ELEMENTOS

VULNERABILIDAD DE LA INFORMACIÓN EN LOS DISPOSITIVOS DOMÉSTICOS INTELIGENTES DEL HOGAR

INTERNET OF THINGS AND HOME SECURITY

VULNERABILITY OF INFORMATION ON SMART HOMES DEVICES

Anderson Flórez Gutiérrez
aflorezg@poligran.edu.co

Angie Paola Gordillo
apagordillo@poligran.edu.co

Luis Alberto Roa H.
laroahuee@poligran.edu.co

Institución Universitaria Politécnico Grancolombiano (POLI)
Maestría Ingeniería de sistemas
Colombia

Recepción:15/01/2022
Aceptación:15/06/2022

ELEMENTOS

RESUMEN

El internet de las cosas (IOT) se ha implementado con gran auge en los últimos años donde se ha impulsado la domótica brindando un fácil control y confort en los hogares, construyendo y renovando las casas tradicionales en casas inteligentes. Los fabricantes en el afán de generar innovaciones en dispositivos no ha tenido en cuenta algunos factores importantes de seguridad en los mismos, generando brechas de seguridad que personas inescrupulosas pueden sacar provecho para explotar las vulnerabilidades y obtener información sensible del propietario o en el peor de los casos provocar un accidente en el hogar por la alteración del dispositivo. En este documento se brinda información clara de las vulnerabilidades y contra ataques identificados a partir de la investigación y análisis de la literatura actual orientada a dispositivos IOT de los últimos tres años.

El OBJETIVO: Identificar en la literatura actual las principales vulnerabilidades en los dispositivos IOT que se encuentren en hogares inteligentes en los últimos tres años.
MATERIALES Y MÉTODOS: Por medio de la investigación en diferentes bases de datos como scopus y CDM, se ejecutaron algunas ecuaciones de búsqueda filtrando por variables específicas como categorías, año de publicación y palabras clave con condicionales que nos permitió una selección de documentación relacionada con la vulnerabilidad actual en dispositivos IOT.
RESULTADOS Y DISCUSIÓN: A partir de la investigación realizada se identificaron algunas ataques y vulnerabilidades en dispositivos inteligentes principalmente orientadas a la autenticación débil, fuga de información de usuarios, cifrado de información sensible, autenticación e interacción por voz y falta controles de acceso por geolocalización. Se generan algunas recomendaciones posteriores que nos permiten mitigar desde el hogar los diferentes ataques mencionados e investigados como una autenticación de voz más segura, monitorio de red para prevención y mitigación, selección de dispositivos con detección de voz y análisis espectral en los usuarios autorización. De acuerdo con la investigación se identifica que en los dispositivos IOT presentan falencias en niveles de seguridad que generan oportunidades de mejora continua en los mismos pero que están sujetos a los constantes hallazgos y cambios sobre las nuevas tecnologías en IOT.

PALABRAS CLAVE

A continuación, se definen las palabras claves que nos permiten entender algunos conceptos específicos definidos en el presente documento:

E L E M E N T O S

IOT
SPA
VULNERABILIDAD
CYBERATAQUES
SCOPUS
CDM DIGITAL LIBRARY
DOMÓTICA
HOGAR INTELIGÉNTE

Recepción: *15/ 01/2022*
Aceptación: *15/ 06/202*

INTRODUCCIÓN

Los artículos científicos que implementan o describen la clasificación, procesos y datos importantes de ataques en los dispositivos domésticos, uso, mecanismos y forma de subsanar dichos ataques , de la misma forma describen que los ciberataques son rápidos en comparación de los ataques físicos por eso es necesario revisar las redes eléctricas inteligentes , redes de distribución , redes de tratamiento de agua , vehículos autónomos e infraestructura de carreteres inteligente todo donde este el involucramiento del cualquier entorno inteligente equipado con dispositivos inteligentes , es más difícil diseñar ataques genéricos observando solo pasivamente el tráfico inalámbrico de los dispositivos domésticos inteligentes.

A continuación, haremos mención de algunos de los artículos:

[...] Detección y clasificación de ataques basada en el comportamiento en sistemas ciber físicos mediante el aprendizaje automático.

[...] Asistentes personales inteligentes para el hogar: una revisión de seguridad y privacidad
[...] Evaluación de vulnerabilidades y tecnología de defensa para la ciberseguridad del hogar inteligente considerando los ciberataques de precios
[...] Mejora de la seguridad del hogar inteligente mediante la monitorización conjunta de dispositivos IOT.

Introducción

La gran mayoría de sensores que son usados en los dispositivos domésticos integrados buscan datos del entorno los cuales clasifican movimientos, datos frecuentes y algunos casos estadísticas que permiten obtener una información detallada sobre algún servicio que brinde el dispositivo. Permitiendo escoger, decidir o adaptar algún servicio debido a alguna necesidad. Es por lo que el sensor determina si hay o no movimiento siendo un ejemplo particular del caso, lo cual el atacante puede ver el estado actual del sensor y visualizar posibles falencias del sistema, bien sea fallas técnicas, actualizaciones de software o haciendo ingeniera social a las víctimas.

El conjunto de tecnologías aplicadas a la domótica entendida como el conjunto de sistemas y dispositivos que permiten el control y la automatización de actividades en un hogar inteligente, de los dispositivos electrónicos en el hogar presentando un avance notorio e incremental en los últimos años, en el presente documento investigamos y analizamos las amenazas cibernéticas que dichas tecnologías conlleva, para ello se hace necesario puntualizar 3 escenarios de forma que el objetivo principal es mitigar los ataques y contramedidas de seguridad y privacidad en los servicios existentes.

Buscamos técnicas para detectar, clasificar los posibles atacante, Para detectar antes y basado en las especificaciones. Es notable que el paradigma ha cambiado y es importante controlar los comandos de voz ya que esto es útil para el ahorro del: tiempo, espacio y dinero permitiendo la iteración rápida con la red eléctrica o la red de distribución que está conectada y está siendo monitoreada de los riesgos subyacentes.

Claramente las capacidades de los dispositivos domésticos inteligente son realmente limitadas , por lo cual es más fácil idear ataques genéricos o contramedidas, por lo que el atacante agrega información que a podido recopilar debido a el entorno en que se encuentre los usuarios , siendo factible si la detección e identificación de la actividad ,para generar ataques a la privacidad que es lo más vulnerable del usuario partiendo del tráfico que presenta los dispositivos domésticos , lo concurrido y usado que es por el usuario o familiares, es por esto que es importante la solución basada en la suplantación de tráfico a abordar .

Abarcaremos en el 2020 se incrementaron un 60% los ataques en comparación al 2019.[6]

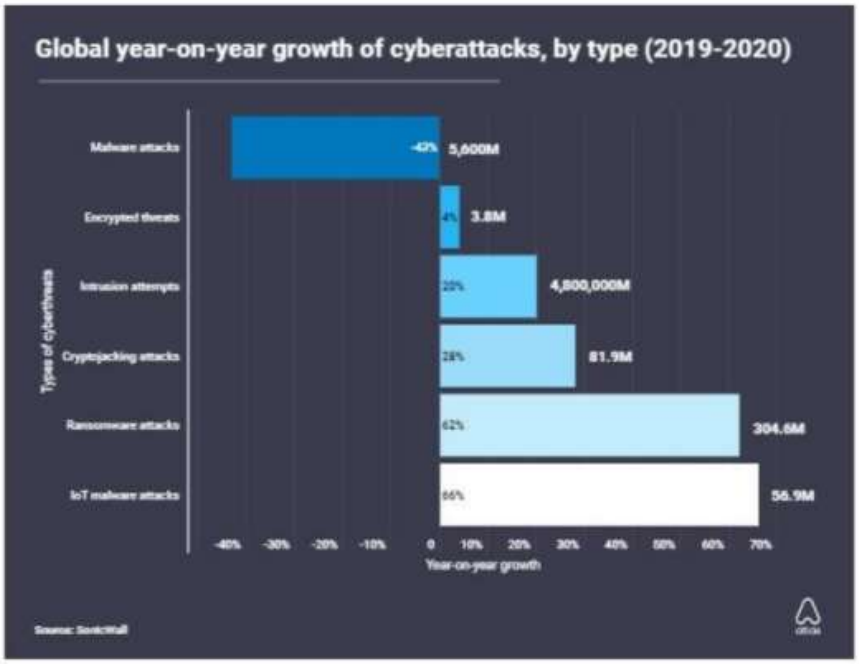

Ilustración 1: grupo de ciberataques por tipo y año.
Fuente: https://www.ventasdeseguridad.com/2021033012600/noticias/empresas/en-un-66-aumentaron-ataques-de-malware-de-iot-en-todo-el-mundo-en-2020.html

América del Norte experimentó un aumento del 152% en los ataques de programa maligno de IOT, Europa se lleva el segundo puesto en ataques de dispositivos IOT, Asia siendo el preceder en tener más ataques en IOT, finalmente Asia, África y América del Sur, a medida que crecen los dispositivos con tecnología IOT crecen las amenazas.[6]

Hoy por hoy buscamos facilitar el trabajo para realizar múltiples tareas con lo cual implementamos dispositivos inteligente en nuestro hogar haciendo uso de la red eléctrica para ello es necesario el apoyo de sistemas de comunicación para asociarse a una red inteligente , ya que utilizan este medidor mediante una estructura avanzada este sistema presenta constantes ataques a los precios debido a esto se presenta una solución ante la curva de consumo con el fin de que los atacantes no reduzcan el gasto , se ponen el alerta si todo consumo sobrepasa el umbral que permite equilibrar y detectar alguna anomalía, el impacto busca tener una interacción humana .

MÉTODO

Teniendo en cuenta la investigación realizada con respecto a las vulnerabilidades que se presentan actualmente en los dispositivos IOT relacionados con hogares inteligentes se define el método de investigación descrito a continuación:

1. **Recolección de fuentes primarias y secundarias**

   Se realiza una selección inicial de documentos que permitan abordar un panorama general de la investigación a realizar. Por medio de las bases de datos Scopus y ACM digital library, se realizan los algoritmos de búsqueda asociados a palabras clave como "iot", "Smart home", "appliance", "platform" y "advantage". Como resultado de esta consulta, se define la siguiente tabla que brinda información de la documentación encontrada:

numeración	Ecuación de Búsqueda	Resultados (No. Doc.)	Años de selección
1	TITLE-ABS-KEY (iot AND smart AND home AND appliance)	875	Existentes
2	TITLE-ABS-KEY (iot AND (iot AND home AND automation AND platform AND advantage) AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021)	413	2021, 2020, 2019
3	[All: vulnerabilities] AND [All: iot] AND [All: smart home] AND [All: appliance] AND [Publication Date: (01/01/2019 TO 12/31/2021)]	200	2021, 2020, 2019

Tabla 1 Ecuaciones de búsqueda literaria.

2. Análisis gráfico identificación palabras clave

Con el resultado de documentos obtenido previamente, se realiza un análisis con la herramienta VOSViewer para identificar una relación directa o indirecta con términos o palabras que nos brindan un mayor alcance en la búsqueda de documentación relacionada a las búsquedas realizadas en las bases de datos scopus y CDM, a continuación se presentan dos gráficos generados que nos dan un panorama en la relación de terminos:

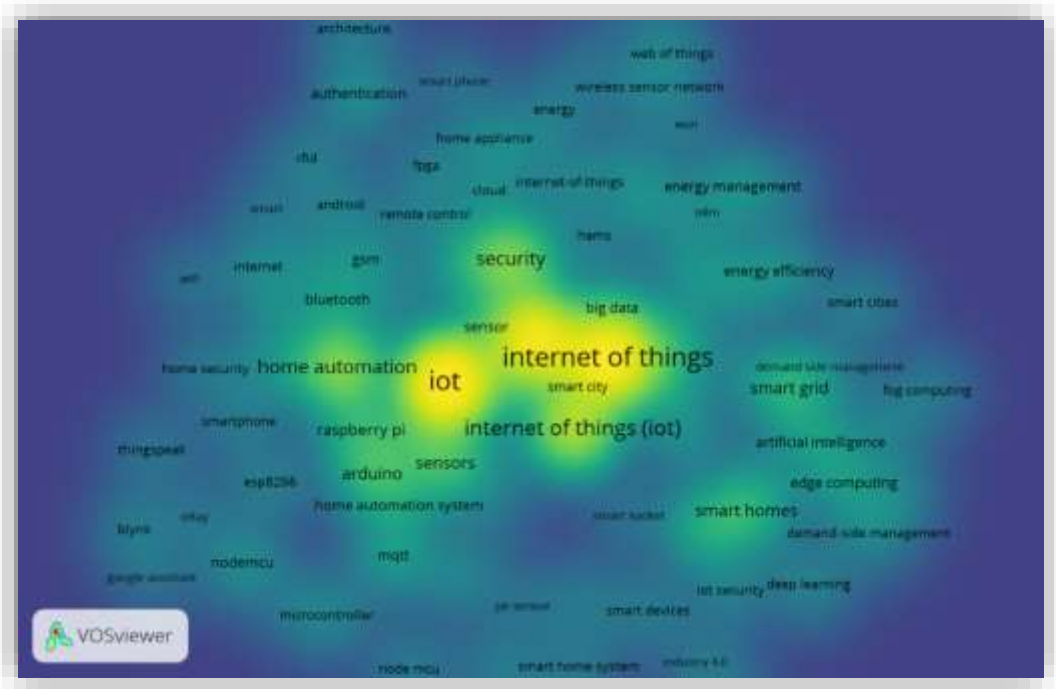

Ilustración 2: Mapa de calor búsqueda documentación.

Se puede identificar en la ilustración anterior que a partir de la búsqueda realizada por medio de las primeras dos ecuaciones mencionadas en la tabla 1 se enmarcan las palabras clave iot, security, home automation, big data y Smart homes. Este mapa nos da una base inicial para encaminar la investigación en temas específicos de seguridad en dispositivos iot en hogares inteligente.

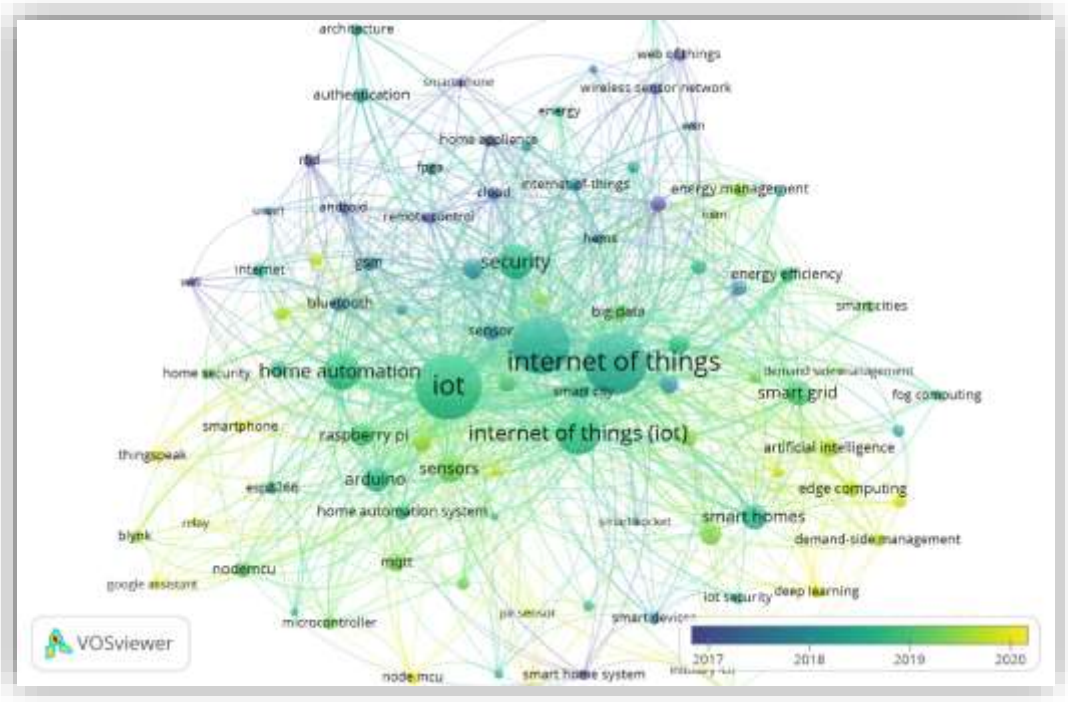

Ilustración 3: Grafico Años de publicación.

Con la anterior ilustración basada en las primeras dos ecuaciones mencionadas en la tabla 1, podemos identificar que desde el año 2018 existe un crecimiento en la investigación relacionado terminos de internet de las cosas, seguridad, hogares inteligentes, ciudades inteligentes, entre otros. Adicionalmente es posible identificar que se encuentra en crecimiento la investigación relacionada a aspectos de inteligencia artificial, y sistemas operativos.

3. FILTRO ESPECIFICO DE DOCUMENTACIÓN

Para realizar un filtrado de literatura objetiva a la investigación, se realiza la lectura de títulos y en algunos casos la introducción de la documentación generada en las primeras dos ecuaciones mencionadas en la tabla 1. A partir de lo anterior, nos surge la necesidad de acotar documentación especifica que nos brinde mayor claridad en las vulnerabilidades y riesgos actuales sobre redes domésticas y dispositivos alojados en las redes, para ello se genera una tercera ecuación que nos da un panorama especifico con doscientos resultados de literatura. Allí se aplican filtros para variables como años de publicación, títulos y en algunos casos la lectura del texto introductorio de la

literatura para finalmente seleccionar diez documentos relacionados a las vulnerabilidades de la información de dispositivos iot en hogares inteligentes, luego se establece la existencia de los problemas principales que se presentan en la seguridad de información de usuarios almacenada en la nube donde los dispositivos móviles tienen acceso y por medio de ataques de ciberseguridad se puede acceder a la misma. Por otra parte, se puede identificar los principales canales de ataque a dispositivos como autenticaciones débiles, accesibilidad de datos sin mayor seguridad, vulnerabilidades en la red, patrones de voz. A continuación, se brinda la siguiente ilustración con el análisis realizado:

Motivaciones	Problemáticas
Identificación de principales ataques en dispositivos domésticos	Diferentes ciberataques sobre dispositivos en hogares.
Evitar posibles pérdidas de datos en dispositivos del hogar.	Perdida de información personal registrada y accedida por medio de dispositivos.
Conocer Accesos no autorizados en dispositivos del hogar.	Desconocimiento de las principales vulnerabilidades en el IOT del hogar.
Identificación de procesos que ayuden a mitigar ciberataques.	Desconocimiento de los medios más vulnerables donde se genera un ataque.
reforzar la seguridad de los Dispositivos del hogar.	Gran masificación del interruptor, bombillas, altavoces, cámaras que se conectan por internet y no están regulados por los mínimos protocolos de seguridad.
Reconocer principales dispositivos vulnerables.	

Tabla 2: Motivaciones y problemáticas de vulnerabilidad en dispositivos IOT.

En la tabla anterior se realiza un análisis e identificación de los problemas que se presentan en la actualidad con respecto a las vulnerabilidades en dispositivos iot y las motivaciones actuales para atender las problemáticas. Desde este punto de vista, en la investigación se selecciona el desconocimiento de las principales vulnerabilidades como objetivo principal de esta investigación, sin embargo, existen varias problemáticas que incentivamos investigar e indagar a profundidad.

A partir de las problemáticas actuales, se han encontrado algunas soluciones principales que en la actualidad se están implementando y que con el avance de la tecnología se lograran ejecutar a corto plazo. Sin embargo, los usuarios de este tipo de

tecnologías en hogares inteligentes deben estar preparados y capacitados para una configuración o programación correcta de los dispositivos que permita reducir en gran parte las brechas de seguridad que se han identificado en la investigación por el desconocimiento o mal manejo de los dispositivos. Algunas soluciones identificadas son la generación de trafico falsificado, autenticaciones robustas de voz, verificaciones de ubicación sobre dispositivos en WI-FI y mejores arquitecturas enfocadas a redes en hogares inteligentes.

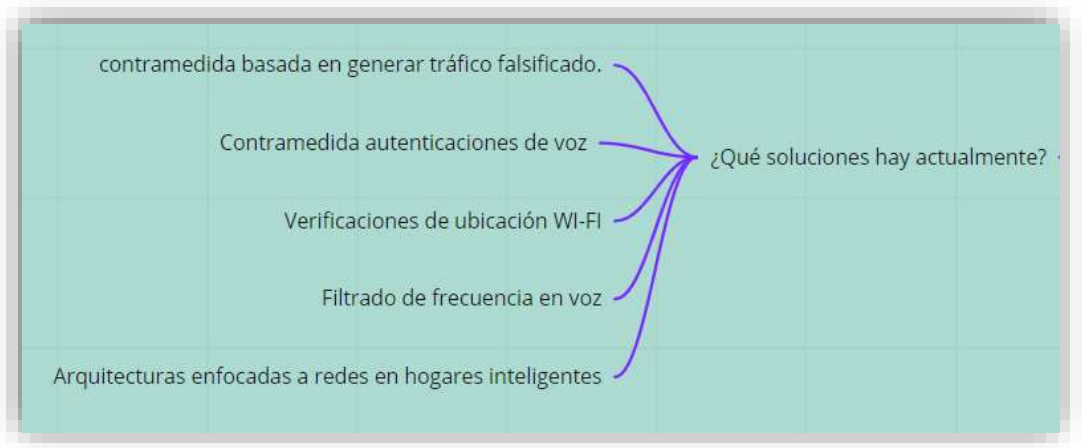

Ilustración 4: Contramedidas de vulnerabilidad en dispositivos iot.

Resultados

De acuerdo con las búsquedas planteadas y documentos analizados se identifica que el gran auge de componentes inteligentes en hogares con IOT, ha generado una gran brecha de seguridad entre el fabricante y el consumidor. Los fabricantes están implementando gran variedad de asistentes personales como son los reconocidos (SPA) con innovación emergente que está cambiando los medios por los cuales los usuarios domésticos interactúan con la tecnología y a su vez, ayudando en la mitigación de vulnerabilidades de seguridad actual.

Los asistentes personales por otro lado están presentando falencias y por ende generando riesgos a los usuarios finales, Jide S. Edu, Jose M. Such y Guillermo Suarez mencionan en el articulo “” diferentes vulnerabilidades identificadas en asistentes personales en donde las principales falencias encontradas se encuentran en la generación de contraseñas débiles, autorizaciones de pago débil y arquitecturas de desarrollo débiles en la fabricación de

dispositivos. A continuación, se brinda una ilustración definida por los autores mencionados en donde se evidencian estas vulnerabilidades:

que “la naturaleza abierta del canal de voz que utilizan, la complejidad de su arquitectura, las características de IA en las que se basan y su uso de una amplia gama de tecnologías subyacentes”. Este artículo presenta una revisión en profundidad de los problemas de seguridad y privacidad de SPA, categorizando los vectores de ataque más importantes y sus contramedidas. En base a esto, discutimos los desafíos de la investigación abierta que pueden ayudar a que la comunidad aborde los problemas actuales de seguridad y privacidad en SPA. Uno de nuestros hallazgos clave es que, aunque la superficie de ataque de SPA es notablemente amplia y existe una cantidad significativa de esfuerzos de investigación recientes en esta área, la investigación hasta ahora se ha centrado en una pequeña parte de la superficie de ataque, particularmente en temas relacionados a la interacción entre el usuario y los dispositivos SPA. A nuestro leal saber y entender, este es el primer artículo que realiza una revisión y caracterización tan exhaustiva de los problemas de seguridad y privacidad y las contramedidas de SPA.

Dentro de este articulo literario se identificó la profundidad de los problemas de seguridad y privacidad de SPA, donde los mayores contrataques que sufren son los dispositivos inteligentes procesadores de voz basados en la nube como lo son Alexa de Amazon, Asistente de Google, Siri de Apple y Cortana de Microsoft. De acuerdo con la arquitectura que decodifica la entrada de voz de los usuarios utilizando NLP para comprender la intención de los usuarios. Una vez que se identifica las ondas sonoras estas se procesan y se almacenan en la nube para luego ser procesadas por los algoritmos de IA; donde la autenticación es débil y adversaria a la información recolectada no solo por el usuario principal sino también de los multiusuarios que tienen un patrón similar de voz. Cabe resaltar que como lo menciona en el artículo Smart Home Personal Assistants la sección de tecnologías subyacentes e integradas la privacidad y confidencialidad de la información es utilizada por terceros. Un atacante podría aprovechar la aplicación laxa de la habilidad implementada. Esto se debe ha las diversas políticas de privacidad de los datos y la exploración de nuevas tecnologías entre el usuario y el sistema SPA, permite un proceso de traspaso, donde con una habilidad maliciosa pueda ceder el control a otro usuario que logra engañar al sistema haciéndole creer al software que el usuario autenticado corresponde al registrado en el sistema pero con una voz diferente conocida como tecnología Voice Masquerad-ing para escuchar las conversaciones de los usuarios y recopilar información confidencial.
Un ejemplo mas detallado se puede ver a continuación la figura con el esquema Seguridad y privacidad muestra como funciona estos elementos al interactuar con la red a través de un

Router, accesos remoto por red móvil o con protocolos de conexión http que no son seguros. Además esta información se puede ver que esta información pasa por desarrollos de terceros donde se expone la información antes de llegar al servicio proveedor de la nube pertinente.

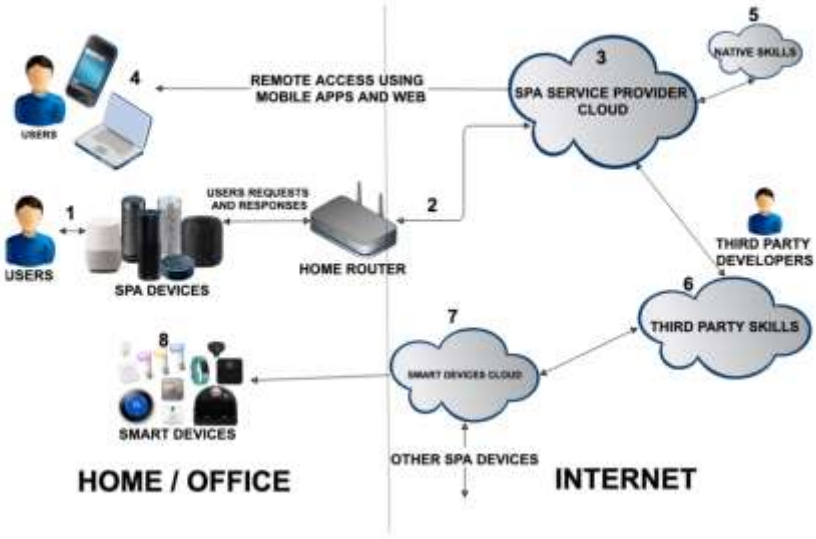

Fig. 1. SPA architecture and its key components [7,32].

También se puede evidenciar que el uso de diferentes dispositivos para conectar por internet es a través de WIFI donde cerca del 80 % de estos dispositivos usan este medio para conectarse mientras que solo un 3% usa el BLE y un 17% el ZigBee, permitiendo un menor soporte y mas costoso de actualizar para aquellos dispositivos, frente a los que tienen un mayor uso por wifi.

		Communication			Capabilities		
ID	Device	WiFi	ZigBee	BLE	Type-I	Type-II	Type-III
1	ApexisCam	●	○	○	○	○	●
2	AirRouter	●	○	○	●	○	○
3	AugustSmartlock	○	○	●	○	●	●
4	BelkinWemoLink	○	○	○	○	●	○
5	DLinkCam	●	○	○	○	○	●
6	DLinkDoorSensor	●	○	○	○	○	●
7	DLinkMotionSensor	●	○	○	○	○	●
8	DLinkSiren	●	○	○	○	○	●
9	EdimaxCam	●	○	○	○	○	●
10	EdimaxSPlug1101	●	○	○	○	●	○
11	EdinetCam1	●	○	○	○	○	●
12	EdinetGateway	●	○	○	●	○	○
13	FitbitAria	●	○	○	○	●	○
14	Lightify2	●	○	○	○	●	○
15	PhilipsHueBridge	●	○	○	●	○	○
16	SMCRouter	●	○	○	●	○	○
17	STMotionSensor	○	●	○	○	○	●
18	STOutlet	○	●	○	●	●	○
19	STMultiSensor	○	●	○	○	○	●
20	TPLinkHS110	●	○	○	○	●	○
21	WansviewCam	●	○	○	○	○	●
22	WemoInsightSwitch	●	○	○	○	●	○

Type-I: Hub-like devices, Type-II: User-controlled devices, Type-III: Sensor-like devices

Fig. 2. *Characteristics of network traces used in experi- ments.*

DISCUSIÓN Y CONCLUSIÓN

Teniendo en cuenta los análisis y la generación de resultado de la literatura en las sesiones anteriores, es posible evidenciar que existen vulnerabilidades latentes en los dispositivos iot que afectan directamente la información de los usuarios. Es posible observar en la imagen x (imagen de vulnerabilidades) las principales vulnerabilidades y como la mayoría de ataques están relacionados con autenticaciones débiles. Se puede observar de manera similar en la imagen x(imagen de contramedidas) las diferentes contramedidas orientadas a la mitigación de autenticaciones débiles.

Validando el detalle que nos brindan las imágenes anteriores podemos concluir que la literatura esta apuntando a las resoluciones de comunicación entre usuario y altavoces inteligentes definidos sobre las arquitecturas SPA. Así mismo sugerimos el tema de seguridad en arquitecturas SPA como un tema principal para seguir investigando y realizando experimento y posibles ataques controlados que nos puedan brindar resultados

Interpreta los resultados de la investigación demostrando la relevancia de la investigación e innovación en el área de conocimiento.

Durante la investigación se encontraron metodologías de investigación sistemáticas de documentación y experimentos realizados que permiten identificar las principales vulnerabilidades en dispositivos IOT en un hogar inteligente. A partir de lo anterior se identifica un análisis de amenazas actuales los usuarios finales de estos dispositivos pueden estar directamente implicados. Así mismo se encuentras diferentes soluciones que permiten suplir las necesidades actuales. Podemos concluir que por medio buenas prácticas podemos prevenir un ciberataque y por otro lado la implementación de dispositivos IOT con algunos elementos adicionales de seguridad pueden ayudar a evitar riesgos en los que un individuo puede incurrir en nuestro hogar.

Podemos ver como los hogares y las personas se encuentran conectadas

Hasta ahora es un modelo de investigación en la cual partir la recopilación de datos de una población medianamente grande en la cual ven la intervención de los adversarios de la información en presencia del uso de la domótica en el día a día es por ello que debemos contemplar los avances tecnológicos y las fallas y las personas que ingresan a nuestros hogar para contemplar diversas formas de la intervención de externos de la misma forma del uso abierto de tecnologías comandadas por la voz , nuestros adversario incluye e constante monitoreo del tráfico de red saliente de
la casa inteligente.

ver el cifrado, identificar el dispositivo e inferir actividades que se conectan a la red, así mismo la cantidad de dispositivos, la topología y estructura de la casa y los horarios donde presenta mayor tráfico.

la minimización de multiusuarios para que esto no cree falso positivos de quien controle o cambie la configuración del dispositivo inteligente de interés o del entorno partiendo del tiempo de uso y el estado del dispositivo. Es importante en los estudios probar efectos de diversos números de modelos, como ya hemos mencionados configuraciones y actualizaciones de la misma forma tener presente e implementar accesos temporales de

emergencia para la detección de un usuario no autorizado o recurrir a dar accesos a funciones específicas.

REFERENCIAS BIBLIOGRÁFICAS

Acar, A., Fereidooni, H., Abera, T., Sikder, A. K., Miettinen, M., Aksu, H., ... & Uluagac, S. (2020, July). Peek-a-boo: I see your smart home activities, even encrypted! In Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (pp. 207-218).

Agrawal, D., Bhagwat, R., Bandopadhyay, R., Kunapareddi, V., Burden, E., Halse, S., ... & Kropczynski, J. (2020, January). Enhancing smart home security using co-monitoring of iot devices. In Companion of the 2020 ACM International Conference on Supporting Group Work (pp. 99-102).

Edu, J. S., Such, J. M., & Suarez-Tangil, G. (2020). Smart home personal assistants: a security and privacy review. ACM Computing Surveys (CSUR), 53(6), 1-36.

https://www.ventasdeseguridad.com/2021033012600/noticias/empresas/en-un-66-aumentaron-ataques-de-malware-de-iot-en-todo-el-mundo-en-2020.html

Junejo, K. N., & Goh, J. (2016, May). Behaviour-based attack detection and classification in cyber physical systems using machine learning. In Proceedings of the 2nd ACM international workshop on cyber-physical system security (pp. 34-43).

Liu, Y., Hu, S., & Ho, T. Y. (2014, November). Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks. In 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD) (pp. 183-190). IEEE.