estudio de SM y SLR. Para realizar la exploración en los repositorios IEEE, ProQuest, Scopus, Science Direct se delimitó un rango de años desde el 2017 hasta 2021 (cinco años) como primer filtro y se compilaron 1175 investigaciones. Como segundo filtro se empleó las cadenas para una búsqueda en los títulos y resúmenes, además de las pautas para incluir o excluir estudios dando como resultado un total de 30 investigaciones, en el periodo de tiempo señalado (ver Figura 1).

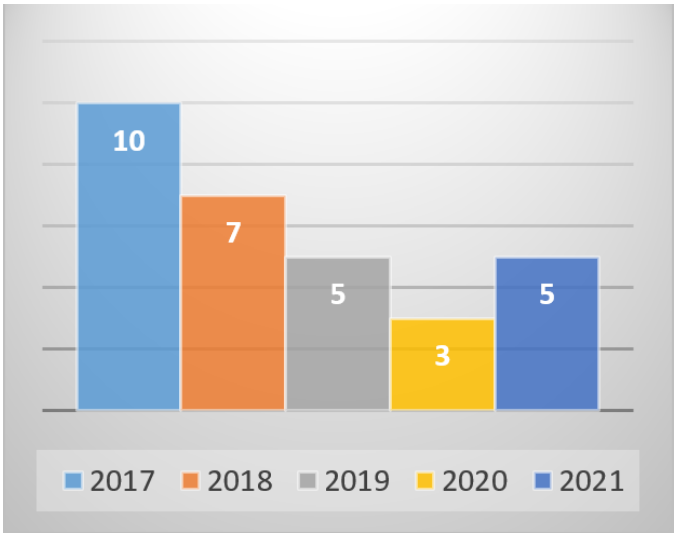

Fig. 1 Investigaciones por año

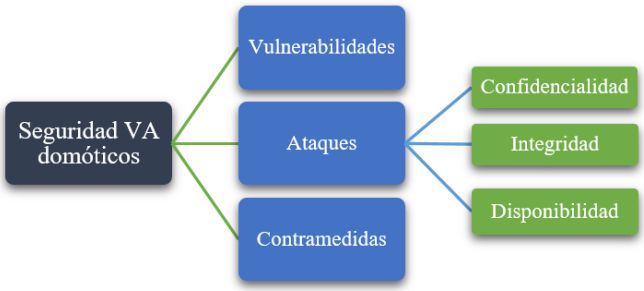

Fig. 2 Distribución de seguridad VA domóticos

C. Etapa 3: Procesamiento de información

En cuanto a la extracción de datos de los diversos artículos que fueron seleccionados con anterioridad, se logró formular una distribución para describir la seguridad de los VA domóticos (ver Figura 2), para ayudar a discernir la información necesaria que respondan a las preguntas de SM y SLR presentadas en la etapa anterior.

1) Seguridad de VA domóticos: Con la implementación de dispositivos IoT como los VA domóticos en nuestros hogares, se han manifestado ecosistemas como SH con varios equipos interactuando entre sí, por lo tanto, se considera seguro cuando se está libre de intrusos, eliminación o pérdidas accidentales de datos y sin modificaciones en la información que no estén autorizadas, logrando así tener privacidad, determinando

cuanto el usuario está dispuesto a compartir su información con otro.Estos dos elementos, la privacidad y la seguridad, deben estar centrando su diseño en el usuario para maximizar su eficacia. La confidencialidad es proteger los datos y los recursos contra los accesos no autorizados, la integridad señala que los datos y servicios están resguardados de sufrir cambios no autorizados, en cuanto a la disponibilidad es que los servicios y los datos sean utilizables cuando se requiera [4].

2) Vulnerabilidades de VA domóticos: Las vulnerabilidades se presentan como una debilidad existente, comprometen la seguridad del dispositivo. Pueden ser catalogadas en varios enfoques destacados en la recopilación de las investigaciones seleccionadas (ver Figura 3). Un factor de aspecto físico o de hardware correspondería a unidades de IoT, que poseen una frágil seguridad, por donde se puede obtener el control del equipo de forma física, implantando una brecha que vulnere el ecosistema de los VA, una de las opciones es implantar software malicioso que robe la información en tiempo real [5]. El usuario también es presentado como una vulnerabilidad en la mayoría de los casos, porque solo busca satisfacción, comodidad y bienestar, olvidando que las empresas recopilan la información personal como nombres, direcciones IP, ubicaciones, tarjetas de pago, etc. [6], que nos pueden solucionar rápidamente varias tareas de forma sencilla, pero también es un riesgo que se está asumiendo intencionadamente, las experiencias individuales de los usuarios pueden generar diferentes formas de abordar el uso de los dispositivos VA y su protección, el articulo [7] describe en más detalle el comportamiento y visión en cuanto a seguridad y privacidad de las personas que usan estos equipos. Una vulnerabilidad adicional a las antes mencionadas es la autentificación escasa, la intervención del canal acústico es afectado y ha mostrado un incremento en su explotación para efectuar ofensivas maliciosas a los equipos VA, una agresión acústica afectará al reconocimiento entre la voz artificial y una real, y quien está dando la orden para ser ejecutada [8], dentro de esta categoría entra la falta de uso de las opciones de doble comprobación para algunas tareas, aunque esta elección en la mayoría de los casos viene desactivada ya que puede llegar a fastidiar al usuario por la interacción más continua entre el dispositivo VA y la persona cuando se utiliza este método, pero se incrementa la seguridad. Los servicios en la nube y el software de los VA pueden ser afectados, en la Tabla **??** se muestra un listado de las vulnerabilidades de VA realizada por la empresa Check Point Software Technologies Ltd. [4] de las cuales las V1 al V4 son debilidades que se encontraron en Amazon Alexa, además de describir los ataques mencionados.

La V4 en cambio es una afectación a los servicios de VA tanto para Google como la empresa antes mencionada. Los ecosistemas VA enriquecen las capacidades de los VA introduciendo funciones extras en función de aplicaciones de terceros, ofreciendo una variedad de servicios que no brindaban los VA , cada empresa tiene su forma de llamar a estas aplicaciones en el caso de Amazon se conocen como Habilidades (del inglés Skill) y google les nombró

Tabla IV Vulnerabilidades de check point software technologies ltd.

Código	Nombre	Referencia
V1	Cross domain attack	[4]
V2	CORS (Cross-origin resource sharing)	[4]
V3	CSRF (Cross-Site Request Forgery)	[4]
V4	XSS	[4]
V5	Amazon Skill / Actions on Google	[4, 9]

Acciones (del inglés Actions) [10]. En los estudios [3, 6, 11] sugieren que la falta de control dentro de estos mercados de aplicaciones, que certifican que no es malicioso y perjudicial para el usuario, se produce después que las aplicaciones pasan todas las regulaciones estipuladas para ingresar en estas tiendas de aplicaciones, los creadores mal intencionados pueden hacer actualizaciones que cambien el trasfondo de estos aplicativos para ejecutar acciones que estén fuera del control del usuario.

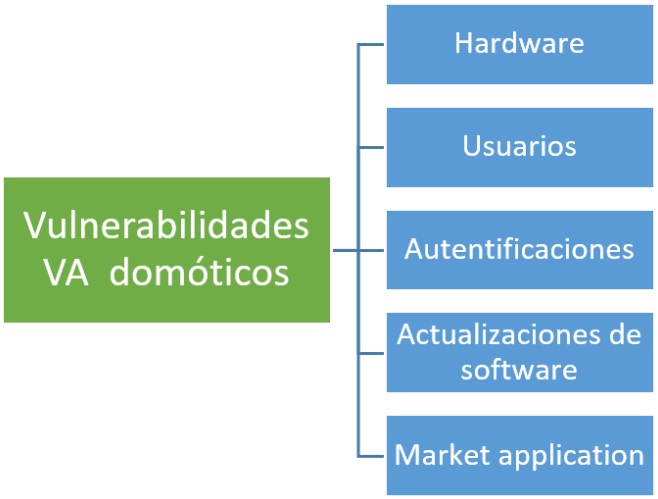

Fig. 3 Distribución de vulnerabilidades de los VA domóticos

3) Ataques a VA domóticos: Los ataques buscan una acción maliciosa para realizar daño, desestabilizando los equipos o servicios, generando perjuicios como el robo de información, a continuación se describirá algunos ataques que sufren los VA [12]. El método es romper el sistema de autenticación buscando una debilidad, esto es conseguido por la función de "siempre escuchar" o "escuchar continuamente" que tienen los dispositivos VA. El desgaste de grupo de palabras para iniciar una acción o habilidad se ha convertido en los problemas más comunes de explotar [13], además los equipos de VA carecen de una protección contra voces artificiales generando otra forma de ataque [14], la deficiencia que tienen las unidades VA para verificar e interpretar la cercanía o distanciamiento del usuario a la hora de dar una orden [15] mostrando una posibilidad de intervenir en el canal acústico, la probabilidad de uso de un dispositivo externo especializado para generar una frecuencia o voz ajustable para que los VA lo escuchen y

ejecuten la orden, pero el usuario no se percate es conocido como Dolphin Attack este tipo de ataque tiene una probabilidad baja de presentarse en un entorno real por el equipo necesario para realizarlo [16].

El Eavesdropping se contextualiza como espionaje, haciendo uso de un conjunto de procedimientos para la escucha digital, afectando las relaciones de sonidos y su espacio acústico al igual que el ataque anterior mencionado, pero el objetivo del Eavesdropping es monitorear y recopilar información del usuario que puede ser beneficioso para realizar otros tipos de ataques [17]. La conexión que tienen las unidades VA y los servicios de la nube VA para intercambiar datos se considera vulnerables para realizar un ataque, el estudio [18] registra una falencia en la protección de la trasmisión, ya que el cifrado ejecutado por defecto, está carente de brindar garantías sólidas de seguridad, que puede ser fácilmente vulnerado conociendo las rutinas que tiene el usuario en el uso de VA.

Los ataques voice squatting interfieren el canal de voz del dispositivo VA domótico, utilizando similitudes fonéticas, homónimos y pronunciación errónea en los nombres de las aplicaciones a usar, permitiendo suplantar y ejecutar una puerta trasera. Este tipo de ataque posee un alto porcentaje de éxito especialmente con dispositivos Amazon. El ataque voice masquerading se produce cuando una aplicación maliciosa prolonga su ejecución sin informar al usuario, creando una idea falsa de haber finalizado su proceso, pero sigue activa y escuchando los comandos entrantes, cuando el usuario realiza otra tarea la aplicación maliciosa es la que responde con una interacción falsa, esto puede ser peligroso y dañino tanto para los VA y el usuario. A lo largo de la recopilación de información se encontró los estudios como [3, 10] describen la forma de atacar el canal acústico, dentro del estudio [9] muestra la falta de precisión cuando tienen que reconocer los nombres de Skill para alexa y action en google presentando una oportunidad de usar aplicaciones maliciosas que sin comprometer a los dispositivos VA domóticos como Amazon Echo o Google Home por dar unos ejemplos pueden dirigir el ataque a otros dispositivos IoT como una cámara o una cerradura electrónica, etc. [11, 19], esta situación es estudiada en gran medida en dispositivos de Amazon en el artículo [20]. En la Tabla V se catalogó los ataques concurrentes mencionados a lo largo de la recopilación de información que afectan a la confidencialidad, integridad y disponibilidad.

4) Contramedidas: Las formas de mitigación se pueden apreciar en la Tabla VI, aunque son opciones con mayor relevancia que serán descritas más adelante, no se deben olvidar las buenas prácticas, son de hecho una forma de mitigación como revisión de la configuración estableciendo un periodo de tiempo medio, eliminación de los archivos grabados de voz de forma más recurrente, en lapsos de tiempo cortos, desactivación de la función “siempre escuchando” y prescindir del uso de información confidencial por ejemplo contraseñas e información como cuentas bancarias, tarjetas de pago, etc. [4], por ejemplo solo son un método de seguridad baja enfocada al usuario como aspectos a tomar en cuenta. En el estudio [1] se describe aspectos de mitigación a niveles

Tabla V Ataques a VA domóticos

Código	Nombre	Referencia
AT1	Spoofing	[3, 4, 5, 8, 14]
AT2	Tampering	[3, 4, 5, 9, 10, 14, 21]
AT3	Denial of Service(DoS)	[3, 4, 5, 8, 22]
AT4	Privilege escalation	[3, 4, 5, 14]
AT5	Vishing Attack	[4, 10]
AT6	Phishing Attack	[4, 5, 10, 14, 22]
AT7	Eavesdropping	[4, 5, 8, 13, 14, 17, 21]
AT8	Dolphin Attack	[3, 9, 11, 15, 16]
AT9	Man-in-the-middle attack	[5, 9, 11, 21, 22]
AT10	Voice squatting attack	[1, 4, 8, 10, 11, 14, 19, 21, 23]
AT11	Voice masquerading attack	[1, 4, 8, 10, 11, 14, 19, 21, 23]

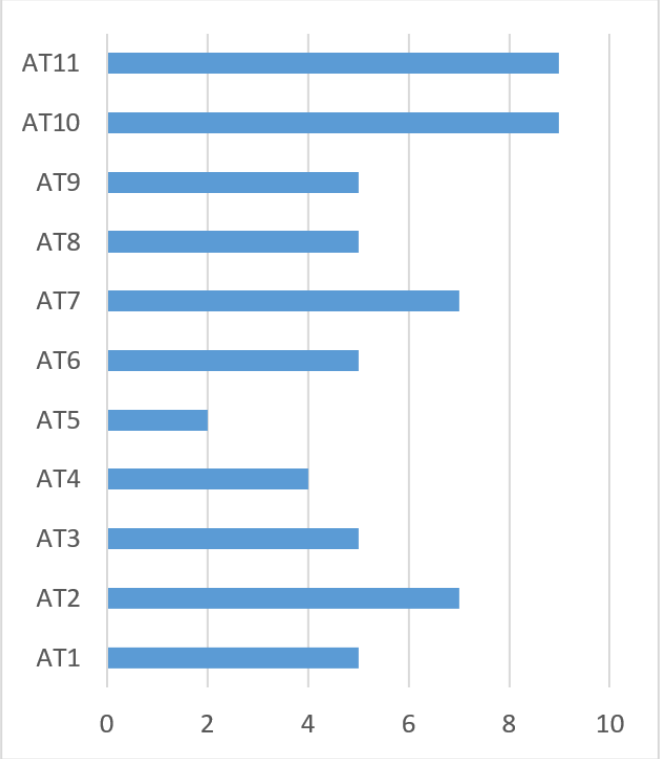

Fig. 4 Recurrencia de ataque a VA domóticos

de software, hardware y red de los ataques a las unidades de VA, generando métodos prácticos, además que la Simulación de Ataques genera resultados mejorando una perspectiva más real de la situación bajo ataque.

Las propuestas mencionadas en la compilación de información muestra como opciones para mejorar la seguridad los siguientes puntos como la autentificación - software son el punto que se mejoró con implementaciones como lo son el “Voice Match” en Google y los “Perfiles de voz” de Amazon [28] desde el 2018. Existen mecanismos como el ”sistema VAuth” [25] que realiza un proceso de autenticación continuo conjugando las ordenes que genera el usuario y la vibración que emite el dispositivo con un mecanismo del (97%) de éxitos en la concordancia de acentos de idiomas y movilidad en la

Tabla VI Métodos de contramedidas a ataques Va domóticos

Código	Nombre	Referencia
C1	Métodos Cifrado y Protocolos	[1, 3, 9, 10, 11, 24]
C2	Machine Learning	[3, 9, 11, 22]
C3	Simulación de Ataques	[3, 9, 11]
C4	Soporte de Hardware	[3, 9, 25, 26, 27]
C5	Autentificación-software	[3, 9, 10, 11, 26, 28]
C6	Control de acceso	[26, 27]

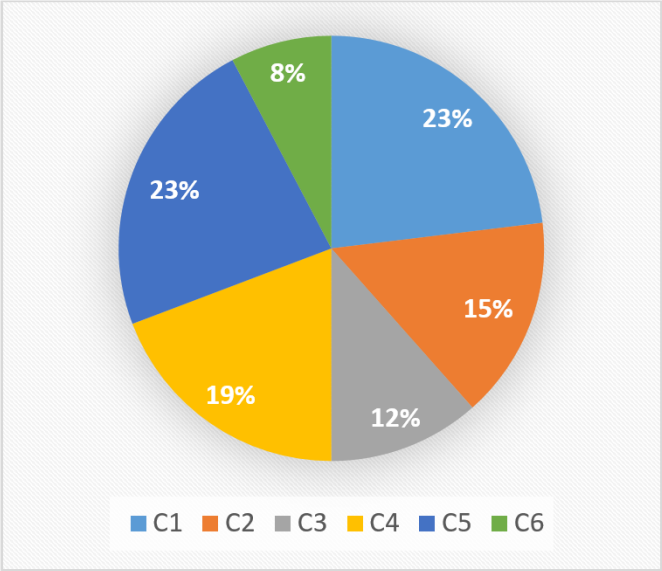

Fig. 5 Distribución de métodos de mitigación

voz, pero a costa de un soporte de hardware adicional, es decir un dispositivo solo para el sistema antes mencionado, de igual forma se puede utilizar un equipo extra para el control de acceso propuestos en los estudios [26, 27] es el "VSButton" que en colaboración con el Wifi puede detectar si el usuario se encuentra o no para que se active él VA. Los métodos cifrados buscan como objetivo proteger la información tratada en las comunicaciones entre los dispositivos VA y sus servicios en la nube, en la investigación [5] menciona a Blockchain como fuerte alternativa, el producir una clave para la seguridad de los datos, ejecutando desde un registro o libro mayor, además de llevar un registro cronológico.

Otro medio es Machine Learning, una solución prometedora por ser un tema de interés en los últimos años, su peculiaridad de generar un aprendizaje adaptativo ofrece ventajas como la tolerancia a fallas [22], sin contar el uso de redes neuronales llevando a una mejor interacción entre usuario y VA [29]. En cuanto a los protocolos, el estudio [24] describe algunos protocolos a tomar en cuenta para la seguridad como son: CoAP, 6LoWPAN, TLS, Message Queuing Telemetry Transport entre otros. En la búsqueda de contramedidas se encontró diversas posibilidades de mitigación, sea que se aplique una o combinar los métodos como en el estudio [30] aunque esto reflejaría la voluntad del usuario de llevar su nivel de protección dependiendo de la situación pueden ser positivos o negativos.

III. Resultados

A. SMP1: ¿Cuáles son los tipos de investigaciones sobre seguridad de asistentes de voz domóticos en los últimos cinco años?

Fig. 6 Distribución de estudios

En el periodo 2017 al 2021 la distribución presentada en cuanto a investigaciones son: conferencias y revistas sobre el tema de seguridad en los VA domóticos. Se muestra una clara supremacía en publicaciones realizadas en revistas dejando en una minoría a las conferencias (ver Figura 6).El resultado refleja que las revistas tienen un índice de aceptación alto, ya que presentan los resultados teóricos o prácticos obtenidos en la investigación de forma detallada. En cambio la conferencia, se muestra más conciso y directo, desde la experiencia del investigador, además de recibir una retroalimentación en el momento de los participantes que pueden influir en la investigación y su resultado.

B. SLRP1: ¿Se cuenta con una clasificación sobre seguridad de asistentes de voz domóticos?

La seguridad de los asistentes de voz domóticos cuenta una clasificación (ver Figura 2) enfocada en tres factores los cuales son: vulnerabilidades, ataques y contramedidas.Para las vulnerabilidades se encontró varios aspectos a tomar en cuenta (ver Figura 3), que son generados por los fabricantes o por los usuarios de estos dispositivos. Mostrando las falencias, donde pueden intervenir los delincuentes para afectar la seguridad. En ataques existe una distribución orientada a estropear la CIA (confidencialidad, integridad y disponibilidad) en los dispositivos VA. Las investigaciones determinaron que los ataques

más frecuentes (ver V), son utilizados como un iniciador para una cadena de agresiones, o a su vez afectar directamente al equipo VA. Por último están las contramedidas encaminadas a minimizar y solventar los problemas de la seguridad, mediante métodos diversos (ver VI).

C. SLRP2: ¿Qué vulnerabilidades se muestran como un riesgo para la seguridad de los asistentes de voz domóticos?

Las vulnerabilidades que se presentaron durante la investigación son de dos tipos: los usuarios y fabricantes. Dentro de estos dos factores se enfocan en 5 categorías (ver Figura 3) que se describen a continuación. El hardware es una vulnerabilidad relacionada al acceso del dispositivo de forma física, por personas no autorizadas, creando la posibilidad de alterar el sistema o algún componente del dispositivo VA. Otra debilidad son los usuarios, afectados por circunstancias como la psicología emocional y la perspectiva de seguridad del individuo, siendo propensos a un ataque de ingeniería social.La siguiente vulnerabilidad es la falta de autentificación en la verificación de la voz del usuario, la cual puede ser reemplazada por voz artificial. Asimismo las actualizaciones de software, pueden generar fallas por parte de los fabricantes, que no se percataron del error, brindado una brecha para los atacantes.Por último, el market application es donde se encuentran aplicaciones que aumentan el número de tareas que realizan los VA domóticos, cada aplicación pasa un primer control de seguridad cumpliendo los requisitos para su publicación, pero no aseguran un control continuo a las actualizaciones que pueden convertirse en aplicaciones maliciosas.

D. SLRP3: ¿Cuáles son los ataques que se exhiben con mayor regularidad en los asistentes de voz domóticos?

En los últimos años se contempló varias formas de atacar a los dispositivos VA. Mientras se reunía la información de los estudios que fueron elaborados en años anteriores, se presentó once tipos de ataques recurrentes (ver Figura 4), los cuales son: Spoofing, Tampering, Denial of Service (DoS), Privilege escalation, Vishing Attack, Phishing Attack, Eavesdropping, Dolphin Attack, man-in-the-middle attack, voice squatting attack, voice masquerading attack.Estas agresiones en su gran mayoría afectan al canal acústico de los dispositivos para realizar el ataque, además de comprometer las comunicaciones en la red, entre equipos y servicios.

E. SLRP4: ¿Cuáles son las contramedidas o formas de mitigación que se implementan para los asistentes de voz domóticos?

Las contramedidas con mayor referencia (ver Figura 5) son: métodos cifrados y protocolos, machine learning, simulación de ataques, soporte de hardware, autentificación – software y control de acceso. Cada método está vigente y tiene un desarrollo constante reforzando la seguridad cuando se implementan.

IV. Conclusiones

Este documento busca presentar una recopilación de la información sobre seguridad de los asistentes de voz domóticos, mediante una distribución que se refleja en tres categorías las cuales son: vulnerabilidades, ataques y contramedidas. Las vulnerabilidades se presentan como las brechas a ser explotadas, los factores como: usuarios, actualizaciones de software, market application, hardware y autentificación, siendo este último el más propenso, en especial la verificación de voz. Porque varios ataques se concentran en esta debilidad para vulnerar los equipos VA. En cuanto a los ataques que se describieron en este documento, muestran una gama de agresiones, que pueden colaborar entre sí o de manera singular para afectar la seguridad de los dispositivos VA. En especial Amazon Echo que gran parte de los estudios que se recopilaron, destacó el uso de este equipo en pruebas de ataques y mitigaciones de las mismas. Finalmente se presentó algunas contramedidas a tomar en cuenta, los métodos de cifrado y protocolos poseen un (23%) de implementación, al igual que, la autenticación – software. Siendo los porcentajes más altos de mitigación, además existe la posibilidad de conjugación entre varios métodos, que brinden seguridad a los dispositivos VA alexa o google home. En cuanto a las metodologías SM y SLR, ayudó a establecer el proceso de búsqueda, recopilación y procesamiento de las investigaciones entre los años 2017 al 2021, que aportaban para el desarrollo de este documento.

Referencias

[1] Y. Park, H. Choi, S. Cho, and K. Young-Gab, "Security analysis of smart speaker: Security attacks and mitigation," *Computers, Materials, Continua*, vol. 61, no. 3, pp. 1075–1090, 2019. [Online]. Available: https://www.proquest.com/scholarly-journals/security-analysis-smart-speaker-attacks/docview/2396003313/se-2http://www.techscience.com/uploads/attached/file/20191122/20191122085856_47721.pdf

[2] V. Këpuska and G. Bohouta, "Next-generation of virtual personal assistants (microsoft cortana, apple siri, amazon alexa and google home)," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Conference Proceedings, pp. 99–103.

[3] P. Cheng and U. Roedig, "Personal voice assistant security and privacy - a survey," *Proceedings of the IEEE*, vol. 110, no. 4, pp. 476–507, 2021. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126314192&doi=10.1109%2fJPROC.2022.3153167&partnerID=40&md5=96a44ec9f59c640fe0fe1d1b35d99c82https://ieeexplore.ieee.org/ielx7/5/9747956/09733178.pdf?tp=&arnumber=9733178&isnumber=9747956&ref=

[4] D. Anniappa and Y. Kim, "Security and privacy issues with virtual private voice assistants," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, Conference Proceedings, pp. 0702–0708. [Online]. Available: https://ieeexplore.ieee.org/document/9375964/

[5] J. S. Pastas Pastaz and J. F. Pujos Tualombo, "Estado del arte utilizando mapeo sistemático de la seguridad del internet de las cosas para infraestructuras en hogares inteligentes," Thesis, 2021.

[6] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for amazon alexa ecosystem," *Digital Investigation*, vol. 22, pp. S15–S25, 2017. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85026735513&doi=10.1016%2fj.diin.2017.06.010&partnerID=40&md5=140fddd2b7a3d48e3c347f081f533260https://www.sciencedirect.com/science/article/pii/S1742287617301974?via%3Dihub

[7] G. Chalhoub and I. Flechais, ""alexa, are you spying on me?": exploring the effect of user experience on the security and privacy of smart speaker users," 2020.

[8] A. Hamed and A. A. Khalek, "Acoustic attacks in the era of iot - a survey," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, Conference Proceedings, pp. 855–858. [Online]. Available: https://ieeexplore.ieee.org/ielx7/8693842/8701225/08701340.pdf?tp=&arnumber=8701340&isnumber=8701225&ref=

[9] T. Bolton, T. Dargahi, S. Belguith, M. S. Al-Rakhami, and S. Ali Hassan, "On the security and privacy challenges of virtual assistants," *Sensors*, vol. 21, no. 7, p. 2312, 2021. [Online]. Available: https://www.proquest.com/scholarly-journals/on-security-privacy-challenges-virtual-assistants/docview/2550403489/se-2https://mdpi-res.com/d_attachment/sensors/sensors-21-02312/article_deploy/sensors-21-02312.pdf?version=1617936862

[10] pp. 1381–1396, 2019 2019. [Online]. Available: https://www.proquest.com/conference-papers-proceedings/dangerous-skills-understanding-mitigating/docview/2292994501/se-2?accountid=32861

[11] p. 465–478, 2019. [Online]. Available: https://doi.org/10.1145/3321705.3329842

[12] H. Chung, M. Iorga, J. Voas, and S. Lee, ""alexa, can i trust you?"," *Computer*, vol. 50, no. 9, pp. 100–104, 2017. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5714311/pdf/nihms923390.pdf

[13] N. Roy, S. Shen, H. Hassanieh, and R. R. Choudhury, "Inaudible voice commands: The Long-Range attack and defense," in *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, Conference Proceedings, pp. 547–560.

[14] 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)*, Conference Proceedings, pp. 1–9. [Online]. Available: https://ieeexplore.ieee.org/document/8433167/

[15] p. 103–117, 2017. [Online]. Available: https://doi.org/10.1145/3133956.3134052

[16] S. J. Neville, "Eavesmining: A critical audit of the amazon echo and alexa conditions of use," *Surveillance Society*, vol. 18, no. 3, pp. 343–356, 2020. [Online]. Available: https://www.proquest.com/scholarly-journals/eavesmining-critical-audit-amazon-echo-alexa/docview/2454694690/se-2

[17] N. J. Apthorpe, D. Reisman, and N. J. A. Feamster, "A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic," vol. abs/1705.06805, 2017.

[18] D. Kumar, R. Paccagnella, P. Murley, E. Hennenfent, J. Mason, A. Bates, and M. Bailey, "Skill squatting attacks on amazon alexa," in *27th USENIX security symposium (USENIX Security 18)*, Conference Proceedings, pp. 33–47.

[19] 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)*, Conference Proceedings, pp. 76–81. [Online]. Available: https://ieeexplore.ieee.org/stampPDF/getPDF.jsp?tp=&arnumber=9283882&ref=

[20] E. Alepis and C. Patsakis, "Monkey says, monkey does: Security and privacy on voice assistants," *IEEE Access*, vol. 5, pp. 17 841–17 851, 2017. [Online]. Available: https://ieeexplore.ieee.org/ielx7/6287639/7859429/08023746.pdf?tp=&arnumber=8023746&isnumber=7859429&ref=

[21] 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.

[22] 2018 Jun 29 2018. [Online]. Available: https://www.proquest.com/working-papers/understanding-mitigating-security-risks-voice/docview/2073841199/se-2http://arxiv.org/abs/1805.01525

[23] S. Chen, K. Ren, S. Piao, C. Wang, Q. Wang, J. Weng, L. Su, and A. Mohaisen, "You can hear but you cannot steal: Defending against voice impersonation attacks on smartphones," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Conference Proceedings, pp. 183–195.

[24] S. M. Felix, S. Kumar, and A. Veeramuthu, "A smart personal ai assistant for visually impaired people," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, Conference Proceedings, pp. 1245–1250. [Online]. Available: https://ieeexplore.ieee.org/document/8553750/

[25] X. Lei, G.-H. Tu, A. X. Liu, C.-Y. Li, and T. J. A. Xie, "The insecurity of home digital voice assistants - amazon alexa as a case study," vol. abs/1712.03327, 2017.

[26] M. Kunz, K. Kasper, H. Reininger, M. Möbius, and J. J. B. . t. B. S. I. G. Ohms, "Continuous speaker verification in realtime," 2017.

[27] M. Jadeja and N. J. a. p. a. Varia, "Perspectives for evaluating conversational ai," 2017.

[28] H. Feng, K. Fawaz, and K. G. Shin, "Continuous authentication for voice assistants," in *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, vol. Part F131210, Conference Proceedings, pp. 343–355. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85034043956&doi=10.1145%2f3117811.3117823&partnerID=40&md5=2f6209b8b8e25f446f00dc953511453bhttps://dl.acm.org/doi/pdf/10.1145/3117811.3117823

[29] M. Algarni, M. Alkhelaiwi, and A. Karrar, "Internet of things security: A review of enabled application challenges and solutions," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 3, 2021. [Online]. Available: https://www.proquest.com/scholarly-journals/internet-things-security-review-enabled/docview/2655119263/se-2https://thesai.org/Downloads/Volume12No3/Paper_25-Internet_of_Things_Security.pdf

[30] N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian, and F. Qian, "Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems," in *2019 IEEE Symposium on Security and Privacy (SP)*, Conference Proceedings, pp. 1381–1396. [Online]. Available: https://ieeexplore.ieee.org/stampPDF/getPDF.jsp?tp=&arnumber=8835332&ref=