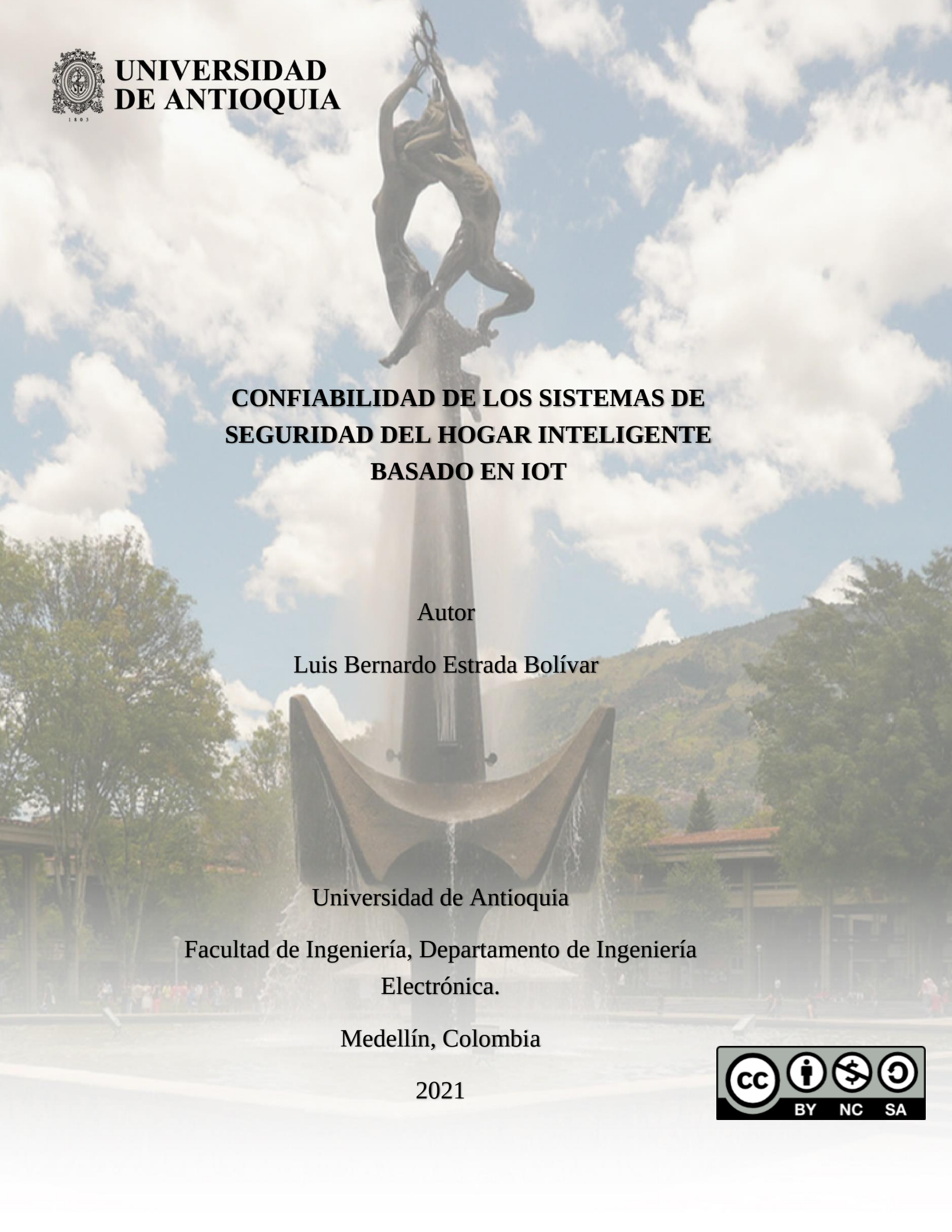

UNIVERSIDAD DE ANTIOQUIA

CONFIABILIDAD DE LOS SISTEMAS DE SEGURIDAD DEL HOGAR INTELIGENTE BASADO EN IOT

Autor

Luis Bernardo Estrada Bolívar

Universidad de Antioquia

Facultad de Ingeniería, Departamento de Ingeniería Electrónica.

Medellín, Colombia

2021

Confiabilidad de los sistemas de seguridad del hogar inteligente basado en IoT

Luis Bernardo Estrada Bolívar

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Ingeniero de Telecomunicaciones

Asesores (a):

Lina María Hincapié Vásquez

Ingeniero de Telecomunicaciones

Universidad de Antioquia

Facultad de Ingeniería, Departamento de Ingeniería Electrónica.

Medellín, Colombia

2021.

Resumen

La confiabilidad de los sistemas de seguridad del hogar inteligente basado en IoT sigue siendo un tema cuestionable en la actualidad; en el presente trabajo se realizó una búsqueda de información en diferentes fuentes bibliográficas para obtener información de relevancia sobre el tema, se analizaron los vacíos técnicos y tecnológicos que se presentan a nivel de seguridad de la información en un hogar inteligente, se elaboró un estado del arte con la información recolectada y por último se hizo una simulación en un escenario de hogar inteligente controlado al cual se le realizaron dos ciberataques en diferentes modalidades, con el fin de afectar tanto la red como la integridad de los dispositivos inteligentes; con esto se concluyó que aún estamos en la fase inicial en términos de seguridad de la información en este tipo de sistemas, ya que se logró vulnerar y bloquear uno de los dispositivos inteligentes más reconocido a nivel comercial.

Introducción

En la actualidad, se espera que los avances y desarrollos tecnológicos sean capaces de ofrecer hogares seguros, cómodos y eficientes en el uso de recursos energéticos. La seguridad de una casa pretende evitar todo tipo de contratiempos que pongan en riesgo las instalaciones, objetos o personas, algunos de estos pueden ser: cortocircuitos, conatos de incendio, inundaciones, robos, desperdicio de recursos, entre otros. La seguridad del hogar está basada en diferentes sistemas tales como los sistemas de video vigilancia, los sistemas de alarma contra intrusos, los sistemas de detección de incendios, los sistemas contra inundaciones, entre otros. En el mercado existen una gran variedad de sensores tales como cámaras de video y equipos de grabación, sensores de movimiento, sensores de rotura de vidrios, sensores de apertura, sensores de humo, sensores de monóxido de carbono y otros gases peligrosos, sensores de nivel, sensores de temperatura, etc.; por otro lado, la seguridad de la información, pretende garantizar al usuario que todos los datos que se procesan al interior de la casa puedan ser almacenados, verificados, supervisados, monitoreados y gestionados solamente por equipos autorizados, con el fin de evitar la pérdida o robo de esta información.

Este trabajo tiene como propósito documentar a profundidad el estado actual de la seguridad de la información del hogar basado en IoT, qué tipo de dispositivos, software y protocolos de comunicación son usados y cuáles pueden llegar a ser posibles estándares para garantizar una hogar inteligente y seguro. Todo esto en pro de reducir los riesgos de los ciberataques y garantizar que este ambiente inteligente sea confiable y seguro para aportar a la consolidación de ambientes inteligentes a gran escala como son las ciudades inteligentes.

En este estudio se logra evidenciar que aún quedan muchos vacíos de seguridad de la información en este tipo de sistemas para el hogar inteligente basado en IoT, adicionalmente no se encuentran entes regulatorios, estandarización de parámetros de seguridad, ni tampoco una normatividad vigente para los fabricantes del mercado, es por eso que pueden realizarse escenarios inteligentes para el hogar con múltiples protocolos de comunicaciones, software y hardware, dándole una heterogeneidad que se vuelve compleja de controlar en términos de seguridad y exponiendo al usuario a ciberataques.

Objetivos

Objetivo general

Analizar la seguridad de los datos en un hogar inteligente desde los puntos de vista comercial, académico, gubernamental y de los organismos de estandarización, con el fin de identificar tanto los avances como también las falencias en esta materia y así proponer mejoras que reduzcan el riesgo de ataques y posibles robos de información.

Objetivos Específicos

1. Documentar la información sobre seguridad de la información en los hogares inteligentes basados en IoT a nivel académico, comercial, gubernamental y de organismos de estandarización de tecnología.

2. Identificar posibles vacíos técnicos y tecnológicos que se presentan en un hogar inteligente a nivel de seguridad de la información, así como los diferentes enfoques planteados para su solución.

3. Elaborar un estado del arte sobre la seguridad de la información en los hogares inteligentes con base en la información recolectada y documentada.

4. Examinar posibles fallas de seguridad de la información ante ataques comunes a los hogares inteligentes, en un escenario controlado de laboratorio que simule un hogar inteligente, mediante hardware y software ya desarrollados y comercializados, y presentar los resultados obtenidos

Marco Teórico

El Internet de las Cosas, o IoT por sus siglas en inglés, hace referencia al concepto básico de conectar "cosas" a Internet, para poder controlarlas desde cualquier lugar, lo cual permite múltiples aplicaciones tales como el control de la temperatura de la casa, la seguridad y la protección, incluso el entretenimiento.

Estas "cosas" son todo tipo de dispositivos electrónicos que pueden o no ser operados por humanos. Es cada vez más común que estos dispositivos electrónicos inteligentes sean fabricados y comercializados para el hogar; muchos electrodomésticos utilizan sensores para la medición, monitoreo y control de los recursos de una casa, brindando seguridad, protección y comodidad; es por esto que los fabricantes de electrónica de consumo para el hogar, son los actores principales en un hogar inteligente basado en IoT, ya que incorporan a sus productos de características inteligentes, conexión a Internet, control remoto e incluso automatización.

La interconexión de todos estos dispositivos se lleva a cabo en la red local del hogar conectada a Internet, garantizando el acceso para el usuario desde cualquier parte

del mundo. Por tanto, debe también garantizarse una red local segura utilizando un cortafuego y una comunicación encriptada entre los dispositivos que hacen parte del hogar. [1]

En términos globales, un hogar inteligente se compone de un controlador principal, unos sensores y unas aplicaciones que permiten al usuario interactuar con todos los dispositivos inteligentes, desde esta perspectiva existen múltiples soluciones como la planteada por Somani [2] que utiliza una Raspberry Pi, sensores de movimiento y de gas MQ-2, y una aplicación móvil desarrollada para Android; o la planteada por Sarmah [3] que utiliza un módulo ESP8266-12E, protocolos como ZigBee, sensores de movimiento, un algoritmo y un servidor en la nube. Como puede verse, no hay un lineamiento absoluto ni una estructura definitiva para un hogar inteligente debido a las múltiples variables que entran en juego.

Se observa entonces que el número de nodos al interior del hogar se incrementa, junto con la diversidad y la heterogeneidad de los protocolos y redes en el borde del Internet. Es necesario usar diferentes protocolos para poder cumplir con los requisitos de un hogar inteligente, tales protocolos varían desde el IEEE 802.11 wireless LAN (WLAN) y 802.3 Ethernet para tasas de bit altas y aplicaciones interactivas hasta 802.15.4/ZigBee, Bluetooth y Z-wave para tasas de bit bajas y requerimientos de bajo consumo de energía. Además, se usan otros protocolos de tasas de bit muy bajas y protocolos de largo alcance como LoRaWAN, Sigfox y NBIoT, añadiendo heterogeneidad extra y con esto mayor complejidad a las redes de borde. [4]

Con el fenómeno del incremento de los datos privados del usuario, las fugas y la vulnerabilidad de la seguridad no deben pasarse por alto en el entorno de IoT. Se han desarrollado una serie de investigaciones importantes que tiene que ver con la seguridad y la privacidad en entornos de IoT de forma tal que estos entornos puedan ser confiables [5]. Es necesario tener una mejor comprensión de los desafíos que plantea un hogar inteligente en términos de gestión, seguridad y privacidad. Según estudios recientes tomados en una muestra aleatoria de hogares inteligentes en Estados Unidos, el tráfico de un Hogar Inteligente basado en IoT, presenta unos volúmenes y patrones temporales, y evidencia ciertas preocupaciones de seguridad

y privacidad, también develan que a pesar de la heterogeneidad, y la aparente fragmentación del hogar inteligente, que en su mayoría está centralizado debido a la dependencia de algunos servicios populares de la nube y los servicios de DNS, junto con aspectos a evaluar como la necesidad de mejorar el control de acceso basado en políticas para el tráfico de IoT y la carencia del uso de cifrado en la capa de aplicación [6]

El hogar puede tener acceso a internet mediante un proveedor de servicios de internet (ISP) y también mediante una red celular. Esto nos plantea una variación del escenario típico de conectividad con la red del hogar. Lee Craig plantea un método multicapa para asegurar el transporte de datos desde un dispositivo IoT con conexión celular (el cual podría ser un controlador de señales de entrada y salida principal) a un host a través de una red celular. Este método emplea muchos elementos de seguridad entrelazados que cuando se implementan en su totalidad proporcionan una alta solución de conectividad segura. [7]

Metodología

La ejecución del trabajo se dividió en 4 actividades en las que se cumplieron cada uno de los objetivos específicos planteados en el proyecto, en la primera actividad se realizó una consulta, recolección y selección de material informativo para hacer el acercamiento al tema planteado; en la segunda actividad se consultaron publicaciones de seguridad, portales de noticias, blogs y foros, con el fin de documentar ataques, vulnerabilidades, exploits y demás debilidades de infraestructura de un hogar inteligente y analizar las correcciones aplicadas ante tales casos; en la tercera actividad se elaboró un artículo sobre el estado del arte sobre los desafíos de seguridad en hogares inteligentes basados en IoT apoyado en toda la información recopilada; y por último se realizó un montaje experimental con hardware y software del mercado, para simular un escenario de hogar inteligente basado en IoT, y evaluar la seguridad y confiabilidad del mismo ante los ataques más comunes.

Resultados y análisis

Por medio de la elaboración del estado del arte se pudo corroborar que existen desafíos de seguridad de la información en los dispositivos IoT para el hogar; los diversos agentes que hacen parte de la cadena que permitiría un ambiente seguro y confiable dejan cabos sueltos y delegan parte de la responsabilidad por ejemplo en los proveedores de servicios de internet y en los usuarios finales.

Los fabricantes deben implementar protocolos de comunicación seguros entre dispositivos IoT seguros y usar la encriptación, así como también generar actualizaciones automáticas del firmware de los dispositivos con el fin de disminuir las brechas por donde puedan llevarse a cabo ataques, mientras que los proveedores de servicios de internet deberían garantizar dispositivos de red mucho más seguros y brindar configuraciones de seguridad como cambiar los inicios de sesión predeterminados, ocultar o cambiar el SSID de la red wifi, brindar contraseñas seguras o recomendar al usuario final como generarlas, desactivar el acceso remoto al router, gestionar las direcciones MAC; mientras que los usuarios finales deberían seguir unos pasos básicos de configuración tales como contraseñas seguras, actualizar los dispositivos una vez adquiridos, también el uso de firewalls y antivirus en los dispositivos de control como laptop, celular, Tablet, entre otros.

Al utilizar un ambiente controlado de simulación de hogar inteligente en laboratorio, lo primero que debe exponerse es la red de datos, esta se puede llegar a vulnerar de muchas formas con los diversos ataques conocidos, como fuerza bruta, hombre en el medio, denegación de servicios, entre otros, sin embargo existen métodos que solo "escuchan" la red de datos y pueden llegar a determinar cuándo se intercambia información entre dispositivos inteligentes y saber si está expuesto el hogar y realizar ataques físicos; también se pueden enviar correos maliciosos con códigos que puedan bloquear los servicios de los dispositivos; por medio de estos códigos se logró sacar de operación y bloquear a Alexa.

Conclusiones

Según la información recolectada se encontró que para Colombia son pocas las investigaciones que se han hecho sobre este tema, sin embargo, este tiene mucha relevancia e importancia a nivel internacional pues encontraron la utilidad de mejorar y simplificar el diario vivir de las personas.

En Colombia los organismos que tiene un control sobre la tecnología son el Ministerio De Tecnología de la Información y Comunicación junto con el Instituto Colombiano para el Desarrollo de la Ciencia y la Tecnología "Francisco José Caldas" (COLCIENCIAS), estos son los que promueven y tienen un control sobre todos los aspectos y avances de las ciencias tecnológicas.

Actualmente para Colombia no existe ningún ente el cual regule lo que es el nivel de estandarización ni normativa vigente para que los dispositivos inteligentes sean seguros en cuanto al manejo de la información del usuario lo que conlleva a que cualquier persona u organización pueda comercializar y modificar tanto el software como el hardware de estos.

La tecnología basada en IoT tiene muchos aspectos en que mejorar, pues los sistemas sobre los cuales se establece la estructura poseen vacíos de seguridad y pueden ser atacados de formas distintas provocando que el usuario no tenga control sobre los dispositivos conectados a una red.

Tecnológicamente los fabricantes deben llevar las mejoras de seguridad al siguiente nivel para evitar que estos sistemas se vuelvan objetivo de ataques por parte de ciberdelincuentes que pretenden robar información de los usuarios.

Se encontró que programas maliciosos creados para diferentes sistemas operativos pueden crear un daño parcial o total en los dispositivos IOT ya que estos son creados en una misma plataforma base.

Uno de los ataques que más efecto tienen son los que se hacen de forma física ante el dispositivo, pues de este garantiza una completa fuga de información ya que los dispositivos no pueden identificar quien es la persona que está accediendo a la información.

Existen varias formas de ataque para extraer información y dejar inactivos los dispositivos IoT, pues unos son más técnicos que otros, pero al final todos tienen el mismo objetivo de extraer, secuestrar y/o modificar la información, dejar inactivos o dañar los dispositivos y crear un sabotaje dentro de la red para desconfigurarla.

Se encontró que por medio de un ataque de denegación de servicios basado en símbolo del sistema de Windows se puede hacer caer una red junto con los dispositivos conectados, esto garantizaría al atacante tener acceso completo al hogar inteligente y toda su información.

Distintos programas maliciosos que afectan el sistema operativo de Windows pueden dañar tanto el software como hardware de una red, ya que están creados para que se transfieran grandes cantidades de datos los cuales los dispositivos de una red o la misma red no pueden procesar.

Es importante que, al momento de establecer una red, los dispositivos sean configurados correctamente, con el fin que una sola persona pueda acceder y hacer cambios a la configuración tanto de la red como la de los dispositivos conectados a esta.

Referencias Bibliográficas

[1] S. u. Rehman y Volker Gruhn, «An approach to secure smart homes in cyber-physical systems/Internet-of-Things,» pp. 126 - 129, 2018.

[2] S. S. Chowdhury, S. Sarkar, S. Syamal, S. Sengupta y P. Nag , «IoT Based Smart Security and Home Automation System,» 2019.

[3] R. Sarmah, M. Bhuyan y M. H. Bhuyan, «SURE-H: A Secure IoT Enabled Smart Home System,» pp. 59-63, 2019.

[4] A. Modarresi y J. P. Sterbenz, «Towards a Model and Graph Representation for Smart Homes in the IoT,» 2018.

[5] J.-H. Han, Y. Jeon y J. Kim, «Security considerations for secure and trustworthy smart home system in the IoT environment,» 2015.

[6] Z. Shafiq y M. H. Mazhar, «Characterizing Smart Home IoT Traffic in the Wild,» 2020.

[7] C. Lee y A. Fumagalli, «Internet of Things Security - Multilayered Method For End to End Data Communications Over Cellular Networks,» 2019.