Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE INVESTIGACIÓN DE UNA GUÍA DE BUENAS PRÁCTICAS DE CONECTIVIDAD SEGURA DEPENDIENDO DEL ENTORNO DE RED DE IoT MEDIANTE EL PROTOCOLO BLUETOOTH

Edwin Haroldo Alvarez Saquec
Asesorado por M.A. Ing. Miguel Eduardo García Juárez

Guatemala, abril 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE INVESTIGACIÓN DE UNA GUÍA DE BUENAS PRÁCTICAS DE CONECTIVIDAD SEGURA DEPENDIENDO DEL ENTORNO DE RED DE IoT MEDIANTE EL PROTOCOLO BLUETOOTH

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

EDWIN HAROLDO ALVAREZ SAQUEC
ASESORADO POR M.A. ING. MIGUEL EDUARDO GARCIA JUAREZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, ABRIL 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Vladimir Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Byron Odilio Arrivillaga Méndez
EXAMINADOR	Ing. Carlos Eduardo Guzmán Salazar
EXAMINADOR	Inga. Ingrid Salomé Rodríguez de Loukota
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE INVESTIGACIÓN DE UNA GUIA DE BUENAS PRÁCTICAS DE CONECTIVIDAD SEGURA DEPENDIENDO DEL ENTORNO DE RED DE IoT MEDIANTE EL PROTOCOLO BLUETOOTH

Tema que me fuera asignado por Dirección de Escuela de Ingeniería Mecánica Eléctrica, con fecha 12 de enero de 2022.

Edwin Haroldo Alvarez Saquec

EEPFI-PP-0153-2022
Guatemala, 12 de enero de 2022

Director
Gilberto Morales Baiza
Escuela De Ingenieria Mecanica
Presente.

Estimado Ing. Morales

Reciba un cordial saludo de la Escuela de Estudios de Postgrado de la Facultad de Ingeniería.

El propósito de la presente es para informarle que se ha revisado y aprobado el Diseño de Investigación titulado: **GUÍA DE BUENAS PRÁCTICAS DE CONECTIVIDAD SEGURA DEPENDIENDO DEL ENTORNO DE RED DE IOT MEDIANTE PROTOCOLO BLUETOOTH** , el cual se enmarca en la línea de investigación: **Internet de las cosas - Internet de las cosas**, presentado por el estudiante **Edwin Haroldo Alvarez Saquec** carné número **200511695**, quien optó por la modalidad del "PROCESO DE GRADUACIÓN DE LOS ESTUDIANTES DE LA FACULTAD DE INGENIERÍA OPCIÓN ESTUDIOS DE POSTGRADO". Previo a culminar sus estudios en la Maestría en ARTES en Ingeniería Para La Industria Con Especialidad En Ciencias De La Computación.

Y habiendo cumplido y aprobado con los requisitos establecidos en el normativo de este Proceso de Graduación en el Punto 6.2, aprobado por la Junta Directiva de la Facultad de Ingeniería en el Punto Décimo, Inciso 10.2 del Acta 28-2011 de fecha 19 de septiembre de 2011, firmo y sello la presente para el trámite correspondiente de graduación de Pregrado.

Atentamente,

"Id y Enseñad a Todos"

Miguel Eduardo García Juárez
Ingeniero en Electrónica, Informática y Ciencias de la Computación
Colegiado: 7982

Mtro. Miguel Eduardo García Juarez
Asesor(a)

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE POSTGRADO
FACULTAD DE INGENIERIA

Mtro. Mario Renato Escobedo Martinez
Coordinador(a) de Maestría

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERIA
DIRECCIÓN
ESCUELA DE POSTGRADO

Mtro. Edgar Dario Alvaréz Cotí
Director
Escuela de Estudios de Postgrado
Facultad de Ingeniería

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

EEP-EIM-0153-2022

El Director de la Escuela De Ingenieria Mecanica de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador y Director de la Escuela de Estudios de Postgrado, del Diseño de Investigación en la modalidad Estudios de Pregrado y Postgrado titulado: **GUÍA DE BUENAS PRÁCTICAS DE CONECTIVIDAD SEGURA DEPENDIENDO DEL ENTORNO DE RED DE IOT MEDIANTE PROTOCOLO BLUETOOTH** , presentado por el estudiante universitario **Edwin Haroldo Alvarez Saquec**, procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería en esta modalidad.

ID Y ENSEÑAD A TODOS

Ing. Gilberto Morales Baiza
Director
Escuela De Ingenieria Mecanica

Guatemala, enero de 2022

Decanato
Facultad de Ingeniería
24189101- 24189102
secretariadecanato@ingenieria.usac.edu.gt

LNG.DECANATO.OI.316.2022

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **DISEÑO DE INVESTIGACIÓN DE UNA GUÍA DE BUENAS PRÁCTICAS DE CONECTIVIDAD SEGURA DEPENDIENDO DEL ENTORNO DE RED DE IoT MEDIANTE EL PROTOCOLO BLUETOOTH,** presentado por: **Edwin Haroldo Alvarez Saquec,** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, abril de 2022

AACE/gaoc

ACTO QUE DEDICO A:

Dios	Por darme la vida, sabiduría, y nunca abandonarme y ayudarme a poder culminar una de mis metas en mi vida.
Mis padres	Juan Eliseo Alvarez Chuc (q. e. p. d.) e Irma Saquec Maczul por brindarme su apoyo incondicional.
Mi esposa	Por estar a mi lado apoyándome.
Mis hijos	Luna y Luca Alvarez Lima por el cambio que le dieron a mi vida y la alegría que me transmiten.
Mis hermanas	Melina y Aracely Alvarez Saquec gracias por el apoyo brindado para poder seguir adelante.
Mi hermano	Mynor Alvarez Saquec gracias por el apoyo para poder terminar cada ciclo.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser la casa de estudios donde pude adquirir conocimientos para formarme como profesional.
Mis amigos	Por los momentos que pude compartir con mis amigos tanto dentro como fuera de cada salón de clases gracias por los momentos que pudimos compartir para poder superar juntos los retos para poder llegar a este momento.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
bps	Bits por segundo
dBm	Decibelio
G	Giga
Hz	Hercio, hertzio o Hertz
m	mili
k	Kilo
W	Watt
$	Dólar

GLOSARIO

Autentificación	Se verifica la identidad de los dispositivos que se comunican o enlazan en función de su conexión Bluetooth.
BLE	Bluetooth de baja energía
BR	Basic rate
DoS	Denegación de servicio
Eavedropping	Es cuando un atacante aprovecha las vulnerabilidades de equipos con versiones antiguas con fallos conocidos.
Firmware	Es el programa que se encarga de controlar que tiene que realizar el hardware de un dispositivo asegurándose que el funcionamiento sea correcto.
IoT	Internet de las cosas
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
OWASP	Proyecto de seguridad de aplicaciones web abiertas
TIC	Tecnologías de la información y las comunicaciones

Wireshark	Es el analizador de protocolos de red más importantes permitiendo ver lo que sucede en una red en específico.

RESUMEN

Se tratará sobre los retos de seguridad que se tienen en el entorno de internet de las cosas en conexiones a través del protocolo bluetooth iniciaremos con una introducción donde nos mostrara un panorama general sobre que se puede realizar con la tecnología de internet de las cosas y que siempre existen vulnerabilidades de red.

Nos apoyaremos en antecedentes de trabajos sobre seguridad donde nos muestran que se puede garantizar mecanismos de autenticación de identidad adecuados y proporcionar confidencialidad sobre los datos.

Se verificará las ventajas y desventajas que tiene bluetooth y bluetooth low energy como también se dará un contexto sobre todo lo que se refiere IoT sus usos ventajas que puede llegar a tener tanto social como económico.

1. INTRODUCCIÓN

Internet de las cosas no es un concepto nuevo se ha desarrollado a partir de la integración de varias tecnologías que se han desarrollado de forma independiente desde su creación, En internet de las cosas involucra que objetos tienen conexión a internet en todo tiempo en otras palabras se integran sensores y dispositivos dentro de objetos cotidianos que tendrían conexión a internet por medio de la red fija o ya sea inalámbricas con esta implementación se pueden obtener datos del comportamiento de cualquier objeto con lo cual se tiene una fuente de información muy valiosa, esto transforma la forma de hacer negocios y la forma de vivir de millones de personas. Realizaremos un estudio sobre los protocolos de comunicación inalámbricas para aportar el mejor en el protocolo de conexión Bluetooth.

Se realizará un recorrido de lo que es IoT su funcionalidad y las ventajas que trae a la sociedad su conexión con dispositivos finales a través de Bluetooth, el sistema IoT busca traer beneficios tanto económicos como sociales.

Las vulnerabilidades de comunicación son muy variadas y siempre existen nuevos descubrimientos, por lo cual se estará abordando el tema específicamente sobre la conexión Bluetooth cómo ha evolucionado, los niveles de seguridad que pueden obtener al tener esta tecnología en nuestro sistema.

2. ANTECEDENTES

Pérez, et al (2018), en su “Análisis sistemático de la seguridad en “Internet of Things” describen la línea de investigación que aborda el estudio y análisis de seguridad en IoT.

Los principales objetivos de seguridad en IoT son garantizar mecanismos de autenticación de identidad adecuados y proporcionar confidencialidad sobre los datos. Se aborda el estudio y análisis de seguridad en IoT. Dicho estudio se fundamenta en el análisis de la seguridad en las diferentes capas de la arquitectura de esta.

Realizan un estudio para el fortalecimiento de la seguridad de los sistemas de software mediante el uso de Métodos, Técnicas y Herramientas de Ingeniería Reversa, En IoT, los objetos físicos como automóviles, televisores, aires acondicionados y otros que nos rodean son identificables de forma única y están interconectados. A través de la red de comunicación los objetos se conectan entre sí recolectando información útil entre ellos. La información es transmitida a los diferentes dispositivos que tomarán acción ejecutando una tarea.

Existen diversos enfoques y técnicas para mejorar la seguridad y existen modelos que permiten contrarrestar e identificar las amenazas, es necesario desarrollar métodos, técnicas y herramientas que ayuden al desarrollo de tecnologías seguras.

Monzón, et al. (2019) en su trabajo “Modelo de Seguridad IoT” presentan un marco de seguridad de IoT para infraestructuras inteligentes como Smart Homes, Smart Grid, Smart Connected Health y otras aplicaciones basadas en IoT.

La seguridad es una necesidad para los sistemas de IoT para proteger los datos confidenciales e infraestructuras físicas críticas. Sin un buen nivel de protección, los usuarios no pueden adoptar muchos sistemas y aplicaciones de IoT. La seguridad en los sistemas de red tradicionales sigue siendo un desafío, mientras que los sistemas de IoT plantean muchos más desafíos para los investigadores debido a varias causas y ataques que se presentan día a día, y como se descubren nuevas vulnerabilidades.

El Internet de las cosas (IoT) no solo conectará computadoras y dispositivos móviles, sino que también interconectará edificios, hogares y ciudades inteligentes, así como redes eléctricas, redes de agua y gas, automóviles, entre otros. IoT liderará al desarrollo de una amplia gama de servicios de información avanzados que deben procesarse en tiempo real. Sin embargo, las infraestructuras y servicios de IoT presentan grandes desafíos de seguridad debido al aumento significativo de la superficie de ataque, la complejidad.

Nos muestra un marco de seguridad de IoT para infraestructuras para varias aplicaciones IoT el cual nos da una amplia vista de donde se encuentra IoT y nos muestra donde nos podemos enfocar y donde tendrá un mayor impacto la seguridad.

Márquez (2019) en su artículo “Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas” expone el riesgo a nivel de la seguridad de la información sobre Internet de las cosas.

Tiene como objetivo principal el estudio de denegación de servicios en una red IoT, efectuar ataques de fuerza bruta mediante programa maligno especializados que escanean Internet en busca de dispositivos que estén conectados al IoT para obtener sus contraseñas y secuestrarlos.

Este tipo de ataque puede tener distintas motivaciones pueden ser políticas, chantaje, o dependiendo la red a infiltrarse, estos buscan dejar fuera de servicio.

Los ataques pueden ser a cualquier nivel ya sea empresarial como también puede ser a nivel domiciliar, generalmente estos dañan a los usuarios, y suelen ser ataques que en muchos casos se pueden evitar. No hay unificación universal que garantice la conectividad compatible entre dispositivos, ya que las empresas que trabajan con IoT, desarrollan protocolos propios adaptados a los servicios que ofrecen, generando una brecha a nivel de seguridad.

Fattori de Andrade (2019) en su trabajo “Análisis del consumo de energía promedio en dispositivos IoT de baja potencia con Blockchain como solución de seguridad” implemento una cadena de bloques de alta capacidad de cómputo de forma externa a los dispositivos y un mecanismo de validación de autenticidad con el objeto de proporcionar seguridad a los dispositivos IoT.

El objetivo principal de este trabajo de grado fue analizar el consumo de energía en dispositivos IoT de baja potencia utilizando Blockchain para agregar seguridad a sus transacciones y la información que transmitan.

Blockchain es una tecnología revolucionaria, que ofrece la posibilidad de compartir datos valiosos de una manera segura y a prueba de manipulación. En la actualidad, muchos sectores privados y públicos ya están inmersos en la tecnología y sus casos de uso se están expandiendo a muchas áreas, incluyendo IoT. La arquitectura utilizada por Blockchain es distribuida y esto puede solucionar muchas de las limitaciones y problemas del modelo actual de cliente servidor con esto se evita suplantación de identidad y obtener una mayor velocidad en las transacciones.

Se pueden ver nuevas formas de poder introducir seguridad en una red de IoT la cual se puede aprovechar de una mejor manera para aprovechar las nuevas tecnologías.

Ordóñez-Camacho (2021) en su trabajo Titulado “Reduciendo la brecha de seguridad del IoT con una arquitectura de microservicios basada en TLS y OAuth2” implementa un nuevo proceso sectorizado basándose en la interdependencia de los equipos, por lo que trabajó en microservicios para que se ejecute como microservicios. El objetivo general fue proporcionar al mundo del IoT una alternativa arquitectural segura y adaptada a las nuevas tendencias tecnológicas, dando especial relevancia a generar una alternativa para hogares inteligentes, y centrándose en la autentificación de clientes al llamar a múltiples servicios y transmitir información sensible para la seguridad. La seguridad de equipos IoT están presentando crecimiento exponencial formando una brecha entre el crecimiento y la seguridad, presentando un aumento en los problemas de seguridad.

Las buenas prácticas en los protocolos de IoT son básicas e importantes y cuando no se llevan a cabo pueden resultar en fallas o deficiencias en la seguridad, por lo que se hace necesario abordarlas ya que los equipos conectados a una red son vulnerables a ataques los cuales podrían protegerse mediante protocolos que contemplen la detección de intrusiones.

3. PLANTEAMIENTO DEL PROBLEMA

Como se sabe los ciber-ataques se producen de un momento a otro, si no se tiene los procesos adecuados para frenar o mitigar un ataque por lo cual es necesario tomar medidas de seguridad los cuales estaremos enlistando unas de ellas.

3.1. Contexto general

En internet de las cosas IoT se tiene un crecimiento exponencial en su uso por lo tanto atrae a ciber-ataques que pueden afectar al sistema de IoT o puede llegar a ser un problema en toda la Red, por lo que es necesario tomar las medidas de seguridad en el sistema, la ciber-seguridad es un flagelo que sufre todos los sistemas.

3.2. Descripción del problema

La ciber-seguridad es un problema que se tiene desde que se inician las comunicaciones ya que siempre han existido las vulnerabilidades que atacantes quieren aprovechar para obtener beneficio alguno, por lo que es necesario analizar los procesos que se toman para disminuir los ataques de éxito.

3.3. Formulación del problema

En nuestra vida cotidiana proporcionamos información de nuestro estilo de vida, gustos, sitios que visitamos sin darnos cuenta además con el avance de la tecnología tenemos información sensible que no la tiene que obtener segundas o terceras personas, pero con el crecimiento exponencial de la tecnología en este caso el internet y la conexión de todo tipo de dispositivos nos vuelve cada vez más vulnerables a que ciber atacantes puedan obtener nuestra información personal por lo que se tiene que tomar muy en cuenta la seguridad en todos los dispositivos.

Pregunta central

- ¿Cuáles son las técnicas de seguridad a considerar en la configuración de protocolos de comunicación bluetooth en IoT?

Preguntas auxiliares

- ¿Existen vulnerabilidades en los protocolos de comunicación Bluetooth en IoT?

- ¿Cuáles son las contramedidas que pueden mejorar la seguridad en la comunicación Bluetooth en IoT?

- ¿Se puede cuantificar y de qué manera se analizan las contramedidas que se toman aplican?

3.4. Delimitación del problema

Se realizará una guía respecto al protocolo de comunicación Bluetooth estándar y Low energy enfocado a seguridad, se presentarán las prácticas que se tienen que llevar a cabo para poder tener un nivel de seguridad confiable y con enfoque en verificar tarjetas de desarrollo en su implementación correcta.

.

4. JUSTIFICACIÓN

La realización de la presente investigación se basa en la línea de investigación de data analitic de la maestría en ingeniería para la industria enfocada en ciencias de la computación.

El problema que se tiene en la Red de Internet es la seguridad en todos los ámbitos ya que existen ciber-delincuentes que se aprovechan de las vulnerabilidades y malas prácticas que se tienen de parte de las empresas como de particulares, por lo que se estará aportando con una serie de buenas prácticas para la configuración del protocolo Bluetooth.

Con mejores prácticas de seguridad se obtiene para mayor seguridad y también tiempo de respuesta ante las amenazas, cabe mencionar que una red nunca llega a ser totalmente impenetrable ante las amenazas.

Tener una red segura nos da confianza de tener nuestro sistema estable y siempre disponible los servicios prestados como también nos da seguridad en toda la red ya que los dispositivos de IoT pueden ser una puerta de acceso.

5. OBJETIVOS

5.1. General

Proponer una guía de seguridad para configuración de protocolos de comunicación de Bluetooth en IoT enfocado al tipo de implementación que se realizará.

5.2. Específicos

- Identificar las vulnerabilidades que tiene el protocolo de comunicación de Bluetooth en IoT.

- Identificar las contramedidas que se pueden realizar para mejorar la seguridad.

- Análisis de las contramedidas que se realizan para mejorar la seguridad.

6. NECESIDADES POR CUBRIR Y ESQUEMA DE SOLUCIÓN

Propuesta de buenas prácticas para configuración de protocolo Bluetooth aplicado a IoT y como obtener mejor seguridad.

La investigación se basará en poder proponer las mejores prácticas de configuración de protocolo Bluetooth aplicado a IoT ya que estos dispositivos tienden a estar disponibles todo el tiempo, por lo que esta guía está enfocada a conexiones Bluetooth que acceden al sistema, servicio y recursos que intercambian información.

El auge de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad ha creado nuevas necesidades de seguridad ya que se pueden producir amenazas que atentan contra la privacidad, desarrollo económico, y un normal funcionamiento de la organización.

La necesidad de auditar las implementaciones de Bluetooth se debe a que la falta de revisión de una gran cantidad de vulnerabilidades que tiene, la ingeniería que tiene el protocolo Bluetooth es muy compleja y al momento de la implementación no se podría decir que se tomó a la ligera el tema de seguridad por lo que existen varios huecos de seguridad en el mismo como también en otras ocasiones no se considera los protocolos con lo que conlleva una ruptura en la seguridad de información relevante.

Se realizará un análisis en los protocolos Bluetooth y Bluetooth low energy en los cuales se podrán en evidencia vulnerabilidades que puedan tener, en la etapa de sincronización, transmisión de paquetes de datos y se aconsejaran las mejores prácticas para evitar la intrusión de personas no autorizadas al sistema se tiene que mencionar que un sistema nunca puede ser infalible, sin embargo, se puede implementar verificadores para que tenga un mejor nivel de seguridad.

7. MARCO TEÓRICO

La seguridad en los dispositivos se toma a la ligera tanto a nivel empresarial como a nivel personal sino hasta que la red en cuestión sea vulnerada por un atacante por lo que se analizara la forma de conexión de dispositivos a través de la comunicación bluetooth segura sin embargo la red nunca es totalmente segura ya que siempre se van encontrando nuevas vulnerabilidades.

7.1. Internet de las cosas (IoT)

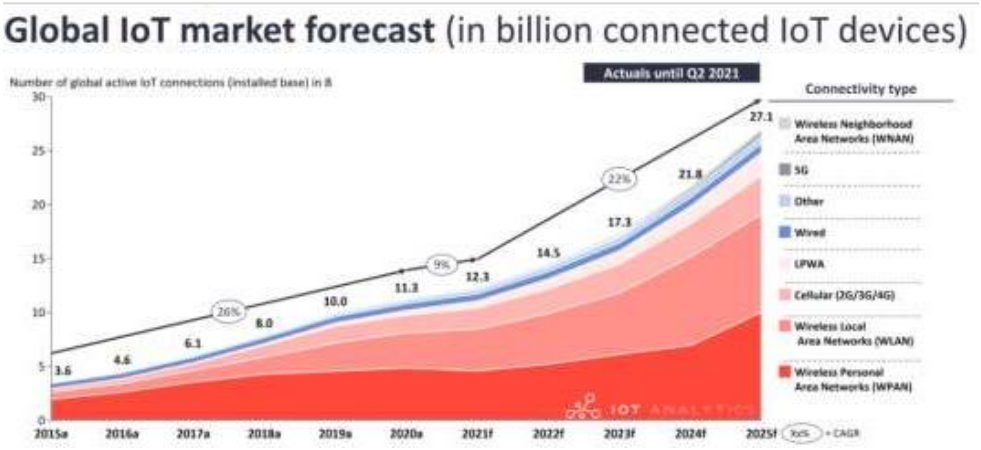
Se puede definir el internet de las cosas como una red interconectada de distintos dispositivos podemos mencionar entre ellos sensores, dispositivos portátiles entre otros que interactúan entre si todo esto en tiempo real y se puede obtener la información y almacenarla en una base de datos para adquirir información importante para decisiones futuras.

En IoT el dispositivo que se conecta puede ser pequeña como también puede ser de grande como un automóvil, avión, y pueden ser proyectos tan grandes como se ha visto en la actualidad el tema de ciudades inteligentes se está adaptando para ayudar a comprender el comportamiento del medio ambiente, la optimización del consumo de energía eléctrica.

Es importante saber el termino de internet de las cosas se utiliza principalmente en dispositivos que usualmente no se esperaría que se pueda conectar a internet se puede mencionar como dispositivo IoT una banda de fitness, un calefactor, sensor de temperatura, entre otros.

IoT se comprende de dispositivos inteligentes que tienen conectados a su vez sensores, y dispositivos que procesan información en la web, los dispositivos usan procesadores, software y hardware de comunicación, los datos se comparten a través de una puerta de enlace de IoT u otro dispositivo que hace la transferencia de datos hacia la nube para realizar un análisis posterior, generalmente estos dispositivos mantienen comunicación entre otros dispositivos IoT los cuales actuaran dependiendo la información obtenida generalmente todo este proceso es automatizado, la intervención humana se enfoca en temas de configuración ya sea de parámetros o de instrucciones o ya sea para acceder a la base de datos almacenada en un tiempo determinado. Por la utilización que se le puede dar a IoT sigue creciendo exponencialmente en todo el mundo ya que se van integrando dispositivos de seguridad, automóviles, automatización, dispositivos médicos IoT seguirá creciendo en todo el mundo, como por ejemplo se puede imaginar tener todo el equipo médico conectado a una base de datos, esto significaría que todo el historial médico de cada paciente estará a disposición de cada médico por lo que para el paciente seria de mucho beneficio esta implementación.

Figura 1. **Grafica de crecimiento de dispositivos IoT**



Fuente: Knud, 2021. IoT *Analytics Research.*

La mala gestión de dispositivos conectados entre sí y que se encuentren conectados a la red de internet esto involucra una fuerte fuente de inseguridad en IoT. Este tipo de conexiones de dispositivos significan un alto porcentaje de problemas de seguridad ya que pueden ocasionar conexiones no autorizadas a dispositivos no autorizados que serían capaces de extraer información y datos sensibles para empresas por lo que es de suma.

7.2. Bluetooth en IoT

Bluetooth es muy conocido en el ámbito de comunicación a cortas distancias entre dispositivos como dispositivos de llamadas de manos libres, dispositivos de audio en la transmisión inalámbrica, ahora es también conocida o es muy familiar que al mencionar IoT vaya de la mano Bluetooth ya que cumple con requisitos como conexión rápida entre dispositivos, conexión inalámbrica y que funciona sin necesidad de conexión a internet la comunicación entre dispositivos finales y la facilidad de interconexión entre dispositivos a gran escala esta conexión se realiza a través de la malla Bluetooth.

7.3. Bluetooth clásico

Es una tecnología específica para dispositivos con alta demanda de pequeñas transmisiones. Bajo este conjunto se agrupan todas las especificaciones antiguas de Bluetooth.

7.4 Bluetooth de baja energía (BLE)

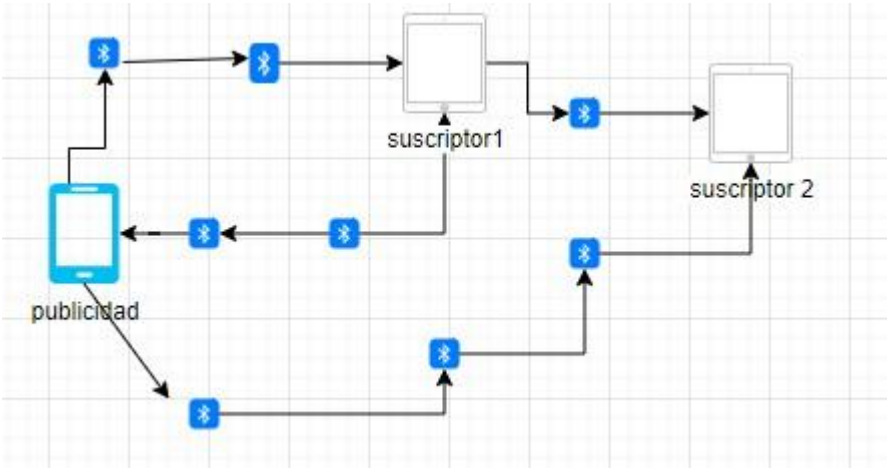
Esta tecnología es ideal para aplicaciones que requieren la comunicación de pequeñas cantidades de datos de forma puntual o periódica.

Para establecer una comunicación Bluetooth se requiere un hardware específico para este protocolo que incluye un módulo de banda base, un módulo de radio y una antena.

Especificación Bluetooth pretende que todas las aplicaciones sean capaces de operar entre sí. Para conseguir esta interoperabilidad, las aplicaciones en dispositivos remotos deben ejecutarse sobre una pila de protocolos idénticos.

Bluetooth Low Energy en IoT es una muy buena opción en IoT ya que el bajo consumo de energía que se requiere en este medio de comunicación es mínimo al mantener los dispositivos suspendidos cuando no están en uso y la velocidad que maneja al volver a conectarse es de seis milisegundos, en comparación de Bluetooth que necesita volver a conectarse cada seis segundos o más con los dispositivos.

Figura 2**.** **Ilustración de conexión entre dispositivos bluetooth**



Fuente: elaboración propia, realizado con draw.io

Se tiene la percepción que la comunicación a través de conexión cableado es más seguro todo lo contrario, con las conexiones inalámbricas, se tienen más vulnerabilidades ya que se pueden capturar datos en este tipo de transmisión.

Tabla I. **Diferencias clave entre *Bluetooth* BR / EDR y *Low Energy***

Características	**Bluetooth BR / EDR**	**Bluetooth Low Energy**
RF Physical Channels	79 channels with 1 Mhz chan- nel spacing	40 channels with 2Mhz channel spacing
Discovery / Connect	Inquiry / Paging	Advertising
Number of piconet Slaves	7 active / 255 total	Unlimited
Device Address Privacy	None	Private device addressing avai- Lable
Max Data Rate	1-3 Mbps	1 Mbps via GPSK MODULA- TION
Pairing Algoritm	Prior to 2.1: E21/E22/SA-	AES-128 / P-256 Elliptic Curve, AES-CMAC
Device Authentication Algorithm	E1/SAFER, HMAC- SHA-256	AES-CCM
Typical Range	30m	50m
Max Output Power	100mW (20 dBm)	10mW(10dBm)

Fuente: elaboración propia.

7.5. Seguridad informática

Se analizará conceptos relacionados a la seguridad informática sus bases, componentes los términos más usados, mecanismos de prevención se establecerá si la seguridad se aborda desde el tema disciplinario donde se podrá exponer los riesgos a los que se encuentra, la seguridad en general se define como la ausencia de riesgo el cual involucra cuatro acciones las cuales son prevención del riesgo, transferir el riesgo, mitigar el riesgo, y aceptar. Con estos cuatro términos se puede relacionar perfectamente como se observa la

seguridad en informática, prevención del riesgo es tomar las medidas que se encuentran establecidas contra los ataques que se conocen para que no suceda en nuestro entorno, mitigar el riesgo cuando se vulnera el sistema tener las métricas.

Para poder resolver la intrusión ya tener definido los pasos a seguir, Aceptar el riesgo toda infraestructura no es segura por completo siempre se tiene un porcentaje de riesgo.

7.6. Vulnerabilidades y amenazas

Vamos a indagar sobre los problemas de seguridad con más probabilidad en la conectividad Bluetooth y poder realizar sugerencias de conexión de dispositivos de forma segura.

Conexión no segura nos referimos cuando no se tiene la versión más reciente de Bluetooth, 5.1 que fue anunciada a inicios de 2019 la versión 5 fue anunciada en 2016 en la actualidad la mayor cantidad de versión que se encuentra en el mercado es la 4.1 inclusive versiones más antiguas que están en el mercado desde 2013. En la versión 4.2 se adaptó el cifrado SSP y AES-CCM, los cuatro tipos de emparejamiento las cuales son *Numeric Comparasion* (comparación numérica), *Just Word*, *Out of Band* y *Passkey Entry* de los cuales se sabe que tienen diferentes vulnerabilidades.

7.7. Funciones de seguridad de *bluetooth*

Se especifican cinco servicios de seguridad básicos en el estándar Bluetooth los cuales detallamos a continuación:

Autentificación: se verifica la identidad de los dispositivos que se comunican o enlazan en función de su conexión Bluetooth.

Eavedropping: Es cuando se aprovechan las vulnerabilidades anteriores o los equipos con versiones antiguas donde un atacante puede interceptar una transmisión y explotar los fallos conocidos leyendo datos o capturando audio de una conversación que se tenga por teléfono a través de auricular Bluetooth.

Bluesnarfing: es utilizado por los ciber-delincuentes donde se realiza una conexión de emparejamiento sin autorización pudiendo obtener a datos almacenados.

Denegación de Servicio: Este ataque tiene el objetivo de saturar de datos un dispositivo para dar de baja la comunicación y por lo tanto hay más consumo de energía por lo que la batería se agotaría rápidamente, con este ataque se puede bloquear el equipo por completo afectando todos los dispositivos.

Confidencialidad: prevenir el que se comprometa la información por escuchas en el sistema y asegurar que solo los dispositivos autorizados pueden acceder y poder ver los datos transmitidos.

Autorización: nos da el control de los dispositivos autorizados para utilizar el servicio antes de permitir que esto suceda.

Integridad del mensaje: nos indica que un mensaje enviado entre dos dispositivos Bluetooth no sea alterado en la transmisión.

7.8. Prueba con *Ubertooth*

Con *Ubertooth One* 2.4 Ghz se obtiene una plataforma de desarrollo inalámbrica adecuada para experimentación Bluetooth cuenta con una antena de 2.4 GHz este dispositivo transmite energía y recibe sensibilidad similar a un dispositivo con conexión *Bluetooth* de clase 1, este dispositivo corre en el sistema Kali Linux la cual es una plataforma de código Abierto con software específico para realizar test de seguridad.

El dispositivo ubertooth tiene la capacidad de funcionar en modo monitor lo cual significa que monitorea el tráfico bluetooth en tiempo real para una verificación necesitaremos.

- Actualización del sistema, verificar que el sistema se encuentre con las ultimas actualizaciones.
- Verificación y actualización de Firmware.
- Correr ubertooth con el analizador de espectros.
- Ejecutar el análisis mediante Wireshark

8. PROPUESTA DE ÍNDICE DE CONTENIDO

9. METODOLOGÍA

El diseño de investigación está enmarcado en la línea de investigación de internet de las cosas y el enfoque es mixto ya que por medio de las buenas prácticas de seguridad se realizarán mejoras en la red sobre el protocolo Bluetooth. El alcance del estudio tiene un enfoque cualitativo-descriptivo ya que se basa en la revisión de variables y depende el tipo de red y sus especificaciones.

Se estará recopilando información y se realizara un estudio estadístico a través de paquetes estadísticos como lo es R y Rstudio para poder ayudarnos a comprender mejor cuan vulnerables estamos conectados a la Red de Internet.

9.1. Características de estudio

El proyecto de investigación se realizará bajo la modalidad cualitativo descriptivo debido a que está orientado a plantear conclusiones sobre la seguridad en protocolo de Bluetooth y Bluetooth low energy los riesgos en un sistema de conexión de objetos inteligentes en IoT, considerando los principales factores de riesgos del sistema de conexión de internet de las cosas. Se proporcionará una breve descripción de la tecnología en sus dos implementaciones principales las cuales son BR/EDR (Basic rate/Enhanced Data Rate) Y LE, donde se expone la estructura de seguridad que las componen en todas las versiones publicadas como la generación de claves, autentificación, cifrado entre otros.

Nos basaremos en el *Open Web Aplication Security Project* (OWASP) para obtener datos ya que es una fundación sin ánimo de lucro que su fin en mejorar el software y publica anualmente una lista de vulnerabilidades IoT el cual nos será de referencia.

A lo largo de la vida de este protocolo se ha puesto enfoque en la mejora de la seguridad en especial a partir de la versión 2.1 con mecanismos como Secure Connections, siempre quedan puntos débiles que pueden ser aprovechados por atacantes maliciosos.

Se recogerá una lista de contramedidas o buenas prácticas que los usuarios de Bluetooth deben conocer y aplicar para mitigar el riego frente a las amenazas expuestas con experiencias que se han tenido.

9.2. Unidades de análisis

Se pretende abarcar BR/EDR (*Basic rate/Enhanced Data Rate*) en la cual se describirá la arquitectura de seguridad de Bluetooth, recopilación y descripción de las vulnerabilidades de Bluetooth, cuáles son las amenazas y posibles ataques, recopilación de contramedidas que permitan mitigar o como sucede en muchos casos reducir el impacto de los ataques, como también una descripción de escenarios hipotéticos con el objetivo de aportar un ejemplo de riesgo que conlleva el uso de Bluetooth.

9.3. Variables

- Facilidad de uso percibida
- Tipo de conexión
- IoT dispositivos
- Tipo de vulnerabilidad

9.4. Fases de estudio

Se definirán los procesos de verificación de vulnerabilidades para poder mitigar riesgos en hardware y software de los dispositivos.

- Se propondrá una guía de revisión de huecos de seguridad en las conexiones Bluetooth.
- Se establecerán procesos de verificación de vulnerabilidades.
- La identificación de metodologías para gestión de seguridad informática del sistema se verificará a través de protocolos o estándares de proveedores y fabricantes de dispositivos.
- Seguridad en Bluetooth se verificará las fases del proceso para establecer la conexión.
- Vulnerabilidades.
- Amenazas y ataques una recopilación BlueBorne.
- Contramedidas.
- Escenarios prácticos.

10. TÉCNICAS DE ANÁLISIS DE LA INFORMACIÓN

Los productos IoT generalmente incorporan aspectos del mundo físico con tecnología digital, por lo cual un ser humano toma decisiones en los cuales nos cambia lo previsto por lo cual se puede determinar si es algún error humano o un error de los dispositivos todo dependerá de las mediciones a realizar serán ejecutados a través de la herramienta estadística R para utilizar los algoritmos que mejor se acoplen a los datos a mostrar a través de la media, mediana y moda como también medida de dispersión para identificar datos fuera de lo normal.

Se realizará un estudio sobre las contramedidas que se realizan y con qué frecuencia se llevan a cabo dependiendo de los factores a su alrededor se podrá observar el porcentaje de seguridad que se tiene en la comunicación Bluetooth podremos observar factores claves como:

- Utilización
- Confiabilidad
- Disponibilidad

Los resultados se estarán mostrando a través de visualización de tabla de datos analizados ya que consiste en una forma de presentar datos y que puedan ser comprendidos con facilidad se estará utilizando la librería ggplot2.

11. CRONOGRAMA

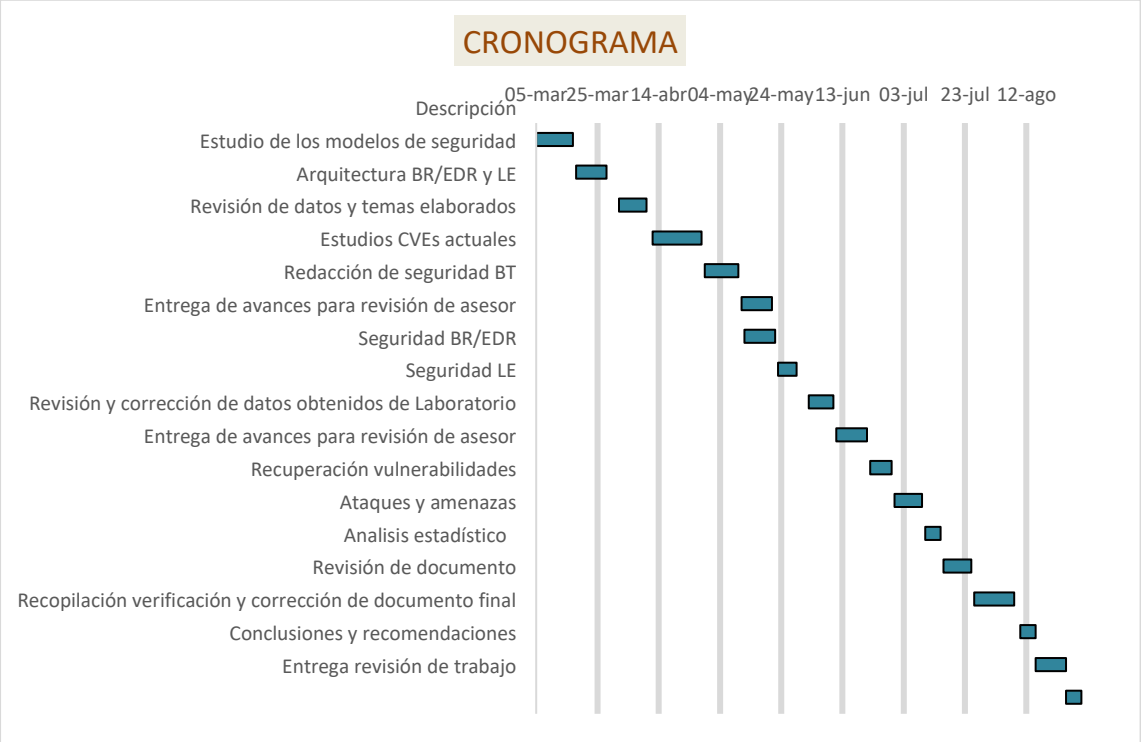
A continuación, el desglose total del trabajo de graduación con una duración aproximada de 6 meses iniciando el 5 de marzo del 2022 para concluir a finales de agosto según detalle.

Tabla II. **Detalle de actividades**

Descripción	Fecha inicio	Duración (días)	Fecha finalización
Estudio de los modelos de seguridad	5/3/22	12	17/3/22
Arquitectura BR/EDR y LE	18/3/22	10	28/3/22
Revisión de datos y temas elaborados	1/4/22	9	10/4/22
Estudios CVEs actuales	12/4/22	16	28/4/22
Redacción de seguridad BT	29/4/22	11	10/5/22
Entrega de avances para revisión de asesor	11/5/22	10	21/5/22
Seguridad BR/EDR	12/5/22	10	22/5/22
Seguridad LE	23/5/22	6	29/5/22
Revisión y corrección de datos obtenidos de Laboratorio	2/6/22	8	10/6/22
Entrega de avances para revisión de asesor	11/6/22	10	21/6/22
Recuperación vulnerabilidades	22/6/22	7	29/6/22
Ataques y amenazas	30/6/22	9	9/7/22
Análisis estadístico	10/7/22	5	15/7/22
Revisión de documento	16/7/22	9	25/7/22
Recopilación verificación y corrección de documento final	26/7/22	13	8/8/22
Conclusiones y recomendaciones	10/8/22	5	15/8/22
Entrega revisión de trabajo	15/8/22	10	25/8/22
Correcciones de trabajo (si fuera necesario)	25/8/22	5	30/8/22

Fuente: elaboración propia

Figura 3. **Cronograma**



Fuente: elaboración propia, realizado con Excel.

12. FACTIBILIDAD DEL ESTUDIO

Se realizarán pruebas con equipo *Open Source* como paquetes en Linux como lo es hcltool este comando nos permite realizar un escaneo general desde nuestro terminal para poder detectar dispositivos emitiendo en el rango de alcance de nuestra antena, obteniendo así nombres y direcciones ya teniendo esa información se puede ampliar con él envió de comandos HCL_inq. Generalmente se puede complementar la información con otras herramientas como: sdptool estas trabajan sobre el protocolo SDP y obtienen información sobre servicios que proporciona el dispositivo.

Existen muchas herramientas que nos sirven para realizar verificaciones de seguridad los costos pueden ser desde unos cientos de dólares hasta miles, en nuestro caso trataremos de utilizar un dispositivo muy popular tanto por sus características como precio que oscila en USD$ 130 el cual es Ubertooth One.

Tabla III. **Gastos estimados a realizar**

Dispositivo	Inversión (USD$)
Ubertooth One	130
Raspberry pi 4	110
Sensores	50
Diseño, ejecución y análisis	400
Asesor	200
Gastos varios (elaboración de interfaz)	100
Total	**990**

Fuente: elaboración propia.

Se estará realizando un estudio de laboratorio para realizar escenarios posibles en el cual se estudiarán las mejores formas de poder realizar conexiones de dispositivos se estarán planteando diferentes escenarios como lo son de punto a punto o punto a multipunto. Los dispositivos se comunican en redes que se llaman piconets, las cuales pueden crecer hasta 8 conexiones punto a punto se puede extender la red al formar Scatternets no es más que la conexión de dos dispositivos pertenecientes a distintas piconets.

13. CONCLUSIONES

1. Podemos decir que se tienen que tomar en cuenta la seguridad de nuestros dispositivos ya que se puede realizar fallas en nuestra red o pérdida de control de nuestros equipos si no se tiene las medidas necesarias, aunque como lo hemos dicho no podemos decir que se tiene el total de seguridad siempre se tiene probabilidades de una vulnerabilidad lo que si podemos confirmar es que podemos mitigar los ataques si se tienen buenas prácticas.

2. Internet de las Cosas es una tecnología que nos puede traer muchos beneficios en nuestra vida cotidiana como también en la industria como en toda tecnología que es relativamente nueva siempre se tiene que tomar en cuenta que puede presentar vulnerabilidades, pero no tiene que ser algo que nos evite que se implemente esta tecnología.

14. RECOMENDACIONES

1. Es necesario tener en cuenta que toda red es susceptible a ataque por lo tanto tenemos que tomar medidas necesarias para estar lo más seguro.

2. Debemos tener un control de nuestros equipos y sobre los permisos de cada usuario y que no se tengan permisos de administrador para todos los usuarios.

3. Tener para una configuración de red para cada escenario distinto en nuestra red ya que no siempre son los mismos requerimientos.

15. REFERENCIAS

1. Chavda, V. N., & Shah, N. A. (2020). Impact of Information Technology on Job-Related Factors. Data Science and Intelligent Applications, 137–144. doi:10.1007/978-981-15-4474-3_15.

2. Dorobantu, O.G., & Halunga, S. (2020). Security threats in IoT. 2020 International Symposium on Electronics and Telecommunications (ISETC),1-4. doi: 10.1109/ISETC50328.2020.9301127.

3. Fernández, L. (2020). Bluetooth Mesh Networking Aplicaciones y pruebas de concepto. [Trabajo Fin de Máster]. Recuperado de: https://eprints.ucm.es/id/eprint/62465/.

4. Fattori, A. C. (2019). Análisis del consumo de energía promedio en dispositivos IoT de baja potencia con Blockchain como solución de seguridad. Recuperado de: http://hdl.handle.net/10554/43607.

5. Ghori, M. R., Wan, T. C., & Sodhy, G. C. (2020). Bluetooth Low Energy Mesh Networks: Survey of Communication and Security Protocols. Sensors (Basel, Switzerland), 20(12), 3590. https://doi.org/10.3390/s20123590.

6. Lounis, K., & Zulkernine, M. (2020). Attacks and Defenses in Short-Range Wireless Techno- logies for IoT. IEEE Access, 8, 88892-88932.

7. Márquez, J. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. Revista de Bioética y Derecho, (46), 85-100.

8. Monzon, G., Todt, C., Bolatti, D., Gramajo, S., Scappini, R. (2019). Modelo de Seguridad IoT. Río Cuarto, XXV Congreso Argentino de Ciencias de la Computación. ISBN: 978-987-688-377-1. PP (1288-1296). Recuperado de: http://sedici.unlp.edu.ar/handle/10915/90359.

9. Ordóñez-Camacho, D. (2021). «Reduciendo la brecha de seguridad del IoT con una arquitectura de microservicios basada en TLS y OAuth2». Ingenius. N.◦ 25, (enero-junio). pp. 94-103. doi: https://doi.org/10.17163/ings.n25.2021.09.

10. Pérez, N., Bustos, M., Berón, M., y Henríquez, P. (2018). Análisis sistemático de la seguridad en Internet of Things. XX Workshop de Investigadores en Ciencias de la Computación. RedUNCI - UNNE - ISBN 978-987-3619-27-4. PP. (1066-1071). Recuperado de: http://sedici.unlp.edu.ar/handle/10915/67063.

11. Tejedor, J. (2020). Pentesting IoT device: smart doorlock. [Trabajo Fin de Máster]. Recuperado de: https://eprints.ucm.es/id/eprint/62476/.