PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
MENCIÓN EN REDES DE COMUNICACIONES

Propuesta metodológica y tecnológica avanzada
(TESIS)

TEMA:

"Estudio de mecanismos de aseguramiento de la información para internet de las cosas IoT en Smart home".

AUTOR: Christian Rafael Cisneros Mera, Ing.

DIRECTOR: Juan Francisco Chafla Altamirano, Ing., MSc.

Quito - 2021

ÍNDICE DE CONTENIDOS

AGRADECIMIENTO

A Dios, por bendecirme y cuidarme en cada paso que doy, por ser mi guía en cada una de mis metas propuestas tanto personales como profesionales.

A mi esposa Patty y a mis hijas Karlita Y Emilia, por su amor, comprensión y apoyo incondicional brindado para culminar con mis estudios.

A mi padre, madre y hermanos, quienes con sus palabras de aliento y apoyo moral me animaron a seguir adelante.

A la Pontificia Universidad Católica del Ecuador, por brindarme la oportunidad de continuar con mis estudios en el programa de maestría y compartir sus conocimientos y experiencia.

A mi director Juan Francisco Chafla A. Ing., Msc. Por su dirección y apoyo en el desarrollo de mi proyecto de titulación.

A mis lectores Javier Cóndor Ing., Msc. Y Edison Mora Ing., Msc., MBA. Por sus valiosos aportes a la culminación de mi proyecto de titulación.

A mi Amigo y compañero Roberto Toapanta Ing., Msc. Por su valioso apoyo incondicional durante toda la carrea de la maestría.

DEDICATORIA

A mi esposa Patty, por brindarme su amor y comprensión incondicional siempre y por ser mi apoyo en todos los pasos que doy.

A mis hijas Karlita y Emilia, por ser la razón de mi vida y quienes me motivan a seguir adelante y a superarme cada día.

A mi padre, madre y hermanos, por ser la base de mis principios y valores con los que he logrado ser la persona que soy.

RESUMEN

La presente investigación se basa en encontrar un mecanismo de seguridad para un sistema IoT Smart Home que brinde privacidad, seguridad, confiablidad, integridad y disponibilidad del sistema, el estudio se basará sobre la investigación, comparación y análisis de los tipos de Mecanismos de Seguridad para Redes IoT existentes, una vez encontrado el mecanismo de seguridad adecuado, este se implementará en un entorno IoT Smart Home con el fin de evaluar su funcionamiento de una forma práctica logrando cumplir con las metas de mejora de los procesos de seguridad en un entorno IoT Smart Home y de sus usuarios.

El estudio de Entornos, Arquitecturas y Protocolos IoT apoyaran y servirán de base para la investigación de Mecanismos de Seguridad IoT Smart Home. Así también, se realizará un estudio exhaustivo de las vulnerabilidades, amenazas y ataques a los que se exponen estos sistemas, un análisis del riesgo que provocan y con la aplicación del Mecanismo evaluar la seguridad del sistema IoT Smart Home.

CAPITULO I

1. GENERALIDADES

1.1 Introducción

Internet de las cosas es una realidad de rápido desarrollo en nuestras vidas. Millones de dispositivos están conectados por medio de diferentes redes de comunicación, desde pequeños sensores que pueden dar información de actividad en el hogar hasta el control de parqueaderos disponibles en un centro comercial. Cada vez más objetos se unen para mejorar y automatizar actividades cotidianas derribando los muros que separan la realidad de lo virtual.

Sin embargo, estas redes no están libres de ataques maliciosos y amenazas de ciberseguridad, para analizar esta problemática se pueden mencionar sus causas, la homogenización de la comunicación es necesaria para que los diferentes dispositivos puedan comprenderse, y la información pueda ser transparente y de bajo costo, por otro lado están las vulnerabilidades que presentan las redes de dispositivos IoT que comprometen la seguridad, privacidad y defensa de datos de los usuarios de dispositivos IoT en Smart home.

Al conectar los dispositivos inteligentes del hogar, los ciberdelincuentes también lo harán. Las industrias IoT que están ansiosas por lanzar sus productos al mercado ponen la seguridad de sus dispositivos en segundo plano, dejando a sus dispositivos en la inseguridad y vulnerables a ataques maliciosos.

Encontrar las vulnerabilidades que se encuentran en las redes de dispositivos IoT y analizar los mecanismos existentes en ambientes IoT, permitirá identificar un mecanismo de seguridad adecuado y el que mitigue de mejor manera la inseguridad y el uso malicioso de información que sólo debería utilizar el usuario y dueño de sus dispositivos IoT.

1.2 Justificación

El descubrimiento tecnológico del Internet de las cosas IoT nos permite mejorar nuestra calidad de vida, las actividades cotidianas serán cada vez más fáciles y eficientes, ya sea en seguridad del hogar, control de nuestra salud, incluso en la utilización de transporte, entre otras. El Internet de las cosas cada vez tiene mayor acogida en la población a nivel mundial, nacional y local.

Las casas inteligentes (Smart Home) se basan en el uso de dispositivos IoT interconectados entre sí, éstos cumplen con la misión de dar información valiosa a sus integrantes de ciertas variables como, la aparición de delincuentes, la posibilidad de un incendio, el uso adecuado de energía eléctrica, etc. Toda esta información generada por estos dispositivos IoT en Smart Home, dan un sustento de vida a sus integrantes y no puede ser usada por otras personas de una forma maliciosa provocando incertidumbre, inseguridad y desconfianza en la información recibida.

La seguridad de los datos e información generados por dispositivos IoT para Smart Home son tan importantes como la seguridad que demandan sus habitantes. Es necesario encontrar los puntos críticos y vulnerables de estas redes y consecuentemente encontrar un mecanismo de seguridad adecuado para brindar beneficios como la tranquilidad y la satisfacción de habitar en una Smart Home.

Internet de las cosas brinda una gran cantidad de beneficios al implementar en diferentes entornos, pero también exige muchos desafíos. Garantizar seguridad y privacidad de los datos generados por el internet de las cosas es un reto a los que deben apuntar las personas que generan soluciones de seguridad, integrar capacidad de protección es imperativo para las redes domésticas inteligentes.

1.3 Antecedentes

Las tendencias de uso de Internet y la cobertura cada vez más extensa, ha estimulado la aparición de esta nueva tecnología conocida como IoT. En el estudio realizado por (Salazar & Silvestre, 2014) a través de su tesis "Internet de las cosas" realiza una descripción la definición, historia y características de las redes IoT que será utilizada para el estudio inicial de la presente investigación.

La aplicación de tecnologías IoT resultan ser transparentes. Es decir, no se tiene un conocimiento completo de su funcionamiento. El análisis realizado por (Vélez Andres, 2019b), presenta las arquitecturas de referencia para IoT, que será utilizada de referencia en el presente trabajo.

El despliegue inseguro tendrá un impacto social y hará que las personas que utilizan esta tecnología IoT sean vulnerables a amenazas, en el estudio realizado por (Cardona, 2016), en su artículo "La seguridad en el Internet de las cosas y el Mundo 3.0 - Globb Security" muestra un escenario donde la aplicación de IoT tiene importantes vulnerabilidades que generan preocupación en la seguridad, el estudio aportará con valiosa información.

Para entender el funcionamiento de las IoT es necesario saber los modelos y plataformas en que se basan los dispositivos IoT. El estudio realizado por (Achila & Sanchez, 2017), menciona el modelo usado en dispositivos IoT así también la información relacionada con las capas de la estructura IoT, que servirá como referencia.

Conocer los protocolos utilizados para cada tipo de aplicación IoT como los métodos de protección de las redes de comunicaciones dará como resultado sistemas más confiables. El estudio realizado por (Eterovic Jorge, Cipriano Marcelo, & Nicolet Santiago, 2018) en su artículo "Análisis de Protocolos de Comunicaciones para Internet de las Cosas" será utilizado como referencia para la comparativa de los mecanismos de seguridad.

Mayor conectividad significa mayor disposición de recursos, lo que plantea nuevos desafíos. El estudio realizado por (Zabalo Arteche, 2019), define protocolos de Ciberseguridad, referencia de estándares y un marco de certificación para dispositivos de IoT.

1.4 Objetivos

1.4.1 Objetivo General

Realizar el estudio sobre mecanismos de seguridad para internet de las cosas IoT en Smart home, realizando un análisis metodológico de mecanismos de seguridad existentes para un mejor desarrollo de dispositivos y de tecnologías de comunicación.

1.4.2 Objetivos Específicos

- Realizar una base teórica y estudio del estado del arte respecto al desarrollo de IoT, historia y estado actual. Campos de aplicación, tipo de tecnología, temas relacionados con la seguridad y protección de información, que sirvan como sustento teórico al presente trabajo.
- Estudiar los tipos de arquitecturas y protocolos que se aplican a las redes IoT en Smart Home, identificar vulnerabilidades a ataques maliciosos, desarrollo de los tipos de mecanismos de seguridad y privacidad con el fin de aplacar las inseguridades al usuario de IoT en Smart Home.
- Realizar un análisis comparativo entre mecanismos y recomendaciones de seguridad existentes para las redes IoT en Smart home, Presentar la propuesta de un mecanismo adecuado de seguridad de datos e información, mostrando las ventajas y prestaciones del mecanismo de seguridad, además que solvente la mayoría de inseguridades y que aporte a una mejor gestión de redes IoT en Smart Home.
- Evaluar el mecanismo encontrado en la investigación, simulando en un ambiente Smart Home la aplicación del mecanismo de seguridad, mostrar resultados y ventajas de seguridad, privacidad y protección de los datos generados en dispositivos IoT Smart Home.

1.5 Alcance

La presente investigación tiene como fin encontrar un mecanismo de seguridad adecuado y buenas prácticas de seguridad para obtener mayor privacidad de datos, protección de información y seguridad en el almacenamiento y transferencia de datos en redes de Internet de las cosas IoT en Smart home.

Para sustentar el estudio se investigarán los tipos de vulnerabilidades existentes, determinar las amenazas y tipos de riesgos en las redes IoT en Smart home, además buscar entre los mecanismos existentes el más adecuado que cubra la mayor parte de los criterios de seguridad.

Finalmente implementar un sistema IoT Smart Home donde, de una manera práctica y didáctica se pongan a prueba las mejores recomendaciones y mecanismos para mitigar en gran parte los riesgos de seguridad y aportar al mejor desempeño de redes IoT en Smart home.

CAPITULO II

2. MARCO TEÓRICO

En este capítulo se dará a conocer el contexto en el cual se realizará la investigación y se expondrán los términos y definiciones que aportarán al estudio de mecanismos de seguridad IoT en Smart Home.

Se pondrá énfasis en términos sobre seguridad, privacidad, integridad y protección de datos en IoT, además en los términos que tratan sobre las tecnologías, fases y arquitecturas empleadas en dichas redes.

2.1 Antecedentes históricos de IoT

El conocimiento de la historia y del nacimiento de la tecnología IoT dará un mayor entendimiento al valor que se le da en el presente, las necesidades de automatización del hogar y de mejorar la calidad de vida de las personas ha dado un impulso al desarrollo de los sistemas IoT, conocer la funcionalidad y las ventajas que brinda su aplicación durante su evolución servirán para un mejor desenvolvimiento futuro tomando muy en cuenta los ámbitos de seguridad y privacidad.

2.1.1 Conexión y Protocolos

Antes de que internet de las cosas se convirtiera en una red de dispositivos interconectados, se hablaban de protocolos de automatización de procesos, conocidos también como fieldbuses, que se usaban comúnmente para implementar sistemas extremadamente complejos y difíciles de manejar como por ejemplo SCADA (*Supervisory Control and Data*), donde con el paso del tiempo los sensores y actuadores también crecían en número y su gestión era muy exigente.

Los sistemas SCADA a menudo implican la conexión de PLCs (*Programable Logic Controllers*), PIV (*Proportional Integral-Derivative*), sensores y actuadores todos conectados a través de fieldbuses como se muestra en la figura 2.1, la problemática que presenta ésta tecnología es que no se ha limitado al uso de un solo protocolo ni a un grupo pequeño de protocolos sino que han existido más de cien protocolos que se han aplicado a la automatización industrial durante los últimos 20 años por ejemplo " *EtherCAT, CAN bus, Modbus, BACnet, LonTalk, MTConnect, y ProfiNet"*. El manejo de estos protocolos interconectados en un solo sistema se ha vuelto muy difícil y complejo.

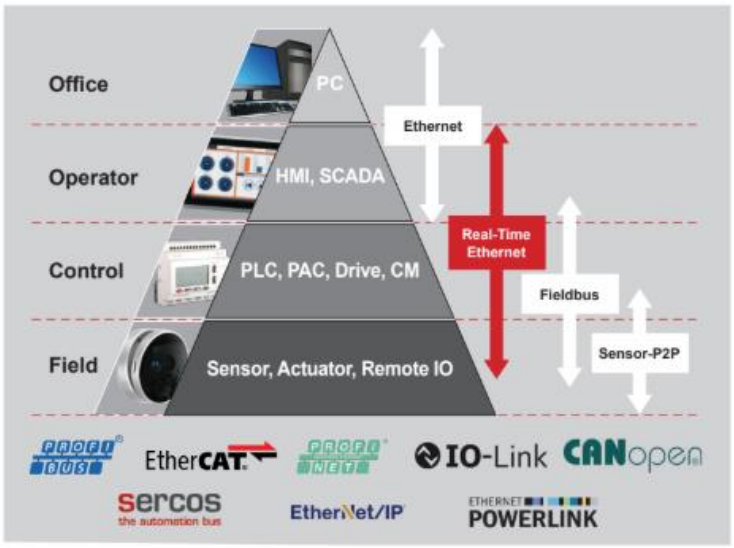


Fig. 2.1.- Pirámide de automatización industrial (Lin, Gurrapu, Manager, & Pearson, 2014).

Con el nacimiento del Internet y de IoT, los protocolos de fieldbus necesitaron conectarse con los protocolos de Internet, para lo cual se reemplazó una capa de fieldbus por una capa IP logrando que IoT se pueda integrar a sistemas que ya existían antes de que aparezca Internet, Por lo tanto, IoT se considera una prolongación de SCADA creando ecosistemas y soluciones con mayor complejidad.

2.1.2 Acontecimientos históricos

A continuación se mostrarán cronológicamente acontecimientos tecnológicos que dan paso en cierto momento a la aplicación del internet de las cosas y que sirven de base para el funcionamiento y buen desenvolvimiento de redes IoT.

En 1926 Nikola Tesla presentó sus trabajos teóricos sobre las comunicaciones inalámbricas y de radio, estas formaron parte de la base de estas tecnologías.

En 1979 se probó el protocolo de red TCP/IP, protocolo base para Internet y la comunicación entre computadoras.

Kevin Ashton cofundador del MIT (*Massachusetts Institute Tecnology*) en 1999, describió el concepto del internet de las cosas IoT (*Internet of Things*). Ashton empieza el camino de Arduino con fines de apoyo en el aprendizaje de estudiantes.

En 2006 la empresa francesa Violet comercializa el Nabaztag (liebre en armenio), trata de un pequeño conejo que se conecta a Internet por WiFi y se comunica produciendo mensajes de audio y también puede dar información sobre el clima, el tráfico, mail, etc.

En 2008 un grupo de industrias como Bosch, Ericsson, Cisco, Motorola, Google, Toshiba o Fujitsu forman una alianza (IPSO Alliance) con el fin de promover el uso del protocolo de Internet en redes de dispositivos inteligentes y hacer posible IoT.

En 2008 inicia el proyecto Pachube para solventar soluciones en la nube para proyectos de internet de las cosas.

En 2011 se realiza el lanzamiento del protocolo IPv6 y se crea la iniciativa IoT-GSI Global Standards para promover la adopción de estándares para IoT a escala global. China invierte e impulsa el desarrollo de Internet de las Cosas con instituciones como Shanghai Institute o la Chinese Academy of Sciences (SorayaPanigua, 2012).

2.2 Evolución de IoT

Internet de las Cosas se ha desarrollado a partir de la convergencia de redes inalámbricas, tecnología de microelectromecánicos (MEMS) e internet. A través de esta convergencia se han acortado las distancias entre la tecnología operacional (OT) y la tecnología de la información (IT) situación clave para el desarrollo de IoT.

La apertura del Internet ha impulsado la industria OT hacia el Internet de las Cosas, mientras que IT ha dado prioridad a la seguridad centrado en la CIA (confidencialidad, integridad y disponibilidad) En la figura 2.2 se muestra la convergencia de los principios de seguridad. (Cheruvu, Kumar, Smith, & Wheeler, 2020a).

Fig. 2.2.- Convergencia IT/OT (Figueras Joan, 2015).

Por otro lado, la evolución del ecosistema de IoT no es tan sencillo, es extremadamente complicado, fragmentado y en evolución, esta evolución depende de varios factores, uno de los cuales es el ciclo de reemplazo para una solución o una industria dada, Por ejemplo, el ciclo de reemplazo para PC es de 3 a 5 años, el reemplazo de teléfonos inteligentes es de 1 a 3 años. En cambio, el reemplazo de un sistema de automatización de un edificio puede ser de 15 a 20 años o el reemplazo de un repuesto de energía nuclear por uno de similares características no puede dejar espacio para la introducción de nuevas tecnologías innovadoras y más seguras.

Internet de las cosas trae consigo una nueva perspectiva, en lugar de utilizar una tecnología existente y extender la conectividad al internet computadoras, teléfonos inteligentes, centro de datos, computación en la nube, computación empresarial para la industria, salud, transporte, infraestructura, hace razonable comprender el impulso que genera la evolución de IoT para implementar un sistema completamente nuevo con generación de aplicaciones únicas para operación por ejemplo de drones, automóviles autónomos, ciudades inteligentes, suministro de energía, automatización de cadenas productivas y aprendizaje autónomo.

Internet de las cosas promueve una nueva forma de internet, una red menos propietario, de menor costo y cada vez menos omnipresente, una tecnología que revolucione la PC, centro de datos y dispositivos móviles de los años 90 y 2000. Además, con los avances tecnológicos, IoT se ha beneficiado también de las innovaciones en microprocesadores, memoria, energía y almacenamiento logrando menores costos en su implementación y plataformas altamente capaces.

2.3 Ecosistema IoT

A medida que los dispositivos y los sectores donde se aplica una tecnología IoT han ido multiplicándose, la forma que cada sector adopta la tecnología también es diferente, el tratamiento de sus datos, algunos los hacen en silos, es decir, datos propietarios de las empresas o sectores definidos en parte por los requisitos técnicos únicos de sus usos y aplicaciones como lo hace M2M donde se despliegan cadenas de sensores que se pueden monitorizar. Por otro lado, los datos generados por IoT son datos abiertos desconociendo quien va a encontrar el valor de esos datos, esto no significa que los datos sean públicos, significa que los datos generados por sensores están abiertos para ser utilizados en otros contextos.

En referencia a la figura 2.3, un ecosistema IoT puede entenderse como una plataforma tecnológica que se utiliza para conectar distribución física y componentes lógicos, la tecnología dentro de un ecosistema es especializado para dicho ecosistema así como también sus componentes son especializados para diferentes aplicaciones resultando dispositivos

únicos para la operación, control, recopilación y análisis de datos, por esta razón es necesario explorar los múltiples segmentos y sectores de IoT ya que usar una sola tecnología parece ser imposible(Cheruvu et al., 2020a).

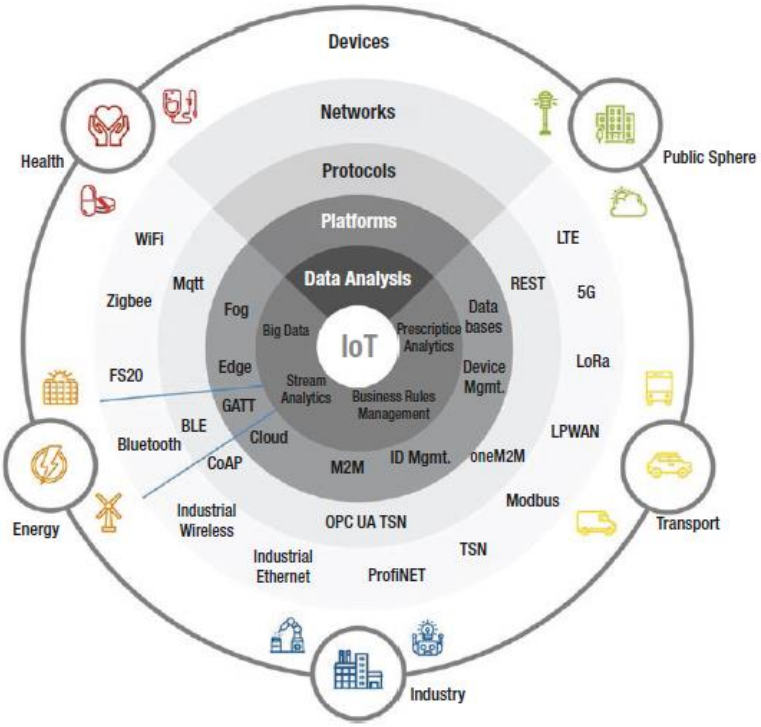


Fig. 2.3.- Ecosistema IoT (Cheruvu, Kumar, Smith, & Wheeler, 2020b)

Los sistemas IoT han ingresado con mucha fuerza en sectores empresariales, aumentando el potencial y el crecimiento de su ecosistema. Por lo tanto, si las soluciones de IoT consiguen dar valor agregado a las empresas y a la industria en general, la demanda de dispositivos IoT crecerá aceleradamente dando cada vez más beneficios a los usuarios.

En la figura 2.4 se muestran los elementos de un ecosistema de IoT, este consiste en la conexión de dispositivos inteligentes a internet. Además, tienen la capacidad de adquirir y transmitir datos generados de sus entornos. Los dispositivos IoT luego se conectan a una puerta de enlace (*Gateway*) para que los datos puedan ser enviados a la nube y ser procesarlos y analizados. A pesar de que los dispositivos IoT pueden realizan sus trabajos solos, los usuarios interactúan con ellos para configurarlos, darles órdenes o acceder a su información.

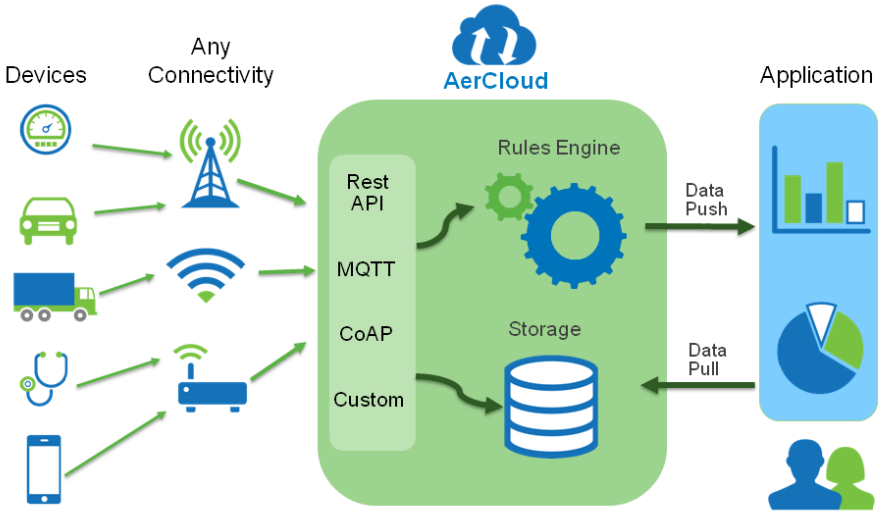


Fig. 2.4. Elementos del Ecosistema IoT(Amazon, 2017)

Los sectores donde ha ganado dominio de aplicación las redes IoT y donde su ecosistema ha impulsado y ha dado ventajas son:

2.3.1 La salud

El IoT tiene números usos en el campo de la medicina por ejemplo incorporar una red de apoyo emocional, incorporar marcos de información basados en IoT, uso de sensores WIFI para monitoreo de elementos imperativos del cuerpo como son temperatura, pulso, frecuencia cardiaca, niveles de colesterol, etc. Las aplicaciones de IoT aportan enormemente al bienestar de las personas sin asistencia personal transmitiendo alarmas en caso de emergencias.

2.3.2 Redes de Suministro y Logística

La aplicación de IoT en la administración de una red minorista, venta, coordinación e inventario tiene sus propios puntos particulares de interés. Estantes inteligentes pueden rastrear los artículos presentes, las existencias pueden ser monitoreadas por etiquetas de radio frecuencia (RFID) para alertar al propietario de la tienda cuando hacer nuevas adquisiciones, esto garantiza tener los artículos a tiempo para el cliente final, además, se pueden medir las

condiciones de almacenamiento, mantenimiento y transporte para ofrecer también artículos de calidad.

2.3.3 Transporte

IoT ofrece varios arreglos a las necesidades encontradas en transporte, Cobros de peajes, inspección de viajeros, requisitos de seguridad para encomiendas, seguimiento de equipaje en aviones son algunas de las aplicaciones de IoT en transporte. Los avances de RFID brindan información constante de partes técnicas en el ensamblaje de autos así también el peso de las llantas y aplicaciones que detectan acciones en los conductores.

2.3.4 Medioambiente

El uso de dispositivos remotos está creciendo en aplicaciones ecológicas para salvaguardar el medio ambiente, monitoreo de incendios, movimientos sísmicos y la contaminación son algunos ejemplos donde IoT reduce el impacto de desastres naturales. Por otro lado el monitoreo de derrames de petróleo y gas disminuirá el riesgo de contaminación de áreas naturales y protegidas. En caso de la aparición de una enfermedad o desastre natural como una inundación, aporta con la identificación de personas y animales resulta beneficioso el uso de etiquetas RFID.

2.3.5 Agricultura

Para mejorar la eficiencia en el campo de la agricultura existe la necesidad de automatizar los procesos y planificación inteligente que pueden funcionar con la adopción de tecnología TIC, como sitios web, teléfonos móviles, marcos de rutas satelitales y computación distribuida aportarán a una era rural automatizada. La aplicación de etiquetas RFID aporta al monitoreo ambiental que afecta directamente a la agricultura, con la recopilación de datos se puede determinar áreas agrícolas y rendimiento de éstas.

2.3.6 Educación

El Internet de las cosas en el entorno educativo hace posible la implementación de nuevos métodos de enseñanza, Las ventajas de hacer uso de esta tecnología son muchas como mejorar el aprendizaje, impulsar las habilidades de los jóvenes, dinamizar las tareas entre otras. Además, a nivel de los campus se puede mejorar la eficiencia operacional, toma de decisiones y seguridad física.

2.3.7 Telecomunicaciones

IoT tiene la capacidad y mayor probabilidad de combinar diversos avances tecnológicos, tales como el Sistema Global para Comunicaciones Móviles (GSM), Comunicaciones de Campo Cercano (NFC), Bluetooth, Sistemas de Posicionamiento Global (GPS), Sistemas de Sensores, etc.

2.3.8 Seguridad

La aplicación de redes IoT en el sector de la seguridad permite descubrir de manera temprana riesgos que afectan a las personas, por ejemplo, protección a los vehículos, la utilización de grabadoras electrónicas en vehículos puede registrar la velocidad y respaldar los datos para evaluar el peligro, utilizar tecnología GPS permite combatir el robo de vehículos, bicicletas, motocicletas, etc. El uso de sensores también previene riesgos como son fugas de agua o presencia de fuego, los reclamos de tuberías dañadas o fugas de agua pueden ser atendidas a tiempo mediante un SMS a los propietarios y programar el cierre de válvulas si es necesario.

2.3.9 Smart home

Debido a la gran cantidad de objetos del hogar que se pueden controlar de forma remota su aplicación es extensa, la combinación de domótica e IoT han hecho posible la creación de Smart home, las personas están cada vez más interesadas en llevar su vivienda a otro nivel de comodidad, ahorro, seguridad y respeto por el medio ambiente. Google, Cortana, Siri, Alexa o Bixby son algunos de los asistentes de hogar más usados para el control inteligente

de viviendas, además, también se han sumado operadoras como Orange que tienen experiencia en protocolos de comunicaciones, datos y clientes.

2.4 Fases del Sistema IoT

En la figura 2.5 se muestra las cinco fases que el sistema IoT requiere, desde la recopilación de datos de los objetos hasta la entrega de datos al usuario final.

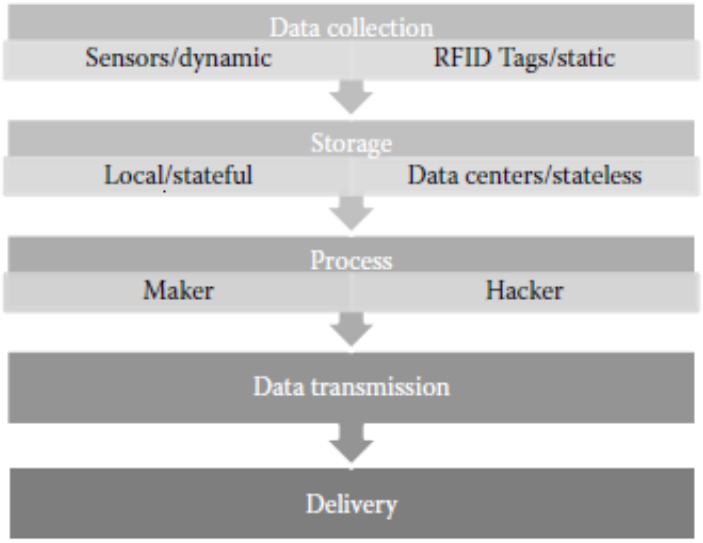


Fig. 2.5. Fases del Sistema IoT (Hu, 2016)

2.4.1 Fase 1. Recopilación de datos, adquisición, percepción

El paso más importante es la recolección o adquisición de datos de los dispositivos u objetos, dependiendo de las características de los objetos se utilizan diferentes recolectores de datos por ejemplo de etiquetas RFID o de sensores y de chips.

2.4.2 Fase 2: Almacenamiento

Los datos recopilados deben ser agrupados y almacenados, los dispositivos IoT generalmente no poseen una alta capacidad de memoria y de procesamiento, por tal motivo esta responsabilidad es asumida por la nube.

2.4.3 Fase 3: Procesamiento inteligente

El sistema IoT analiza los datos almacenados en los data center de la nube y proporciona servicios inteligentes tanto para ambientes de trabajo como para ambientes de la vida diaria en tiempo real. IoT se encarga de brindar varios servicios inteligentes para procesamiento y control para todos los objetos dentro del sistema.

2.4.4 Fase 4: Transmisión de Datos

El proceso de transmisión de datos ocurre desde:

- Desde sensores, actuadores y chips hasta los data center.
- Desde los Data Center hasta las unidades de procesamiento.
- Desde procesadores hasta usuarios finales.

2.4.5 Fase 5: Entrega

La entrega de datos a tiempo y sin errores a los usuarios finales es una tarea delicada de IoT que siempre debe llevarse a cabo (Hu, 2016).

2.5 Arquitectura IoT

En la figura 2.6 se describen los elementos de un sistema IoT centrado en 3 aspectos importantes, arquitectura del dispositivo, arquitectura de red y arquitectura de gestión.

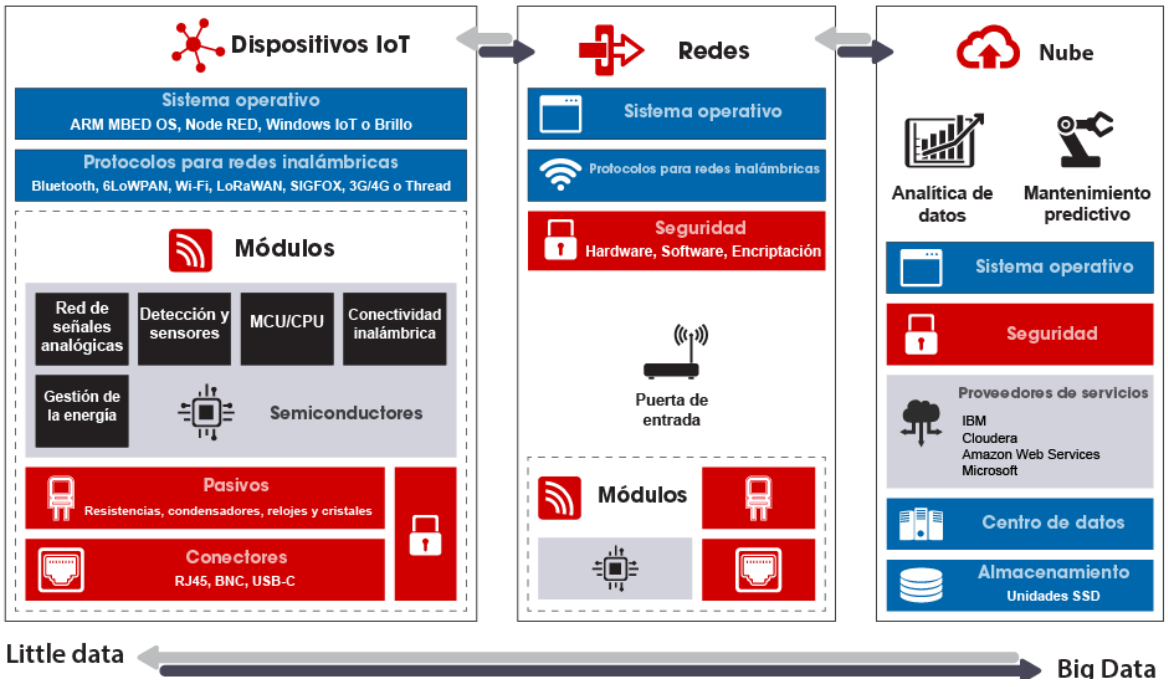


Fig. 2.6.- Arquitectura IoT (RS Components, 2019)

2.5.1 Dispositivo IoT

El término dispositivo por si sólo puede significar diferentes cosas, si se lo describe desde una perspectiva de fabricación el dispositivo es un componente físico que se compone de hardware, firmware y software del sistema, cuando se lo ve desde una visión de gestión de red, un dispositivo IoT funciona como un nodo que tiene una dirección de red y podría ser parte de varios dispositivos interconectados y cuando vemos desde una perspectiva en un marco de IoT, un dispositivo es un contexto lógico que expone interfaces de paso de mensajes, las interfaces se utilizan para intercambiar datos estructurados de acuerdo con una definición de interfaz.

Puede decirse que la capa dispositivos IoT es la interfaz entre lo físico y lo virtual, por ejemplo, existen dispositivos u objetos como un termómetro inteligente con un único sensor utilizado para comunicar la temperatura ambiental, o dispositivos complejos que poseen una capacidad de procesamiento mayor y que funcionan como intermediarios con la interfaz de red conocido como Gateway.

2.5.1.1 *Interoperabilidad*

El uso de dispositivos que sean interoperables con otros dispositivos o infraestructuras es de suma importancia para IoT, en especial cuando la variedad de dispositivos es enorme en grandes sistemas IoT, las validaciones basadas en la web permiten a los proveedores verificar que sus productos puedan interoperar con protocolos y estándares asegurando la compatibilidad con dispositivos de otros proveedores y se puedan integrar dentro de diferentes plataformas IoT.

2.5.1.2 *Escalabilidad*

Como se mencionó anteriormente la integración de dispositivos IoT a plataformas puede ser muy común, por lo tanto, estas plataformas deben tener una alta capacidad de escalabilidad y ser capaz de soportar un gran número de dispositivos IoT, que envían, reciben y actúan sobre datos constantemente, esta escalabilidad debe ser elástica tanto en software como en hardware y no debe obstaculizar el rendimiento de los dispositivos.

2.5.2 Red de IoT

Cuando varios dispositivos IoT están conectados entre sí forman una red IoT, los dispositivos dentro de esta conexión deben tener la capacidad de interoperar en una aplicación distribuida, para que ocurra esto los dispositivos necesitan cumplir algunos comportamientos básicos:

- Capacidad de descubrir nodos pares, funciones e interfaces.
- Habilidad para conexión, implica autenticar y construir un canal seguro o asociación criptográfica.
- Capacidad de enviar y recibir datos, analizarlos y procesarlos de acuerdo con la aplicación específica.

La red y la conectividad son muy importantes para IoT, los sistemas deben estar habilitados para conexiones de cortas, medianas y largas distancias, además se deben considerar características como son las perturbaciones ambientales e interferencias o emisiones de otros equipos de baja potencia que no garanticen la calidad de servicio.

Para abordar las necesidades multifacéticas de IoT han surgido variedad de tecnologías de red como, por ejemplo: *Zigbee, Industrial Ethernet, LoRa, LPWAN, Modbus y TSN* entre otros, algunos de estos altamente especializados para aplicaciones específicas como las redes de área de control (CAN), que cubre de forma exclusiva los problemas críticos de seguridad automatizados. Mientras que otros no tan especializados son de uso más general como *WiFi, Bluetooth, 5G y Ethernet.*

2.5.3 Gestión de IoT

La gestión de sistemas IoT se encarga del correcto funcionamiento del sistema para lo que brinda varias herramientas que permiten al usuario y al operador controlar y observar el comportamiento de dicho sistema. El *cloud* (nube) brinda varias funciones relacionadas con la visualización y analítica que operan sobre datos generados por objetos y que los procesa de acuerdo con los objetivos y necesidades que requieren los sistemas IoT, ofrece funciones de seguridad, almacenamiento y mantenimiento que aportan a la administración y finalmente ofrece un dominio de tiempo de ejecución y una disposición de API (*Application Programming Interface*) para que los operadores ensamblen varios modelos de programación y protocolos (Hu, 2016).

2.6 Seguridad y Privacidad IoT

La conexión e información de IoT es una tendencia generalizada que lo transforma todo, desde ciudades inteligentes y hogares hasta la industria 4.0, empresas, infraestructuras críticas, salud, comercio minorista, etc. Grandes flujos de datos son procesados utilizando algoritmos de aprendizaje autónomo que están alterando la existencia y la calidad de vida. Esta escala de omnipresencia e interconectividad crea un entorno donde la seguridad, privacidad e integridad de estas aplicaciones se convierten en una preocupación primordial, ataques a infraestructuras críticas como la generación y distribución de energía, vulnerabilidades en nuestros automóviles y *malware* en dispositivos como cámaras web,

teléfonos inteligentes y PC de nuestros hogares, demuestran la vulnerabilidad colectiva provocada por atacantes y donde IoT crea un conjunto de desafíos de seguridad.

En este mundo en expansión de IoT, la seguridad se vuelve crítica cuando se conectan miles de millones de dispositivos nuevos y otros previamente desconectados, la seguridad es una parte vital cuando los ataques se expanden de formas complejas y profundas. Según datos de NVD (*National Vulnerability Database)* perteneciente a *CVSS (Severity Distribution Over Time)*, muestra que durante los años 2016 – 2018 el número de vulnerabilidades con severidad media se triplicó, aquellas con severidad alta se duplicó y el total de vulnerabilidades casi se triplicaron en dispositivos *Gateway* y dispositivos IoT.

No es suficiente simplemente conectar dispositivos IoT sino que es preciso que estos dispositivos se autentiquen mutuamente y se autoricen servicios, es imperativo tener seguridad de extremo a extremo, incluyendo cada elemento a lo largo de las rutas de datos y control desde el sensor y el actuador, hasta el borde y el *Gateway* y todo el trayecto hasta la nube, protegiendo tanto los dispositivos como los datos, interfaces y software asociados.

Con la implementación de redes IPv6 y 5G, millones de cosas heterogéneas pasarán a formar parte del Internet de las cosas, la seguridad y privacidad serán los factores de preocupación en un marco IoT vulnerable frente a todo tipo de ataques y amenazas, para esto los problemas de seguridad se han diferenciado en tres dimensiones, según la fase, la arquitectura y los componentes (Hu, 2016).

2.6.1 Ataques de fase de adquisición

En la figura 2.7 se muestran tipos de ataques que se presentan en las 5 fases de IoT, las principales amenazas de seguridad en las distintas fases son: fuga de datos, soberanía, violación y la autenticación(Hu, 2016).

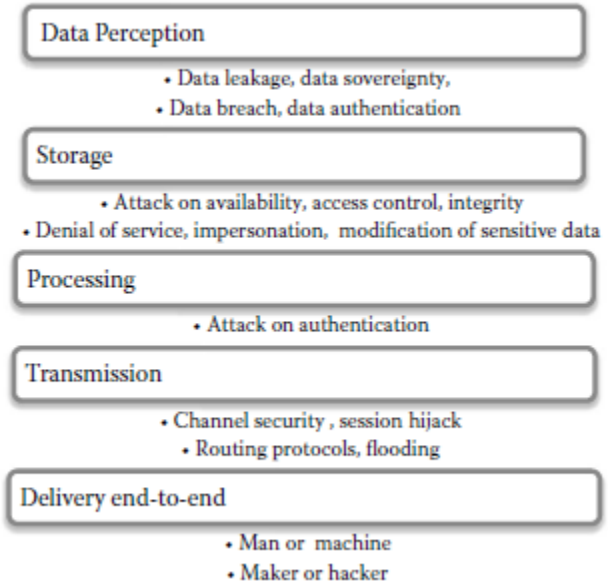


Fig. 2.7.- Ataques en fases (Hu, 2016).

2.6.1.1 *Fuga o violación de datos*

La exportación de datos o información no autorizada a un destino no deseado es fuga de datos, esta exportación suele ser realizada por empleados deshonestos o insatisfechos de una organización, la fuga de datos es una amenaza seria a la fiabilidad. También los datos que se encuentran en la nube están expuestos a esta amenaza, a medida que los datos se mueven de un usuario a otros usuarios en la nube existe un grave riesgo de fuga de datos, la severidad de esta amenaza se puede disminuir con el uso de DLP (*Data Leakege Prevention*).

2.6.1.2 *Soberanía de datos*

El sistema IoT abarca todos los objetos del mundo, los datos almacenados digitalmente deberán cumplir con leyes que protejan la soberanía de los datos del usuario, y que además ofrecen mayores garantías a grandes tecnologías como IoT.

2.6.1.3 *Autenticación de datos*

Los usuarios pueden percibir datos desde cualquier dispositivo (teléfonos inteligentes, *tablets*, etc.) en cualquier lugar y a cualquier momento, estos datos pueden ser forjados por

intrusos convirtiéndose en una amenaza de seguridad, se debe garantizar que los datos percibidos se reciban de forma intencionada y legitima, es obligatorio verificar que los datos no hayan sido alterados durante el tránsito en la red. La autenticación de los datos podría proporcionar integridad y originalidad al usuario final.

2.6.1.4 *Ataque a la disponibilidad*

La disponibilidad es una de las características más importantes para los usuarios de sistemas IoT, un ataque de DDoS (*Distributed Denial of Service*), es una condición de sobrecarga causada por una gran cantidad de atacantes distribuidos, pero esta no es la única condición para que data centers no estén disponibles para los usuarios, también existen otras condiciones que hace que los data centers pierdan disponibilidad y son las siguientes:

- Inundación por atacantes
- Inundación por multitud de usuarios.
- Inundación por suplantación de identidad (*spoofing*).
- Inundación por usuarios legítimos agresivos.

2.6.1.5 *Modificación de datos sensibles*

Los datos obtenidos de los sensores o dispositivos IoT pueden capturarse, modificarse y reenviarse a un nodo deseado, la modificación de los datos puede llevarse a cabo de tres maneras:

- Modificación de contenido, en la que parte de la información puede ser alterada.
- Modificación de secuencia, desordenando los datos entregados haciendo que el mensaje no tenga sentido.
- Modificación de tiempo, que podría provocar un ataque de repetición.

2.6.2 Ataques según la arquitectura

El IoT no se ha limitado a una arquitectura en particular, distintos proveedores y las aplicaciones adoptan su propio modelo de arquitectura. En general, IoT tiene 4 capas básicas, percepción de nivel más bajo o de detección, de red, de transporte y de aplicación. La figura 2.8 muestra además de las capas también las posibles amenazas que se pueden dar en cada una de ellas.

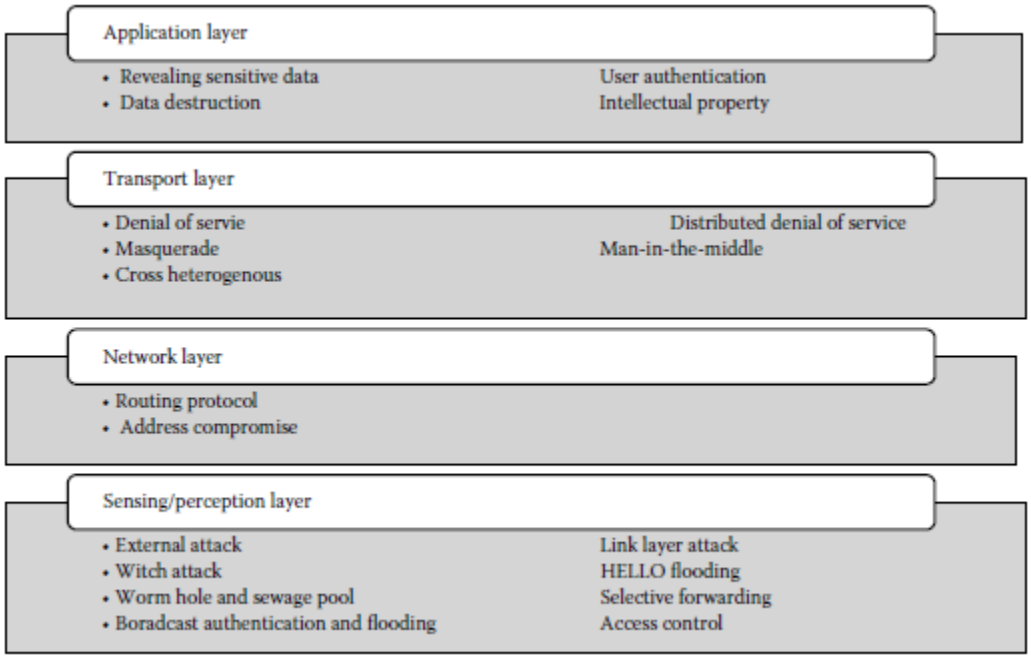


Fig. 2.8.- Posibles ataques basados en la arquitectura (Hu, 2016).

2.6.3 Ataques basados en componentes

Los sistemas IoT conectan todos sus componentes a través de Internet, estos componentes son heterogéneos y comunican datos confidenciales a distancia. Además de atenuación, robo, pérdida, incumplimiento y desastre, los datos también pueden ser fabricados y modificados por sensores manipulados por intrusos. La figura 2.9 muestra los posibles tipos de ataques en el nivel de los componentes.

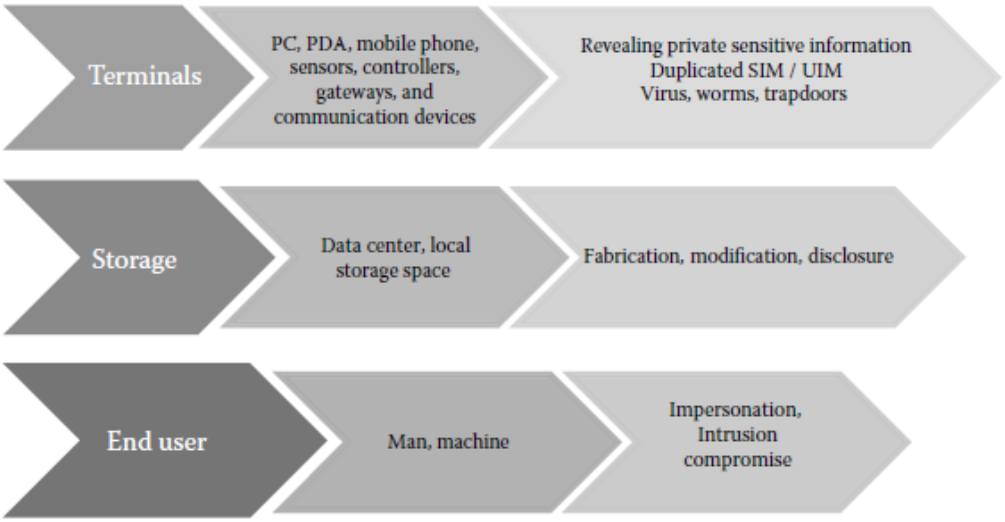


Fig. 2.9.- Posibles ataques basados en componentes (Hu, 2016).

Verificar al usuario final en el nivel de entrada del sistema IoT es obligatorio, distinguir entre humanos y máquinas es extremadamente importante. Diferentes tipos de pruebas de Turing sirven para distinguir a los computadores de los humanos, CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*) ayuda en esta discriminación fundamental (Hu, 2016).

Finalmente podemos decir que los problemas principales aparte de los problemas técnicos de IoT, están relacionados con la privacidad de las personas y la protección de los datos lo que implica desafíos sociales y éticos de IoT que pueden ser monitoreados a través de políticas estrictas, entonces podemos decir que la seguridad y privacidad de IoT se centra en tres aspectos importantes: aspectos éticos, aspectos legales y aspectos sociales que los toparemos más adelante.

2.7 Seguridad IoT en Smart Home

A medida que aumenta el bienestar y los dispositivos tecnológicos se vuelven omnipresentes, las personas aligeran su vida diaria automatizando tareas comunes, la creciente adopción de sistemas de hogares inteligentes SHS (*Smart Home Systems*) lleva a la necesidad no solo de mayor funcionalidad, sino también de un entorno seguro y funcional en este contexto, una área específica que está experimentando un desarrollo tecnológico particular es la domótica para uso personal, Encontrar dispositivos de IoT en el hogar cada vez es más común, con el objetivo de automatizar la iluminación, persianas, calefacción, enfriamiento, cerraduras, entre otros.

2.7.1 Vectores de ataque en SHS

Los posibles vectores de ataque SHS pueden agruparse en 5 categorías de vulnerabilidad como se muestra en la figura 2.10.

- **Servidor:** para la gestión del estado y para proporcionar una interfaz de control o API.
- **Bus:** de comunicación con los dispositivos.
- **Dispositivos de control:** para interactuar con ellos.
- **Dispositivos de usuario:** teléfono inteligente.
- **Servicios remotos:** que amplíen la funcionalidad central del sistema.

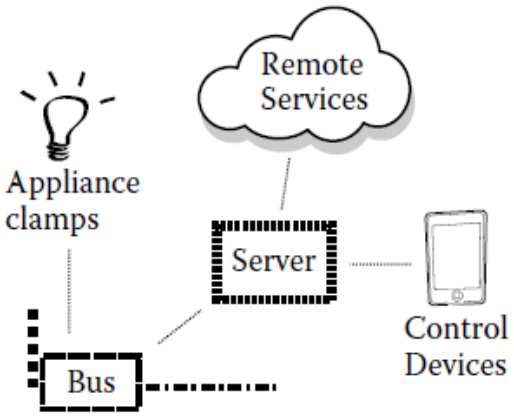


Fig. 2.10.- Las cinco categorías de riesgo (Hu, 2016).

2.7.2 Ciberataques en Smart Home

La eficacia y efectividad en los sistemas de seguridad inteligentes se basa en su conectividad mediante la red, esto provoca que el sistema sea susceptible a ataques de *hackers* o ciberataques. Entre los principales ciberataques a una *Smart Home* se pueden nombrar los siguientes(Mapfre, 2018):

- ***Man-in-the-middle***: Consiste en la colocación de un atacante entre dos dispositivos este atacante puede obstaculizar la transmisión de datos afectando a un tercero.
- **Robo de datos y de identidades**: los datos generados por dispositivos inteligentes pueden proporcionar información personal sensible que es deseada por ciberdelincuentes para ser utilizada en actividades fraudulentas.
- **Secuestro de dispositivos**: Este tipo de ataque es difícil de detectar, el dispositivo secuestrado no cambia su funcionalidad, pero puede llegar a infectar a otros dispositivos con algún tipo de malware.
- **Denegación de servicio**: Es uno de los ataques más populares dentro de las redes de IoT Smart Home, consiste en inhabilitar un dispositivo de forma temporal o indefinida, pero el principal objetivo es reclutarlo para hacerlo parte de una *botnet* para continuar con los ataques de DDoS.

- **Denegación de servicio permanente**: Son ataques similares a los anteriores pero este ataque puede dañar a los dispositivos de una manera grave.

Como conclusión, la gran cantidad de dispositivos conectados provocará importantes ataques a la seguridad de una Smart Home, por tal motivo es imperativo implementar medidas de prevención y seguridad.

CAPITULO III

3. ESTUDIO DE SEGURIDAD Y PRIVACIDAD IOT

3.1 Situación actual Seguridad y Privacidad IoT

El Internet de las cosas conecta a internet tantos dispositivos como puntos de datos, todos deben estar protegidos, debido a su amplio ecosistema la seguridad y la privacidad de IoT son en este momento los principales factores de preocupación.

Debido a la gran cantidad de dispositivos de IoT conectados, los ciberdelincuentes encuentran una superficie de ataque muy extensa, basta con encontrar una vulnerabilidad para cometer algún tipo de delito informático como manipulación de información personal, nombres, números de cuentas bancarias, direcciones, incluso cuentas de redes sociales, es información valiosa para los cibercriminales que pueden beneficiarse económicamente de los datos invadiendo la privacidad de los usuarios.

Desde la perspectiva de la academia o la industria, Internet de las cosas aún no ha alcanzado la madurez en términos de seguridad y privacidad, por esta razón se ha mencionado a IoT como *Internet of Thefts, Internet of Threats, Insecurity of Things, s*on varios los significados que se le han dado a las siglas IoT que querían describir un avance tecnológico (Hu, 2016).

La figura 3.1 muestra el crecimiento del número de dispositivos IoT en el tiempo, así también el número de dispositivos que no son IoT por ejemplo teléfonos inteligentes, *tablets*, Pc, etc. Se observa claramente un crecimiento acelerado desde el año 2015, triplicando su número al año 2020 y casi tres veces más para el año 2025 llegando a 21,5 mil millones de dispositivos para ese año. Mientras que para los dispositivos que no son IoT el crecimiento permanece plano y no tiene mayor crecimiento del número de dispositivos para el año 2025.

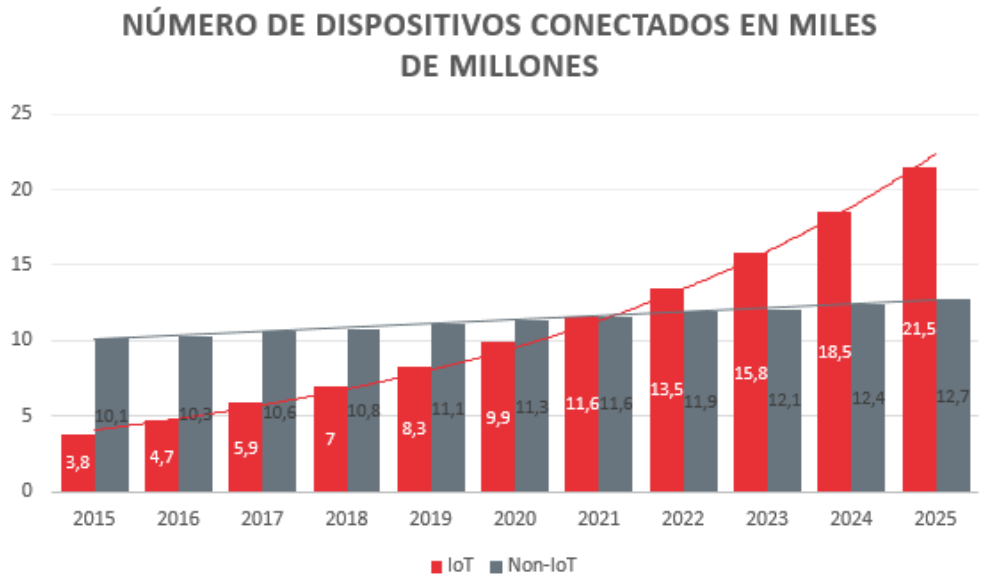


Fig. 3.1.- Estadística de dispositivos IoT en el tiempo(Lasse Lueth, 2018)

La cantidad de dispositivos conectados equivale a más o menos 4 dispositivos por habitante en el planeta y si suponemos un porcentaje bajo tuviese vulnerabilidades, de todas maneras serían mucha la cantidad de dispositivos comprometidos a nivel mundial.

Para nombrar algunos de los casos de ataques realizados a través de IoT, se puede nombrar a *Stuxnet* cuyo objetivo era espiar y reprogramar los sistemas industriales SCADA, otro ataque muy conocido es el de la Botnet Mirai cuyo código ha sido infectado y que de forma remota se puede realizar diferentes ataques como envío de correos basura y ataques de DDoS.

Además, de las vulnerabilidades que presentan los dispositivos IoT, también los servidores con los que tienen comunicación adolecen de seguridad provocando mayores riesgos a la infraestructura IoT(Catalunya, 2018). A pesar de que la industria ha invertido más en seguridad las consecuencias todavía pueden ser desastrosas, el desarrollo de nuevas Botnets como Omni, VPN Filter, Sora, Wicked, Pure Masuta y OMG justifican la necesidad de mayor seguridad y privacidad en los dispositivos IoT(Zedadra et al., 2019).

3.2 Estudio de arquitecturas IoT

La funcionalidad del ecosistema IoT depende de un modelo de arquitectura funcional, exploraremos varias arquitecturas destacando similitudes y diferencias ya que diferentes arquitecturas tienen la intención de abordar diferentes requisitos y casos de uso y otros que tienen capacidades similares que abordan mismos requisitos pero lo hacen de diferente manera. Esto causa varios problemas de incompatibilidad, estas diferencias entre arquitecturas puede no ser dañino cuando trabajan de forma aislada pero agregan una complejidad cuando se implementan en múltiples sistemas.

3.2.1 Arquitectura IoTWF

El IoT *World Forum* (WF) propone un modelo que se compone de siete capas, modelo técnico en el que se asignan actividades precisas a cada capa o transversalmente.

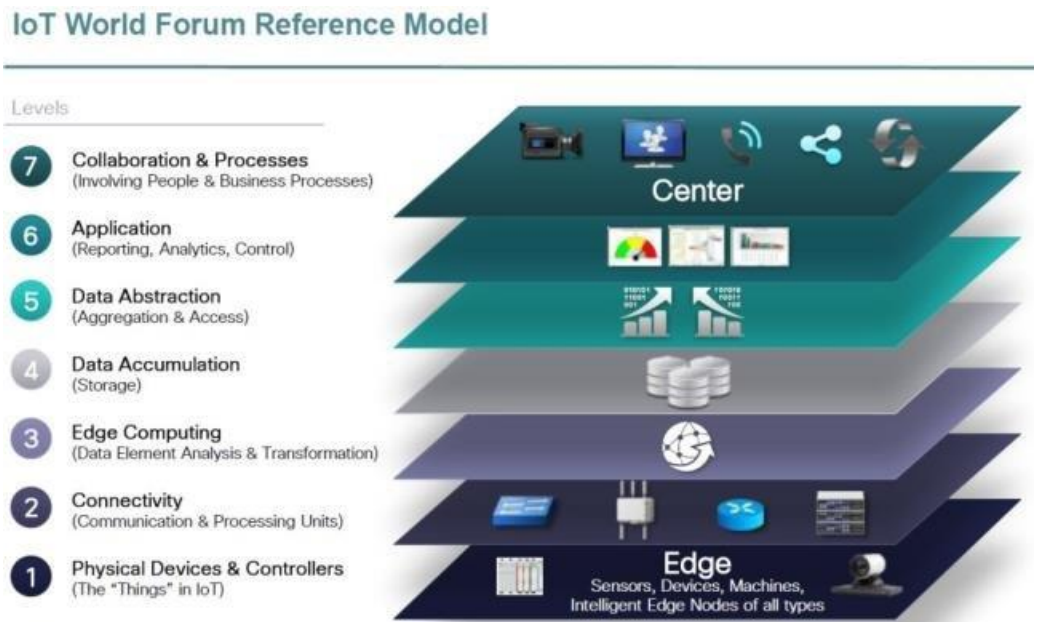


Fig. 3.2.- IoT World Forum Reference Model (Hamed El Hakim, 2018)

En este modelo de arquitectura, los datos son transmitidos, normalizados y filtrados usando *edge computing* para su análisis y transformación, después, esta será almacenada y se pondrá

a disposición de las aplicaciones las cuales se encargan de procesar la información para que los usuarios finales puedan interactuar con ellos.

Como se muestra en la Figura 3.2, la arquitectura IoTWF centraliza el flujo de información desde los dispositivos, maneja características de interoperabilidad e integración con las personas y las empresas.

En la tabla 3.1 se describen las funciones de cada capa de la arquitectura IoTWF.

Capa	Funciones
Capa 1, Dispositivos físicos y controladores	Todos los dispositivos de diferentes tamaños lo cuales pueden enviar o recibir información.
Capa 2, Conectividad	Es la encargada de transmitir los datos en el medio deseado, swicth, router, comunicación con la capa 1.
Capa 3, Edge Computing	Transformar los datos antes de su disposición final de almacenamiento.
Capa 4, Almacenamiento de Datos	Almacenar toda la información generada.
Capa 5, Abstracción de datos	Darles forma a los datos generados
Capa 6, Aplicación	Aplicaciones para análisis de datos, reportes y monitoreo.
Capa 7, Procesos y Colaboración	Son los procesos de negocio, es decir, la interacción que se da con entre IoT personas y negocios.

Tabla. 3.1.- Capas y Funciones Modelo IoTWF (Hamed El Hakim, 2018).

3.2.2 Arquitectura ITU

En la figura 3.3 se muestra la arquitectura recomendada por la ITU (*International Telecommunication Union*), se compone de cuatro capas: de dispositivo, de red, de apoyo a servicios y aplicaciones y aplicación, además consta de dos módulos transversales: el módulo de gestión y el módulo de seguridad(Salazar & Silvestre, 2014).

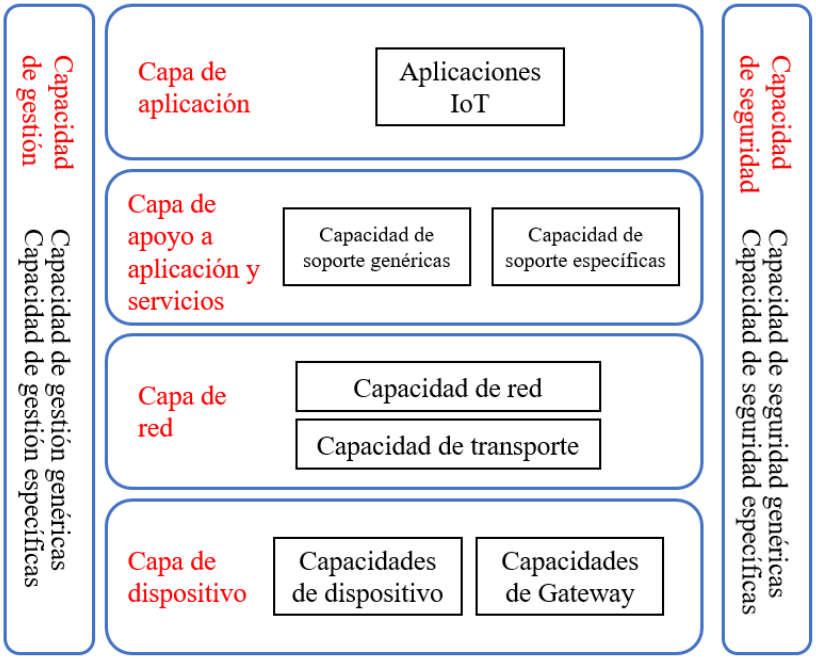


Fig. 3.3.- Modelos de arquitectura de referencia de IoT ITU (Jesús, 2017).

Profundizando en los módulos de seguridad y de gestión se encuentran capacidades que se describen a continuación:

3.2.2.1 *Módulo de gestión:*

Capa transversal encargada de la gestión de dispositivos, diagnóstico, actualizaciones y activación y desactivación de forma remota. Además de la topología y tráfico de la red.

3.2.2.2 *Módulo de seguridad:*

Capa transversal encargada de la autenticación y autorización de dispositivos, además de la confidencialidad, privacidad, integridad, auditorias, antivirus y protección de datos.

3.2.3 Arquitectura de tres capas

En la figura 3.4 se presenta un modelo de arquitectura menos detallado, con estructura de tres capas que sirve de base para distintos ecosistemas IoT.

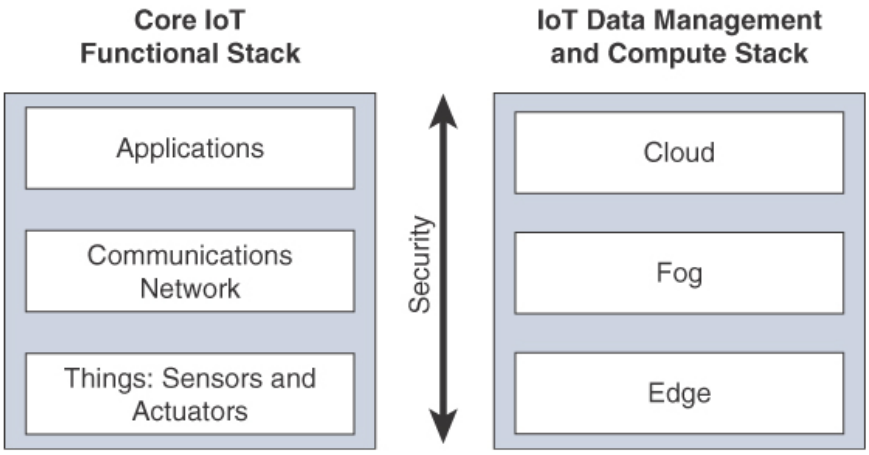


Fig. 3.4.- Arquitectura IoT simplificada (Vélez Andres, 2019).

Este modelo de arquitectura tiene una expansión de sus tres capas principales dividiéndose como se muestra en la figura 3.5, en las subcapas encontramos:

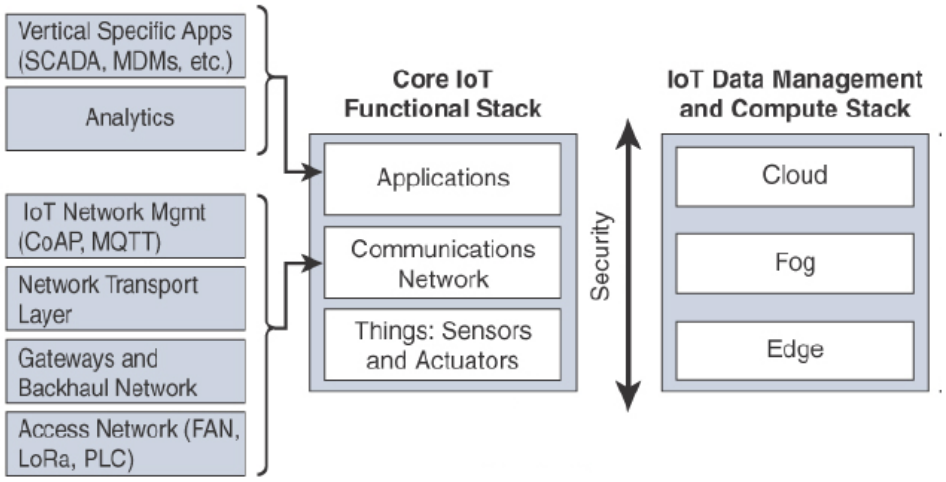


Fig. 3.5.- Arquitectura de tres capas expandida (Vélez Andres, 2019).

- *Access Network*: aquí se realiza la conexión con los sensores.
- *Gateway and Backhaul Network*: Aplicación que recolecta los datos.
- *Network transport*: Capa donde se aplican protocolos TCP/UDP IP.
- IoT *network management*: Mensajeria de datos CoAP y/o Bróker.

- *Aplicaction and analytics*: Capa de análisis y procesamiento aplicaciones para la toma de decisiones(Vélez Andres, 2019b).

3.2.4 Arquitectura IEEE

En la figura 3.6 se muestra otra arquitectura de tres capas muy parecida a la anterior es la que propone un grupo de la IEEE P2413.

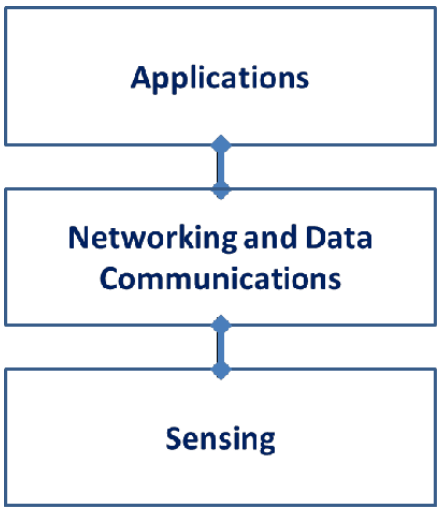


Fig. 3.6.- Arquitectura IEEE tres capas de IoT (Oriwoh & Conrad, 2015).

Los objetivos del grupo de trabajo IEEE P2413 que proponen esta arquitectura son:

- Acelerar el crecimiento del mercado de IoT al permitir la interacción entre dominios y la unificación de la plataforma a través de una mayor compatibilidad del sistema, interoperabilidad e intercambiabilidad funcional.
- Definir un marco de arquitectura IoT que cubra las necesidades arquitectónicas de los diversos dominios de aplicación IoT.
- Aumentar la transparencia de las arquitecturas del sistema para apoyar la evaluación comparativa del sistema, la seguridad y las evaluaciones de seguridad.

- Reducir la fragmentación de la industria y crear una masa crítica de actividades de múltiples partes interesadas en todo el mundo (Oriwoh & Conrad, 2015).

A pesar de que esta arquitectura tiene como fin la protección, seguridad y privacidad. Además, de introducir interoperabilidad y compatibilidad con otros sistemas sigue estando en proceso de investigación.

3.2.5 Análisis y recomendación de una arquitectura IoT

Se han expuesto algunas de las arquitecturas más utilizadas en sistemas IoT, las cuales se pueden clasificar en dos grupos:

Arquitecturas Genéricas

- Modelo ITU.
- Modelo IEEE.

Arquitecturas Comerciales

- Modelo IoTWF.
- Intel IoT (*Platform Reference Architecture).*
- IoT simple.
- IBM IoT.
- Azure IoT.

Todas las arquitecturas mostradas garantizan los siguientes requisitos mínimos:

- Seguridad.
- Interoperabilidad entre dispositivos.
- Análisis.
- Almacenamiento.
- Flexibilidad
- Escalabilidad

- Control de dispositivos(Vélez Andres, 2019b)

Por ahora no existe un modelo de arquitectura IoT que garantice la seguridad de extremo a extremo, solo se puede elegir métodos que permitan una mayor seguridad. Además, estas arquitecturas por si solas no proporcionan buenas prácticas para garantizar la seguridad de los dispositivos IoT.

Para recomendar una arquitectura revisaremos los siguientes requisitos:

- Capa transversal de seguridad.
- Interoperable.
- Administrable.
- Heterogéneo.
- Independiente de un fabricante.
- Compatible con proveedores de plataforma(Vélez Andres, 2019b).

Realizando un análisis de los requisitos mencionados, se puede decir que el modelo ITU es el más adecuado, cumple con los principios de seguridad y garantiza un mínimo riesgo de transferencia de información ya que el modelo va ligado a una tecnología, además, su estructura y su funcionalidad permitirá una implementación mayormente flexible.

3.3 Estudio de los Protocolos de Comunicación IoT

Al igual que las arquitecturas IoT existen también numerosos protocolos de comunicación y mensajería, dentro del ecosistema IoT existe una gran cantidad de fabricantes que cuentan con infraestructura necesaria para implementar IoT, dentro de su hardware existen sistemas operativos o programación embebida que cuentan con dichos protocolos.

En la mayoría de implementaciones, un dispositivo IoT se comunica con un *Gateway* que a la vez se comunica con un controlador o un servicio web, existen varias opciones de *Gateway* algunos tan simples como un dispositivo móvil como un teléfono inteligente que pude comunicarse con un punto final de IoT a través de un protocolo de RF como Bluetooth-LE,

ZigBee o Wi-Fi y otros más poderosos que pueden estar ubicados en centros de datos capaces de admitir distintos protocolos de IoT dedicados o propietarios como por ejemplo MQTT (*Message Queuing Telemetry Transport)* o de comunicaciones REST (*Representational State Transfer)*, para que finalmente la información sea recogida por servicios en la nube o servicios web.

3.3.1 Comunicación IoT Smart Home

Los dispositivos IoT también pueden comunicarse horizontalmente lo que permite interactuar con algunas funciones poderosas, haciendo posible habilitar flujos de trabajo a través de una API con varios tipos de dispositivos IoT. IoT *Smart Home* es un claro ejemplo donde se puede observar esta interacción, al despertar por la mañana su dispositivo portátil transmite una señal de activación a través de la señal Wi-Fi a los dispositivos conectados, la televisión inteligente enciende en su canal de noticias favorito, las persianas se levantan automáticamente, la cafetera se pone en marcha, la ducha se prepara para un baño caliente y su vehículo prende un temporizador para calentarlo antes de salir de casa. Todas las interacciones están habilitadas a través de comunicaciones de dispositivo a dispositivo e ilustran el potencial de la aplicación de IoT en *Smart Home*.

Como se mencionó anteriormente dentro de un dispositivo IoT y su red host se puede utilizar una amplia gama de protocolos para la comunicación y transferencia de mensajes, la selección de una gama apropiada de los protocolos de comunicación y mensajería depende de su aplicación y requisitos de seguridad del sistema, sin embargo, hay protocolos comunes con características valiosas(Russell & Van Duren, 2016).

La figura 3.7 se muestran los protocolos más utilizados por cada capa y que pueden ser aplicados por dispositivos IoT y formar una plataforma de comunicaciones completa.

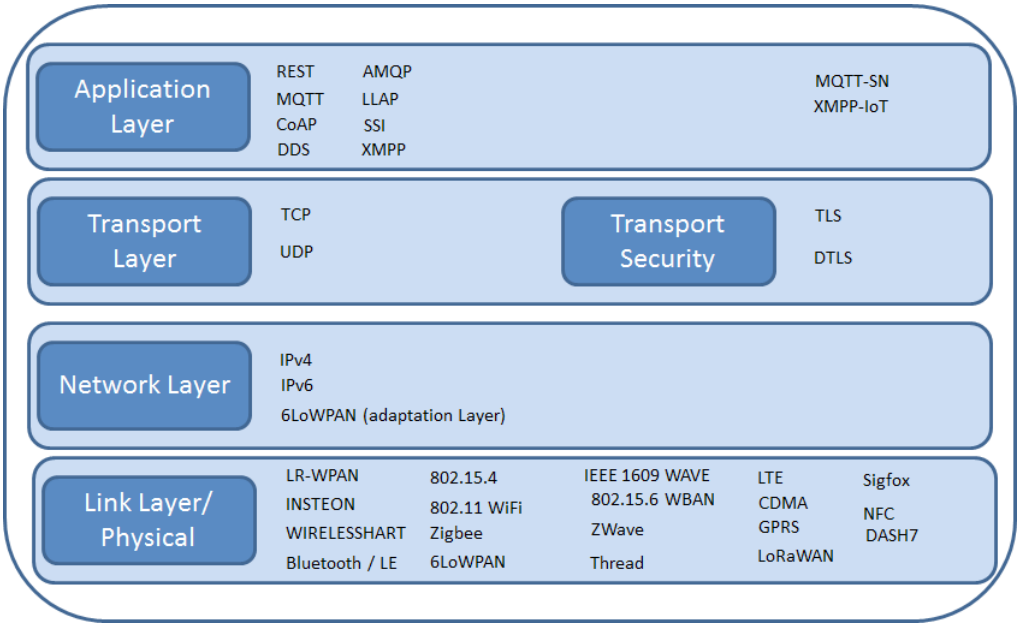


Fig. 3.7.- Protocolos más utilizados por IoT (Russell & Van Duren, 2016).

3.3.2 Descripción de las capas

3.3.2.1 *Capa física*

Corresponde a las tecnologías utilizadas para intercambiar paquetes, en el caso de IoT la capa física se basa en la comunicación inalámbrica, se han especificado varios estándares para esta capa como la serie IEEE 802.11 Wi-Fi y 802.15.

3.3.2.2 *Capa de red*

Esta capa es la encargada de entregar paquetes donde sea necesario, la función de los protocolos de esta capa es abordar, entregar y evitar la congestión.

3.3.2.3 *Capa de transporte*

El propósito de esta capa es permitir que los mensajes partan desde el origen hasta su destino, manteniendo una conversación.

3.3.2.4 *Capa aplicación*

Corresponden los protocolos de servicio específico para la comunicación de datos a nivel de proceso a proceso, el protocolo de aplicación más utilizado para proporcionar servicios web

es HTTP, sin embargo, tiene mucha complejidad computacional y consumo de energía alto para dispositivos IoT.

3.4 Descripción de protocolos por capa

3.4.1 Capa física

3.4.1.1 *Estándar IEEE 802.15.4 y IEEE802.11 WiFi*

El grupo IEEE 802.15 especifica una variedad de WPAN (*wireless personal area network)*, incluidos *Bluetooth*, UWB, BAN entre otros. IEEE 802.15.4 representa el estándar más alto para WPAN de baja velocidad de datos, el objetivo principal es proporcionar una base para que otros protocolos se puedan agregar en capas superiores.

Este protocolo estándar actúa sobre la capa de red física, el consumo de energía y modulación de los datos, es adoptado por varios grupos de desarrollo de objetos y protocolos IoT como *Zigbee Alliance y Thread group.* Este estándar define protocolos de interconexión para la comunicación de datos entre dispositivos de baja velocidad de transferencia (hasta 250 Kb/s), bajo consumo y baja complejidad, usando radiofrecuencia de corto alcance entre 915Mhz y 2.4Ghz hasta 10 metros de distancia.

Por otro lado se encuentra el estándar IEEE 802.11 WiFi, que a pesar de ser una tecnología que trabaja de forma inalámbrica sobre una banda libre, no es empleada en redes WPAN, aunque pueden llegar a interactuar con ellas. Esta tecnología transmite con potencias muy elevadas, esto hace que el estándar no sea el más apropiado para mantener una WPAN, más bien estas tecnologías son complementarias a las WPAN ya que es posible conectar a una WLAN por medio de un interfaz apropiado.

3.4.1.2 *Zigbee*

Conjunto de especificaciones desarrolladas por *Zigbee Alliance* para su uso en *Smart Home* e IoT, define las capas posteriores a las capas establecidas por IEEE 802.15.4 y que ofrecen servicios de seguridad, tolerancia a errores y conexión de nuevos dispositivos.

3.4.1.3 *Thread*

Otro conjunto de especificaciones para uso en *Smart Home* e IoT, al igual que *Zigbee*, *Thread* define las capas que se utilizan sobre el estándar IEEE 802.15.4, sin embargo, no proporciona la capa aplicación. Los estándares de protocolo abierto siempre se utilizan para garantizar la integridad del paquete, utilizando los protocolos UDP y 6LoWPAN. También proporcionan servicios de seguridad y tolerancia a errores.

3.4.2 Capa de Red

3.4.2.1 *6LoWPAN*

Tanto IPv4 como IPv6 juegan un papel importante dentro de muchos sistemas IoT, el protocolo 6LoWPAM (*Low Rate Wireless Personal Área Networks*) da permiso para que los paquetes IPv6 se transmitan en redes de bajo consumo energético, su tarea principal es la compresión de encabezados y de los mensajes enviados reduciendo el tamaño en la transmisión, otras tareas importantes de 6LoWPAN es la fragmentación y la reagrupación de paquetes, así como su distribución dentro de la red.

6LoWPAM se basa en las redes 802.15.4 de menor velocidad, la capa de adaptación proporciona características que incluyen IPv6 con compresión de encabezado UDP y soporte para la fragmentación, permitiendo el uso de sensores restringidos, por ejemplo en automatización y seguridad de casas y edificios. Con 6LoWPAM, los diseñadores pueden aprovechar el cifrado de enlace ofrecido dentro del IEEE 802.15.4 pero también puede aplicar la capa de transporte cifrado como DTLS (Russell & Van Duren, 2016).

3.4.3 Capa de Transporte

3.4.3.1 *TCP/UDP*

TCP (Transmission Control Protocol): Protocolo para las comunicaciones actuales basadas en la web como el transporte subyacente y confiable, algunos dispositivos IoT han sido diseñados para operar utilizando TCP aquellos lo suficientemente robustos y que puedan

hablar HTTP o MQTT a través de una conexión segura, a menudo su uso no es adecuado en redes que sufren alta latencia y limitado ancho de banda.

UDP (User Datagram Protocol) es una alternativa útil, proporciona un mecanismo de trasporte ligero para comunicaciones sin conexión, muchos dispositivos de sensores IoT altamente restringidos son compatibles con UDP, por ejemplo, protocolos como MQTT-SN versión personalizada de MQTT funciona con UDP, al igual que CoAP también está diseñado para funcionar bien con UDP, entre otros.

3.4.4 Capa aplicación

Los dispositivos IoT deben enviar sus datos a un servidor que funciona como cliente, los mensajes se envían directamente mediante protocolos estándar o mediante intermediarios como agentes de mensajería, la mayor parte de la información se concentra en el uso de un sistema de colas. Protocolos como MQTT (*Message Queue Server Telemetry Transport), CoAP* (*Constrained Application Protocol), DDS (Data Distribution Service), AMQP (Advanced Message Queuing Protocol),* y XMPP (*Extensible Messaging and Presence Protocol),* proporcionan la capacidad tanto para los clientes como para los servidores acuerden eficientemente el intercambio de datos dentro de sistemas IoT.

Dos protocolos emergentes en el mundo de IoT son MQTT y CoAP, ambos tienen características de bajo consumo ya que tiene mensajes pequeños, administrador de mensajes y pequeña sobrecarga, ideal para usarlos en dispositivos integrados. El protocolo MQTT a pesar de su antigüedad ha ganado fuerza con la llegada de IoT, mientras que CoAP fue desarrollado específicamente para IoT (Russell & Van Duren, 2016).

3.4.4.1 *MQTT*

En la figura 3.8 se muestra el funcionamiento del protocolo más usado de mensajería en IoT, es un modelo de publicación/suscripción el dispositivo es el publicador y quien recibe el mensaje es el suscriptor y necesita de un bróker MQTT para administrar y rotar mensajes dentro de la red, una de las ventajas más importantes de MQTT es la eficiencia energética del modelo pub/sub que también escala muy bien y viene equipado con seguridad de red.

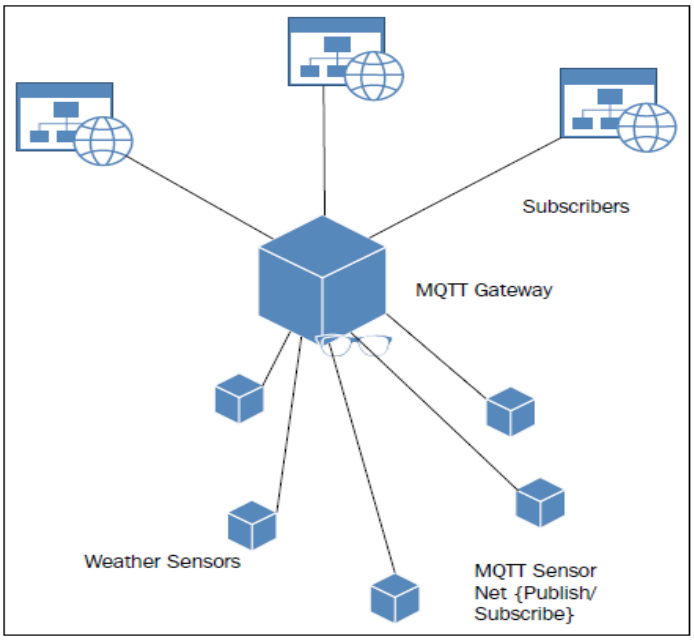


Fig. 3.8.- Modelo del protocolo MQTT (Russell & Van Duren, 2016)

3.4.4.2 *CoAP*

En la figura 3.9 se muestra al siguiente protocolo para IoT basado en UDP y destinado a ser utilizado en dispositivos de internet con recursos limitados, a diferencia de MQTT CoAP nació para satisfacer la necesidad de protocolo IoT, desarrollado para interoperar con arquitecturas HTTP y RESTful volviéndose compatible con internet. Al usar el protocolo UDP, CoAP presenta menor consumo computacional y de energía, su uso permite un menor tiempo de respuesta cuando se activa, ya que mantiene una conexión activa entre nodos convirtiéndose en el protocolo más adecuado para enviar comandos a nodos locales.

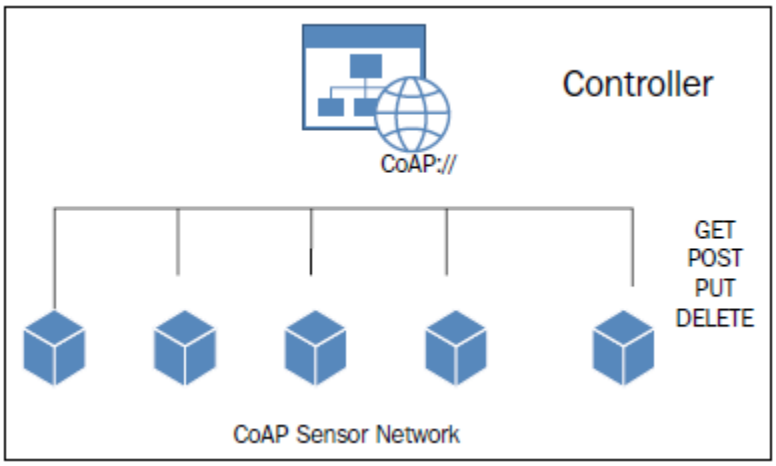


Fig. 3.9.- Modelo protocolo CoAP (Russell & Van Duren, 2016)

3.5 Seguridad y Privacidad del Ecosistema IoT Smart Home

La disponibilidad y diversidad de dispositivos IoT en *Smart Home* y su rápido crecimiento está revolucionando la forma de interactuar con espacios en el hogar. Sin embargo, las casas que tienden a usar más dispositivos IoT también tienden a plantear un mayor número de importantes problemas de seguridad y privacidad de información.

Las vulnerabilidades dentro de entornos domésticos inteligentes se encuentran presentes, estas normalmente son consideradas cuando se tratan de infraestructuras más grandes dando poca atención a la privacidad personal e información sensible creada dentro de una *Smart Home*. Así la multitud de *Smart Homes* interconectadas se convertirá en una plataforma adecuada para realizar actividades delictivas, violaciones de privacidad y otro ciberataques que da como resultado inseguridad para los usuarios de estos espacios inteligentes.

Ahora las personas están generando mayor cantidad de datos sin tener conciencia de sus acciones y sus consecuencias, sin importar la cantidad de dispositivos conectados en los hogares se generan grandes cantidades de datos personales que cuando se exponen a los proveedores de servicios (ISP) u otros servicios de terceros se convierte en una amenaza de vulnerabilidad a las personas y a otras partes involucradas de tipo legal y ético.

Por otro lado los contenidos, patrones y metadatos del tráfico de red pueden revelar información confidencial sobre la actividad de un usuario. Los sensores siempre activos de una *Smart Home* transmiten información sobre las actividades de un usuario sin necesidad de conexión a internet, todo esto hace que los dispositivos IoT en *Smart Home* sean vulnerables a nivel del mismo dispositivo doméstico o a nivel de su conexión como pueden ser espías de WiFi (Hu, 2016).

3.5.1 Dispositivo doméstico inteligente

Por ahora no existe un dispositivo en la red o en entornos inteligentes IoT protegidos contra piratería o infección de algún tipo de malware, dispositivos poderosos IoT controlan y monitorean dichos entornos conectados pero así mismo como estos dispositivos brindan mayores características y funcionalidades también presentan nuevos riesgos.

Por lo tanto, cualquier dispositivo diseñado para uso doméstico y que esté conectado a internet es definido como "dispositivo doméstico inteligente", por ejemplo: termostato, tomacorriente, cafetera, cerradura, etc. O un dispositivo de tipo *hub* (concentrador) que conecta y controla dispositivos de un solo propósito como por ejemplo: *Samsung Smart Things Hub* (Figura 3.10), *Amazon Echo*, etc. Interactuar con un dispositivo doméstico inteligente o vivir dentro del ambiente de una Smart Home hace que los dispositivos se comuniquen con servidores remotos como un ISP (Proveedor de Servicios de Internet) que interactúan como observadores pasivos del tráfico y que pueden inferir en el comportamiento del usuario frente a esta preocupación.

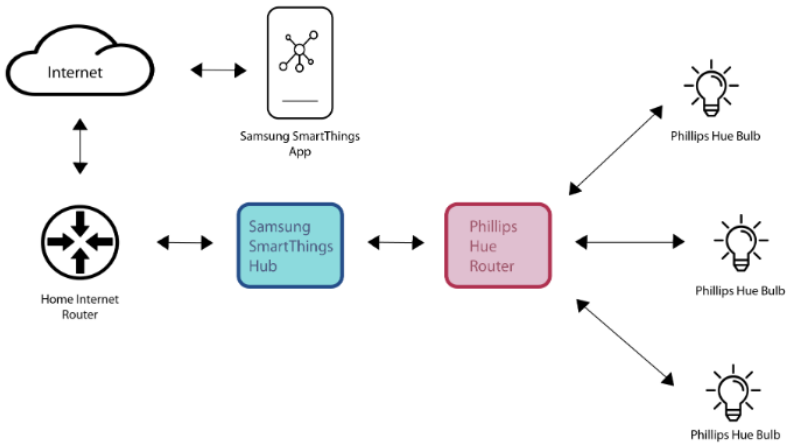


Fig. 3.10 Arquitectura Samsung Smart Home(Ramos, 2018)

3.5.2 Entorno IoT en Smart Home

Para estudiar los problemas de seguridad en profundidad se debe revisar el ecosistema, características y funcionalidades propias de la aplicación de IoT en *Smart Home*, en la figura 3.11 se muestra la conectividad de un entorno IoT en *Smart Home*, sus elementos principales y su interacción con usuarios y proveedores.

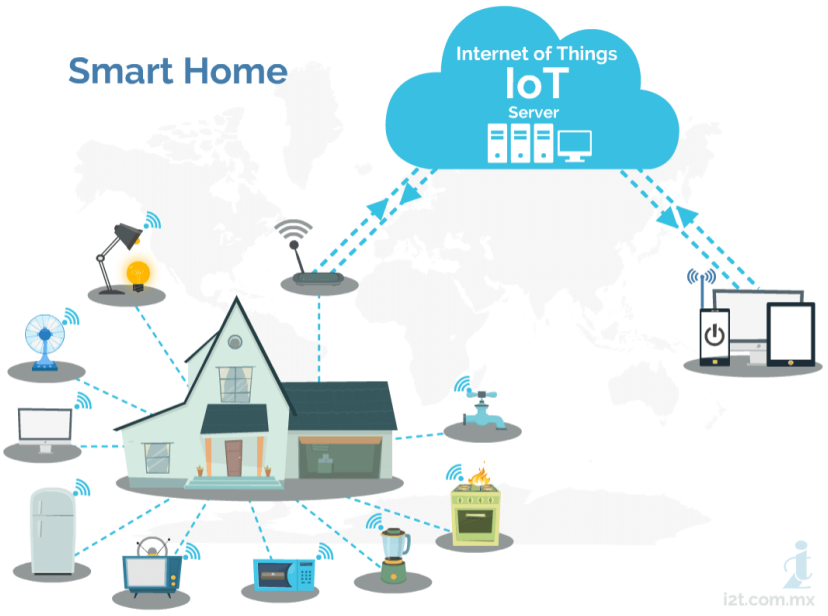


Fig. 3.11.- Entorno IoT en Smart Home(i2t, 2014)

La automatización de dispositivos del hogar ha creado la visión de un hogar inteligente (SHS), lleva a la necesidad no sólo de mayor funcionalidad sino también de un entorno seguro y eficiente, el uso de aplicaciones de seguridad y control de variables del hogar como energía, acceso, fugas, etc. Complementa el sistema dando un control total a los usuarios(i2t, 2014).

En la figura 3.12 se muestran los tres principales componentes de una *Smart Home*:

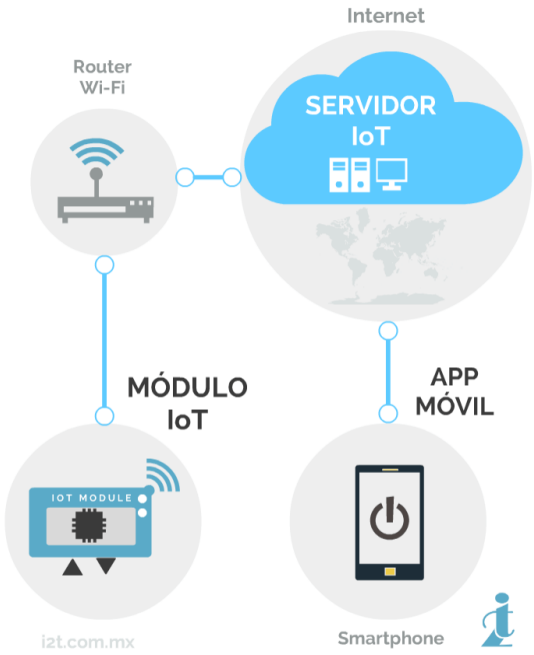


Fig. 3.12.- Componentes IoT en Smart Home(i2t, 2014)

3.5.2.1 *Módulo IoT*

Se encarga principalmente de la operación a distancia de los dispositivos por medio de aplicaciones IoT.

3.5.2.2 *Servidor IoT*

Se encarga de gestionar la comunicación entre el módulo IoT a las aplicaciones para el intercambio de información y comandos.

3.5.2.3 *Aplicaciones*

Se encarga de la configuración y del control del Módulo IoT, se controla el estado de los sensores y la activación de los actuadores(i2t, 2014).

En la figura 3.13 se presentan los componentes de hardware para un módulo doméstico inteligente que sirven para llevar a cabo su función.

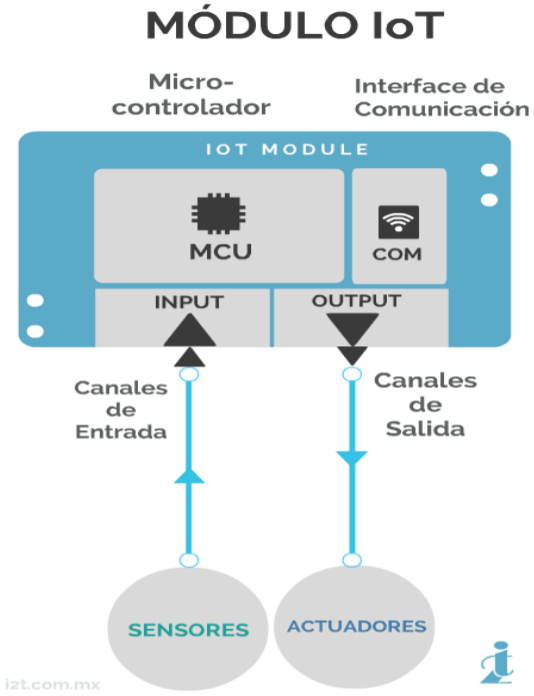


Fig. 3.13.- Elementos de un dispositivo doméstico inteligente(i2t, 2014)

El módulo IoT se compone de cuatro elementos importantes: microcontrolador, interface de comunicación, canales de entrada y canales de salida.

3.5.2.4 *Microcontrolador*

Administrar los estados de los canales de entrada y salida para comunicación con el servidor IoT.

3.5.2.5 *Interface de comunicación*

Conexión del Módulo IoT a la nube para establecer el traspaso de información.

3.5.2.6 *Canales de entrada*

Entradas de información desde los sensores hacia el microcontrolador para su análisis y procesamiento.

3.5.2.7 *Sensores*

Dispositivos que extraen información del mundo físico como movimiento, temperatura, humedad, gases, etc. Y transformarla a una señal eléctrica medible.

3.5.2.8 *Canales de salida*

Salida de información en forma de señal eléctrica para controlar actuadores.

3.5.2.9 *Actuadores*

Dispositivos que cumplen ordenes programadas, transforma una señal eléctrica en una variable física la cual cumple con un trabajo específico.

Para lograr encontrar las amenazas y vulnerabilidades dentro de IoT *Smart Home* lo primero es saber qué tipos de dispositivos IoT se usan en este ecosistema, que tipos de sensores y actuadores son los que van a interconectarse dentro del sistema, que tipos de protocolos manejan y cuáles son sus ventajas y desventajas de usarlos.

3.6 Estudio de Amenazas, Vulnerabilidades y Riesgos en IoT Smart Home

Se debe tomar en cuenta el crecimiento acelerado de la conexión de dispositivos IoT Smart Home, para darnos cuenta que el flujo de datos e información aumenta vertiginosamente, este fenómeno provoca a los cibercriminales a atacar y afectar estos dispositivos, ocasionando cada vez mayores amenazas, vulnerabilidades y riesgos para los dispositivos IoT Smart Home.

Una tecnología que se encuentra en auge y que ha tomado un desarrollo significativo y particular es la domótica para uso personal, varios fabricantes ofrecen productos para automatizar iluminación, cortinas, calefacción, enfriamiento y similares, sistemas vulnerables a amenazas tanto en el campo virtual como en el físico comprometiendo aspectos informáticos y funcionales de IoT Smart Home.

Razones por las que los desarrolladores de malware encuentran oportunidades de realizar actos delictivos cibernéticos hacia dispositivos inteligentes incluyen:

- La ubicuidad de los dispositivos móviles como teléfonos inteligentes en general.
- El aumento del poder computacional de los dispositivos donde virtualmente se están volviendo tan poderosos como sistemas de escritorio.
- El desconocimiento total de las amenazas y el riesgo asociado a los dispositivos.
- Cada dispositivo inteligente es en realidad una expresión del propietario, lo que proporciona una puerta de enlace a la identidad.
- La mayoría de dispositivos inteligentes funcionan en plataforma abierta, lo que provoca la descarga de aplicaciones tanto del mercado de aplicaciones de confianza como también de terceros.

3.6.1 Amenazas

Las amenazas de IoT son las acciones que aprovechan una vulnerabilidad del sistema para atacar la seguridad, incluyen todas las amenazas a la garantía de información segura. Además, los dispositivos de IoT están sujetos a la misma seguridad física, hardware, calidad

de software, medio ambiente, cadena de suministro y muchas otras amenazas inherentes a los dominios de seguridad y protección (Russell & Van Duren, 2016).

3.6.1.1 *Tipos de amenazas*

DDoS, espionaje, vigilancia y *ransomware* son las amenazas más comunes en entornos IoT *Smart Home* y en otros entornos. Los ataques DDoS son las amenazas más efectivas, es por esta razón, que los cibercriminales la aplican enviando grandes flujos de información logrando inutilizar dispositivos, robar información o causar daños graves a los dispositivos.

Otra amenaza común es el espionaje y la vigilancia, este ciberataque no se lo realiza con el fin de generar daños a los dispositivos por el contrario desean tener el acceso a la información que generan los dispositivos tomando el control por ejemplo de cámaras con la intención de espiar.

Otro tipo de amenaza común y que alerta a los sistemas IoT es el *ransomware* que es aprovechado por hackers, es considerado muy peligroso, impide el acceso a la información del usuario, secuestrando la información y pidiendo un rescate a cambio de un valor económico. Este tipo de ataque se manifiesta a través de un *malspam* o mensaje de correo, este puede incluir un archivo de Word, PDF o un link que re direcciona a la ruta que se encuentra el malware(Morales Suárez et al., 2019).

Todas estas amenazas aprovechan las debilidades de los dispositivos IoT y se utilizan para realizar ataques, que afectan la infraestructura de red y ponen en riesgo la información generada por los dispositivos IoT Smart Home.

3.6.2 Vulnerabilidades

Vulnerabilidad es el término que se usa para identificar una debilidad, ya sea en el diseño, integración u operación de un sistema o dispositivo, las vulnerabilidades están siempre presentes y cada día se descubren nuevas e innumerables variantes. Las vulnerabilidades pueden ser deficiencias en la protección física de un dispositivo, calidad del software, configuración, idoneidad de la seguridad del protocolo para su entorno o idoneidad de los propios protocolos.

Las vulnerabilidades pueden estar presentes en el dispositivo, en las deficiencias de implementación de hardware, en la arquitectura e interfaces físicas internas, en el sistema operativo o las aplicaciones. Los atacantes conocen bien las potenciales vulnerabilidades y buscarán atacar las más fáciles, de menor costo y más rápido de explotar.

Otras vulnerabilidades se pueden encontrar en interfaces web, cloud, móviles no seguras, ya que no cuentan con un sistema de bloqueo por intentos fallidos, autenticaciones débiles expone a los servicios de red, falta de cifrado pone en riesgo las comunicaciones y configuraciones obsoletas pone en riesgo la seguridad física del entorno.

3.6.3 Riesgos

Para evaluar el riesgo generalmente se usan métodos cualitativos o cuantitativos, en pocas palabras, el riesgo es la cantidad de exposición a la pérdida, el riesgo es diferente de la vulnerabilidad porque depende de la probabilidad de un evento, ataque o condición particular y tiene un vínculo fuerte con las motivaciones de un atacante. También depende de que tan grande sea el impacto de un ataque único o de una campaña de eventos de ataque, la vulnerabilidad no involucra directamente impacto o probabilidad, pero es la innata debilidad misma de los dispositivos IoT.

La gestión de riesgos se basa en la mitigación contra los tipos de vulnerabilidades que se sabe están presentes y que pueden ser objeto de amenazas. Debido a que la mitigación de los controles de seguridad nunca es perfecta, todavía nos queda una cantidad menor de riesgo restante, generalmente llamado riesgo residual. El riesgo residual a menudo se acepta tal cual o se compensa mediante la aplicación de otros mecanismos de compensación de riesgos(Russell & Van Duren, 2016).

3.6.4 Tipos de ataques comunes de IoT

Los siguientes son algunos de los ataques más importantes en lo que respecta al ecosistema IoT:

- Ataques de escaneo y mapeo por cable e inalámbrico
- Ataques de protocolo

- Ataques de escucha clandestina (pérdida de confidencialidad)
- Algoritmo criptográfico y ataques de gestión de claves
- *Spoofing* y enmascaramiento (ataques de autenticación)
- Ataques a la integridad del sistema operativo y las aplicaciones
- Denegación de servicio e interferencias
- Ataques de seguridad física (por ejemplo, manipulación, exposición de la interfaz)
- Ataques de control de acceso (escalamiento de privilegios)

Los ataques mencionados son una muestra de los que hay en el mundo real, la mayoría de ataques son altamente personalizados para una vulnerabilidad, controles de seguridad bien ubicados en el sistema son de vital importancia para reducir la probabilidad o la gravedad de la explotación de un ataque a una vulnerabilidad (Russell & Van Duren, 2016).

3.6.5 Ataques comunes IoT Smart Home

Una gran parte de los dispositivos de IoT son vulnerables a ataques generalizados. La conexión de dispositivos inteligentes (como luces, dispositivos o cerraduras) que creemos que son independientes de la red local traerán grandes riesgos de seguridad.

Si tomamos en cuenta un sistema de iluminación inteligente no es muy atractivo para un ciberdelincuente a primera vista. Sin embargo, pueden ser utilizados como ingreso para perpetuar ataques a otros dispositivos como un Gateway o un Router para luego tomar el control de una ventana o una cerradura.

En resumen nombremos los principales ataques que puede sufrir una Smart Home.

- ***Man-in-the-middle***: Consiste en la colocación de un atacante entre dos dispositivos este atacante puede obstaculizar la transmisión de datos afectando a un tercero.
- **Robo de datos y de identidades**: los datos generados por dispositivos inteligentes pueden proporcionar información personal sensible que es deseada por ciberdelincuentes para ser utilizada en actividades fraudulentas.

- **Secuestro de dispositivos**: Este tipo de ataque es difícil de detectar, el dispositivo secuestrado no cambia su funcionalidad, pero puede llegar a infectar a otros dispositivos con algún tipo de malware.
- **Denegación de servicio**: Es uno de los ataques más populares dentro de las redes de IoT Smart Home, consiste en inhabilitar un dispositivo de forma temporal o indefinida, pero el principal objetivo es reclutarlo para hacerlo parte de una *botnet* para continuar con los ataques de DDoS.
- **Denegación de servicio permanente**: Son ataques similares a los anteriores pero este ataque puede dañar a los dispositivos de una manera grave.

Los tipos de ataque a los sistemas IoT crecerán con el tiempo y en algunos casos seguirán la tendencia en el negocio del malware, mediante el cual los atacantes emplean algoritmos criptográficos para cifrar datos personales para luego devolver los datos descifrados por una tarifa conocida como *ransomware*, este potencial ataque en el ecosistema IoT es aterrador considerando que la seguridad de las personas se encuentra en peligro, marcapasos, puertas de garaje, cerraduras de hogares, etc. Son vulnerados por actores malintencionados que desean obtener un retorno económico. El mayor desafío de la seguridad IoT es encontrar mecanismos de defensa a los ataques de hoy y mañana (Mapfre, 2018).

3.7 Estudio de Mecanismos de Seguridad IoT e IoT Smart Home

Para realizar un mejor estudio sobre los mecanismos de seguridad IoT Smart Home, tenemos que definir y diferenciar lo que significa seguridad de la información y seguridad informática, la primera trata sobre la protección de la información mientras que la segunda se relaciona con la protección de infraestructura y componentes del sistema.

Algunas estrategias y recomendaciones se consideran mecanismos de seguridad tanto para la información como para la informática, en conjunto son herramientas de seguridad que se pueden utilizan para detectar o prevenir ataques a la infraestructura inalámbrica que conecta dispositivos para hogares inteligentes.

La confidencialidad, disponibilidad, integridad y autenticación se los conoce como los cuatro pilares de seguridad de las comunicaciones, dentro de estos cuatro pilares se deben enmarcar los mecanismos de seguridad para una red IoT Smart Home así como los protocolos y modelos de arquitectura estudiados en esta investigación.

3.7.1 Proyecto abierto de seguridad de aplicaciones web OWASP

Por otro lado el Proyecto Abierto de Seguridad de Aplicaciones Web OWASP (*Open Web Application Security Project*) nació con el objetivo de ayudar a los desarrolladores a tomar mejores decisiones con respecto al desarrollo y uso de sistemas IoT, el proyecto OWASP IoT Top 10, muestra a los desarrolladores las diez cosas que se deben evitar diseñar, crear, desarrollar, implementar y administrar en sistemas IoT. El proyecto brinda mecanismos de seguridad que buscan aplacar la mayor parte de riesgos y vulnerabilidades a los que se exponen los dispositivos IoT(Achila & Sanchez, 2017).

Enseguida se enumera el Top 10 OWASP del IoT, las vulnerabilidades a las que se exponen los dispositivos IoT y los mecanismos de seguridad sugeridos para aplacar estas vulnerabilidades.

1.- Contraseñas débiles, adivinables o codificadas.- Gran parte de los dispositivos IoT no están configurados para permitir que los usuarios actualicen la contraseña predeterminada, lo que deja frágiles a una serie de ataques, contraseñas fijas en dispositivos inteligentes puede facilitar el control por técnicos remotos, pero también lo hace para piratas informáticos que intentan obtener acceso a sus dispositivos o a su red. Además de incluir puertas traseras en firmware o software cliente que otorgan acceso no autorizado a los sistemas implementados.

2.- Servicios de red inseguros.- Las herramientas de seguridad de red como *firewalls* son relevantes cuando entran en juego los dispositivos de IoT.

Algunos métodos adicionales que evitan que dispositivos IoT puedan ser parte de una red de *Bots* que puedan provocar amenazas de DDoS y se conviertan en participantes involuntarios en dichas actividades y fortalecer la seguridad en la red incluyen:

- Apagar puertos innecesarios y servicios innecesarios.

- Tener una red dedicada para dispositivos inteligentes.
- Deshabilitar servicios que brinden acceso remoto.
- Instalar actualizaciones periódicas.
- Tener cuidado de no conectarse a través de redes inseguras (como WiFi públicas).

3.- Interfaces inseguras del ecosistema.- Las interfaces web, *cloud*, móvil y APIs que permiten interactuar con dispositivos inteligentes, pueden presentar vulnerabilidades de seguridad que pueden eventualmente causar daños al dispositivo o cualquiera de sus componentes relacionados.

4.- Mecanismo seguro de actualización.- La carencia de muchos dispositivos IoT de capacidad de actualizarse de forma segura debe ser la preocupación de los fabricantes de dispositivos IoT, los procesos de actualización no sólo tratan de colocar parches y mantener bajo control vulnerabilidades, también contienen procesos como:

- Procesos anti-*rollback*.
- Transmisión segura (no enviar la actualización en texto sin cifrar, no enviar la actualización sin firmar, etc.).
- Validación de firmware en el dispositivo.

Con la falta de un mecanismo de actualización seguro, no hay garantía de que la seguridad del dispositivo IoT sea proyectada para los usuarios finales o la prevista por los desarrolladores.

5.- Software y componentes inseguros y obsoletos.- El uso de un software o hardware obsoleto o de terceros puede ser perjudicial para la seguridad del dispositivo, las vulnerabilidades de IoT dependen de las debilidades que puedan ingresar a un dispositivo y aprovechar para realizar un ataque malicioso.

Los riesgos asociados con una cadena de suministro comprometida pueden alterar el proceso de fabricación y permanecer sin ser detectados y afectar gravemente la seguridad del dispositivo.

6.- Inseguridad a la privacidad.- El almacenamiento de datos personales inseguro, la divulgación de esta información provocan inseguridad a la privacidad de los usuarios. Un

estudio de la Universidad de Cornell en el año 2017 analiza la información que pueden obtener los observadores pasivos (como los ISP) con solo analizar el tráfico de la red de IoT, incluso cuando ese tráfico está encriptado.

La privacidad de los datos, específicamente en lo que respecta a IoT, está comenzando a abordarse a través de acciones legislativas, la recolección y almacenamiento de datos de los usuarios sin el consentimiento expreso ha sido un problema desde siempre, podría llegar a poner en peligro nuestra seguridad física.

7.- Transmisión y almacenaje de datos inseguros.- En este punto, puede parecer obvio mantener la seguridad de los datos con expertos que nos advierten constantemente sobre el cifrado, la clasificación de datos y el manejo adecuado de la información confidencial, pero considerando todas las violaciones de datos que todavía vemos en los titulares a diario, no es de extrañar por qué seguimos hablando de ello.

A más de restringir en general el acceso a datos confidenciales, se debe garantizar que los datos puedan ser encriptados tanto en reposo como en tránsito y en proceso. Si el cifrado no se implementa los datos quedan vulnerables e inseguros.

8.- Gestión de dispositivos insuficiente.- Conocer qué activos se encuentran conectados a la red, y administrarlos de manera eficiente es muy importante. Independientemente del tamaño de los dispositivos o de los costos individuales, si interactúan con la red y tienen acceso a ella, administrarlos metódicamente debería ser una de las principales preocupaciones. La gestión de actualizaciones es una buena práctica para una red segura así como el monitoreo de sistemas debe ser una parte integral del proceso.

9.- Configuración de inicio insegura.- La configuración predeterminada de los dispositivos inteligentes generalmente no es segura. Aunque a veces esto es solo descuido del fabricante, en otras ocasiones, la configuración del sistema no se puede cambiar, como contraseñas predeterminadas, servicios que se establecen con privilegios de administrador, etc.

Afortunadamente, algunos legisladores están luchando contra estas prácticas inseguras. Por ejemplo, California tiene una ley que requiere que los fabricantes de dispositivos de IoT establezcan contraseñas programadas únicas o que los usuarios cambien sus contraseñas antes de usar los dispositivos.

10.- Falta de seguridad física.- Fortalecer los dispositivos inteligentes contra ataques físicos protege información confidencial y el control del dispositivo. Entre los ataques físicos más relevantes están los siguientes:

- Los puertos de depuración que generalmente no se eliminan o desactivan dejan sus dispositivos vulnerables al acceso de piratas informáticos.
- Simplemente quitar una tarjeta de memoria para leer su contenido puede revelar contraseñas u otros datos confidenciales.
- El uso de un arranque seguro ayuda a validar el firmware y garantiza que solo se pueda ejecutar software confiable en el dispositivo.

3.7.2 Amazon Web Service AWS

AWS en su documento *Securing Internet of things* (IoT) *with* AWS muestra como su empresa brinda soporte a millones de clientes con diversos requisitos de confidencialidad y sensibilidad de datos. AWS invierte de manera significativa recursos para garantizar que la seguridad se incorpore en cada proceso de sus servicios y dispositivos IoT.(Amazon, 2019b).

3.7.2.1 *Capacidad y servicios de seguridad de AWS IoT*

AWS proporciona una pila de servicios para IoT para proteger los dispositivos de los clientes, los servicios proporcionan seguridad para los datos que se encuentran en tránsito y en reposo de extremo a extremo. También proporcionar políticas de seguridad necesarias para cumplir con sus estándares.

En la figura 3.14 se muestran los cinco servicios fundamentales para la seguridad de AWS IoT.

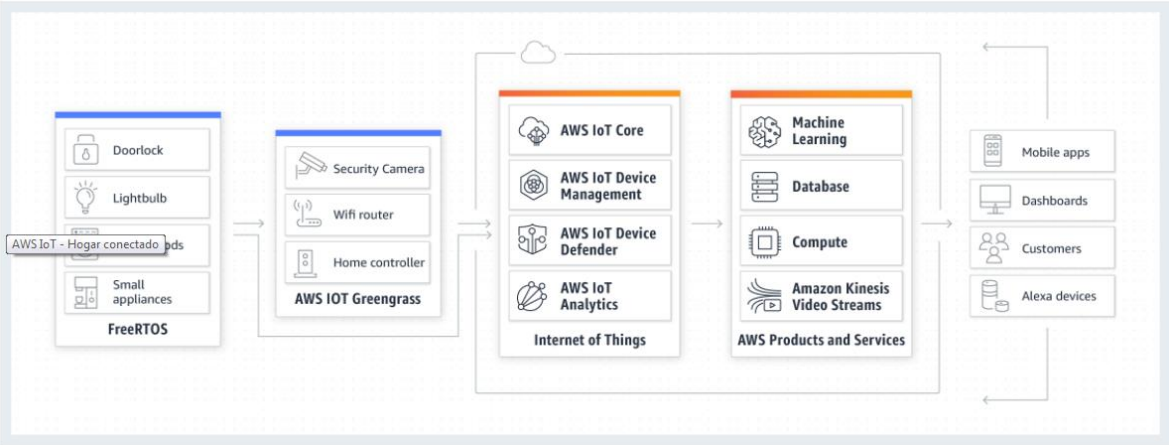


Fig. 3.14.- Servicios fundamentales AWS IoT (Amazon, 2019a).

- ***Amazon FreeRTOS*.-** Sistema operativo de código abierto para producción de microcontroladores de pequeños dispositivos fáciles de programar, implementar, proteger, conectar y administrar.
- ***AWS IoT Greengrass*.-** Software de ejecución para clientes, permite ejecutar programación local, almacenamiento de datos, sincronización, mensajería, y capacidades de interacción con dispositivos IoT conectados.
- ***AWS IoT Core*.-** Servicio alojado en la nube que permite la interacción de dispositivos de una forma fácil y segura.
- ***AWS IoT Device Management*.-** Servicio de gestión de dispositivos apoyado en la nube que incorpora, organiza, monitorea y administra de forma remota y segura los dispositivos IoT.
- ***AWS IoT Device Defender*.-** Servicio de supervisión y auditoría de IoT, garantiza las mejores destrezas de seguridad.

3.7.2.2 *Mejores prácticas clave de seguridad en AWS IoT*

Dependiendo del entorno IoT, de los dispositivos y de los servicios que se dispongan, se pueden recomendar prácticas de seguridad de extremo a extremo:

- Incorporar seguridad en la fase de diseño
- Construir sobre marcos de seguridad de TI y ciberseguridad reconocidos

- Centrarse en el impacto para priorizar las medidas de seguridad

3.7.3 Plataforma Samsung IoT y Seguridad

La plataforma Samsung es básicamente compuesta por: nube *Smart Things*, dispositivos *Smart Things*, aplicaciones *Smart Things* y espació de trabajo para desarrolladores. Además, es compatible con otros dispositivos como por ejemplo luces Phillips Hue, estos dispositivos están conectados directamente a la nube a través de un *Smart Things Hub* o de nubes de terceros, el usuario puede tener conectados todos los dispositivos y manipularlos a través de la aplicación de teléfono inteligente, manualmente o con aplicaciones específicas llamadas *Smart Apps*. Las *Smart Apps* se implementan en la nube y se puede interactuar con los dispositivos conectados. Además, las *Smart Apps* pueden conectarse con nubes de terceros para más funcionalidades. La figura 3.15 muestra la Plataforma Samsung IoT (Ramos, 2018).

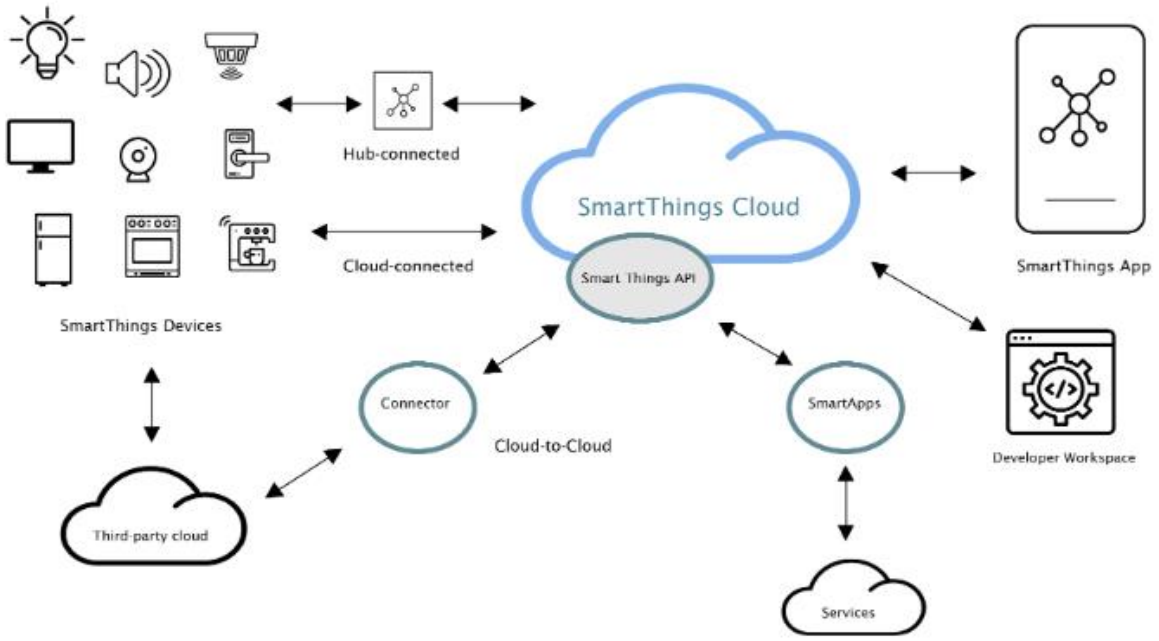


Fig. 3.15.- Plataforma Samsung IoT (Ramos, 2018).

3.7.3.1 *Samsung Smart Things App*

Esta interfaz permite al usuario tomar el control de todos los dispositivos conectados al Samsung Hub Smart Things, incluso cuando el usuario está fuera de casa. En este

experimento, el enrutador Phillips Hue está conectado al dispositivo Samsung. Por tanto, las luces pueden ser controladas desde la aplicación Samsung.

Profundizando un poco más en la aplicación, presenta 4 partes principales o utilidades. El "Panel de control" muestra información sobre las "cosas" favoritas del usuario y hace recomendaciones personales de Smart Apps. Una Smart App es un servicio o programa que se ejecuta en la nube Samsung Smart Things para permitir automatizaciones domésticas utilizando dispositivos conectados al entorno Samsung. Incluye varias secciones. Por ejemplo, la sección "Mi casa" nos permite agregar nuevos dispositivos finales o controlar los que ya están conectados al hub. Es posible agrupar los dispositivos ya conocidos según la habitación. Además, el usuario puede definir un conjunto de configuraciones para los dispositivos. Por ejemplo, por la noche podemos configurar un brillo fijo para las luces y volumen de los altavoces. La sección "Automatización" permite que la red se comporte de determinadas formas cuando se realiza una acción con “Rutinas” y “Smart apps”. La sección "Marketplace" permite al usuario comprar "cosas" nuevas para su hogar así como descargar nuevas Smart apps desarrolladas por usuarios o empresas.

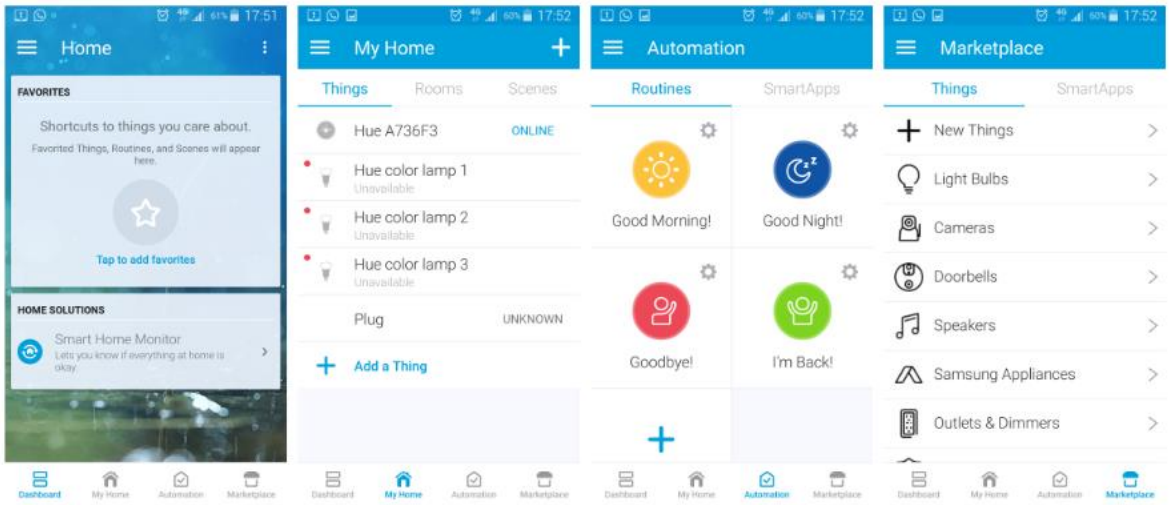


Fig. 3.16. - Interfaz Samsung Smart Things App (Ramos, 2018).

3.7.3.2 *Samsung Smart Things Cloud*

Smart Things Cloud es el punto central que conecta todos los componentes. Los dispositivos finales se pueden conectar a la nube de dos formas, directamente si tienen Internet conexión

a través del concentrador Samsung Smart Things si no lo hacen. De este modo, la aplicación del teléfono inteligente interactúa con los dispositivos a través de la nube. Sin embargo, Muchos dispositivos están conectados a dispositivos de otros fabricantes y no pueden conectado al concentrador de Samsung o a la nube de Samsung. En este caso, Samsung permite que una API *Rest* conecte otras nubes a su nube. Además, la API puede ser se utiliza para conectar otros servicios y realizar determinadas automatizaciones.

3.7.3.3 *Espacio de trabajo del desarrollador*

Samsung creó un espacio de trabajo para desarrolladores comunitarios, que pueden crear fácilmente muchas automatizaciones o Smart Apps que pueden ser publicadas y descargadas por otros usuarios en el mercado. Es relevante decir que la plataforma de desarrollo está actualmente migrando de su primera versión a una más nueva. Sin embargo, la última versión tiene Aún no se han migrado todos los procesos.

Como desarrollador de IoT, puede integrar fácilmente su dispositivo con Samsung *Smart Things cloud*, independientemente si está conectado al hub, conectado a la nube o conectado a otra nube.

Si es necesario controlar el dispositivo en un nivel inferior, se puede descargar un SDK también. Además de conectar el dispositivo a la nube, el SDK permite al usuario Señalización de la interfaz de usuario del dispositivo, o codificación de otras acciones aparte desde la conexión a la nube.

En la versión anterior, la plataforma permitía al usuario desarrollar y publicar SmartApps. El espacio de trabajo obliga al desarrollador a crear lo que se llama una ubicación, que las SmartApps deben estar vinculadas a. Además, los concentradores y dispositivos finales físicos pueden vinculado a la cuenta del desarrollador para ser utilizado al probar SmartApps. De esta manera, se puede realizar la implementación previa para la depuración después de publicar la aplicación. Entonces, la sección "Controladores de dispositivos" es donde el desarrollador puede vincular nuevos dispositivos a la aplicación real.

Las Smart Apps normalmente se estructuran en 3 partes principales: definición, preferencias y funciones. La definición le da a la aplicación la metadatos necesarios, como nombre, autor,

descripción o categoría. Además, las preferencias son las entradas que recibe el programa. Pueden ser medidas de sensores, capacidades del dispositivo o variables fijas, como el tiempo. Por lo tanto, al instalar o actualizar la Smart App, la aplicación le preguntará al usuario qué sensor o sensores de la casa con la que quiere que funcione la aplicación. A que vamos especificar en el programa es la capacidad de detectar que la aplicación va a funcionar con. En general, estas entradas pueden ser obligatorias u opcionales para la aplicación.

Además, hay 4 funciones importantes que deben declararse: "instalado", "Actualizado", "inicializar" y "suscribirse". "Instalado" y "Actualizado" son funciones que se llaman cuando la aplicación se descarga e instala por primera vez y cuando tiene que actualizarse a una versión más reciente respectivamente. Ambas llaman a la función “Inicializar ", que utiliza la función" Suscribir "para activar controladores para otros funciones codificadas. "Suscribir" utiliza una entrada y un estado de la capacidad de la entrada para activar una función. Cuando el estado del sensor cambia al estado elegido, el programa ejecuta el código del controlador.

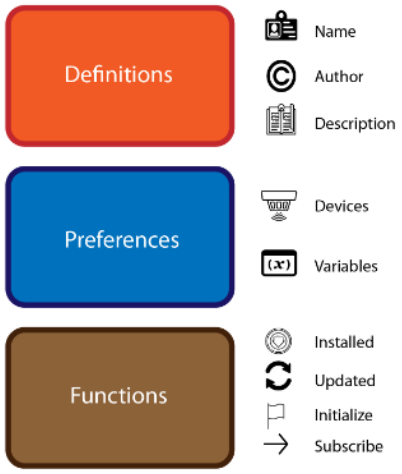


Fig. 3.17.- Plataforma de desarrollo Samsung (Ramos, 2018).

Para probar la aplicación, el IDE proporciona un simulador de los sensores y dispositivos finales que utiliza la aplicación. Sin embargo, también se puede probar en un entorno que vincula dispositivos reales con el espacio de trabajo del desarrollador en "*My Hubs*" y Secciones "Mis dispositivos".

CAPITULO IV

4. ANALSIS DE MECANISMOS DE SEGURIDAD PARA IOT SMART HOME

4.1 Introducción

Después de un amplio estudio del ecosistema IoT, arquitecturas, protocolos, amenazas, vulnerabilidades y riesgos y mecanismos de seguridad aplicados por investigadores y empresas prestadoras de servicios IoT, se puede decir que la seguridad de IoT no se basa únicamente en una ciberseguridad tradicional, que aborda datos, servidores, infraestructura de red y seguridad de la información. Además se debe incluir el monitoreo y/o control directo o distribuido del estado de los sistemas físicos conectados a través de internet, en otras palabras, lo que distingue al IoT de la ciberseguridad tradicional es la seguridad de los sistemas físicos y de la información que reciben y envían al mundo físico.

Entonces, el tema de seguridad IoT no es la aplicación de un único conjunto de reglas de seguridad que se aplican a dispositivos y *host* de red, se requiere de una aplicación o un mecanismo para cada sistema en los que participan dispositivos IoT. La seguridad del dispositivo de IoT debe actuar en función del uso del dispositivo, del proceso físico afectado o controlado por el dispositivo, y la sensibilidad de los sistemas a los que se conecta el dispositivo.

Para hablar de aspectos prácticos de amenaza, vulnerabilidad y riesgo se deben identificar los componentes básicos y esenciales del aseguramiento de la información para *IoT e IoT Smart Home*, los cuales se enumeran a continuación:

- **Confidencialidad:** Mantener la información confidencial en secreto y protegida contra la divulgación.
- **Integridad:** Garantizar que la información no se modifique, accidental o intencionalmente, sin ser detectada.

- **Autenticación:** Asegurarse de que la fuente de datos provenga de una identidad o punto final conocido (generalmente sigue a la identificación).
- **No repudio:** Asegurarse de que un individuo o sistema no pueda negar posteriormente haber realizado una acción.
- **Disponibilidad:** Garantizar la disponibilidad de la información cuando sea requerida.

Cada uno de los cinco pilares del aseguramiento de la información se aplica al IoT porque IoT combina información con el entorno, la fisicalidad, las fuentes de datos, los receptores y las redes de un dispositivo. Sin embargo, debemos introducir dos garantías más que se relacionan con aspectos ciberfísicos del IoT, la resiliencia y la seguridad.

- **Resiliencia:** Mantener la conciencia del estado y un nivel de aceptable de normalidad operativa en respuesta a perturbaciones, incluidas amenazas de naturaleza inesperada y maliciosa.
- **Seguridad:** Condición de estar a salvo de sufrir o causar daño, lesión o pérdida.

Satisfacer un objetivo de seguridad de la información no implica necesariamente que un sistema deba mantener todas las garantías anteriores, no todos los datos requieren confidencialidad por ejemplo, la categorización de información y datos permitirá diferenciar la información críticamente sensible de información importante, además, de la sensibilidad de datos individuales como de datos en forma agregada que se alojan en dispositivos y aplicaciones IoT. Categorías de datos bien definidas permiten que se definan garantías específicas como la confidencialidad o la integridad para cada elemento de datos o tipo de información compleja (Russell & Van Duren, 2016).

La convergencia de IoT en los cinco pilares más resiliencia y seguridad permitirán la construcción de mecanismos de seguridad para IoT y más específicos para sistemas y/o dispositivos IoT Smart Home.

4.2 Construcción mecanismo de seguridad para IoT Smart Home

Las *Smart Homes* cada vez está más cerca de ser una realidad cotidiana, el incremento de las *Smart Homes* es grandioso, la innovación tecnológica facilita cada vez más el uso de sistemas

inteligentes en el hogar a costos cada vez menores, por esta razón se dispone de más dispositivos IoT en las casas, desde vigila bebes, cerraduras inteligentes, electrodomésticos hasta sistemas de control de temperatura.

La introducción de inteligencia en el hogar, provoca mayores riesgos desde el punto de vista de seguridad, las *Smart Homes* han creado una serie de debilidades (vulnerabilidades) conocidas de las que ciberdelincuentes pueden usarlas para beneficio propio.

Para lograr construir mecanismos de seguridad para un sistema *IoT Smart Home* es necesario identificar los requerimientos de seguridad que se consideran importantes para un sistema IoT Smart Home y que se podrían expresar de la siguiente manera:

- Mantener la integridad de los datos dentro del sistema.
- Mantener la confidencialidad de los datos sensibles dentro del sistema.
- Mantener la disponibilidad del sistema tanto en su conjunto como de cada uno de sus componentes individuales.

El impacto de estos requerimientos de seguridad en sistemas *IoT Smart Home* pueden ser bajo, medio o alto dependiendo del efecto causado a la integridad, confidencialidad, y disponibilidad del sistema, datos y componentes (Russell & Van Duren, 2016).

Para lograr cumplir con los requerimientos de seguridad del sistema IoT, en la figura 4.1 se plantea un modelo de evaluación de las amenazas a las que se expone un entorno *IoT Smart Home*, para después plantear mecanismos de seguridad que mitiguen dichas amenazas y ataques desde los niveles más bajos hasta los niveles superiores.

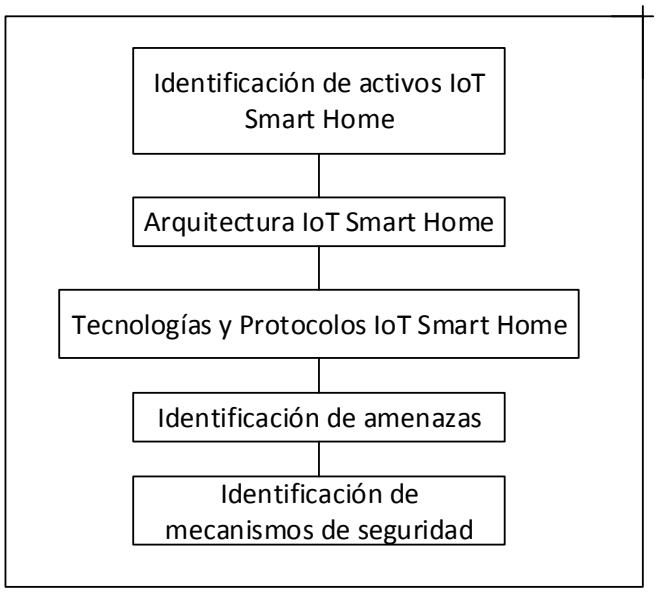


Fig. 4.1.-Modelo de evaluación de mecanismos de seguridad (Autor).

4.2.1 Identificación de activos IoT Smart Home

Se identificarán y documentarán los activos que pueden ser de interés para un atacante, por lo tanto, comprender lo que se debe proteger de ciberataques es primordial. Los dispositivos *IoT Smart Home* pueden clasificarse en tres grupos los cuales abarcan la mayor parte de dispositivos utilizados comúnmente en un hogar inteligente, estos son los siguientes:

- Seguridad del hogar, monitoreo y automatización.
- Accesorios electrónicos para el hogar.
- Dispositivos multimedia y entretenimiento para el hogar.

En la figura 4.2 se identifican varios ejemplos de los activos a los que se refiere la clasificación dentro de un sistema *IoT Smart Home*, la documentación de estos activos proporcionará la comprensión de lo que debe estar protegido y cuáles son los dispositivos más sensibles a un ataque o amenaza, cuáles son sus vulnerabilidades y cuáles son los que están sujetos a un mayor riesgo, por tal motivo, se debe categorizar los activos de la red y conocer sus vulnerabilidades y posibles ataques a los que están expuestos (Cvitić, Peraković, Periša, & Botica, 2018).

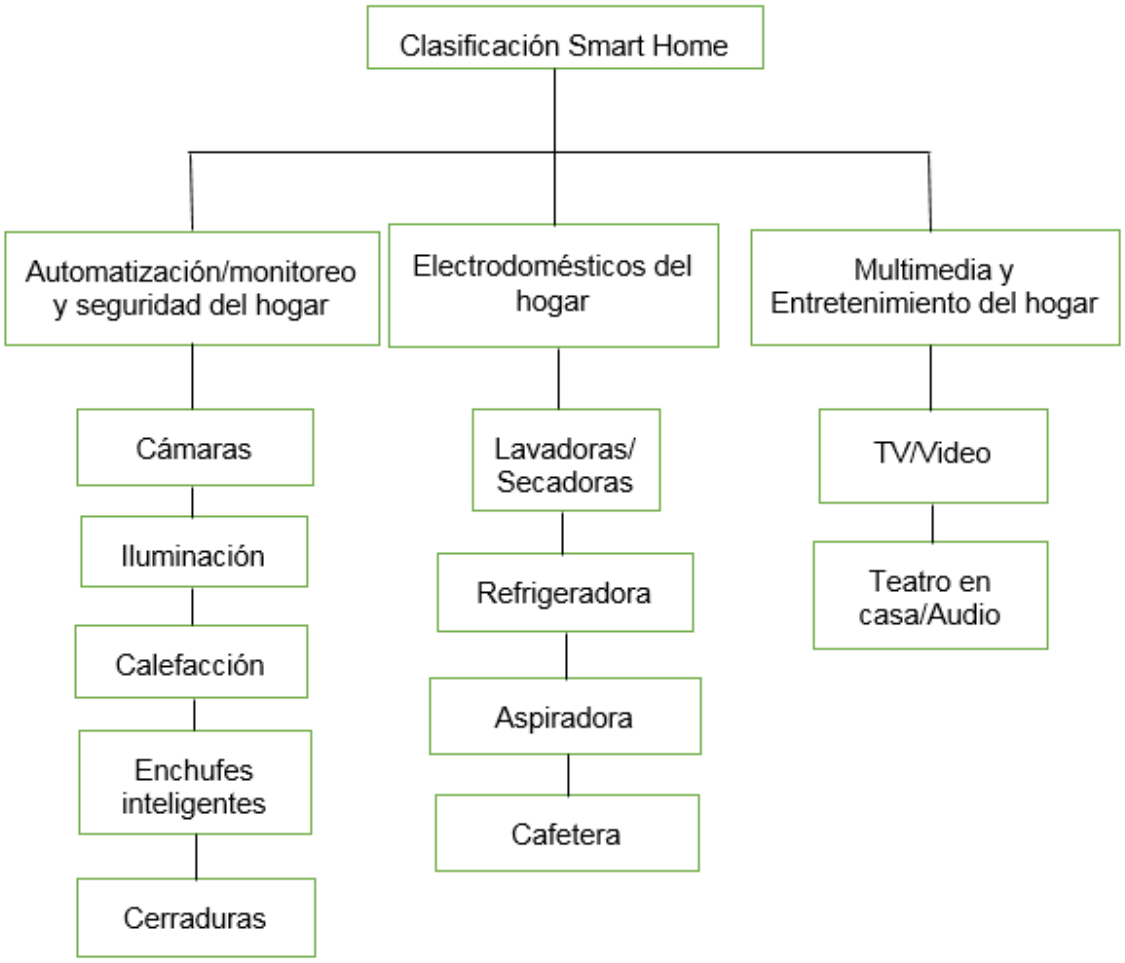


Fig.-4.2.- Identificación y Clasificación de activos IoT Smart Home (Autor).

Todos los dispositivos IoT son atractivos para un atacante, tomar el control de alguno de estos dispositivos permitirá al atacante no solo tomar datos generados sino también el ingreso a la red de dispositivos IoT, Gateway y routers de la Smart Home. Poniendo en peligro la seguridad del hogar y de sus ocupantes. En la tabla 4.1 se muestran los activos más comunes y el rol que cumplen dentro de un hogar inteligente.

ACTIVOS	DESCRIPCIÓN
Cámaras IP	El acceso a las grabaciones y al video en directo permite tener vigilancia del perímetro del hogar.
Iluminación	A través de un dispositivo móvil establecer la intensidad de la luminosidad en los ambientes del hogar, ahorrar energía al recibir luz natural con el uso de sensores.
Enchufes inteligentes	Proporcionan control e información sobre el consumo de aparatos que tenemos conectados además de encender la cafetera antes de llegar a casa.
Cerraduras	Con un control remoto podemos bloquear o garantizar un libre acceso, a través de dispositivos móviles saber si se ha accedido al hogar.
Calefacción/Aire acondicionado	Controlar a distancia la climatización de las habitaciones determinando temperaturas específicas, además controlar el aire acondicionado.
Electrodomésticos: Lavadoras/Secadoras Refrigeradores/Hornos Aspiradoras/Cafeteras	Capacidad de conexión a la web, programar tareas específicas y controlarlas de manera remota. Capacidad de funcionar de manera más eficiente.
Audio/Video: Entretenimiento Televisores Reproductores Auriculares Parlantes	Dispositivos con capacidad de interacción con otros dispositivos IoT Smart Home, mayor rendimiento para el contenido de audio y video que capturan o reproducen, consumo de energía optimizado e interfaz de usuario amigable. Fácil integración con Alexa.

Tabla.-4.1.- Identificación de activos IoT Smart Home (Autor).

4.2.2 Descripción del sistema IoT Smart Home

El planteamiento de un diagrama arquitectónico del sistema detalla los componentes del sistema, sus interacciones y las tecnologías y protocolos empleados en dichas interacciones, este diagrama detalla también las amenazas a las que se disponen los dispositivos en cada una de sus interacciones, la figura 4.3 se modela el diagrama arquitectónico de la solución IoT Smart Home basado en cuatro capas básicas, percepción, red, middleware y aplicación.

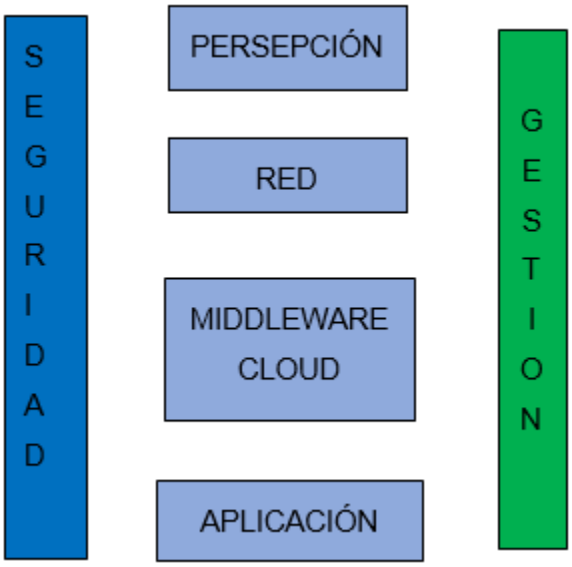


Fig.-4.2. - Diagrama arquitectónico IoT Smart Home (Autor).

La capa de percepción incluye sensores y actuadores que incluye una tecnología de comunicación de datos al concentrador Gateway Home ubicado en la capa de red a continuación. Los sensores y actuadores utilizan tecnología de comunicación energéticamente eficiente debido a sus requerimientos, los más utilizados en entornos de hogares inteligentes son tecnologías de corto alcance como Zigbee 802.15.4, WiFi 802.11, Z-Wave G.9959 o Bluetooth de baja energía (BLE). En la tabla 4.2 se muestra una comparación entre tecnologías más usadas en entornos IoT Smart Home, las características y funciones que se presentan ayudarán a escoger la mejor opción en cuanto a seguridad se refiere en la capa de percepción de la arquitectura.

	ZIGBEE	**Z-WAVE**	**BLUETOOTH BLE**	**WI-FI**
Especificación	IEEE 802.15.4	ITU-T G.9959	IEEE 802.15.1	IEEE 802.11
Frecuencia de Operación	2.4 Ghz, 915 Mhz, 868 Mhz	900 Mhz	2.4 Ghz	2.4 Ghz, 5 Ghz
Rango máximo	~ 500m	~ 100m	~ 50m	~ 100m
Velocidad máxima	250 Kbps	40Kbps – 100Kbps	~ 1 Mbps	~ 600 Mbps
Número de Nodos máximo	65.536	232	N/A for BLE, 8 is default for Classic Bluetooth	N/A

Consumo de corriente medio	Tx = 25-35 mA; Rx = 20-30 mA;	Tx = 30-40 mA; Rx = 20-30 mA;	Tx = 15-20 mA; Rx = 15-20 mA;	Tx = 220+ mA; Rx = 215+ mA;
Capacidad Multi-hop	Yes	Yes	Yes	No
Certificación/Costo de Calificación	Medium	Medium	High	High
Adopción de la comunidad de desarrollo	High	High	Low	High
Interoperabilidad	High	High	Medium	High
Fiabilidad	Low	Low	Medium	Medium
Ancho de banda	0.3/0.6Mhz; 2Mhz	0.1Mhz	2Mhz	10Mhz
Encriptación	AES	AES	AES	WEP Y AES
Autenticación	CBC-MAX		Secreto compartido	WPA2(802.11i)
Protección de datos	16 bits CRC		24 bits CRC	32 bits CRC

Tabla 4.2.- Comparación de tecnologías en la capa de percepción utilizadas en un entorno IoT Smart Home (González García, 2017).

La capa red incluye un concentrador que cumple el papel de Gateway y permite la comunicación entre dispositivos de la capa percepción y la conexión de la capa percepción con la capa de red de acceso para transmitir los datos hacia la siguiente capa de middleware. En la tabla 4.3 se describe el papel que cumple un concentrador dentro del sistema IoT Smart Home.

ACTIVOS	DESCRIPCIÓN
Gateway	• Sirve de puente de conexión entre los controladores, sensores y dispositivos inteligentes con la nube, traducción de protocolos como WiFi, Zigbee, Bluetooth, BLE, etc., agregación, filtrado, correlación, seguridad, actualizaciones y administración. • Realiza un pre procesamiento de los datos generados localmente antes de ser enviados a la nube, minimizando los volúmenes de datos y por tanto los tiempos de respuesta (latencia). • Agrega seguridad adicional a la red IoT Smart Home contra ataques externos maliciosos con herramientas como detección de manipulación de datos y motores de cifrado.

Router	• Integra dos o más redes mientras ejerce control del tráfico de datos hacia la red global (internet) y asegurando que los paquetes digitales lleguen a su destino. • Permite el acceso de redes que presenten arquitecturas y protocolos similares. • Minimiza la congestión de datos entre los caminos de enrutamiento, se deben configurar varias tablas de enrutamiento para trazar el camino de los datos dentro de la red. • Ofrece funciones de seguridad para la red y su propia integridad ya que es un dispositivo vulnerable y puerta de entrada a los dispositivos de su red.

Tabla 4.3.- Descripción de un Concentrador en un entorno IoT Smart Home (Russell & Van Duren, 2016).

Tecnologías de acceso convencionales como xDSL, fibra óptica, redes de datos móviles (3G, 4G y 5G) y similares se utilizan para transmitir datos desde una capa red a una capa de middleware. En la tabla 4.4 se muestra la comparación de las prestaciones que tienen las tecnologías más usadas dentro de entornos IoT Smart Home.

TEC. / **CARAC.**	**ADSL**	**FIBRA OPTICA**	**3G**	**4G**	**5G**
Tecnología	Alámbrica Par trenzado	Fibra Óptica	CDMA 2000, UMTS, EDGE	Wi-Max LTE WiFi	WWWW (cooming soon)
Ancho de banda	475Khz (UL), 650 KHz (DL)	1-2 Gbps	2Mbps	200Mbps	1Gbps
Servicio		Servicio completo (POTS, Ether, TDM)	Integra alta calidad de audio, video y datos	Acceso de información dinámica, Wearables devices	Acceso de información dinámica, Wearables devices con alta capacidad
Multiplexación	FDM/TDM	TDM/ WDM/ CDWM	CDMA	CDMA	CDMA
Switching	N/A	N/A	Packet	All packet	All packet

Core network	N/A	N/A	Red de paquetes	Internet	Internet
Encriptación	Si	Si (AES)			
FEC	Si	Si			

Tabla 4.4.- Comparación de tecnologías de la capa de red utilizadas en un entorno IoT Smart Home (García Barranco, 2019).

La capa de middleware se basa en el concepto de *Cloud Computing* y contiene recursos de procesamiento para datos generados en esta capa y convertirlos en información útil para los usuarios de un entorno de hogar inteligente. En la tabla 4.5 se muestra la descripción de los recursos que puede prestar el *cloud computing*.

CLOUD	DESCRIPCIÓN
Cloud Computing IoT Smart Home	Complemento idóneo a la plataforma IoT e IoT Smart Home, aumenta la eficiencia a los procesos y tareas cotidianas de un hogar inteligente., procesamiento y análisis en tiempo real,
Procesamiento y análisis	Analítica IoT edge basado en machine learning, se realiza el pre procesamiento y análisis de datos, tareas de filtrado y agregación de datos se ejecutan en el límite de la red.
Almacenamiento	Debido a la producción de datos generados por el sistema IoT Smart Home, la nube brinda almacenamiento prácticamente ilimitado.
Tecnología	El usuario asegura el uso de tecnología actualizada y optimizada, las actualizaciones se realizan automáticamente.
Seguridad	Los datos generados por el sistema IoT Smart Home se aseguran en la nube, la información se asegura con copias de seguridad y cifrado seguro a prueba de cualquier ataque de hackers.
Acceso	El usuario de un hogar inteligente tiene capacidad de acceso a sus dispositivos desde cualquier lugar, basta con una conexión a internet podrá acceder a las aplicaciones y control de su sistema IoT Smart Home

Tabla 4.5.- Descripción de los recursos que presta el Cloud Computing para los requerimientos de un entorno IoT Smart Home (Sataloff, Johns, & Kost, 2019).

La capa aplicación permite la prestación de diversos servicios, así como la gestión de dispositivos mediante el uso de diferentes aplicaciones. La seguridad, la privacidad y la confianza están orientadas a cubrir el entorno IoT Smart Home horizontalmente. En la tabla 4.6 y 4.7 se muestra la comparación de los protocolos más utilizados en la capa aplicación y los protocolos de transporte utilizados por estos protocolos.

Protocolos de Aplicación	HTTP	CoAP	MQTT	XMPP	AMQP	DDS
RESTFul	Si	Si	No	No	No	No
Transporte	TCP	UDP	TCP	TCP	TCP	TCP/UDP
Publicación/Suscripción	No	Si	Si	Si	Si	Si
Petición/Respuesta	Si	Si	No	Si	No	No
QoS	No	Si	Si	No	Si	Si
Tamaño cabecera		4 bytes	2 bytes		8 bytes	

Tabla 4.6.- Comparación de protocolos utilizados en la capa aplicación en un entorno IoT Smart Home (González García, 2017).

PROTOCOLO	**TCP**	**UDP**
Sentido	Establece conexión antes de transmitir los datos	Envía datos sin tener respuesta del sistema si está listo para recibir o no
Tipo	Orientado a la conexión	Sin conexión
Método de transferencia	Los datos se envía en secuencia	Los datos se envían en flujo
Velocidad	Baja	Alta
Confiabilidad	Alta	Baja
Detección y corrección de errores	Si	No
Control de congestión	Si	No
Acuse de recibo	Si	No (Sólo el *checksum*)
Tamaño del encabezado	20 Bytes	8 Bytes

Tabla 4.7.- Comparación de protocolos de transporte en un entorno IoT Smart Home (González García, 2017).

En base a la recomendación que se realizó en el capítulo 3 Estudio de Arquitecturas IoT ITU, se adicionan dos capas más que actúan verticalmente en el modelo que son capa de gestión y capa de seguridad y que son parte fundamental en el este estudio.

Capa de gestión:

Capa transversal encargada de la gestión de dispositivos, diagnóstico, actualizaciones y activación y desactivación de forma remota. Además de la topología y tráfico de la red.

Capa de seguridad:

Capa transversal encargada de la autenticación y autorización de dispositivos, además de la confidencialidad, privacidad, integridad, auditorias, antivirus y protección de datos.

4.3 Consideraciones de Seguridad de un Sistema IoT Smart Home

4.3.1 Ataques en IoT *Smart Home*

La interconexión de dispositivos inteligentes para el hogar como luces, cámaras, calefacción, cerraduras, entre otros, no contemplan un sistema de seguridad que evite ciberataques, por tal motivo, es importante entender el tipo de ataque y el valor sustancial que tiene para un atacante, ya sea en información comprometida, manipulación del dispositivo para un efecto físico u oportunidades para penetrar a otra parte de la red del dispositivo. Sin embargo, en la práctica un ataque suele ser parte de una campaña de subataques u otras actividades agrupadas y/o secuenciales elegidas cuidadosamente entre una variedad de métodos de inteligencia por ejemplo: ingeniería social humana, elaboración de perfiles, escaneo, investigación en internet, familiaridad con el sistema, etc. Cada actividad diseñada para lograr su objetivo tiene cierto nivel de dificultad, costo y probabilidad de éxito.

4.3.2 Escenarios de ataques sistemas IoT Smart Home

En todo tipo de ataque, el ciberdelincuente arremete a lo que se conoce como superficie de ataque que es el conjunto de vulnerabilidades que presenta el dispositivo, dentro de esta superficie se identifican vectores de ataque, las que se muestran como rutas utilizadas con fines maliciosos (Russell & Van Duren, 2016).

4.3.2.1 *Mapeo y Reconocimiento Inalámbrico*

El uso de protocolos de comunicación inalámbrica como Zigbee, ZWave, Bluetooth-LE, WiFi entre otros, provocan ataques para identificar miles de dispositivos IoT habilitados, el escaneo de red con herramientas como Nmap es comúnmente utilizado por piratas

informáticos para recopilar información sobre dispositivos IoT, subredes, puertos y protocolos, cosas que pueden abrir la puerta de un garaje, cerrar la puerta de entrada con llave, encender y apagar las luces, etc.

4.3.2.2 *Ataques de Protocolos de Seguridad*

Muchos ataques se dan contra vulnerabilidades en el diseño, implementación e incluso en configuración de protocolos de seguridad, procedimientos de emparejamiento de dispositivos vulnerables permiten la identificación de claves de red tomando el control del dispositivo, comprender las limitaciones de un protocolo es fundamental para determinar que niveles de seguridad adicionales se deben implementar para mantener el sistema seguro.

4.3.2.3 *Ataques de Seguridad Física*

Los ataques a la seguridad física se dan por atacantes que ingresan físicamente a un host, dispositivo integrado u otro tipo de plataforma de IoT para acceder a su procesador, dispositivos de memoria, y a otros componentes sensibles. Una vez que el atacante accede a través de una interfaz expuesta se tiene acceso a la memoria, material clave sensible, contraseñas, datos de configuración y una variedad de parámetros sensibles. Por ahora existen varias técnicas y controles de seguridad de penetración física de dispositivos, como por ejemplo mecanismos de respuesta a la manipulación (borrado automático de la memoria), chips de tarjetas inteligentes, módulos de seguridad de hardware, módulos criptográficos para proteger variables criptográficas como la identidad y datos del dispositivo.

4.3.2.4 *Ataques de Seguridad de Aplicaciones*

Los ataques a aplicaciones de dispositivos y conexiones IoT pueden explotarse a los puntos finales que incluyen servidores web y aplicaciones de dispositivos móviles por ejemplo iPhone y Android que desempeñan el control de dispositivos. La aplicación fuzzing por ejemplo puede encontrar formas de comprometer el host de la aplicación y tomar el control de sus procesos, otros ataques pueden descubrir vulnerabilidades de implementación como claves codificadas, contraseñas y otras cadenas en el binario de la aplicación que pueden ser útiles para varios exploits.

4.3.3 Modelado de Amenazas, Vulnerabilidades y Riesgo en un sistema IoT Smart Home

Para evaluar un sistema o diseño de un sistema IoT Smart Home, se modelaran las amenazas a las que están expuestas desarrollando una guía que ayude a la comprensión de los actores, puntos de entrada y activos dentro del sistema y que proporcione una vista detallada de las amenazas a las que está expuesto el sistema.

En la Tabla 4.8 se evalúa las amenazas a las que se expone un entorno IoT Smart Home, el riesgo y los activos afectados para luego plantear mecanismos de seguridad que mitiguen dichas amenazas y ataques, el sistema consta de varios puntos finales que alimentan un repositorio de datos (backend), infraestructura, procesamiento y aplicaciones API para teléfonos inteligentes para interacción con el usuario.

Tipo de amenaza	Análisis de Riesgo IoT Smart Home	Activos afectados
Seguridad física	• Los dispositivos IoT Smart Home pueden ser vulnerables a ser robado físicamente esta es otra instancia de riesgo. • Los dispositivos están expuestos a sabotaje o vandalismo.	• Dispositivos IoT Smart Home. • Gateway. • Plataforma y backend. • Infraestructura.
Suplantación de identidad	• Suplantación de identidad en los dispositivos IoT Smart Home, los atacantes pueden explotar el automatismo de los dispositivos y la relación entre ellos. • Quebrantamiento de protocolos que configuran la comunicación entre dispositivos. • Intrusión en los procesos de ingreso de nuevos dispositivos. • Obtener información privada y acceso con credenciales falsas.	• Dispositivos IoT Smart Home. • Gateway. • Comunicación. • Información • Plataforma y backend. • Infraestructura. • Aplicaciones y servicios.
Manipulación de datos	• Manipulación de datos en las rutas del sistema, manipulación de datos sensibles en	• Dispositivos IoT Smart Home. • Gateway.

	puntos de recopilación, procesamiento, transporte y almacenamiento. • No reside en dañar los dispositivos, sino en manipular información para causar caos o algún beneficio económico.	• Comunicación. • Información. • Plataforma y backend. • Infraestructura. • Aplicaciones y servicios.
Man in the middle	• El atacante intercepta los datos que intercambian los dispositivos IoT Smart Home. • Mientras los datos están en tránsito SSL o TLS pueden ser motivo de amenaza y ataque.	• Dispositivos IoT Smart Home. • Comunicaciones. • Información.
No Repudio	• El sistema IoT Smart Home presenta debilidades que pueden permitir a un atacante adicionar un dispositivo (nodo) malicioso que alimente datos incorrectos que pueden confundir procesos de análisis y de operación. • Se pueden visibilizar cambios de estado y variaciones de tiempo en los procesos de funcionamiento de un hogar inteligente. • Estos dispositivos cuentan normalmente con puertas traseras que pueden emplearse para atacar otros activos.	• Dispositivos IoT Smart Home. • Gateway. • Información. • Comunicación. • Plataforma y backend. • Infraestructura.
Divulgación de información	• Intrusión de un atacante en los métodos de procesamiento de información provoca riesgo de divulgación de información confidencial. • Datos en reposo son susceptibles a ser robados, los nodos de almacenamiento deben tener especial cuidado. • Esta amenaza afectan tanto a la privacidad del usuario como la exposición de los elementos en red a personas no autorizadas.	• Dispositivos IoT Smart Home. • Gateway. • Comunicación. • Información. • Plataforma y backend. • Infraestructura. • Aplicaciones y servicios.
Denegación de servicio	• La infraestructura de mensajería, de datos, de variables y APIs son procesos en los	• Dispositivos IoT Smart Home.

distribuido (DDoS)	cuales puede incurrir la amenaza de denegación de servicios, puede inutilizar un dispositivo, recurso de red o el servicio de un host. • El riesgo de que un nodo deshonesto bloquee las transmisiones a un nodo legítimo provoca la interrupción del funcionamiento temporal o permanente del sistema. • El riesgo de que ciberdelincuentes secuestren dispositivos para reclutarlos de forma de Botnet supone un perjuicio importante para los usuarios de hogares inteligentes.	• Gateway. • Plataforma y Backend. • Infraestructura. • Aplicaciones y servicios.
Elevación privilegiada	• Las capacidades de los dispositivos no suelen ser iguales, existen niveles de autenticación y distintas cuentas de usuario, esto provoca riesgo de intrusión de un ataque debido a que existen métodos de autenticación débiles. • Las funciones administrativas a nivel de usuario dentro de los dispositivos IoT Smart Home pueden ser débiles en cuanto a la capacidad de administración.	• Dispositivos IoT Smart Home. • Gateway. • Plataforma y backend. • Infraestructura.
Secuestro de dispositivos	• Los dispositivos IoT Smart Home son susceptibles a ser secuestrados por atacantes, estos dispositivos no varían su función pero sirven como herramienta para infectar a otros dispositivos con algún malware, así por ejemplo un enchufe inteligente vulnerable puede ser secuestrado y usado para tener acceso a la cerradura y abrirla.	• Dispositivos IoT Smart Home. • Gateway. • Información. • Comunicaciones.
Ingeniería social	Los usuarios de hogares inteligentes pueden ser manipulados para entregar información y accesos al sistema IoT Smart Home aprovechándose de las emociones de las personas.	• Dispositivos IoT Smart Home. • Gateway. • Información. • Comunicaciones.

		• Plataforma y Backend. • Infraestructura
Problemas con la cadena de suministro	El sistema en su conjunto y sus relaciones pueden presentar vulnerabilidades a ataques.	• Dispositivos IoT Smart Home. • Gateway. • Información. • Comunicaciones. • Plataforma y Backend. • Infraestructura.

Tabla 4.8.- Evaluación de amenazas, riesgo y activos IoT Smart Home afectados (Russell & Van Duren, 2016).

Una vez que se han revisado y se han comparado protocolos y tecnologías más utilizadas en un entorno IoT Smart Home y ataques, vulnerabilidades y amenazas que conlleva este sistema, se continuará con la construcción del mecanismo de seguridad más adecuado que disminuya al máximo el riesgo asociado a ataques y amenazas para un sistema Smart Home, se evaluarán sus posibles contramedidas y en base a lo estudiado se escogerán las mejores recomendaciones de seguridad para un mejor desenvolvimiento de un hogar inteligente.

4.3.4 Consideraciones de Seguridad para un Sistema IoT Smart Home

El diseño de un mecanismo seguro para un sistema IoT Smart Home depende de una lista de recomendaciones de seguridad, el propósito de este documento es describir un conjunto de criterios de seguridad que disminuyan el riesgo o mitiguen las vulnerabilidades a un creciente número de amenazas que apuntan a las redes IoT Smart Home con recursos limitados, en la actualidad todavía no se cuentan con dispositivos con capacidad de cumplir criterios de seguridad básicas para resguardar datos sensibles almacenados y proteger el intercambio de datos a través de redes vulnerables. En la tabla 4.9 se describen los niveles del sistema IoT Smart Home y se describen algunas consideraciones que se deben tener en cuenta al momento de construir una base de mecanismos de seguridad para el sistema (González García, 2017).

NIVEL	DESCRIPCIÓN	CONSIDERACIONES

Dispositivos/Gateway	Entre los dispositivos o a través del Gateway publican los datos del sensor y reciben las instrucciones para ejecutar las funciones de control.	- Autenticación - Cifrado de mensajes - Suministro y verificación de certificados - Arranque seguro - Transporte seguro - Firewalls - Actualizaciones de firmware y parches
Red/Transporte	Plataforma de mensajería IoT Smart Home	- Autenticación de dispositivos - Autorización - Seguridad de la API - Configuración de seguridad - Transporte seguro
Aplicación	Despliegue de aplicaciones IoT Smart Home	- Seguridad de la aplicación (API segura) - Descifrado de mensajes - Mensaje de verificación de checksum - Seguridad de Node-RED

Tabla 4.9.- Consideraciones de seguridad para un sistema IoT Smart Home (González García, 2017).

Estas consideraciones son fundamentales para la construcción de un mecanismo de seguridad para un sistema IoT Smart Home, con este estudio se puede mitigar en gran parte la falta de

seguridad, tomando en cuenta que disponer de dispositivos conectados involucra graves inconvenientes a la confidencialidad y privacidad de información que sumada la aparición de técnicas más poderosas de hacking se obtiene cada vez un mayor número de ciberataques exitosos.

4.4 Mecanismo de seguridad para un Sistema IoT Smart Home

Los criterios de evaluación se dividen en tres niveles representativos del sistema IoT Smart Home. Se han tomado en cuenta los mecanismos y recomendaciones de seguridad implementados por fabricantes IoT reconocidos y con experiencia (AWS, DigiKey, Samsung, etc.), también estándares y recomendaciones de seguridad de proyectos e instituciones reguladoras y de control (Proyecto OWASP de IoT, IEEE, etc.).

En la tabla 4.10 se muestra el mecanismo de seguridad más adecuado para un sistema IoT Smart Home, la aplicación del mecanismo en su respectivo nivel tomando en cuenta las recomendaciones cumplirá con el propósito de dar seguridad, privacidad y confidencialidad a la información y de mitigar las vulnerabilidades, amenazas y riesgos del sistema IoT Smart Home.

NIVEL	MECANISMO DE SEGURIDAD IOT SMART HOME	RECOMENDACIÓN
Dispositivos IoT Smart Home y Gateway	Seguridad física	• Asegurar la funcionalidad de activación y desactivación de puertos físicos en dispositivos IoT Smart Home Ej. Puertos USB. • Limitar las capacidades de administración de dispositivos a un interfaz local. • Asegurarse de utilizar un mínimo número de puertos físicos externos. • Garantizar la no transferencia de datos con la pertenencia de los dispositivos.

	Autenticación	• Credenciales de autenticación o claves criptográficas: • Los dispositivos IoT Smart Home deben incluir opciones de contraseña, las opciones de contraseñas mayores a ocho caracteres y autenticación deben ser posibles ya que cada vez existen mejores plataformas de cifrado y seguridad (autenticación de dos factores). • Permitir el cambio de nombre y de contraseña predeterminado. • Insertar mecanismos de recuperación de contraseñas de manera segura. • Insertar la opción de contraseña caducada para cambio después de ciertos periodos de tiempo. • La capacidad de seguridad de los dispositivos IoT Smart Home dependen fundamentalmente de la seguridad de las claves y datos secretos utilizados por los algoritmos criptográficos
	Cifrado de mensajes	• La criptografía debe hacer cumplir los tres principios de seguridad de la confidencialidad, la autenticación (verificar la fuente del mensaje), el no repudio (probar que el remitente creo un mensaje cifrado o firmado) y la integridad. Recopilar la mínima cantidad de datos personales en lo posible es una regla primordial. • El uso de una tecnología que cifre la comunicación protegerá los datos en tránsito entre dispositivos o hacia el Gateway (tabla 4.2).Por otra parte cifrar en lo posible los datos antes de su transferencia es una tarea inevitable. • Incluir opciones de cifrado AES128-AES 256 que son seguras contra ataques de fuerza bruta y da un mejor rendimiento al sistema. • Permitir la opción de detección de actividad fraudulenta y de autodefensa en caso de que se detecte un compromiso a los dispositivos.

		• El uso de dispositivos IoT Smart Home que contengan circuitos integrados dedicados a la seguridad y aceleradores de criptografía mejoran notablemente la seguridad a estos sistemas.
	Arranque seguro	• El arranque seguro o el reinicio de los dispositivos es un mecanismo importante de seguridad para restablecer el funcionamiento correcto del sistema que se ha desestabilizado accidental o intencionalmente. • Incluir una cadena de confianza establecida en el momento del arranque y que se extienda a través de todas las capas del entorno de ejecución ya que en la práctica el reinicio no garantiza la integridad del sistema, con un firmware comprometido por un hacker el sistema continuará bajo el control de él. • Permitir que la imagen del firmware del sistema se pueda firmar con una clave privada de un par de claves privadas-públicas creadas con un algoritmo criptográfico sólido. • Incluir almacenamiento seguro y aceleradores de criptografía en dispositivos con mayor capacidad de un arranque seguro.
	Software y Firmware seguro	• Es fundamental la planificación de actualizaciones y parches de software para conservar la continuidad de los dispositivos IoT Smart Home en el transcurso del tiempo. • Los dispositivos deben tener la capacidad de actualización y actuar rápidamente al existir vulnerabilidades. • Asegurar actualizaciones que contengan cifrado y descifrado, firmas criptográficas que puedan ser detectadas por los dispositivos que no permitan enviar descargas por canales que no son de confianza.

		• Mantener un firewall instalado y actualizado aporta a la seguridad para protegerse contra un malware en el sistema.
Red/Transporte	Cifrado de transporte	• Hacer uso de protocolos con cifrado o cifrar datos antes de su transmisión protegerán los datos en tránsito. • Cifrar la comunicación de extremo a extremo, el cifrado permite que los puntos finales validen la identidad y garanticen que las comunicaciones no sean interceptadas o redirigidas. • Verificar la aplicación de seguridades de protocolo MQTT (Tabla 4.6) verificar y autenticar la presencia del usuario autorizado para prevenir ataques. • Proteger el Gateway (puerta de enlace) para evitar fugas y transferencias de información no deseadas.
	Autorización	• Efectuar controles de acceso para prevenir desvío o modificación de información en las vías de transmisión desde el dispositivo IoT Smart Home hacia la nube, ataques mediante Man in the middle invalidando la difusión o suplantando dispositivos o usuario. • Implementar controles para prevenir la divulgación de información, los ciberdelincuentes una vez que interceptan la comunicación pueden acceder y divulgar información sin autorización. • Efectuar controles para mitigar ataques de DDoS (denegación de servicio) con ello el atacante evita enviar la información a su destino.
	Configuración de seguridad	• Tomar en cuenta los vectores de ataque que pueden presentar la red y los servicios del dispositivo.

		• Utilizar interfaces de red probadas y comprobadas. • Aseguramiento de las interfaces de red de prueba y mantenimiento, estas se encuentren deshabilitadas y protegidas adecuadamente. • Asegurar el uso de protocolos autenticados y canales cifrados. • Bloqueo de servicios innecesarios e implementación de reglas de firewall.
Aplicación (Plataforma de la Nube)	Seguridad en la nube	• Consultar al proveedor de Cloud sobre las políticas y estrategias que se utilizan para mitigar las amenazas a aplicaciones IoT Smart Home. • Revisar que las interfaces en la nube puedan encontrar vulnerabilidades por ejemplo interfaces web. • Impulsar el uso de políticas de protección a la confidencialidad de información, los proveedores de servicios en la nube comparten infraestructura y plataforma que pueden ser exploradas por terceros y hacer un mal uso de información confidencial. • Verificar a nivel de protocolo (MQTT, HTTP, CoAP) se cumpla con los permisos de acceso para mitigar ataques de DDoS (denegación de servicio) a las App en la nube. • Verificar que los servicios de *Cloud* mantengan sitios alternos de almacenamiento de datos (*Data Centers*), en caso de desastres naturales evitar la pérdida de ellos.
	Suministro y verificación de certificados, autenticación y autorización	• Asegurar el uso de autenticación de conexión y autorización de uso de dispositivos y recursos en la nube como métodos de seguridad. • Asegurar el uso de controles de acceso a la plataforma de la nube como son: control de credenciales e identidad.

		• Realizar controles para evitar riesgos de software operativo en la nube como: partición del sistema operático de sólo lectura, imagen cifrada y firmada. • Verificar el uso de cifrado y firmas en el almacenamiento de datos, con esto asegurar la privacidad de la información.

Tabla 4.10.- Descripción del mecanismo de seguridad para un entorno IoT Smart Home (Autor).

Después de haber realizado un análisis completo de todo el sistema IoT Smart Home podemos decir que la construcción de un mecanismo seguro depende de una serie de recomendaciones de seguridad, la seguridad de un entorno IoT Smart Home depende de múltiples capas de protección que se van desde la base de hardware de dispositivos IoT hasta su entorno de ejecución por el usuario.

La aplicación de un solo mecanismos de seguridad para un entorno IoT Smart Home no sería suficiente para enfrentar diferentes técnicas de hacking y cada vez nuevos ciberataques peligrosos, la velocidad con la que crece la tecnología IoT y a su vez las seguridades es la misma con la que ciberdelincuentes incrementan su poder de causar daño y obtener información de un sistema IoT Smart Home, la obligación de fabricantes y de diseñadores de este entorno es el desarrollo y aplicación de nuevos mecanismos de seguridad, actualizar sus metodologías es un deber continuo contra ataques y vulnerabilidades del sistema.

CAPITULO V

5. SIMULACIÓN Y EVALUACIÓN DEL MECANISMO DE SEGURIDAD IOT SMART HOME

5.1 Introducción

Como se vio en los capítulos anteriores de este trabajo, todos los sistemas IoT y específicamente IoT Smart Home están expuestos a varias amenazas y ataques de seguridad que vulneran la seguridad de dispositivos IoT conectados al internet. Después, se logró encontrar un mecanismo que mitigue dichas amenazas y ataques perpetrados por personas que se dedican a la ciberdelincuencia, la aplicación de dicho mecanismo y sus respectivas recomendaciones en un sistema IoT Smart Home dará como resultado un sistema más seguros, brindando, privacidad, confiabilidad y disponibilidad de sus datos y de su sistema.

La aplicación práctica de un entorno IoT Smart Home dará un conocimiento más profundo y real sobre la seguridad del sistema, mostrará tanto el funcionamiento, la automatización y las prestaciones que brinda el sistema como también las vulnerabilidades, amenazas y riesgos a los que se expone, ya que sabemos de la presencia de ciberdelincuentes que siempre van a intentar irrumpir en el entorno IoT Smart Home. Además, analizar las consecuencias y daños que pueden ocurrir en el entorno y finalmente aplicar los mecanismos y recomendaciones de seguridad adecuados para poder enfrentar y mitigar los ataques que pueden concluir con violación a la privacidad, robo de información e incluso daños a la propiedad privada.

5.2 Implementación sistema IoT Smart Home

Para realizar la aplicación del mecanismo de seguridad y simular lo que los ciberdelincuentes pueden causar a un sistema IoT Smart Home, se implementó un hogar típico inteligente. Tomando como referencia la arquitectura IoT Smart Home de este estudio, este hogar inteligente incluyó dispositivos IoT Smart Home, la red a la cual se integrarán dichos

dispositivos para su comunicación, la plataforma del internet y la nube y finalmente los servicios de APIs y la interacción con los usuarios finales del hogar inteligente.

En la figura 5.1 se muestra la arquitectura IoT Smart Home implementada, la arquitectura muestra 4 capas de conexión, la primera es la de dispositivos o capa de percepción, la segunda es la capa de red, la tercera la plataforma de cloud e internet y finalmente la de aplicación y usuario.

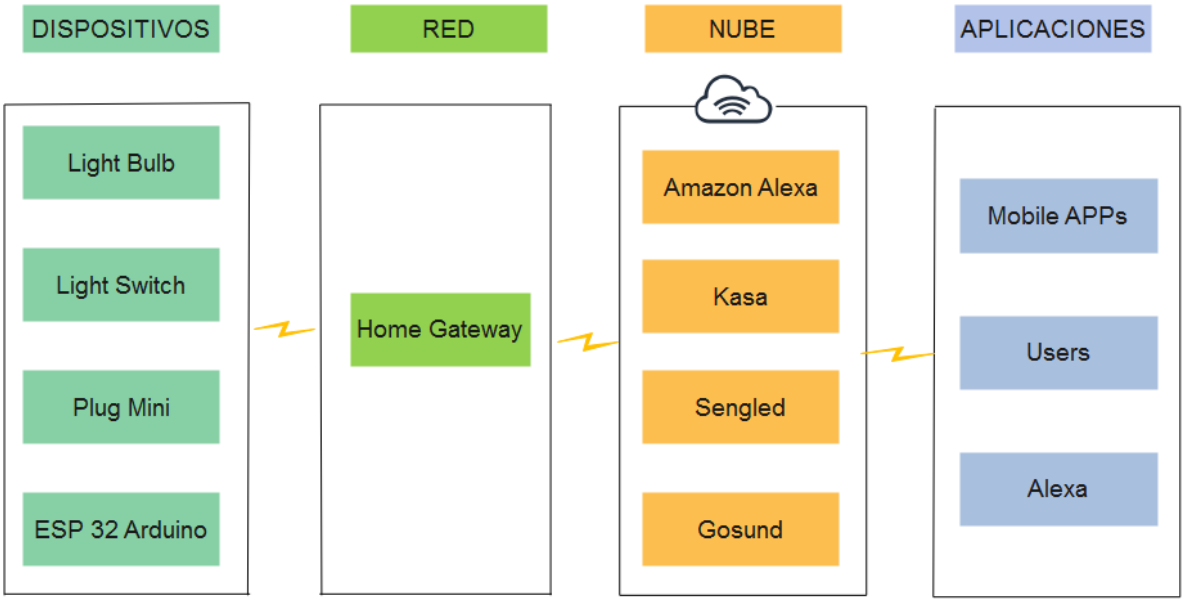


Fig.-5.1. - Arquitectura IoT Smart Home implementado (Autor).

La capa de dispositivos IoT Smart Home se conecta en una topología estrella, esta topología hace que todos los nodos inalámbricos se comuniquen directamente con un controlador, la ventaja del uso de esta topología es el bajo consumo de energía, esta ventaja es necesaria ya que los dispositivos están conectados al sistema de forma continua las 24 horas y los 365 días del año.

Los distintos dispositivos IoT utilizados en nuestro hogar inteligente se comunican por medio del estándar 802.11 WiFi y del estándar 802.15 Bluetooth, esto hace que la aplicación práctica se acerque más a la realidad de un hogar inteligente típico donde interactúan dispositivos de distintos fabricantes con distintas tecnologías, lo que da como resultado la interoperabilidad de dispositivos dentro de un sistema IoT Smart Home.

En la capa middleware cloud, se utilizan las aplicaciones y los servicios de los fabricantes de cada uno de los dispositivos, como también la aplicación y servicios del controlador Echo Dot Alexa, estas aplicaciones son descargadas a un dispositivo inteligente para la interacción con el usuario final del sistema Smart Home, en este caso a un Smartphone.

En la tabla 5.1 se muestra el listado de dispositivos inteligentes que se implementaron en el sistema IoT Smart Home como son: interruptores, toma corrientes, luces, controlador de cerraduras y persianas, un concentrador con el que se controlará los dispositivos y un Gateway para la conexión a internet y la nube.

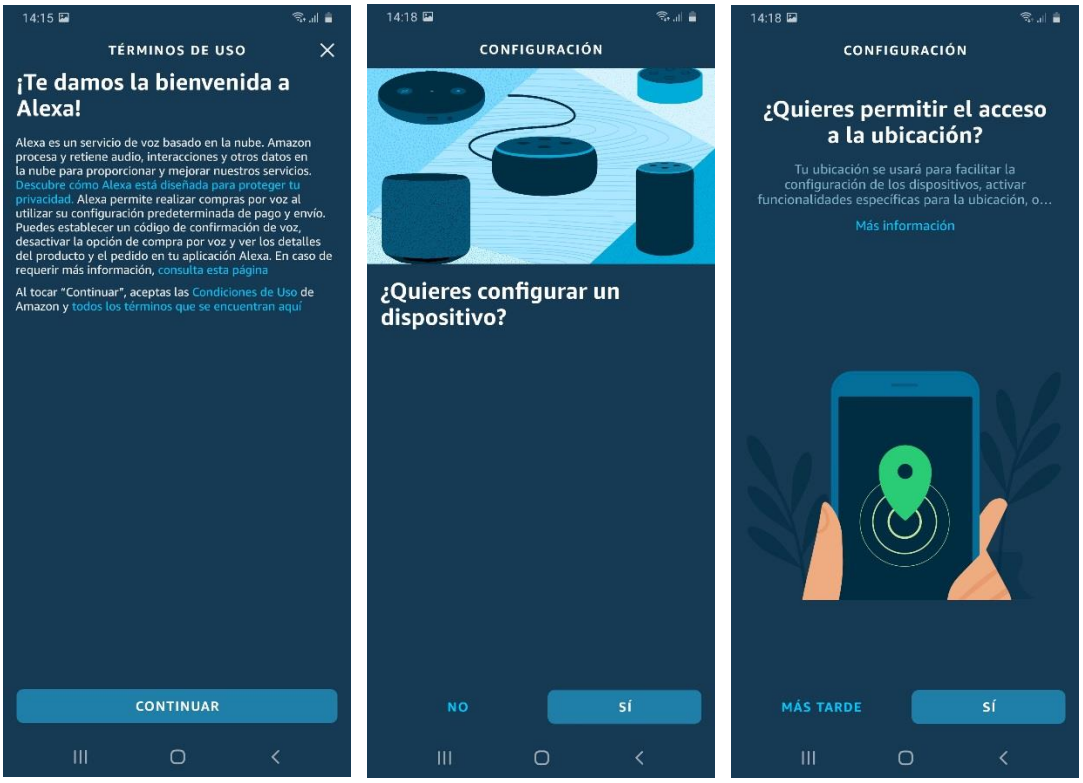
ITM	DISPOSITIVO	DESCRIPCIÓN	MARCA	CANTIDAD
1	Luces	WI-FI LED Light Bulb	Nite Bird	4
2	Luces	Bluetooth Smart LED Light Bulb	Sengled	1
2	Tomacorriente	Kasa Smart WI-FI Plug Mini	Tp-link	4
3	Interruptor	Kasa Smart WI-FI Light Switch	Tp-link	1
4	Cerradura-Persiana	WI-FI ESP-WROOM-32	Arduino	1
6	Router	Echo Life Home Gateway	Huawei	1
7	Alexa	Echo Dot Alexa	Amazon	1

Tabla 5.1.- Dispositivos IoT Smart Home implementados (Autor).

Los dispositivos IoT fueron distribuidos en distintas áreas de la Smart Home. Los dispositivos se encargan de automatizar distintos ambientes y sistemas de seguridad, estos dispositivos nos servirán para probar la seguridad del sistema IoT Smart Home como las amenazas y vulnerabilidades que se pueden presentar y evaluar las recomendaciones del mecanismo de seguridad estudiado.

5.2.1 Configuración de la red IoT Smart Home

Una vez seleccionados y ubicados los dispositivos IoT dentro de la Smart Home se procede a la conexión, primeramente se vinculó el controlador Echo Dot Alexa a un dispositivo móvil inteligente para nuestro caso un Smartphone Android Samsung, para esto se tuvo que descargar e instalar una aplicación móvil de la tienda Amazon a nuestro dispositivo móvil, la aplicación Amazon Alexa solicitó el registro de un correo electrónico personal y contraseña para inicio de sesión, se solicitó además la activación de la ubicación y de la comunicación Bluetooth del Smartphone para el reconocimiento de dispositivos, una vez reconocido el controlador Echo Dot Alexa este pide vincularse a la red WiFi del hogar logrando tener comunicación al Gateway Doméstico Huawei y su conexión a Internet. En la figura 5.2 se muestra el proceso de vinculación del dispositivo Echo Dot Alexa a la red.



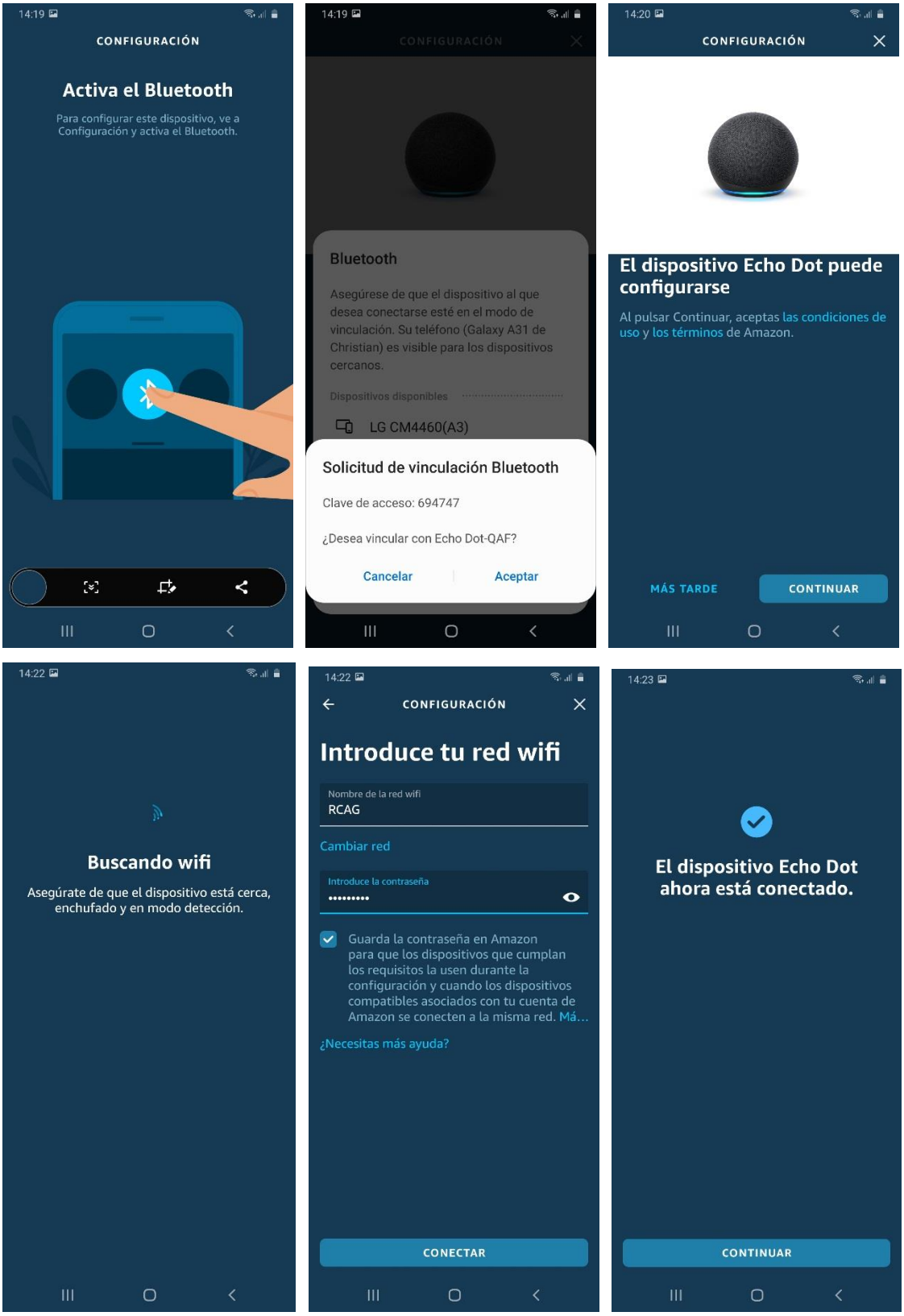


Fig. 5.2.- Proceso de vinculación del dispositivo Echo Dot Alexa a la red (Autor).

Una vez realizado el proceso de vinculación del controlador Echo Dot Alexa, continuamos con la vinculación de los demás dispositivos en los distintos ambientes del hogar como se muestra el proceso de la figura 5.3.

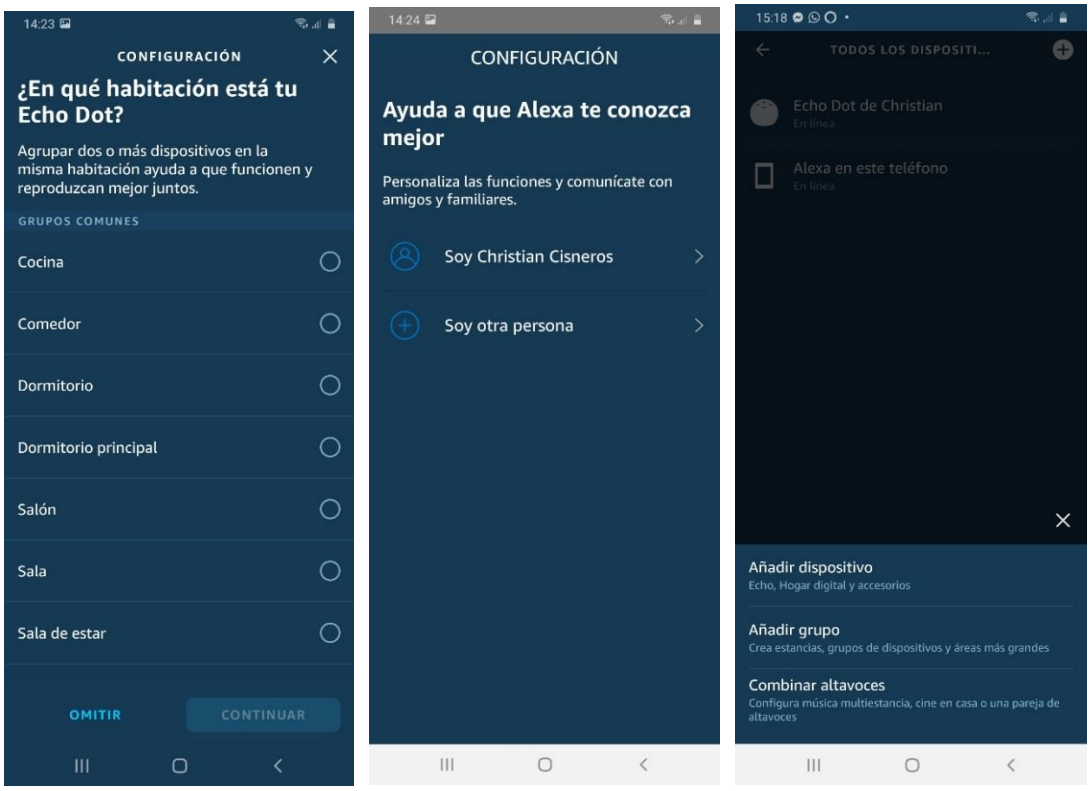


Fig. 5.3.- Proceso de vinculación de dispositivos en distintos ambientes Smart Home (Autor).

Sin embargo, para la inicialización y activación de los dispositivos se debe utilizar la aplicación de los fabricantes de cada dispositivo. Después los dispositivos se integraran al controlador Echo Dot Alexa con el que finalmente los usuarios tendrán que interactuar para el manejo y control del hogar inteligente.

En la figura 5.4 se muestran los pasos a seguir para inicializar el interruptor y los tomacorrientes inteligentes con la app Kasa, la aplicación de igual forma se descarga de la tienda al dispositivo móvil, se crea una cuenta, se aceptan los términos y políticas de privacidad y se inicia la configuración.

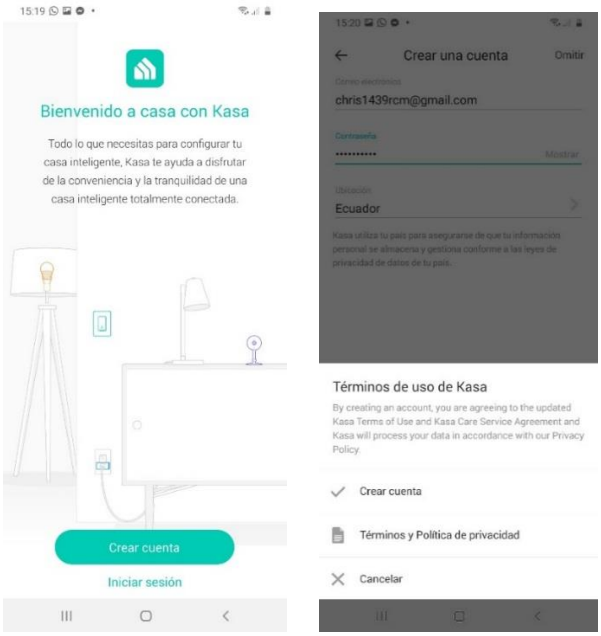


Fig. 5.4.- Descarga de la App Kasa (Autor).

Después se continúa con la integración de la App Kasa con la App de Amazon Alexa, en la figura 5.5 se muestra el procedimiento para la integración de las aplicaciones, la App Kasa permite trabajar con servicios de terceros como son Amazon Alexa, Asistente de Google y Samsung Smart Things para ayudar a que la administración de dispositivos sea más inteligente y sencilla.

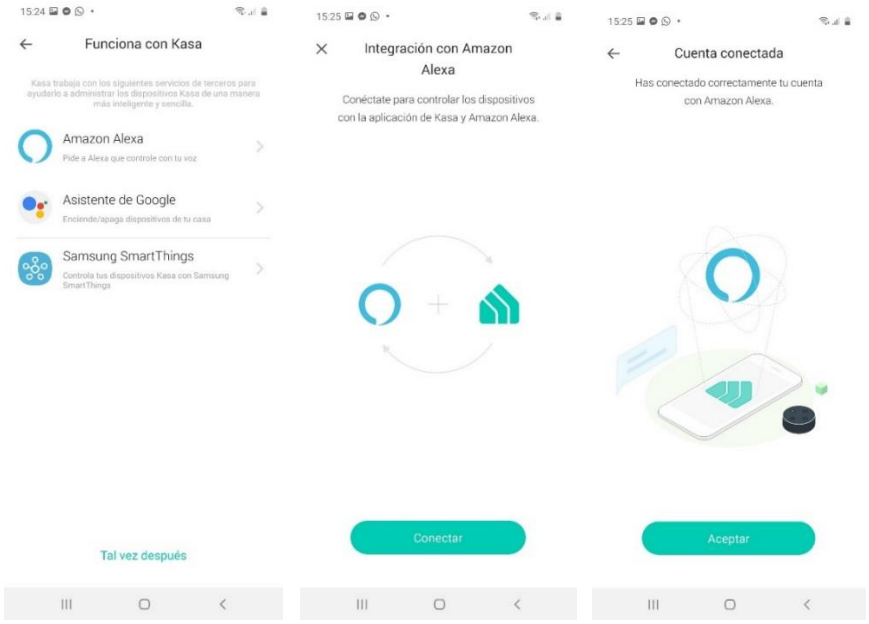


Fig. 5.5.- Procedimiento para integración de aplicaciones (Autor).

A continuación se empieza a conectar dispositivos a la red realizando una prueba de su funcionamiento tanto por el comando de control de las aplicaciones como por comandos de voz con ayuda del controlador Echo Dot Alexa. En la figura 5.6 se muestra el procedimiento para vincular dispositivos Kasa al sistema.

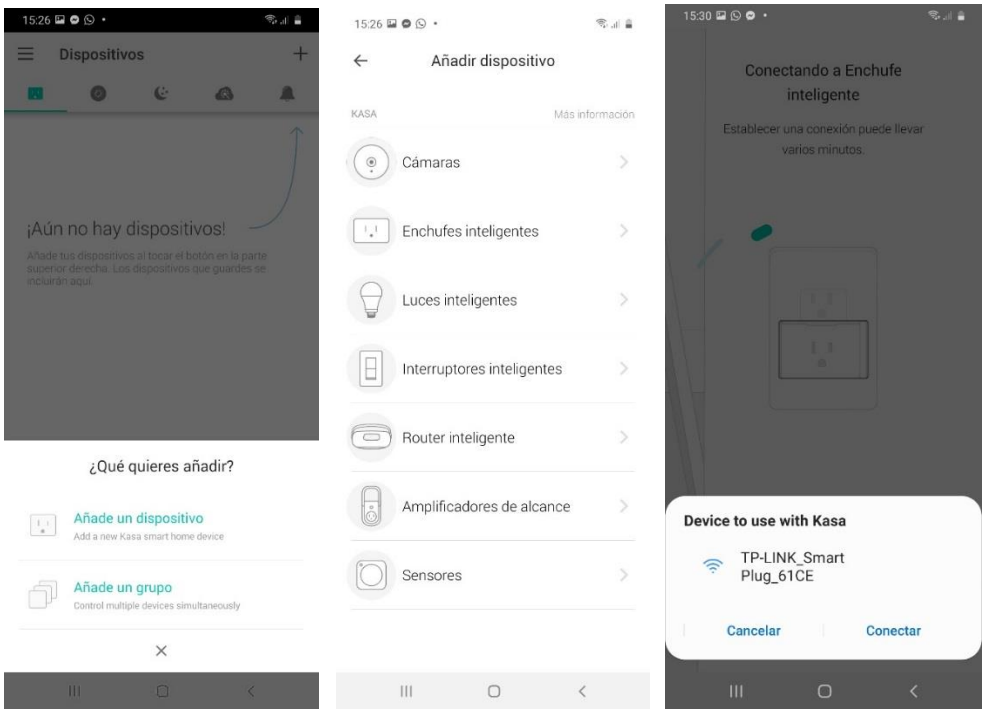


Fig. 5.6.- Procedimiento para vincular dispositivos Kasa al sistema IoT Smart Home (Autor).

El tipo de conexión que se usa para añadir dispositivos Kasa a la red del sistema es por medio de WiFi, el mismo procedimiento se usa para añadir un interruptor y cuatro tomacorrientes inteligentes.

Se procede de la misma manera para conectar dispositivos IoT Smart Home de la marca Nite Bird que usa la App Gosund y de la marca Sengled que usa la App Sengled Home, este último mantiene una conexión continua Bluetooth con el controlador Echo Dot Alexa. En las figuras 5.7 y 5.8 se resumen los procedimientos para conexión a las Apps de Gosund y Sengled y finalmente al controlador Echo Dot Alexa.

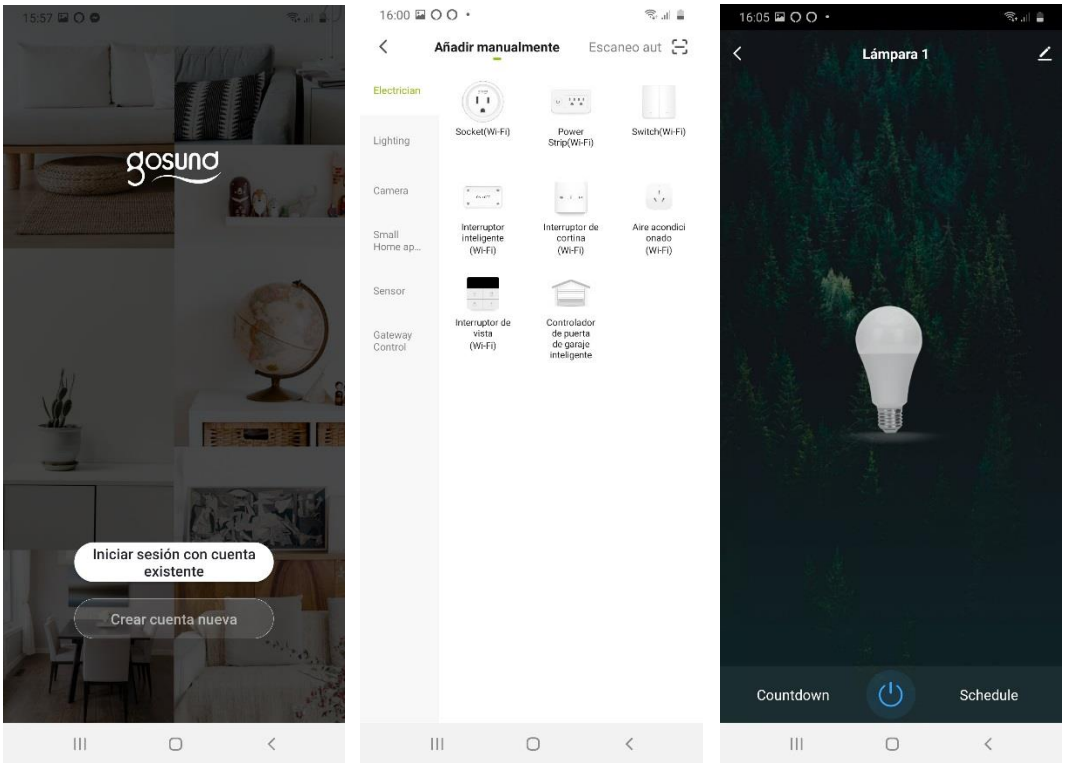


Fig. 5.7.- Descarga de la App Gosund y conexión de dispositivos al sistema IoT Smart Home (Autor).

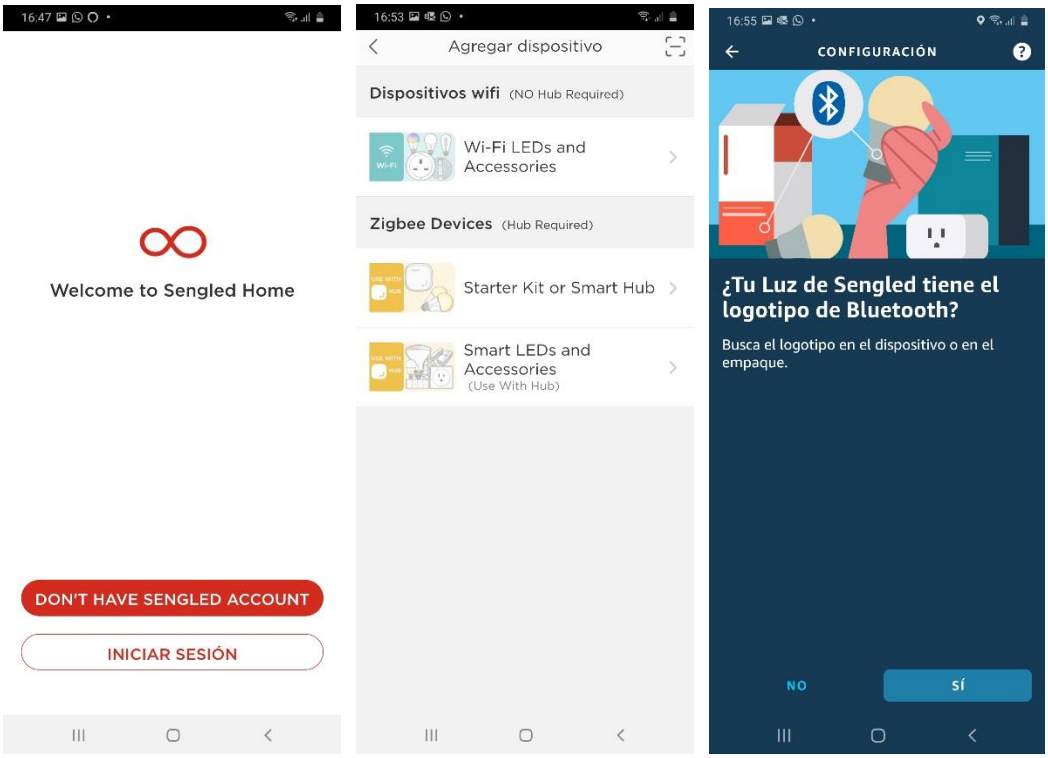


Fig. 5.8.- Descarga de la App Sengled Home y conexión de dispositivos al sistema IoT Smart Home (Autor).

Una vez implementada la Smart Home se puede observar las prestaciones que ofrece un sistema inteligente, automatizar ambientes, controlar luces y electrodomésticos, aseguramiento del hogar, etc. Muestra las razones del desarrollo y crecimiento acelerado de estos sistemas, pero como vimos en capítulos anteriores este crecimiento hace que los ciberdelincuentes encuentre un entorno cada vez más amplio para la aplicación de amenazas y ataques que ponen en riesgo a los sistemas IoT Smart Home y a sus ocupantes, a continuación se va a realizar intentos de irrupción del sistema y se revisarán las vulnerabilidades y amenazas a las que se expone y los posibles mecanismos de seguridad que mitiguen dichas inseguridades.

5.3 Análisis de vulnerabilidades y amenazas del sistema IoT Smart Home

Una vez implementada la red de dispositivos IoT Smart Home, el usuario puede manipular estos dispositivos manualmente a través del teléfono inteligente por medio de la aplicación Amazon Alexa o por las aplicaciones específicas de cada fabricante como son Kasa, Gosund y Sengled Home o por comandos de voz por medio del dispositivo Echo Dot Alexa, las *SmartApps* se implementan en la nube y también pueden interactuar con nubes de terceros para obtener mayores funcionalidades.

Desde el momento en que se inicializa el sistema IoT Smart Home los dispositivos se conectan a internet y empiezan a compartir información, los datos que transmiten y reciben los dispositivos inteligentes son llevados desde sus actuadores hasta la nube pasando por el Gateway y retornan a los dispositivos después de que esos datos sean procesados por las aplicaciones y sus sistemas, todo este proceso expone al sistema a amenazas y ataques de seguridad, provoca descubrimiento de vulnerabilidades del sistema IoT Smart Home y por consiguiente riesgo a la privacidad, seguridad y confiabilidad de los usuarios del hogar inteligente.

La aplicación de un mecanismo de seguridad y de las recomendaciones presentadas en este estudio brindará al sistema IoT Smart Home mayor privacidad, seguridad y confiabilidad de la información, a continuación vamos a observar las vulnerabilidades que se encontró en el sistema, las amenazas más comunes a las que se expone el sistema y las recomendaciones

que se pueden poner en práctica para mitigar en lo posible la inseguridad en el sistema IoT Smart Home.

5.3.1 Explorando vulnerabilidades

Para describir las posibles vulnerabilidades del sistema IoT Smart Home, existen varias herramientas útiles de auditoria para identificar vulnerabilidades de sistemas conectados a internet, el software que se han utilizado para este propósito es el siguiente:

- Advance IP Scanner.
- MobaXTerm.
- Nmap de Kali Linux.
- Hydra de Kali Linux.
- Wireshark.

Todos estos motores de búsqueda son utilizados para realizar pruebas de penetración y análisis de malware para los dispositivos IoT.

Los resultados que se lograron obtener con la aplicación de estas herramientas en el sistema IoT Smart Home son los siguientes:

Advance IP Scanner: En la figura 5.9 se muestra los dispositivos descubiertos y conectados a la red WiFi y Bluetooth de la Smart Home.

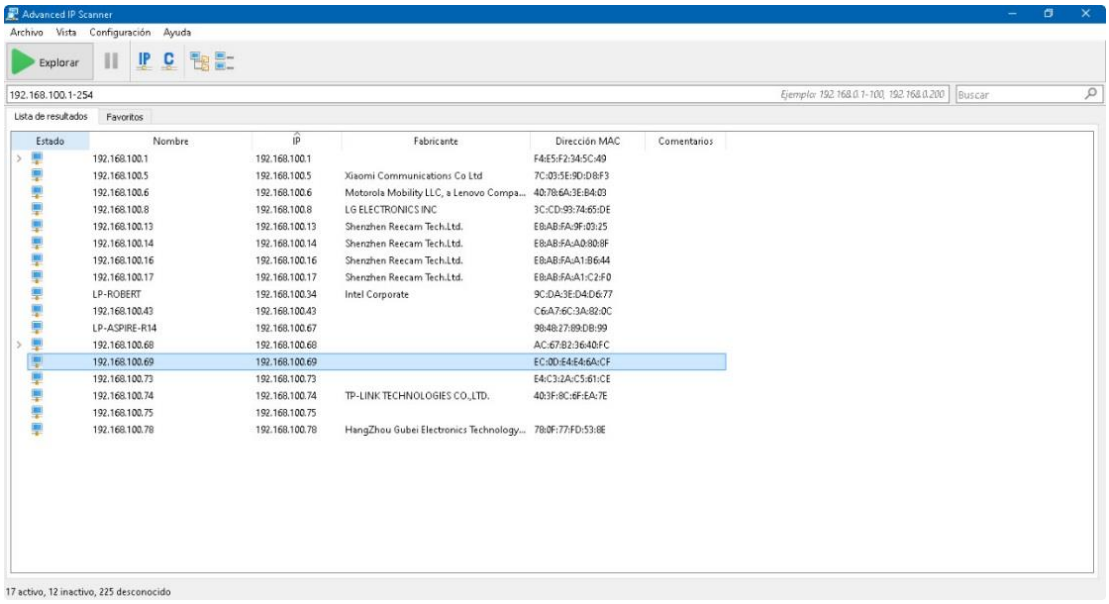


Fig. 5.9.- Auditoria con Advance IP Scanner al sistema IoT Smart Home (Autor).

MobaXTerm: En la figura 5.10 se muestra los puertos abiertos de los dispositivos conectados a la red IoT Smart Home.

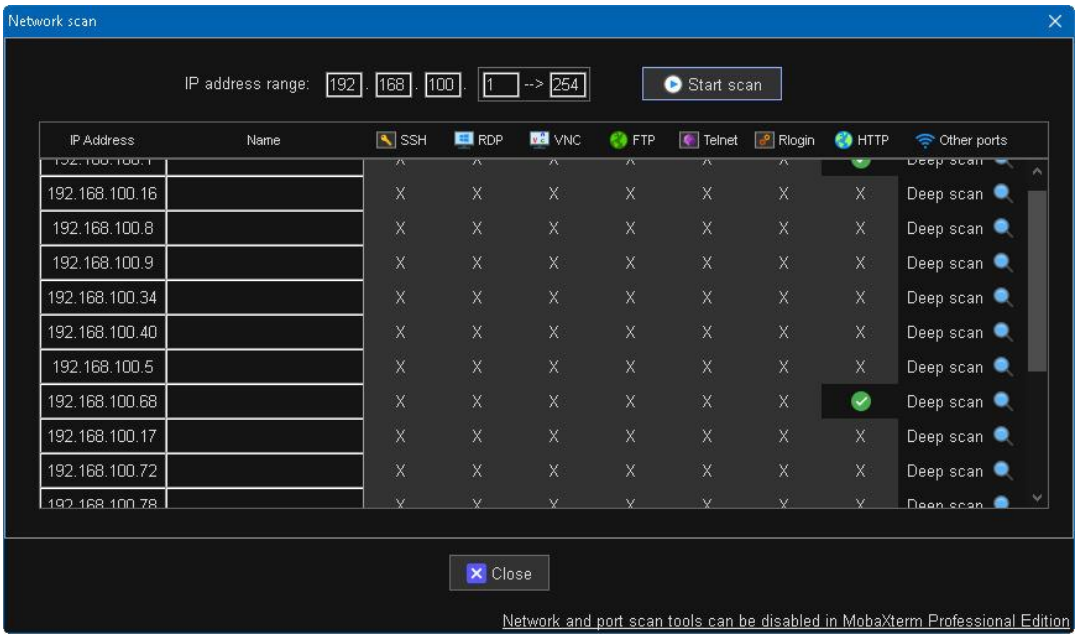


Fig. 5.10.- Auditoria con MobaXTerm al sistema IoT Smart Home (Autor).

Nmap e Hydra de Kali Linux: En las figuras 5.11 se expone información del estado de funcionamiento de los puertos de los dispositivos IoT Smart Home.

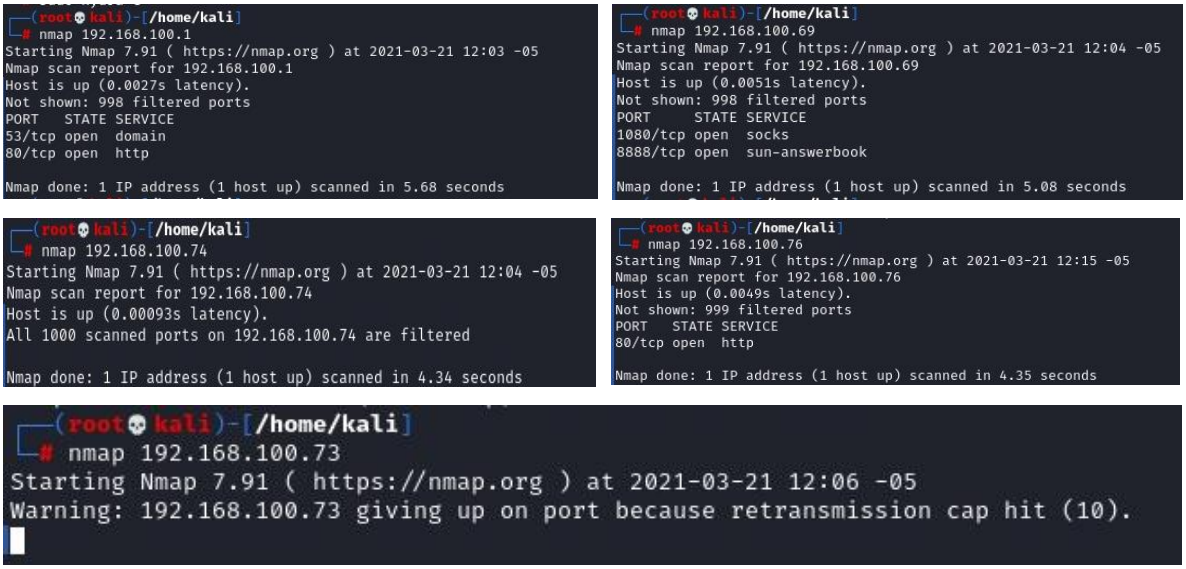


Fig. 5.11.- Auditoria con Nmap de Kali Linux al sistema IoT Smart Home (Autor).

Wireshark: En la figura 5.12 se indica la actividad de la red WiFi IoT Smart Home.

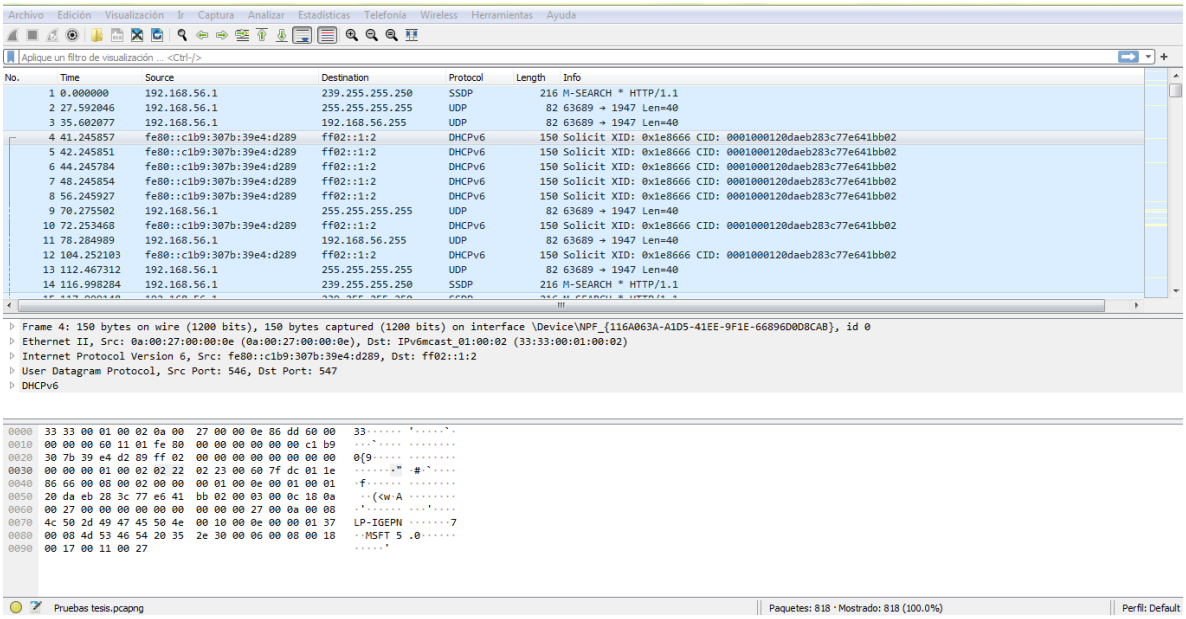


Fig. 5.12.- Auditoria con Wireshark al sistema IoT Smart Home (Autor).

Todas estas pruebas arrojan información importante sobre la red IoT Smart Home, la información no puede ser muy interesante para los usuarios finales pero si para un hacker o un cibercriminal ya que estos son puntos vulnerables de la red a la cual se podría perpetrar un ataque causando varias amenazas y riesgos a los datos, dispositivos y seguridad del sistema Smart Home.

En base a la auditoria, a continuación se mostrarán las vulnerabilidades más sobresalientes que se encontraron en la red IoT Smart Home.

5.3.1.1 *Aplicaciones y servicios en la nube inseguros*

Con la descarga de aplicaciones a nuestro dispositivo inteligente, los usuarios no tienen un conocimiento de cómo funciona la Smart App y que está haciendo con los datos y accesos que entregamos para su instalación, como ejemplo podemos ver que a la hora de la instalación de la App Amazon Alexa nos solicitó acceso a la ubicación, a nuestros contactos y a nuestras llamadas y mensajes. En la figura 5.13 se expone el proceso de solicitud de acceso.

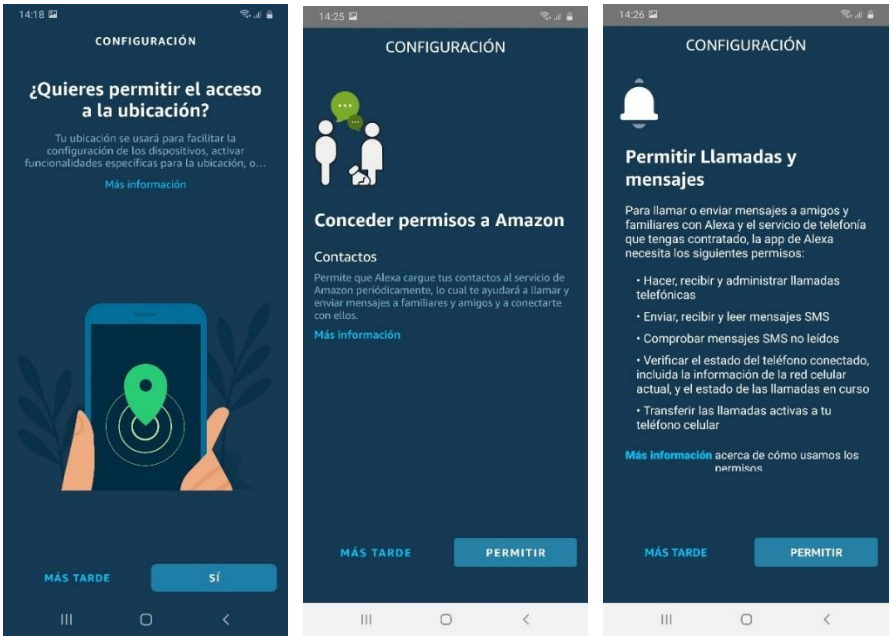


Fig. 5.13.- Solicitud de acceso a recursos al descargar las Smart Apps (Autor).

Se puede observar que la App puede hacer más cosas de las que el usuario espera, el usuario al dar permiso de acceso a ciertos recursos como contactos, llamadas, SMS, etc., de nuestro Smartphone está dando acceso a la información personal almacenada en nuestro dispositivo, además que si se da acceso a dispositivos internos como la cámara, teléfono, receptor GPS, etc., pueden ser utilizados para recuperar datos personales y registrar información dentro del hogar, datos que pueden estar en etapas de recopilación, procesamiento, transporte o almacenamiento en la nube, todo esto con el fin de que datos privados puedan publicarse o exponerse en nubes de terceros sin permiso del usuario o notificación.

Esto ocurre con la descarga de todas las Apps de los fabricantes de dispositivos IoT Smart Home, lo que provoca, que datos privados se compartan con un mayor alcance ya que cada aplicación puede compartir información con más nubes de terceros que sirven para brindar mayores servicios a los usuarios de dispositivos inteligentes.

5.3.1.2 *Autenticación de dispositivos*

Las Smart Apps y los dispositivos IoT Smart Home solicitan para acceder a los servicios la creación de una cuenta, para lo cual se solicita ingresar un correo y una contraseña, esta contraseña suele ser muy sencilla lo que hace que pueda ser adivinable o fácilmente

descubierta por ciberdelincuentes, en pruebas realizadas con distintas contraseñas se logró reconocer la clave de usuarios tipo. El acceso a las aplicaciones es una vulnerabilidad grave ya que el ciberdelincuente toma el control de los dispositivos, un dispositivo comprometido como un tomacorriente, un interruptor, una lámpara o una cerradura inteligente de nuestro hogar provoca riesgos de privacidad y seguridad. En la figura 5.14 se muestra la solicitud de un correo y una contraseña de las 3 Apps utilizadas para la implementación de nuestro sistema IoT Smart Home.

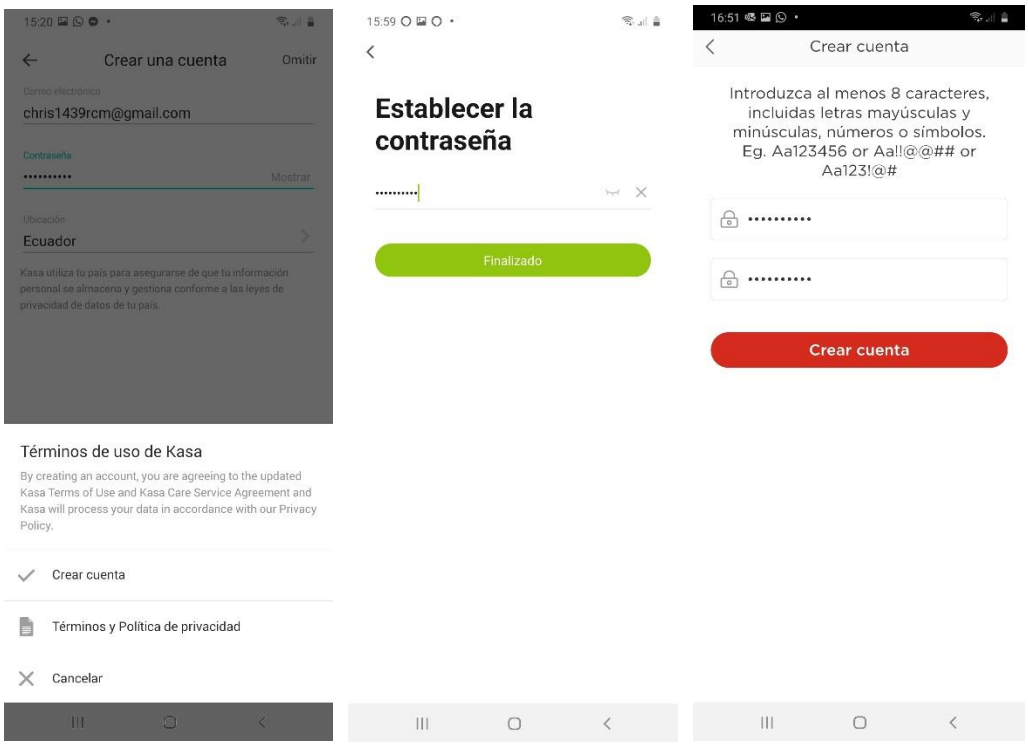


Fig. 5.14.- Solicitud de usuarios y contraseñas al descargar las Smart Apps (Autor).

Ahora bien si el Gateway Home es el objetivo de un ataque y se logra encontrar una vulnerabilidad en el Gateway Home podría ser catastrófico, los delincuentes podrían obtener el control total de los dispositivos IoT Smart Home como deshabilitar los controles de seguridad o denegar su uso. El uso de contraseñas débiles en el Gateway Home es una de las vulnerabilidades encontradas, con ayuda de software especializado y relativamente fácil de conseguir y descargar a un computador el sistema puede ser comprometido.

Software dedicado a descubrir contraseñas como: *WiFi Password Revealer, XenArmor WiFi Password o Password Kit* se puede lograr descubrir ciertas contraseñas cortas y débiles,

abriendo las puertas de nuestro hogar inteligente a intrusos y delincuentes. En la figura 5.15 se muestran las contraseñas encontradas por software, este proceso puede ser muy complejo el ataque que se realiza es de fuerza bruta, en nuestro caso fue menos complicado ya que las contraseñas utilizadas fueron muy sencillas y fáciles de descubrir por fines didácticos, aunque en la realidad existen este tipo de contraseñas que vulneran el Gateway Home y por ende el sistema IoT Smart Home.

Complete Wi-Fi Password Report:

Index	Wi-Fi Name (SSID)	Security Settings	Type	Password Key (Hex)	Password Key (Text)	Wi-Fi Security Analysis
1	Cacao Ecologde	WPA2-Personal (AES)	PassPhrase	6361**********	ca*******	Alert: Recommended to use WPA3 for better security.
2	Claro_CISNERSO	WPA2-Personal (AES)	PassPhrase	3137**********	17********	Alert: Recommended to use WPA3 for better security.
3	Claro_TORRES0002215186	WPA2-Personal (AES)	PassPhrase	544F**********	TO**********	Alert: Recommended to use WPA3 for better security.
4	CYBERDINNE	WPA2-Personal (AES)	PassPhrase	6361**********	ca********	Alert: Recommended to use WPA3 for better security.
5	Electronica	WPA2-Personal (AES)	PassPhrase	3136**********	16********	Alert: Recommended to use WPA3 for better security.
6	EPN-LA100	WPA2-Enterprise (AES)	EAP Auth		[Password is empty or not found]	Good: Recommended to use WPA3 for better security.
7	Galaxy A310BE2	WPA2-Personal (AES)	PassPhrase	7063**********	pc******	Alert: Short password can be cracked easily. Recommended to use strong password with more than 10 chars.
8	HOSTAL ARBOLITO 1	WPA2-Personal (AES)	PassPhrase	6172**********	ar******	Alert: Short password can be cracked easily. Recommended to use strong password with more than 10 chars.

CYBERDINNE	WPA2-Personal (AES)	PassPhrase	6361**********	ca********	Alert: Recommended to use WPA3 for better security.

Fig. 5.15.- Descubrimiento por software contraseñas del Gateway Home (Autor).

En la figura 5.16 se presenta un listado de credenciales predeterminadas comunes que usa el malware de Mirai y que hizo que sea tan eficiente en años anteriores, estas contraseñas eran establecidas por el administrador y una configuración deficiente de los dispositivos IoT provocaron ataques que causaron varios problemas de seguridad y privacidad en el mundo.

```
1  // root      xc3511     // root      vizxv          // root      admin
2  // admin     admin      // root      888888         // root      xmhdipc
3  // root      default    // root      juantech       // root      123456
4  // root      54321      // support   support        // root      (none)
5  // admin     password   // root      root           // root      12345
6  // user      user       // admin     (none)         // root      pass
7  // admin     admin1234  // root      1111           // admin     smcadmin
8  // admin     1111       // root      666666         // root      password
9  // root      1234       // root      klv123         // Administrator admin
10 // service   service    // supervisor supervisor    // guest     guest
11 // guest     12345      // guest     12345          // admin1    password
12 // administrator 1234   // 666666    666666         // 888888    888888
13 // ubnt      ubnt       // root      klv1234        // root      Zte521
14 // root      hi3518     // root      jvbzd          // root      anko
15 // root      zlxx.      // root      7ujMko0vizxv   // root      7ujMko0admin
16 // root      system     // root      ikwb           // root      dreambox
17 // root      user       // root      realtek        // root      00000000
18 // admin     1111111    // admin     1234           // admin     12345
19 // admin     54321      // admin     123456         // admin     7ujMko0admin
20 // admin     1234       // admin     pass           // admin     meinsm
21 // tech      tech
```

Fig. 5.16.- Listado de usuarios y contraseñas utilizado por malware Mirai.

5.3.1.3 *Suplantación de identidad*

Una vez que se ha descubierto la contraseña de nuestro Gateway Home (Router), se pudo adicionar a la red un nuevo dispositivo inteligente, la ESP-WROOM-32 es una placa de desarrollo que combina capacidades inalámbricas WiFi y Bluetooth, por ahora es una opción de bricolaje de IoT e IoT Smart Home, este dispositivo logró hacerse pasar por un dispositivo más de la red, por medio de la red WiFi del hogar el controlador Echo Dot Alexa lo reconoció como un dispositivo más del sistema, encontrando otra vulnerabilidad que pone en riesgo la seguridad y la privacidad de la red IoT Smart Home. En la imagen 5.17 se presenta una foto de la tarjeta de aplicación y desarrollo ESP-WROOM-32 (Tutorials, 2019).

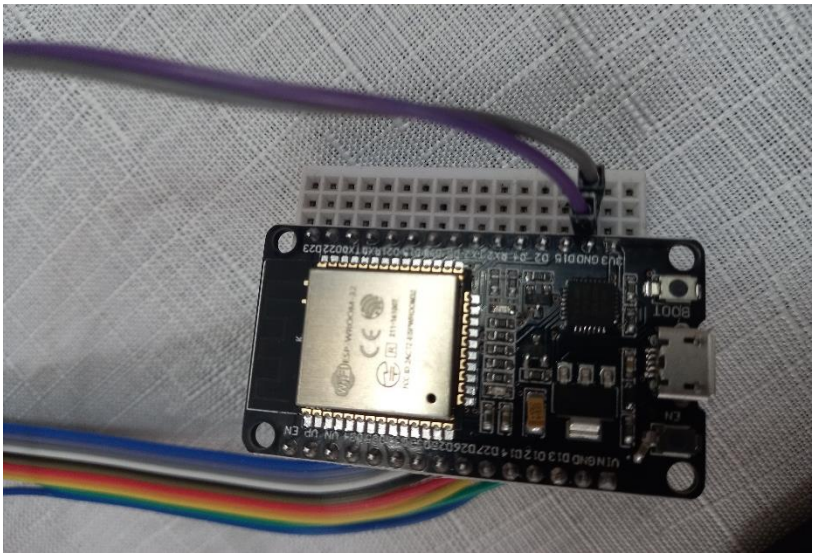


Fig. 5.17.- Tarjeta de desarrollo ESP-WROOM-32 (Autor).

Con la capacidad de programación de la placa ESP-WROOM-32 es posible poner en riesgo dispositivos e información sensible del hogar inteligente, podría extraer información del Echo Dot Alexa ya que Alexa desde una perspectiva de privacidad no cumple las exigencias para ser clasificado como un dispositivo seguro, de hecho se ha confirmado que desarrolladores pueden escuchar conversaciones de los usuarios (Marrugat, 2019).

En la figura 5.18 se muestra el código que se programó para que el dispositivo pueda ser reconocido por el Echo Dot Alexa, el código se puede encontrar en varias prácticas de desarrollo, lo que demuestra que la intrusión con ayuda de estas placas en la red de dispositivos no tiene mayor dificultad.

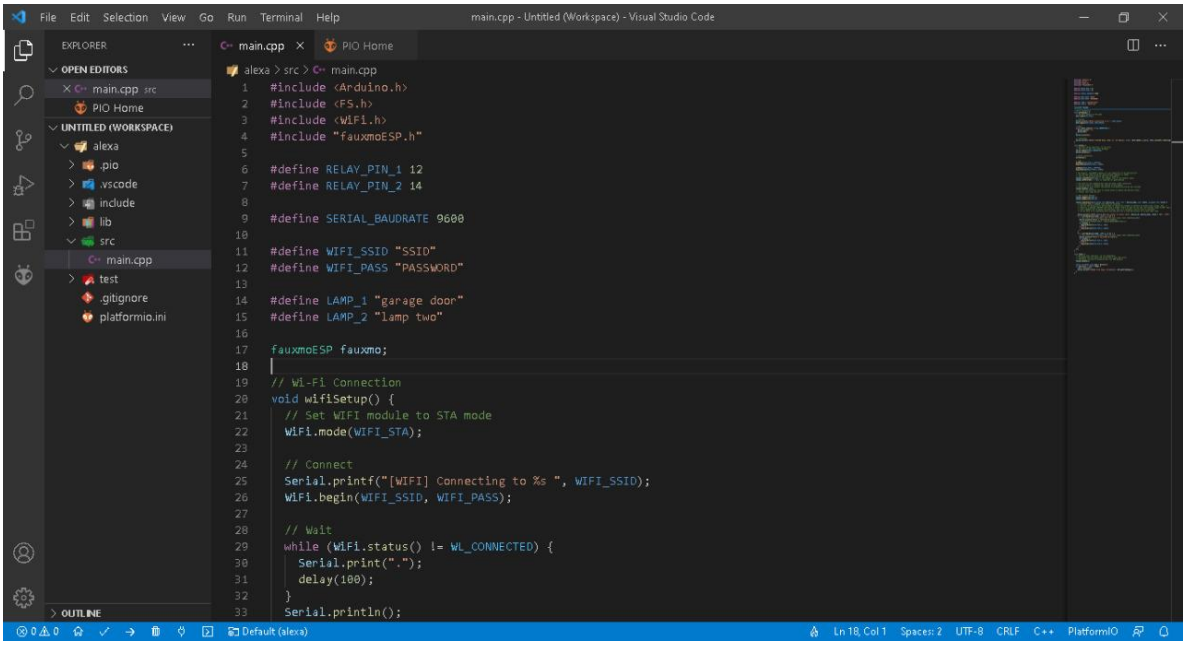


Fig. 5.17.- Código ESP-WROOM-32 para acceso a Echo Dot Alexa (Autor).

De esta forma se podrían provocar otros ataques al sistema como: suplantación de identidad, no repudio y denegación de servicio distribuido DDoS.

5.4 Aplicación de Mecanismos de Seguridad

Se evidenciaron vulnerabilidades y amenazas a las que se expone nuestro sistema IoT Smart Home, ahora podemos aplicar mecanismos y recomendaciones de seguridad para disminuir y mitigar el riesgo que provocan a la seguridad y privacidad de información del hogar inteligente, vamos a revisar el mecanismo de seguridad propuesto en el capítulo anterior para mostrar su funcionamiento.

5.4.1 Mecanismo de seguridad para aplicaciones y servicios en la nube

Los accesos que se solicitan para el funcionamiento de las SmartApps de nuestro Smartphone pueden ser controlados, el sistema Android de nuestro Smartphone brinda seguridad para la información personal, se puede configurar los accesos mínimos que requieren las Apps para su correcto funcionamiento, es decir, entre menos permisos otorguemos menor será la información personal que se pueda obtener de nuestro Smartphone y enviada hacia la nube.

En la imagen 5.18 se manifiesta la administración de permisos que se conceden a las SmartApps del Smartphone.

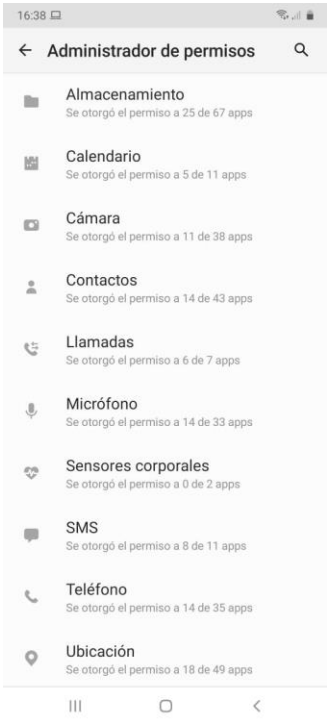


Fig. 5.18.- Configuración de permisos en un sistema Android Smartphone (Autor).

Para este estudio intentar incurrir en mecanismos de seguridad en la nube se hace muy difícil, la nube de la Plataforma de Amazon a la cual nos referimos es muy fiable y segura pero se pueden tomar en cuenta ciertas recomendaciones para el uso de otras plataformas en la nube de otros fabricantes y de terceros, estas se enumeran a continuación:

- Asegurar que se revisen los interfaces API e interfaces web para detectar vulnerabilidades.
- Asegurar que las políticas y protocolos que brinde el *Cloud* se apliquen para paliar las amenazas.
- Impulsar el uso de políticas de protección a la confidencialidad y privacidad de información.
- Verificar a nivel de protocolo (MQTT, HTTP, CoAP) se cumpla con los permisos de acceso para mitigar ataques de DDoS (denegación de servicio) a las App en la nube.

- Asegurar el uso de controles de acceso a la plataforma de la nube como son: control de credenciales e identidad.
- Verificar el uso de cifrado y firmas en el almacenamiento de datos, con esto asegurar la privacidad de la información.

5.4.2 Autenticación de dispositivos

Los nombres de usuario y contraseñas para accesos son muy importantes para la seguridad de un sistema IoT Smart Home, el descubrimiento de estas contraseñas como se pudo observar en la implementación causa graves problemas de privacidad y de inseguridad de la red y de los usuarios del hogar. La aplicación de mecanismos de seguridad para proteger y autenticar contraseñas debe ser constante y continuo en el manejo de sistemas IoT Smart Home. A continuación se muestran algunas recomendaciones que se aplicaron a las contraseñas de las SmartApps, dispositivos inteligentes y dispositivos IoT del sistema IoT Smart Home implementado:

- Se realizó cambio de nombre de usuario y contraseña predeterminado.
- Las contraseñas creadas constan mínimo de ocho caracteres y contienen números, letras mayúsculas, letras minúsculas y signos especiales.
- Autenticación de dos factores, las SmartApps para inicializar los dispositivos solicitaron ingresar al correo y verificar un código de acceso, Amazon también soporta autenticación de dos factores lo que hace que sea una plataforma segura y confiable.
- De la misma manera las plataformas de las aplicaciones soportan mecanismos de recuperación de contraseñas de manera segura y de caducidad después de ciertos periodos de tiempo.

Con estos cambios en las contraseñas se logró mejorar la seguridad de las Smart Apps, del Smartphone, de los dispositivos IoT y del dispositivo más importante el Gateway Home. Para asegurar las nuevas contraseñas se probó el mismo software para tratar de descubrir las contraseñas y no fue posible, aunque no se puede estar 100% seguros ya que existen

softwares más fuertes y poderosos que hoy en día se usan para propósitos delincuenciales y de malware.

5.4.3 Suplantación de identidad

El ingreso de un dispositivo no autorizado por los usuarios del sistema provocó un riesgo alto de seguridad al funcionamiento del sistema, como se expuso anteriormente la autenticación es primordial para que esto no pueda ocurrir, pero si a pesar del mecanismo de autenticación infringiera un dispositivo a la red se deben tener en cuenta otros mecanismos de seguridad que protejan los datos, la privacidad, la seguridad, la integridad y disponibilidad del hogar inteligente

La placa ESP-WROOM-32 tiene mucha capacidad para irrumpir el sistema IoT como se mencionó anteriormente, puede provocar ataques de manipulación de datos, no repudio, suplantación de identidad y denegación de servicio distribuido DDoS. A continuación se mostrará los mecanismos de seguridad necesarios para mitigar estas posibles amenazas.

- Arranque seguro del sistema y de los dispositivos IoT Smart Home.
- Uso de software y firmware seguro y confiable, planificar actualizaciones y parches de seguridad.
- Cifrado de transporte, hacer uso de protocolos con cifrado o cifrar datos antes de su transmisión protegerán los datos en tránsito.
- Cifrar la comunicación de extremo a extremo, el cifrado permite que los puntos finales validen la identidad y garanticen que las comunicaciones no sean interceptadas o redirigidas.

CONCLUSIONES

La tecnología y los sistemas IoT es un mundo que abarca muchos servicios enfocados a perfeccionar las actividades cotidianas de las personas y a satisfacer necesidades en diferentes entornos, IoT se proyecta como una de las tecnologías más utilizadas y prometedoras en un futuro cercano dando lugar a la automatización y sistematización de tareas y actividades cotidianas de las personas mejorando notablemente su desempeño personal y laboral.

La naturaleza del entorno y la cantidad de aplicaciones potenciales IoT, implica que sea una tecnología expuesta a riesgos y amenazas a la seguridad, los sistemas IoT constituyen una recolección de debilidades y vulnerabilidades que los atacantes pueden utilizar para realizar actividades fraudulentas, como hacer un mal uso de información privada, introducir alguna clase de malware, tomar el control de dispositivos IoT, etc.

La aplicación de IoT en el hogar brinda muchos beneficios a sus usuarios, automatizar tareas que normalmente se las realiza manualmente son cosas que hacen de IoT Smart Home una opción de implementación a corto plazo en los hogares de todo el mundo. Por tal motivo, es imperativo la implementación de mecanismos de seguridad a los sistemas IoT Smart Home que aporten a la seguridad de los servicios que brinda esta tecnología.

Se construyó un mecanismo de seguridad para IoT Smart Home que proporciona a los usuarios finales la tranquilidad y satisfacción de su uso, la aplicación de mecanismos de seguridad permitirá al sistema autenticación esencial, garantizará comunicaciones seguras y un manejo responsable de información personal sensible. Satisfaciendo así las principales preocupaciones de seguridad de los usuarios del sistema IoT Smart Home.

La implementación práctica y real de una red IoT Smart Home permitió conocer a fondo las vulnerabilidades y amenazas a las que se expone el sistema, la aplicación de mecanismos de seguridad para mitigar dichas amenazas cumplieron con su objetivo, la seguridad no debe tratarse como un tema aislado, la importancia que se dé a temas de seguridad es la importancia con la que protegemos nuestro hogar y nuestras familias.

BIBLIOGRAFÍA

Achila, A., & Sánchez, A. (2017). Universidad francisco de paula Santander Ocaña. Recuperado de http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/2290/1/32100.pdf

Amazon. (2019). *Securing Internet of Things (IoT) with AWS Secure Cloud Adoption Securing IoT with AWS Securing IoT with AWS*. (April).

Cardona, M. (2016). La seguridad en el Internet de las cosas y el Mundo 3.0 - Globb Security. *Globb Security*. Recuperado de http://globbsecurity.com/seguridad-iot-y-mundo-3-0-37652/

Cheruvu, S., Kumar, A., Smith, N., & Wheeler, D. M. (2020). Demystifying Internet of Things Security. En *Demystifying Internet of Things Security*. https://doi.org/10.1007/978-1-4842-2896-8

Cvitić, I., Peraković, D., Periša, M., & Botica, M. (2018). *Smart Home IoT Traffic Characteristics as a Basis for DDoS Traffic Detection*. (January). https://doi.org/10.4108/eai.6-11-2018.2279336

Eterovic Jorge, Cipriano Marcelo, & Nicolet Santiago. (2018). Análisis de Protocolos de Comunicaciones para Internet de las Cosas. *XX Workshop de Investigadores en Ciencias de la Computación*, 138-141. https://doi.org/http://hdl.handle.net/10915/67176

Figueras Joan. (2015). Seguridad, Sistemas y Privacidad Principios de seguridad.

González García, A. J. (2017). *«IoT: Dispositivos, tecnologías de transporte y aplicaciones»*. Recuperado de http://openaccess.uoc.edu/webapps/o2/handle/10609/64286

Hamed El Hakim. (2018). IoT World Forum Reference Model. Recuperado de https://www.researchgate.net/figure/IoT-World-Forum-Reference-Model_fig2_323525875

Hu, F. (2016). *Security and privacy in Internet of things (IoTs): Models, Algorithms, and Implementations*. CRC Press.

i2t. (2014). *Internet de las cosas*. Recuperado de http://es.wikipedia.org/w/index.php?title=Internet_de_las_cosas&oldid=76451697

Jesús, R. J. & T. (2017). *Modelo de referencia de red - Universidad PROFINET*. Recuperado de https://profinetuniversity.com/automatizacion-industrial/modelo-referencia-red/

Lasse Lueth, K. (2018). State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. Recuperado de IoT Analytics website: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Mapfre. (2018). Amenazas más comunes a la SmartHome así se pueden contrarrestar. Recuperado de https://blogmapfre.com/seguridad/amenazas-mas-comunes-a-la-smarthome-asi-se-pueden-contrarrestar/

Marrugat, X. (2019). *Trabajo de Fin de Grado ¿Son seguros los dispositivos inteligentes de casa ? MEMORIA Director :* Recuperado de https://upcommons.upc.edu/bitstream/handle/2117/165801/144180.pdf

Martínez Caro, J., & Cano Baños, M. (2016). Un caso práctico de aporte de seguridad en IoT. *Anuario de Jóvenes Investigadores*, *9*(9), 220-223.

Morales Suárez, A. C., Díaz Ávila, S. S., & Leguizamón Páez, M. Á. (2019). Mecanismos de seguridad en el internet de las cosas. *Revista vínculos*, *16*(2), 288-297. https://doi.org/10.14483/2322939x.15758

Oriwoh, E., & Conrad, M. (2015). «Things» in the Internet of Things: Towards a Definition. *International Journal of Internet of Things*, *4*(1), 1-5. https://doi.org/10.5923/j.ijit.20150401.01

Peluffo, D. H., Surcolombiana, U., Ivan-rios, J., Castro-silva, J. A., & Llanos, L. H. E. (2017). *Sistema de Riego Basado En La Internet De Las Cosas (IoT)*. (April), 1-9.

Ramos, P. (2018). *Security research and vulnerability analysis on IoT devices*. Recuperado de http://castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/229/TFG Pablo Cid Ramos.pdf?sequence=1

RS Components. (2019). Internet de las Cosas | RS Components. Recuperado de https://es.rs-online.com/web/generalDisplay.html?id=i%2Fiot-internet-of-things

Russell, B., & Van Duren, D. (2016). Practical Internet of Things Security. En *Practical Internet of Things Security*. Recuperado de www.packtpub.com

Salazar, J., & Silvestre, S. (2014). Internet de las cosas. *Universidad Católica*, 1-27.

Sataloff, R. T., Johns, M. M., & Kost, K. M. (2019). *Security Designs for the Cloud, Iot, and Social Networking*.

SorayaPanigua. (2012). Un poco de historia sobre Internet de las Cosas | SorayaPaniagua Ⓢ. *15 de Abril*, p. 5. Recuperado de https://www.sorayapaniagua.com/2012/04/15/un-poco-de-historia-sobre-internet-de-las-cosas/

Tutorials, R. N. (2019). *Alexa (Echo) with ESP32 and ESP8266 Random Nerd Tutorials*. Recuperado de https://randomnerdtutorials.com/alexa-echo-with-esp32-and-esp8266/

Vélez Andrés, 2019. (2019). *ARQUITECTURAS DE REFERENCIA PARA IOT CON TRANSFERENCIA SEGURA DE INFORMACIÓN*.

Zabalo Arteche, E. (2019). *La ciberseguridad como norma. Estudio del estado del arte en estándares y certificación en materia de seguridad cibernética aplicada a industria 4.0 e IoT*. Recuperado de https://addi.ehu.es/handle/10810/32240

Ziegler (FHGR), P. (2020). (Internet of Things)(Internet of Things) - Unknown.pdf. *Radio Interfaces in the Internet of Things Systems*, pp. 1-14. Recuperado de https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf