Estado del arte: Desafíos de seguridad del Hogar Inteligente basado en IoT.

State of the art: Smart Home security challenges based on IoT.

Autor: Luis Bernardo Estrada Bolívar.

Correo: bernardo.estrada@udea.edu.co

Título de la tesis: Confiabilidad de los sistemas de seguridad del hogar inteligente basado en IoT.

Ingeniería de telecomunicaciones.

Universidad de Antioquia.

Resumen: Las necesidades actuales de un mejor control, seguimiento y gestión en muchas áreas, es esencial y esto a su vez ha originado la aparición y creación de múltiples sistemas como el hogar inteligente, la ciudad inteligente y la red inteligente, todos estos sistemas se basan en el Internet de las cosas (IoT)**,** el cual es una nueva tecnología que permite que todos los dispositivos se conecten a una red e intercambien información bajo ciertos protocolos de comunicación. En este escenario existen vacíos informáticos donde personas inescrupulosas pueden interceptar y sacar provecho de los datos, permitiéndoles controlar los diferentes los dispositivos inteligentes y demás dispositivos conectados a la red local del usuario, conocer las rutinas de los usuarios, las claves de acceso a diferentes plataformas, realizar ataques a mayor escala o simplemente espiar a las personas dentro de un hogar inteligente, por tal motivo se requieren una serie de medidas de seguridad dentro de las que se encuentran la encriptación o cifrado de los datos, el uso de firewalls, antivirus y VPNs.

Palabras clave: Amenazas, Dispositivos IoT, Internet de las cosas, Hogar Inteligente, Seguridad, Vulnerabilidades.

Abstract: The current needs for better control, monitoring and management in many areas, is essential and this in turn has led to the emergence and creation of multiple systems such as smart, smart city and smart grid, all these systems are based on the Internet of Things (IoT), which is a new technology that allows all devices to connect to a network and exchange information under certain communication protocols, in this scenario there are computer gaps where unscrupulous people can intercept and take advantage of the data, allowing them to control the different smart devices and other devices connected to the user's local network, know the routines of the users, the access codes to different platforms, carry out larger-scale attacks or simply spy on people inside a home intelligent, for this reason a series of security measures are required, among which are still the encryption or encryption of data, the use of firewalls, antivirus and VPNs.

Keywords: Threats, IOT devices, Internet of things, Smart home, Security, Vulnerabilities.

1. 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. Cuando se habla de la seguridad de una casa, se aborda tanto la seguridad física como la seguridad de la información que se maneja entre los dispositivos inteligentes y estos con la red y el usuario. Dentro de cada una de estas casas inteligentes existen diferentes dispositivos que hacen que se automaticen las tareas del hogar, para Proptech la cual es una compañía encargada de analizar los dispositivos IoT, los nuevos avances deben de estar enfocados en que exista un mayor control sin estar en casa, la seguridad también es fundamental pues se debe salvaguardar los bienes y la integridad física, otro aspecto importante son los robots que deben hacer las tareas matutinas, todo lo anterior debe de estar fundamentado en que las casas sean más eficientes y respetuosas con el medio ambiente . [1]

La seguridad del hogar se divide en dos factores esenciales, la seguridad física que pretende evitar cortocircuitos, conatos de incendio, inundaciones, robos, desperdicio de recursos, entre otros; por otro lado, se encuentra la seguridad de la información del hogar, que pretende garantizar al usuario que todos los datos que se procesan al interior, solo puedan ser almacenados, verificados, supervisados, monitoreados y gestionados por equipos autorizados para evitar la pérdida de esta información [2]; en esta última categoría, entran los sistemas para controlar y supervisar el hogar, tales como los sistemas de video vigilancia, de alarma contra intrusos, de detección de incendios, sistemas contra inundaciones, entre otros; en el mercado existe una gran variedad de sensores tales como cámaras de video y equipos de grabación para estos vídeos, 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.

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 o hardware, software, protocolos de comunicación son usados y cuáles pueden llegar a ser posibles estándares para garantizar una hogar inteligente y seguro, reduciendo los riesgos de los

ciberataques y estructurando el concepto mencionado, lo que ha futuro puede ser base para celdas o bloques de información cada vez mayores como las ciudades inteligentes. 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 control de la temperatura ambiente de la casa, seguridad y protección, incluso 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. Dentro de este artículo se analizarán las principales amenazas y vulnerabilidades comunes en el IoT, específicamente en un hogar inteligente.

2. Definiciones

Hogar inteligente: Es un sistema compuesto por un controlador principal, diferentes sensores y actuadores, así como aplicaciones móviles que permiten al usuario llevar a cabo las tareas del hogar de forma automatizada; desde esta perspectiva existen múltiples soluciones electrónicas, por ejemplo el uso de una Raspberry Pi, sensores de movimiento y de gas MQ-2, y una aplicación móvil desarrollada para Android [3]; o la planteada por Juan Gabriel Pérez Zúñiga en su trabajo de grado de maestría, en donde se analizan los módulos ESP8266-12E, protocolos como ZigBee, sensores de movimiento, un algoritmo y un servidor en la nube. [4] 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.

Dispositivo inteligente: Es un dispositivo electrónico, el cual está conectado a otros y puede ser configurado tanto para recibir órdenes como para controlar otros dispositivos, tienen su propia forma de comunicación por medio de protocolos inalámbricos como lo son Bluetooth, NFC, Wifi, 3G, entre otros, estos pueden funcionar de forma autónoma e interactiva. [5]

Conexión de dispositivos: 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. [6]

IoT: El internet de las cosas es uno de los inventos del nuevo siglo, ya que este es un gran concepto que caracteriza la próxima transformación en la evolución del internet [6]. Hace uso de diferentes sensores y actuadores, así como la inteligencia artificial, para facilitar las tareas diarias. Por otro lado, el internet de las cosas cambiará todo, pues tiene aplicaciones en la educación, la comunicación, los negocios, el gobierno, la ciencia y la vida de las personas, también este invento es uno de los más importantes y más potentes de la historia. [7]

Red de área local: Es el conjunto de hardware de la red interna del usuario; incluye modems de los proveedores de servicios de internet (ISP) los cuales son los elementos de borde hacia la nube, routers del usuario o de los ISP , access points, entre otros, los cuales brindan conectividad vía ethernet o WiFi al interior del hogar. Los elementos de borde de la red local cuentan con medidas para controlar los riesgos de seguridad [8], en la resolución 3066 de 2011 se encuentra más información.

Seguridad inteligente: Es un conjunto de sistemas integrados y automatizados; se desarrolla con modelos de aprendizaje artificial y gestión de riesgos [9]. Se usa para evitar fugas de información.

3. Metodología de análisis

El presente artículo tiene como principal objetivo la elaboración del estado del arte sobre los desafíos de seguridad en hogares inteligentes basados en IoT. Como estrategia de búsqueda se combinaron las siguientes palabras claves (dispositivos IoT, seguridad, vulnerabilidades, amenazas) con smart home, domótica, casa inteligente, en las diferentes bases de datos (scielo, redalyc, google académico, dialnet y bases de datos de diferentes universidades). Además, se consultaron documentos públicos elaborados por entes internacionales y empresas creadoras de antivirus como Panda Security, Eset, Avast y AVG los cuales crean programas para protección de todo tipo de equipos. De los documentos analizados un factor clave es que estos no superen una antigüedad máxima de 5 años ya que la tecnología avanza a grandes pasos, para este estudio se encontró que los documentos del año 2021 representan el 3.23%; para el 2020 el 12.90%; para el 2019 el 22.58%; para el 2018 el 35.48% y para el 2017 el 25.81%, de estos documentos la mayoría son de tipo internacional en el idioma inglés.

Tabla 1. *Registro de publicación de artículos.*

Año	Frecuencia
2021	3,23%
2020	12,90%
2019	22,58%
2018	35,48%
2017	25,81%

Fuente: *Autor del proyecto.*

Los tipos de documentos también son importantes por tal motivo se clasificaron y se encontró que las tesis de maestrías aportan el 19.23%, estas tesis tienen diferentes enfoques de estudio que van desde el desarrollo de una aplicación móvil para contribuir con el incremento y la personalización de las smart home, otro enfoque es el de un modelo de negocio de viviendas domóticas, también se analiza la calidad de servicios en la nube; las tesis doctorales representan el 3.85% en donde el enfoque que establece el autor es una relación para integrar los IoT con las redes sociales; mientras que los artículos tanto investigativos como argumentativos aportan el 76.92%, siendo estos los más importantes pues abordan el tema desde distintos ámbitos y también proponen métodos de solución para cada problema aportado, en la tabla 2 se detalla mejor la información. Los artículos analizados son presentados en el anexo 2.

Tabla 2. *Tipos de documentos.*

Tipo de documento	Frecuencia
Tesis de maestría	19,23%
Tesis de doctoral	3,85%
Artículos	76,92%

Fuente: *Autor del proyecto.*

De los artículos seleccionados se revisó el objetivo del estudio, la problemática o el estudio que se quería hacer, la metodología usada para dar solución a esta problemática y los resultados obtenidos junto a posibles implementaciones o cambios que pudieron hacer para tener un mayor beneficio, siendo estas últimas las de mayor importancia, ya que permitirá entender cómo se puede ordenar, formular y direccionar el presente artículo, de igual forma se estudiaron las conclusiones y recomendaciones.

3.1.Arquitectura de activos IoT

Un hogar inteligente o un smart home puede tener acceso a internet mediante un proveedor de servicios de internet (ISP) o también mediante una red celular. Esto nos plantea una variación del escenario típico de conectividad con la red del hogar. Pero para esto se debe conocer la infraestructura de hardware y software, la cual emplea muchos elementos de seguridad entrelazados que cuando se implementan en su totalidad proporcionan una alta solución de conectividad segura. [10] En la arquitectura general se encuentran los componentes lógicos (BaaS o mBaaS o Backend as a Service, la plataforma, la instalación, los servicios con

las aplicaciones, las decisiones de datos y la información) y los componentes físicos (Dispositivos IoT y de comunicaciones).

Los tipos de activos lógicos se clasifican en dos grupos: Backend o BaaS y las instalaciones; en el primero se encuentran activos como la infraestructura de la nube, el procesamiento de datos y los servicios basados en la web; en el segundo se encuentran la fuente de alimentación, la puerta de enlace, las redes de seguridad y el router. Los componentes físicos se clasifican en tres grupos: los dispositivos IoT, en donde se encuentran activos como actuadores, dispositivos para administrar objetos, hardware, interfaces de conexión con los dispositivos IoT, sensores, software y sistemas embebidos; la comunicación con activos como los protocolos y redes; y por último la información, con activos como el reposo, tránsito y uso. Normalmente para que cualquier dispositivo se pueda conectar a la nube necesita una serie de elementos para garantizar el intercambio de información, cuando se depende de una red de área local, lo esencial es el repetidor el cual se usa para extender la longitud de la red en caso de que esta sea muy débil y no alcance a dar señal a los dispositivos; los hubs son repetidores multipuertos, este permite diferentes conexiones, una desventaja de estos es que no poseen inteligencia para encontrar la mejor ruta en él envió de paquetes, conllevando a la ineficiencia y desperdicio. Por último, se tiene el router el cual enlaza los segmentos de red LAN, este recibe y envía paquetes por la ruta más óptima a la nube. [11]

3.2. Tipos de dispositivos IoT

Para conocer los tipos de dispositivos IoT se debe identificar su funcionalidad, importancia, ventajas y desventajas.

Funcionalidad de los dispositivos inteligentes: Estos dispositivos para su funcionamiento se valen de diferentes sensores y actuadores los cuales monitorean el entorno y son capaces de usar comandos de voz para establecer una comunicación con el usuario. [12]

Importancia de los dispositivos inteligentes: Los dispositivos IoT usados en el hogar pretender brindar seguridad por medio de sistemas como los de videovigilancia mediante el uso

de cámaras IP permitiendo conocer la situación en tiempo real del hogar inteligente, el ahorro de los diferentes servicios públicos como la energía, está a cargo de iluminación y termostatos inteligentes, entre otros, adicionalmente se ha logrado que un nivel de integración y compatibilidad con otros dispositivos IoT diferentes marcas. Por último, los dispositivos IoT buscan brindar tranquilidad, conveniencia y comodidad para los usuarios y representan una optimización en cuanto al uso de los recursos dentro del hogar y a la realización de las tareas diarias. [12]

Algunas ventajas son [13]**:**

- Todos los dispositivos se pueden administrar y configurar por medio de una sola matriz.
- Poseen una flexibilidad pues son capaces de comunicarse con otros dispositivos de diferentes marcas.
- Pueden actuar sobre el ambiente de casa para modificar sus variables.

Como desventajas se tiene [13]**:**

- La adquisición de estos dispositivos tiene un alto costo.
- Se necesita una red de banda ancha para conectar múltiples dispositivos.
- Pueden existir fallas que no basta de una simple configuración para corregirla, por lo tanto, se debe llamar a un profesional para que este lo haga.

Clasificación de dispositivos inteligentes

En el mercado existe una gran variedad de dispositivos inteligentes para el hogar, estos se clasifican dentro de 4 grandes grupos [14]:

- Accesorios de uso personal: como relojes inteligentes, zapatillas deportivas, pañales inteligentes, junto con los smartphones y demás dispositivos conocidos como *weareables* (usables).
- Asistentes: Dispositivos que pueden controlar los demás dispositivos IoT, entre los asistentes más comunes se tiene a Alexa de Amazon’s Echo, Siri de Apple y Google Home.

- Electrodomésticos inteligentes: Son todos los productos de la línea blanca que se pueden encontrar en un hogar.
- Productos conectados que optimizan el hogar: como bombillas, termostatos, cámaras de circuito cerrado, cortinas, enchufes, entre otros.

3.3. Comunicación entre dispositivos IoT

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 NB-IoT, añadiendo heterogeneidad extra y con esto mayor complejidad a las redes de borde. [15]

Con el aumento de los datos privados de los usuarios, no se pueden ignorar las vulnerabilidades de seguridad y las fugas en el entorno de IoT. Se han llevado a cabo una serie de importantes investigaciones relacionadas con la seguridad y privacidad en entornos IoT para que estos entornos sean de confianza. Se debe comprender mejor los desafíos que plantean las casas inteligentes en términos de administración, seguridad y privacidad. Según un estudio reciente sobre una muestra aleatoria de hogares inteligentes en los Estados Unidos, los dispositivos presentan un patrón de número y tiempo, con ciertos problemas de seguridad y privacidad. También revelaron que, a pesar de la heterogeneidad, hogares inteligentes la obvia fragmentación del hogar, debido a la dependencia de algunos servicios populares en la nube y servicios DNS, está mayoritariamente centralizada, 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. [16]

3.4. Seguridad de la información en un ambiente IoT

La seguridad de la información también es importante pues estos dispositivos manejan y acceden a información personal del usuario como correos electrónicos, reconocimiento de voz, ubicación en tiempo real tanto del usuario como de los dispositivos conectados a la red, el horario laboral, distribución de la casa y hábitos o rutina que posee el usuario [17] por tal motivo estos son blanco de ataques pues muchos de los usuarios no poseen un programa de seguridad el cual salvaguarde y mantenga de forma segura la información.

Actualmente no existe una seguridad perfecta, pero existen algunas formas de hacerla más efectiva, este es un factor que siempre hay que tener en cuenta, pero las sugerencias o buenas prácticas en algunos casos no siempre son adoptadas por empresas o familias. Ya sea por cuestiones económicas, de recursos humanos o simplemente por desconocimiento de las mismas, la seguridad del Internet de las Cosas se ha convertido en el tema más importante por múltiples acontecimientos y ataques, donde la información de los usuarios se ha visto comprometida, lo que hace necesario evaluar todo el entorno para encontrar posibles nuevos puntos de acceso y vulnerabilidades, pero también se debe hacer referencia a un mal método en el diseño, desarrollo y posterior implementación, dejando la seguridad en un segundo plano. Al mejorar la seguridad de la red se logra reducir el riesgo de un ataque.

La infección de equipos con código malicioso no es un tema nuevo en el mundo de la seguridad en internet, pero antes de comenzar a hablar de la arquitectura hay que hablar del modelado de riesgos, cuyo objetivo es conocer la forma en que un atacante puede poner en peligro y luego tomar las precauciones necesarias para evitarlo.

Para analizar la seguridad del IoT se tuvo en cuenta la categoría del ataque bajo la amenaza, el nivel de impacto y los activos afectados. Se encontraron categorías de ataques que usan amenazas comunes como el malware, los kits de aprovechamiento, los ataques dirigidos a un dispositivo, el ataque de denegación distribuida del servicio (DDoS), ataques a la privacidad, falsificación de dispositivos maliciosos, modificación de la información, hombre en el medio (man in the middle), secuestro de protocolos y sesiones en la comunicación de dispositivos IoT; otros ataques directos de forma física exponen la red al atacante, el cual logra obtener

información de la víctima, además ocasionan fallas o caídas de red, fallas de los dispositivos y sistemas, pérdida del soporte o servicio, filtrado de información, y sabotajes.

Tipos de ataques a los hogares inteligentes

En el blog de Mapfre se estima que las amenazas a una Smart Home alcanzan un 80% [18] pues existen dispositivos que se pueden conectar a la red principal y estos presentan fallos en su seguridad y son la puerta de entrada para establecer conexión y conocer la IP del router para hacer caer toda la red. Los ataques más famosos que se le hacen a estos dispositivos son:

- Man in the middle.
- El robo de datos e identidades.
- El secuestro de dispositivos inteligentes.
- Denegación de Servicio (DoS).
- Denegación Distribuida de Servicio (DDoS)

Algunas de las amenazas comunes las cuales son usadas para atacar los hogares inteligentes son:

- Malware.
- Ataques dirigidos.
- Kits de aprovechamiento.
- Falsificación de dispositivos maliciosos.
- Modificación de la información.
- Ataques a la privacidad.
- Secuestro de protocolos de comunicación en el IoT.
- Secuestro de sesión.
- Reconocimiento de red.
- Caídas de la red.
- Fallos de dispositivos y sistemas.
- Pérdida del soporte o servicio.
- Vulnerabilidad del software.
- Fallo en plataformas operadas por terceros.

- Modificación parcial o total de partes del dispositivo o sabotaje.

3.5. Contramedidas para evitar ataques

- El usuario debe informarse antes de adquirir dispositivos inteligentes, conocer las ventajas, las desventajas, el funcionamiento y los requerimientos de la red.
- El usuario debe realizar la configuración de nombres de usuarios y contraseñas, evitando dejar las que traen por defecto estos dispositivos inteligentes, facilitando el entorno a los atacantes. [19]
- Se deben revisar los ajustes de seguridad y privacidad una vez haya instalado y configurado los dispositivos con el fin de confirmar la información que se suministró en los mismos.
- Idealmente se debe configurar una red de Wifi independiente solo para los dispositivos IoT, esto con el fin de evitar que toda la red sea infectada y controlada a distancia.
- El usuario debe configurar su red con cifrado WPA2-PSK y si es posible debe desactivarse la opción WPS.
- Se deben usar contraseñas robustas que incluyan mayúsculas y minúsculas combinadas con números, así como caracteres especiales, con el fin de garantizar una mayor dificultad para el atacante al momento de ingresar a la red.
- Se debe instalar software legal y las actualizaciones de las páginas oficiales de los dispositivos, esto evitará que archivos maliciosos o que vengan contaminados con malware de terceros ingresen a la red local.
- Usar routers inteligentes los cuales están creados únicamente para la comunicación los dispositivos IoT, añadiendo un cifrado extra a la red.

3.6. Problemas de investigación abiertos y desafíos

La seguridad de los datos del usuario en un hogar inteligente sigue siendo uno de los temas críticos que debe enfrentarse desde múltiples frentes, por una parte, los fabricantes deberían implementar unos protocolos de seguridad tales como la encriptación de los datos que

se comparten entre los dispositivos IoT, sin embargo no existe un organismo que estandarice las normas que deben cumplir estos dispositivos con el fin de minimizar las brechas de seguridad que pueden ser utilizadas por los atacantes para conseguir información privada del usuario, a su vez es deber de los usuarios seguir una serie de pasos que reduzcan aún más estos vacíos de seguridad.

Con la evolución de la Internet de las cosas, se ha vuelto obvio en el análisis de datos en tiempo real y la gestión dinámica del campo [20]. Sin embargo, la implementación de Internet de las cosas se enfrenta a una serie de desafíos:

- **La estabilidad de red:** Si los hogares inteligentes planean ingresar al Internet de las cosas, necesitan conexiones ininterrumpidas. Incluso con una conexión a Internet por fibra óptica, no se garantiza una disponibilidad del 100%. Ya sea por mantenimiento o por otras razones, en algún momento se puede perder la conexión. En este caso, se podría pensar en tener sistemas de respaldo tanto para la red de datos como para la red eléctrica, sin embargo esto incrementa el costo de la solución.

- **Almacenamiento y manejo de datos:** En la actualidad, todas las actividades de pronóstico dependen en gran medida de los datos almacenados a lo largo de la operación de los sistemas. Los dispositivos IoT permiten recopilar miles de puntos de datos que son fundamentales para su uso futuro, esto requiere una capacidad de almacenamiento alta, y por tanto debe ser planificada de forma segura, bien sea mediante las memoria interna de los dispositivos o por medio del almacenamiento en la nube, lo que implica subir información a internet la cual podría en algún momento quedar expuesta.

- **Seguridad:** Hay muchos casos de ciberataques. Si los hogares inteligentes planean superar estos ataques, es necesario introducir nuevas herramientas de seguridad en las redes tales como firewalls, redes virtuales, routers para IoT, entre otros, lo que significa mayores costos y altos costos de mantenimiento. Lo que

puede generar desconfianza por parte de los futuros posibles usuarios de estos sistemas afectando este mercado.

- **Identificación de eslabones débiles en el hogar:** El usuario debe saber identificar cual o cuales de los dispositivos que componen su red pueden ser vulnerables a ataques informáticos. Sin embargo, con el crecimiento y la heterogeneidad de las redes, es más difícil encontrar un medio de supervisión de todos los dispositivos, esto podría llevarse a cabo mediante el desarrollo de una aplicación móvil que informe o alerte al usuario sobre las posibles fallas de configuración tales como contraseñas por defecto, direcciones IP por defecto, contraseñas débiles, entre otras.

En cuanto a investigaciones abiertas se pueden encontrar que los dispositivos IoT pueden ser de gran ayuda a en la industria, pues si son capaces de optimizar un hogar de igual forma pueden hacer que las diferentes líneas productivas funcionen de forma eficaz pues esto serán capaz de interpretar grandes flujos de datos que le servirán a la empresa para predecir el mercado y hacer ajustes a sus líneas productivas. [21] algunos de los temas que no han sido explorados en la IoT de la industria son:

- Podrían tener una mayor rapidez en la comercialización de los productos.
- Aportarían mayor productividad y excelencia operativa.
- Los procesos serían más óptimos.
- Los montajes en cuanto a la maquinaria usando este tipo de dispositivos permitirían conocer tiempos muertos o de inactividad.
- Permitirían mejorar los tiempos en cuanto a precisión, fiabilidad y flexibilidad.

Otro campo en el cual el IoT ha sido poco incluida es en el ámbito académico, pues estos les serviría de gran ayuda tanto a los estudiantes como a los docentes para orientar sus clases, también se podrían aplicar a diferentes entornos educativos, como aulas 4.0, edificios o entornos inteligentes, laboratorios, etc. [22] Actualmente en EEUU hasta ahora se están aplicando en

escuelas K-12, algunos beneficios que se podrían obtener si se usan el IoT en escuelas como universidades son:

- Se podrían controlar las salas de conferencias y de estudio, ya que estos dispositivos pueden configurar tanto el clima como el audio de estas.
- Se podrían realizar seguimientos de los principales activos de las instituciones, tanto computadores como Tablet que estén en funcionamiento.
- Se pueden adaptar para aquellos estudiantes que poseen discapacidades y necesidades especiales a la hora de estar en clase.

También se podrían aplicar en campos como la hotelería, almacenes de cara al público, para monitorear flotas de vehículos para logística, en la gestión de almacenes de logística o inventarios, en la agricultura y ganadería, en la salud, gestión de suministros, de tráfico y ambiental, en estos campos las investigaciones son pocas [23], por lo tanto existe mucho que mejorar, pero se puede decir que es una tecnología prometedora la cual ayuda a la vida de las personas. Vale la pena señalar que Internet de las cosas no solo se trata de conectar objetos y administrarlos desde dispositivos remotos, sino que también la información precisa, automatizada y en tiempo real es una característica clave de las aplicaciones de Internet de las cosas. Por lo tanto, las interpretaciones de estos datos provienen del mundo real y pueden dar lugar a la aparición de varios servicios comerciales nuevos que pueden proporcionar importantes beneficios económicos y sociales.

Conclusiones

El IoT y la Computación en la Nube todavía existen preocupaciones sobre la privacidad, la seguridad y la falta de interoperabilidad que se presenta en ambas áreas, por tal motivo deben mejorar aspectos y corregir las constantes fallas que tienen.

El IoT es una tecnología emergente que poco a poco avanza para formar parte de muchas facetas de nuestra vida. Sin embargo, debido a las limitaciones de IoT como se presenta en este

documento y la necesidad de características complejas hacen que la seguridad en cuanto a los datos del usuario se vea comprometida.

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.

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.

Bibliografía

[1] Proptech, 7 Junio 2019. [En línea]. Available: https://proptech.es/ultimos-avances-domotica/. [Último acceso: 1 Julio 2021].

[2] J. Jimenez, 1 Noviembre 2020. [En línea]. Available: https://www.redeszone.net/tutoriales/seguridad/consejos-seguridad-informatica-hogar/. [Último acceso: 1 Julio 2021].

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

[4] J. G. Pérez Zúñiga, «Calidad de servicios en la nube en combinación con el internet de las cosas: revisión sistemática de la literatura y modelo de calidad.,» Cuenca, 2017.

[5] Mokos smart, 18 Agosto 2020. [En línea]. Available: https://www.mokosmart.com/es/what-is-a-smart-device/. [Último acceso: 10 Julio 2021].

[6] S. C. Ochoa Forero y J. S. Arguello Sandoval, «Modelo de Negocio Enfocado en la Creación y Diseño de Viviendas Inteligentes,» Bogotá, 2021.

[7] Abril 2011. [En línea]. Available: https://www.cisco.com/c/dam/global/es_es/assets/executives/pdf/Internet_of_Things_IoT_IBSG_0411FINAL.pdf. [Último acceso: 8 Julio 2021].

[8] Comisión de regulación de comunicación, 14 Octubre 2011. [En línea]. Available: https://www.crcom.gov.co/uploads/images/files/1_Documento_soporte_RITEL.pdf. [Último acceso: 11 Julio 2021].

[9] Coesdesign, [En línea]. Available: https://coesdesign.com/seguridad-inteligente/. [Último acceso: 10 Julio 2021].

[10] O. A. Huaman Ugarte, «Desarrollo de un prototipo de domotica para el control y monitoreo del condominio los parques de Villa el Salvador II,» Lima, 2018.

[11] A. Aller, 15 Agosto 2020. [En línea]. Available: https://www.profesionalreview.com/2020/08/15/componentes-fisicos-de-una-red/. [Último acceso: 10 Julio 2021].

[12] J. Controls, 24 Noviembre 2019. [En línea]. Available: https://blogseguridad.tyco.es/consejos/3-motivos-para-integrar-la-seguridad-inteligente-en-el-hogar/. [Último acceso: 10 Julio 2021].

[13] B. Garcia, 6 Agosto 2019. [En línea]. Available: http://fuencarralelpardo.com/2019/08/06/ventajas-e-inconvenientes-de-los-productos-inteligentes-que-tenemos-en-casa/. [Último acceso: 12 Julio 2021].

[14] M. Franco. [En línea]. Available: https://smart10.top/dispositivos-inteligentes/. [Último acceso: 10 Julio 2021].

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

[16] J. Martino Perrota, 29 Enero 2020. [En línea]. Available: https://www.telesemana.com/blog/2020/01/29/dispositivos-inteligentes-para-hogares-en-estados-unidos/. [Último acceso: 3 Julio 2021].

[17] Avast, 19 Mayo 2021. [En línea]. Available: https://www.avast.com/es-es/c-iot-security-risks. [Último acceso: 10 Julio 2021].

[18] El blog de Mapfre, 25 Octubre 2018. [En línea]. Available: https://blogmapfre.com/seguridad/amenazas-mas-comunes-a-la-smarthome-asi-se-pueden-contrarrestar/. [Último acceso: 12 Julio 2021].

[19] Incibe, 2020. [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-iot.pdf. [Último acceso: 9 Julio 2021].

[20] Signals IOT, 28 Noviembre 2018. [En línea]. Available: https://signalsiot.com/cinco-principales-desafios-para-iot-industrial/. [Último acceso: 10 Julio 2021].

[21] J. C. Diago Julian y M. L. Muñoz Bedoya, «Internet de las cosas analizado desde distintos entornos,» Pereira, 2017.

[22] CPV, 8 Enero 2020. [En línea]. Available: https://cpvmicro.com/incorporando-iot-en-centros-educativos-aplicacion-y-beneficios/. [Último acceso: 10 Julio 2021].

[23] G. Budiño, 14 Junio 2021. [En línea]. Available: https://www.evaluandosoftware.com/campos-de-aplicacion-de-internet-of-things-o-internet-de-las-cosas/. [Último acceso: 10 Julio 2021].