UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

INTEGRIDAD Y CONFIDENCIALIDAD DE DATOS EN REDES IoT LoRaWan

TRABAJO MONOGRÁFICO
PARA OBTENER EL GRADO DE

INGENIERO EN REDES

PRESENTA

CRISTOPHER ANTONIO SANDY CASTA

SUPERVISORES
DR. JAVIER VÁZQUEZ CASTILLO
M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA
DR. JAIME SILVERIO ORTEGÓN AGUILAR
M.M. JOSÉ RAÚL GARCÍA SEGURA
M.S.I. LAURA YÉSICA DÁVALOS CASTILLA

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2021

UNIVERSIDAD DE QUINTANA ROO

DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

TRABAJO MONOGRÁFICO TITULADO

"INTEGRIDAD Y CONFIDENCIALIDAD DE DATOS EN REDES IOT LORAWAN"

ELABORADO POR:

CRISTOPHER ANTONIO SANDY CASTAN

BAJO SUPERVISIÓN DEL COMITÉ DEL PROGRAMA DE LICENCIATURA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

COMITÉ SUPERVISOR

SUPERVISOR: _____

DR. JAVIER VÁZQUEZ CASTILLO

SUPERVISOR: _____

M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA

SUPERVISOR: _____

DR. JAIME SILVERIO ORTEGÓN AGUILAR

SUPERVISOR SUPLENTE: _____

M.M. JOSÉ RAÚL GARCÍA SEGURA

SUPERVISORA SUPLENTE: _____

M.S.I. LAURA YESICA DÁVALOS CASTILLA

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2021

Resumen

La conceptualización de redes IoT (Internet of Things, por sus siglas en inglés) se basa en grupos de dispositivos y su conectividad a través de redes privadas o de internet, y donde cada uno de los dispositivos u objetos son visibles para interactuar entre sí. El uso y la aplicación de los dispositivos IoT en el mundo actual es extensa, por ejemplo: en ropa, refrigeradores, hornos microondas, transporte, relojes, sensores diversos, cámaras web y fotográficas, entre otros. Sin embargo, la seguridad en las redes IoT juega un papel importante debido a que los usuarios de dispositivos IoT pueden llegar a comprometer su privacidad, y, en consecuencia, externos puedan acceder a sus datos e información. Por este motivo, es necesario que el usuario de sistemas IoT utilice dispositivos con características acorde a sus necesidades y nunca se sobreexponga ya que los dispositivos cuentan con la característica de la conexión a Internet siendo éste el principal problema. La vulnerabilidad de los sistemas IoT se tiene que atender como prioridad, debido a que una mala configuración o mal diseño, puede generar puntos débiles para un posible ataque en el dispositivo IoT en el que un tercero pudiera acceder, y como consecuencia, el conocer la información de la red domestica/empresarial.

Lo antes expuesto ha llevado el interés de realizar una investigación a fondo de las distintas áreas de seguridad de las redes IoT y específicamente en redes con tecnología LoRa (long range, por sus siglas en inglés) por ser la más utilizada y en constante crecimiento. La importancia de la investigación del trabajo monográfico radica en dar a conocer a las personas interesadas y usuarios de estas redes, lo necesario para dar integridad y confidencialidad a sus redes brindado información de su estructura a nivel de trama, estándares asociados utilizados en sistemas IoT, arquitectura de red IoT, niveles de seguridad, así como también, la implementación de las distintas llaves de seguridad disponibles a implementar acorde a los escenarios de uso asociados en redes IoT-LoRaWAN. Así mismo, la investigación cubre la descripción de los distintos métodos de seguridad correspondientes de LoRaWAN y los distintos problemas que se presentan debido a errores humanos por la interacción con los dispositivos. Adicionalmente, se brinda información de la seguridad utilizada en sistemas IoT y su conectividad en la nube IoT con la finalidad de incrementar la seguridad de los datos y dispositivos.

Agradecimientos

Agradezco al Dr. Freddy Chan, por guiarme como tutor en todo el transcurso de mi carrera y por apoyarme en todo momento.

Mi sincero agradecimiento al Dr. Javier Vázquez, por el apoyo e interés para la realización de este trabajo monográfico.

Agradezco al M.C. Luis Carlos Rodríguez, por sus enseñanzas como profesor, sus consejos y por su gran amistad.

Finalmente, agradecer a mi gran amigo Abner Márquez, que siempre me demostró su apoyo y confianza durante estos años

Dedicatoria

A mis padres, por todo su esfuerzo, cariño y apoyo incondicional que me han brindado durante estos años, para forjarme en mi camino como persona. Gracias por todo su sacrificio y los valores que me inculcaron para concluir con mis estudios.

A mi hermano, que siempre ha estado conmigo y me ha motivado a seguir adelante para ser un gran ejemplo de persona.

A mi abuelo, que me demostró su gran apoyo y cariño, además de ser un gran padre y maestro de vida.

Contenido

Tabla de Figuras

Lista de Tablas

Capítulo 1

Introducción

1.1 Planteamiento del problema

Uno de los problemas principales de la actualidad, es la falta de conocimiento de la seguridad en la adaptación de los entornos tecnológicos para ambientes laborales y del hogar para la selección de las tecnologías de comunicación que existen en el mercado como las redes IoT. Las redes IoT están compuestas por objetos físicos como sensores, software, entre otras tecnologías, con el objetivo de intercambiar información entre los dispositivos que se encuentran en la red. La popularidad de estas redes va en aumento al igual que sus aplicaciones para las necesidades, pero de igual forma carecen de la información necesaria en temas de seguridad y la privacidad de los datos de sus usuarios que interactúan con estas redes. Con la finalidad de revertir el problema previamente expuesto, es necesario definir e informar los distintos métodos de seguridad que utilizan las redes IoT, en relación con el funcionamiento de su arquitectura y el manejo de los datos confidenciales y salvaguardar la privacidad de los usuarios.

1.2 Justificación

La importancia que tienen las redes IoT hoy en día, es muy amplia debido al cambio y características que ofrecen en comparación a las redes tradicionales que conocemos, así como la conexión con dispositivos IoT que va en aumento con el paso del tiempo. Se estima que, en los próximos años, se tendrán todo tipo de dispositivos que se conecten a estas redes que mejorarán el día a día de las personas, pero que al mismo tiempo genera una preocupación por la seguridad de los datos de los usuarios que tengan interacción con estas redes.

Todo esto ha llevado a la necesidad de realizar una investigación a fondo de las distintas áreas de seguridad de las redes IoT y más específicamente en las redes con la tecnología LoRa/LoRaWAN. La importancia de la investigación del trabajo monográfico radica en dar a conocer a las personas interesadas y usuarios de estas redes, lo necesario para dar integridad y confidencialidad a sus redes conociendo su estructura a nivel de trama, estándares, esquemas, niveles de seguridad y la implementación de las distintas llaves de seguridad para la amplia variedad de escenarios que pueden existir en las redes IoT LoRaWAN.

1.3 Metodología

La realización de este documento es generada por la investigación y recopilación de información del mundo actual, para la búsqueda de nuevas tecnologías en redes IoT. El documento cuenta con información referenciada de la empresa que certifica el estándar LoRaWAN (LoRa Alliance), libros digitales y empresas a nivel mundial que documentan el funcionamiento de LoRaWAN y las redes IoT en general.

La búsqueda de información que se utilizó como método principal, fueron los medios digitales a través de la red donde se recopilaron distintos documentos que involucran la implementación y la administración del estándar LoRaWAN considerando sus condiciones para determinar la integridad y confidencialidad de los datos.

1.4 Objetivo general:

Definir los esquemas de seguridad para proporcionar integridad y confidencialidad de los datos en redes IoT LoRaWAN.

1.5 Objetivos específicos

1. Conocer los estándares principales para implementar redes IoT.
2. Conocer la importancia de establecer esquemas de seguridad en redes IoT.
3. Revisión de esquemas, o niveles, de seguridad considerados en redes para IoT.
4. Estudiar los esquemas de seguridad en redes LoRaWAN.
5. Proporcionar una guía del esquema de seguridad empleado en redes IoT LoRaWAN.

1.6 Alcance

Este documento de investigación abarca la descripción de los diferentes esquemas de seguridad IoT en redes LoRaWAN, para obtener un mayor conocimiento de los estándares actuales, niveles de seguridad, arquitectura de la red, estructura de los distintos tipos de mensajes además del estudio, revisión y documentación de la integridad y confidencialidad en las redes IoT LoRaWAN.

Capítulo 2

Marco Teórico

2.1 Qué son las redes IoT

Las redes IoT se componen de grupos de dispositivos y su conexión entre ellos es a través de una red privada y con conectividad a internet, donde los dispositivos y objetos son visibles para interactuar entre sí. La aplicación de las redes IoT es variada, por ejemplo: ropa, refrigeradores, horno microondas, sensores, entre otros. Cualquier objeto en la imaginación de los usuarios con una conexión a la red internet y la capacidad de interactuar sin la intervención de una persona física en el proceso, podría pertenecer a una red IoT. La misión principal de las redes IoT, es la interacción que puede existir máquina a máquina o como comúnmente se le conoce: Machine to machine (M2M). [1]

Así mismo, este tipo de redes actualmente están teniendo mucha popularidad debido a que actualmente con internet, se encuentran en una extensa variedad de aplicaciones que prácticamente son casi infinitas, esto a causa de los distintos dispositivos que se pueden encontrar en el mercado actual.

Se puede encontrar una gran variedad de aplicaciones para el caso de la domótica y que van desde asistentes de voz hasta cortinas, enchufes y electrodomésticos en general que funcionan por Wifi contribuyendo en la automatización de los hogares en todos los aspectos posibles.

En el caso de los dispositivos domésticos (refrigeradores, aires acondicionados y televisiones), las modalidades de operación pueden ser diferentes como: alertas a distancia, detección de productos dentro de un refrigerador con la finalidad de conocer su fecha de caducidad, la

cantidad de comida que se encuentra en el refrigerador. Otros casos como el aire acondicionado, o la televisión, se manejan mediante programación remota para el encendido y apagado de tales dispositivos.

Así, se puede comentar que la importancia que tienen estas redes hoy en día es muy grande ya que ofrecen la conexión entre dispositivos. Se puede decir que en los próximos años se tendrán todo tipo de dispositivos conectándose a estas redes, pero que al mismo tiempo se genera una gran preocupación por la seguridad de los datos de las personas que interactúen con estas redes.

2.2 Estándares para redes IoT

2.2.1 Sigfox

Sigfox es una de las tecnologías IoT fundada en el año 2010 por Christophe Fourtet y Ludovic Le Moan con el objetivo de conectar todos los objetos que se puedan encontrar en nuestro entorno físico con el mundo digital. Sigfox es una red global que se dedica al IoT en el manejo datos pequeños que al mismo tiempo sean de largo alcance además de ofrecer una conectividad de punto a punto. [1]

Sigfox cuenta con una presencia en los 4 continentes incluyendo más de 70 países del mundo siendo los usuarios desde grandes empresas hasta las nuevas que se agregan a diario. El objetivo de Sigfox es conectar a toda la población y de forma paralela, obtener un mundo sostenible con las tecnologías que se utilizan para la innovación de este proyecto.

Tecnología Sigfox

La implementación de esta tecnología tiene como consecuencia la primera red 0G, que es la encargada de recibir una enorme cantidad de datos transmitidos por distintos objetos o dispositivos. Este tipo de conectividad inalámbrica es única en su tipo con un protocolo optimizado, sin sobrecarga y donde los dispositivos y objetos no están necesariamente conectados a la red. Sigfox brinda una solución de comunicaciones, donde su complejidad

informática y la complejidad de la red, se encuentra gestionada en un servicio de la nube en lugar de los dispositivos. Todo este conjunto reduce drásticamente el consumo de energía y los costos de los dispositivos conectados. [1]

La tecnología Sigfox, debido a sus características, tiene distintos usos en diferentes aplicaciones como:

- ✓ Logística en la cadena de suministros
- ✓ Manufactura
- ✓ Ciudades inteligentes
- ✓ Servicios públicos y Energía
- ✓ Venta minorista
- ✓ Agricultura
- ✓ Hogar y estilo de vida
- ✓ Seguridad

Todas las categorías antes mencionadas cuentan con soluciones muy comunes y de poca complejidad para la satisfacción del usuario como puede ser: alarmas, detectores de presencia, entre otros. Lo anterior dependerá de las necesidades que se requieran cubrir en un momento dado.

Ultra-Narrow Band (UNB)

Utiliza un ancho de banda de 192 KHz **(Figura 1. Tecnología Sigfox basada en Ultra-Narrow Band)** para el intercambio de mensajes a través del aire como se puede observar en la figura. La banda ultra estrecha considera mensajes de 100 Hz de ancho de banda, con una velocidad de transferencia de datos de 100 o 600 bits por segundo. Esta velocidad es tomada en cuenta por la región debido a que las velocidades son variantes.

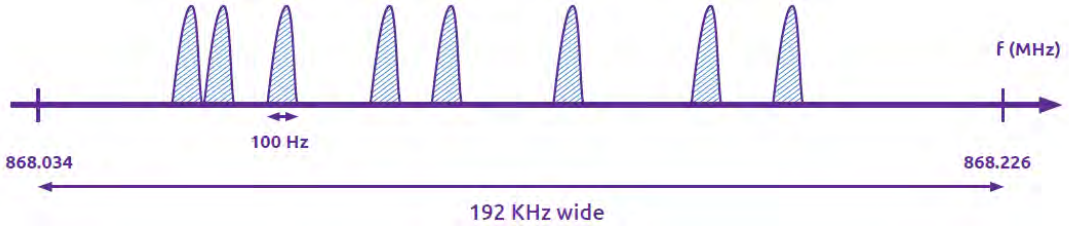

Figura 1. Tecnología Sigfox basada en Ultra-Narrow Band

Acceso aleatorio

El acceso aleatorio cuenta con una característica principal con la cual se obtiene una alta calidad del servicio, en donde el dispositivo se encarga de emitir un mensaje en una frecuencia de forma aleatoria **(Figura 2. Saltos de frecuencia en replicas)** y después envía dos más de igual manera aleatorias tanto en frecuencia como en tiempo. [2]

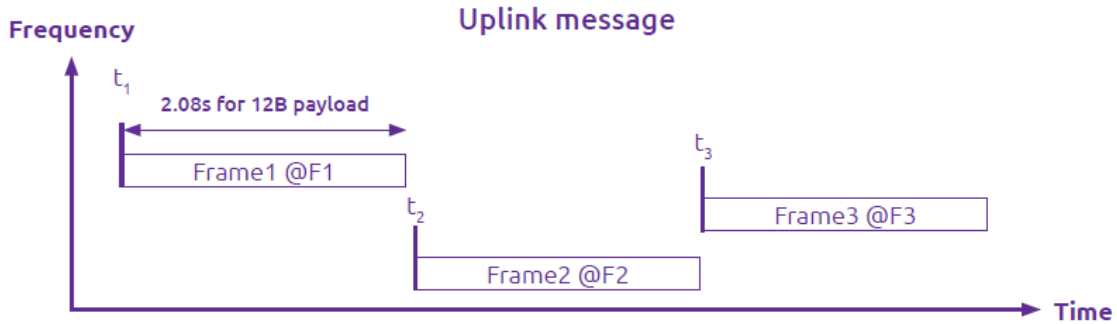

Figura 2. Saltos de frecuencia en replicas [2]

Recepción cooperativa

En el principio de la recepción cooperativa **(Figura 3. Recepción de mensajes por estaciones múltiples Sigfox),** un objeto no se adjunta a una estación base específica a diferencia de los protocolos definidos para telefonía celular. [2]

Los mensajes que se emiten son recibidos por cualquiera de las estaciones que estén en su área de alcance. En promedio se pueden encontrar 3 estaciones base

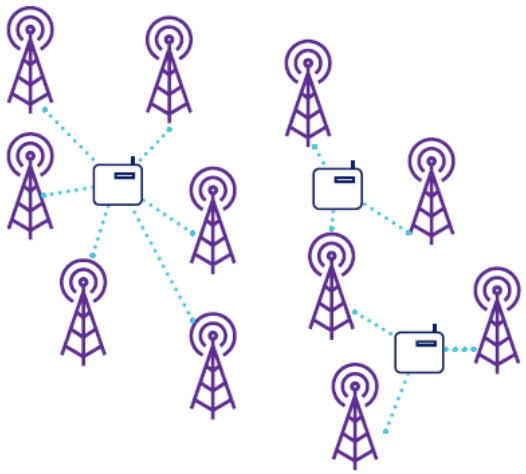

Figura 3. Recepción de mensajes por estaciones múltiples Sigfox

Mensajes pequeños

El tamaño de los mensajes pequeños **(Figura 4. Tamaños de carga útil)** es de 1 a 12 bytes. Este tamaño de carga es útil para la transferencia de datos de un sensor, coordenadas de un GPS o algún otro tipo de datos que se puedan transferir.

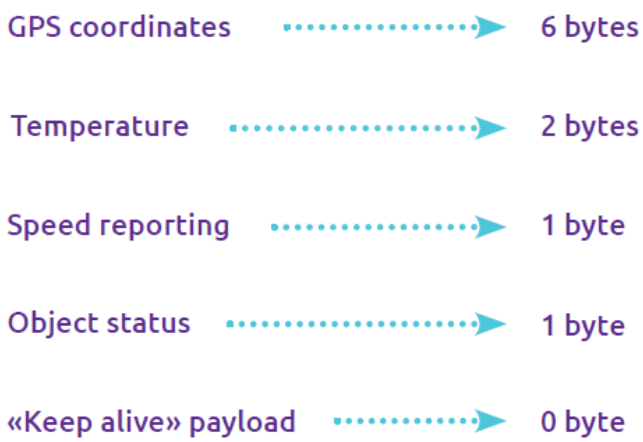

Figura 4. Tamaños de carga útil

Bidireccional

El mensaje de enlace descendente lo inicia el objeto en donde existe un retraso de 20 segundos. Esto sucede entre el primer cuadro transmitido y la ventana de recepción que dura 25 segundos máximo. La frecuencia de enlace descendente es la frecuencia del primer mensaje de enlace ascendente más un delta conocido. [2]

Arquitectura de la red

La arquitectura de la red Sigfox **(Figura 5. Arquitectura de la red Sigfox)** es muy simple y fácil de entender. Esto se debe a que la podemos encontrar dividida en 2 capas principales que son: La capa de equipo de red o equipamiento de red y la capa de sistema de soporte Sigfox. Cada una con sus características y las partes que la conforman para una buena estructura de la red. La primera capa (equipo de red) está conformada por estaciones que hacen referencia a las antenas para la recepción de mensajes de los distintos objetos o dispositivos que estén emitiendo y el envío a la siguiente capa (sistema de soporte Sigfox) que se encarga de la mayoría de la arquitectura de Sigfox.

El sistema de soporte de Sigfox, está formado por una central que es la encargada de procesar los mensajes que fueron recibidos en la capa de equipo de red y después enviarlos en forma de devoluciones de llamada al sistema del cliente. Las características de la capa son amplias y esenciales para la operación y el monitoreo de la red, lo cual es muy importante hablando desde el punto de vista del administrador. [2] También se tienen características como soporte comercial, soporte de planificación de radio y la información que contiene el repositorio con las herramientas para hacer análisis de lo recopilado y lo que va generando la red con el paso del tiempo.

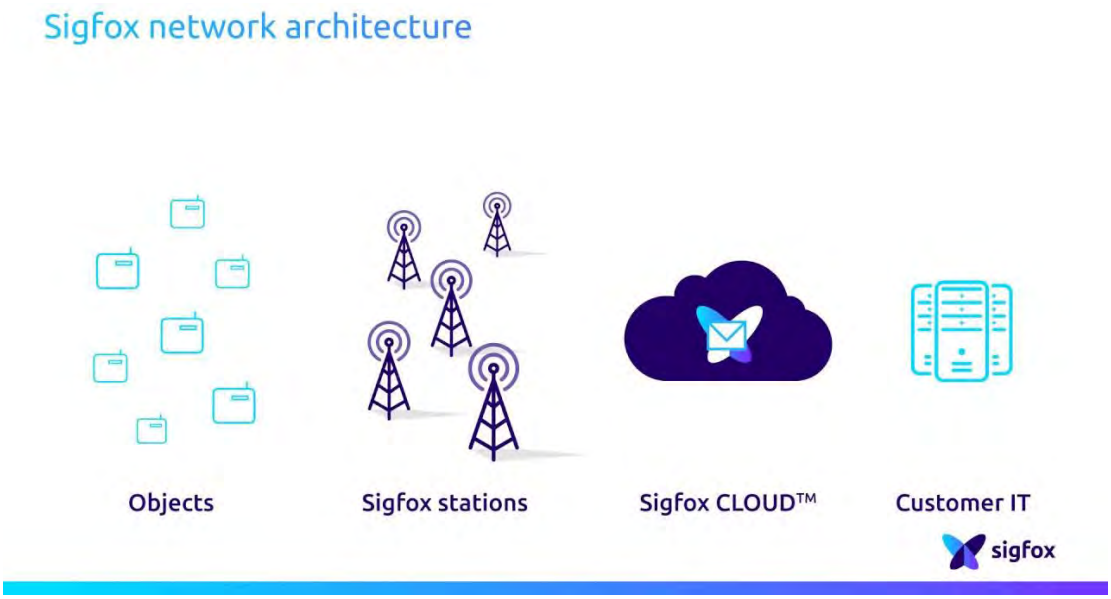

Figura 5. Arquitectura de la red Sigfox

Seguridad Sigfox.

En la rama de la seguridad para Sigfox, podemos encontrar un número considerable de amenazas y temores comunes de los usuarios que adquieren este tipo de servicios en las diferentes categorías donde es utilizado y conforme a esto las características pueden variar.

Este entorno maneja de forma predeterminada la seguridad acorde a lo siguiente:

- ✓ Cifrado para garantizar a los usuarios una confidencialidad en los datos de la red.
- ✓ La criptografía basada en AES (Advanced Encryption Standard) sin la llave por transmisión por el aire.
- ✓ La característica de aislar un segmento del entorno ante posibles ataques para su revisión.

Como segundo apartado en la seguridad del entorno Sigfox, se maneja un apartado donde los dispositivos son los principales puntos del entorno por su interacción con el usuario. En Sigfox la seguridad está basada en 3 niveles que van desde el nivel medio hasta el nivel de muy alto:

- ✓ **Nivel medio:** En este nivel, las credenciales correspondientes a la seguridad son almacenadas en el dispositivo.
- ✓ **Nivel alto:** En este nivel, las credenciales correspondientes a la seguridad son almacenadas en un área protegida basada en el software.
- ✓ **Nivel muy alto:** En este nivel, las credenciales correspondientes a la seguridad son almacenadas en un elemento que sea seguro.

LoRa

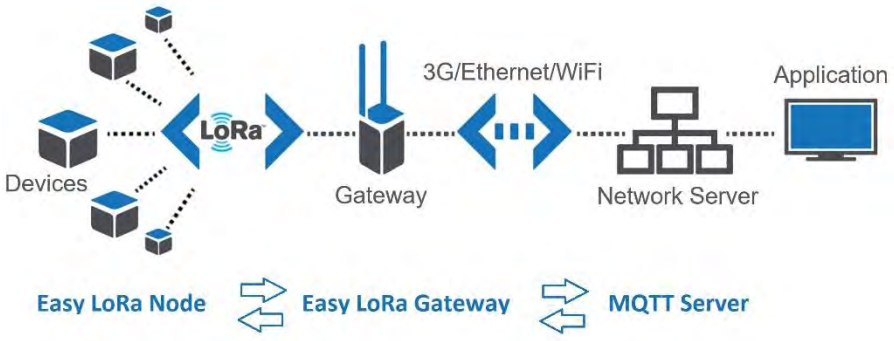

Figura 6. LoRa

LoRa es una tecnología inalámbrica de modulación **(Figura 6. LoRa),** que está destinada para redes de baja potencia pero que al mismo tiempo cuenta con una cobertura muy amplia. Su nombre viene del inglés Long-Range que significa: “De largo alcance o de rango amplio”. Esta tecnología se encuentra patentada por la empresa Semtech que se encarga de fabricar chips de radio y la encargada de administrarla “Lora Alliance”, siendo quien certifica a los deseen trabajar con esta tecnología. [3]

LoRa es una tecnología de las más importantes y populares en el mercado IoT al ser software libre en comparación a otras tecnologías en el mercado actual (p.ejemp., Sigfox que es de paga), atribuyendo a que sus características son muy atractivas para los usuarios que deseen utilizarlas. Al proporcionar comunicaciones de largo alcance como lo son 5 kilómetros en la urbanización y hasta 15 kilómetros en áreas rurales, causa que las personas tengan mayor interés en esta tecnología. Una característica fundamental en la que compite con otras

tecnologías del mercado es el consumo bajo de energía, logrando un impacto significativo en la vida de las baterías de los dispositivos de la red logrando así una larga duración de la vida de los dispositivos.

LoRaWAN es un estándar nacido de LoRa, cuenta con una alta demanda para ser utilizado en el desarrollo de aplicaciones en fábricas y pequeñas empresas estableciendo una comunicación de forma interna y con una topología en forma de estrella. LoRaWAN es ideal para cubrir las necesidades de un entorno de trabajo para la transmisión y recepción de datos de longitud pequeña.

	Sigfox	LoRa
Frecuencia	868/902 MHz (ISM)	433/868/780/915 MHz (ISM)
Alcance urbano	3-10 km	2-5 km
Alcance en campo	30-50 km	15-20 km
Tamaño de paquete	12 bytes	Definido por usuario
Nodos por punto	1M	100000
Topología	Estrella	Estrella

Tabla 1. Tabla comparativa LoRa/Sigfox

Tecnología

Las características atractivas de LoRa, además de sus amplias aplicaciones, son la flexibilidad y confiablidad. LoRa cuenta con un control absoluto (software libre) del sistema, donde se pueden realizar diferentes aplicaciones para cubrir todo tipo de necesidad en lo que se refiere a sistemas IoT. [3]

Algunas características adicionales y sobresalientes de los sistemas LoRa son:

- ✓ Alta capacidad
- ✓ Larga duración en la vida de la batería
- ✓ Geolocalización
- ✓ Seguridad
- ✓ Bajo costo

Categorías de uso

LoRa es ideal para la diversidad de aplicaciones IoT **(Figura 7. Usos de LoRa)** que pueden requerirse en el mercado tanto personales, empresariales, entre otras.

Algunas de las aplicaciones en las que LoRa-IoT puede ser utilizado son:

- ✓ Ciudades inteligentes
- ✓ Seguridad
- ✓ Agricultura
- ✓ Localización
- ✓ Casas inteligentes
- ✓ Logística

Figura 7. Usos de LoRa

Además, LoRa/LoRaWAN contiene esquemas de seguridad que garantizan la integridad de los usuarios mediante la confidencialidad de estos, aumentando la certeza de que los datos estarán protegidos dentro de la red.

2.2.2 NB-IoT

NB-IoT o banda estrecha, es uno de los estándares actuales del IoT que se encarga de las comunicaciones inalámbricas además de ser el más nuevo estándar en el mercado actual, a comparación de Sigfox y LoRa que son más conocidos en IoT. NB-IoT pertenece a LPWAN, que son las redes de área amplia de baja potencia. Esto indica que el estándar brinda características para conectar diferentes tipos de dispositivos con cantidades de datos muy pequeños al igual que LoRa y Sigfox, con una batería de duración muy alta como característica fundamental y de bajo ancho de banda.

La tecnología NB-IoT, tiene un entorno muy consistente y amplio para ser uno de los más recientes en su rama, con una confiabilidad buena para los usuarios. Su popularidad se debe a su calidad de servicio de extremo a extremo y tiene una escalabilidad mejor que las LPWAN celulares que se pueden encontrar en el mercado actual. [4]

Tecnología NB-IoT

La tecnología de banda estrecha está destinada para aplicaciones M2M y todo tipo de dispositivos que se puedan conectar en redes IoT, por las distintas características antes mencionadas sobre el rango extendido y el consumo bajo de la energía, lo que es de gran ayuda para la batería. En el año 2016 NB-IoT se convirtió en el estándar para las comunicaciones inalámbricas, para todo tipo de categorías disponibles en el mercado **(Figura 8. Usos de NB- IoT)** y a su alcance por el gran potencial que demuestra.

Al igual que su competencia en el mercado, es necesario transmitir un número de datos pequeños al igual que la frecuencia. La red NB-IoT tiene una amplia gama de usos con el propósito de facilitar su uso en aplicaciones convencionales como es la obtención de datos en tiempo real y monitoreo de variables físicas.

Algunas de las aplicaciones NB-IoT son:

- ✓ Agricultura y Ganadería
- ✓ Cuidado de la Salud
- ✓ Seguimiento de personas y animales
- ✓ Manufactura y Logística
- ✓ Ciudades inteligentes

Especificaciones NB-IoT

NB-IoT funciona utilizando bandas de espectro tipo estrecho como su nombre lo indica de 180 kHz o 200 kHz. El estándar da trasferencias de 250 Kbit/s, con latencias de 1.6 s hasta 10 s. [4]

Esta tecnología utiliza bandas de comunicación celular y opera de 3 maneras completamente diferentes:

- ✓ **Standalone:** Utiliza la banda GSM para el reemplazo de implementaciones existentes.
- ✓ **In-band:** Utiliza la banda LTE mientras la comparte.
- ✓ **Guard-band:** Utiliza el espacio entre los canales LTE para maximizar el espectro de comunicación.

NB-IoT es semidúplex, esto quiere decir que permite una conexión a la red celular, la asignación de recursos de red al nodo y la transmisión de datos. [5]

La amplia gama de dispositivos con soporte para NB-IoT, tienen distintas formas operación como: Los estados de conexión de los dispositivos (Un dispositivo se puede encontrar en estado de desconexión hasta que tenga disponibles datos en su entrada, para después transmitirlos y regresar a su estado original).

Figura 8. Usos de NB- IoT

Este tipo de conexión durante el tiempo que esta activa, tiene la capacidad de solicitar datos para su transmisión al igual que la capacidad de configurarlos. Todo ésto mientras se encuentre activo para después regresar a la desconexión. La forma en la que se realiza este proceso tiene relación con la arquitectura que maneja LTE. [5] Con todas las especificaciones y las características del NB-IoT, se tiene previsto que, en el futuro, se adquiera una amplia gama de usos y de dispositivos los cuales ayudaran en la vida diaria de los usuarios y en las grandes industrias.

Para lograr todas estas aplicaciones, se requieren las siguientes características:

- ✓ Bajo costo.
- ✓ Cobertura amplia.
- ✓ Latencia de transmisión baja.
- ✓ Movilidad y localización.
- ✓ Consumo bajo de energía para larga duración.

Arquitectura

En la arquitectura de NB-IoT **(Figura 9. Estructura de NB-IoT)** se puede encontrar similitud con la arquitectura LTE, pero en realidad es la misma y la encontramos por sus siglas en ingles EPC (Evolved Packet Core), en donde la única diferencia es la optimización para una cantidad de dispositivos grande con transmisiones de datos cortas.

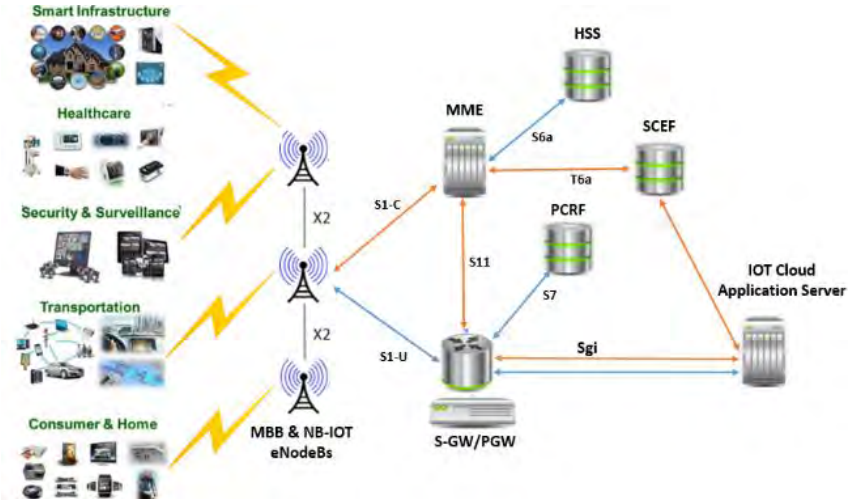

Figura 9. Estructura de NB-IoT

2.2.3 Importancia de la seguridad en redes IoT

Seguridad

La seguridad en las distintas redes IoT del mercado tiene un papel importante en la selección de la tecnología IoT de sus potenciales usuarios. La mayor parte de los potenciales usuarios, se encuentran con el temor de que un ajeno a la red pueda comprometer su privacidad, y de esta forma, acceder a sus datos.

Los dispositivos IoT cuentan con características de conexión a internet siendo el problema principal al ser una vulnerabilidad por atender de alta prioridad. En general, esto es atribuido a una mala configuración o diseño donde se pueden encontrar puntos débiles para un posible ataque, en donde un tercero accede al dispositivo, y como consecuencia, a la información que se contenga en el dispositivo de una red domestica o laboral.

Así mismo, los dispositivos IoT quedan expuestos a ciber-delincuentes que, en su mayoría, crean estrategias para aprovechar las vulnerabilidades encontradas en la configuración de los nodos de red. Por este motivo se tiene cierto rechazo al uso de las redes IoT, además de que, existe aún un debate en cuanto a la selección de las tecnologías que se encuentran en el mercado actual como lo son: LoRa, Sigfox y NB - IoT. [6]

Privacidad

Los conocidos ciber-delincuentes se dedican a la infiltración en las redes, para acceder a los dispositivos que contienen información de la red o para obtener información de gran relevancia de una empresa. [6] El objetivo de estos ataques generalmente es afectar a una persona o un grupo con la información obtenida, para una suplantación de identidad con fines económicos o solo dañar la imagen. Para cumplir con la importancia de la seguridad y privacidad en las redes IoT, se requiere una buena estructura para evitar vulnerabilidades desde la raíz, tener control absoluto de las contraseñas y control de las llaves de sesión. Todo el conjunto de características tiene el objetivo de no incidir en ataques y obtener una buena gestión de los dispositivos.

2.2.4 IoT en la nube

La nube tiene un papel fundamental en las redes IoT por su sistema centralizado que ayuda al transporte de datos y a la entrega a través de la conexión a internet. También conocido como “Cloud Computing” es una solución económica por no requerir una infraestructura para almacenar y procesar datos. [7]

En Cloud Computing se puede encontrar seis categorías de uso:

1) **Software como servicio (SaaS):** Las aplicaciones se encuentran basadas en la nube y son accesibles a través de ésta.
2) **Plataforma como servicio (PaaS):** La nube es la encargada de tener las herramientas para construir aplicaciones basadas en la nube.
3) **Infraestructura como servicio (IaaS):** Es la encargada de proporcionar servidores, centros de datos y almacenamiento a las empresas.
4) **Nube publica:** Espacios que proporcionan acceso a los usuarios públicos.
5) **Nube privada:** Contiene las mismas características que la nube pública con la excepción de que es controlada por alguna empresa.
6) **Nube hibrida:** Es la conformación de la nube privada como principal, con un acceso público.

La tecnología de las redes IoT y la nube, es una complementación para una mayor escalabilidad, con características diferentes siempre buscando brindar soporte para la resolución de problemas de los usuarios.

Cloud Computing y IoT

El Cloud Computing **(Figura 10. IoT en la nube)** cuenta con las funciones y características de aumentar la eficiencia y el alcance de las tareas que se realizan en ambientes de trabajo o privados. Con el IoT se tiene el complemento para aumentar aún más las capacidades y los resultados en el procesamiento, pero a una mayor escala con la combinación de ambas tecnologías. Ambas tecnologías han cambiado la forma de trabajo de las empresas, ayudando a la creación de herramientas de trabajo para tener mayor eficiencia. Debido a estas necesidades, se tiene un gran mercado en la nube que están especializadas en las redes IoT y de la misma forma, muchas empresas grandes tienen la necesidad de involucrarse en IoT que es el futuro de las redes y comunicaciones en el mundo. [7]

Cada empresa de Cloud tiene diferentes servicios disponibles y herramientas que se pueden diferenciar unas de otras para la elección de los usuarios como pueden ser:

- ✓ Microsoft Azure
- ✓ Amazon Web Services
- ✓ Huawei
- ✓ Google

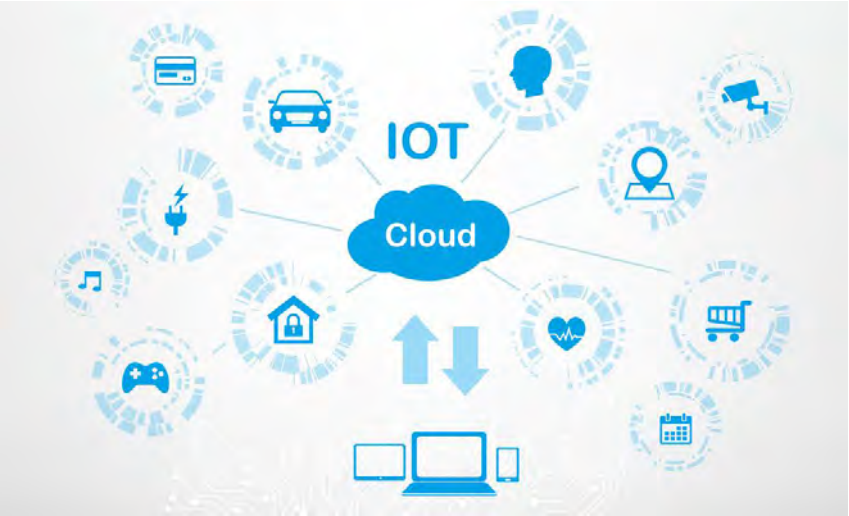

Figura 10. IoT en la nube

Big Data

Big data se encarga del proceso del análisis de datos en cantidades muy grandes ya sean estructurados o no estructurados, para la obtener de información como lo pueden ser las redes IoT y clasificarla para su revisión. Big Data hace referencia a datos que son complejos de procesar con los métodos tradicionales incluidas las siguientes cuatro:

- ✓ **Volumen:** Cantidad de datos recopilados.
- ✓ **Variedad:** Tipos de datos con formatos diferentes transferidos entre sistemas.
- ✓ **Veracidad:** Capacidad de herramientas y análisis de Big Data para la clasificación de datos (Baja calidad/Alta calidad).
- ✓ **Velocidad:** Velocidad del procesamiento de datos.

La relación que existe entre Big Data y Cloud **(Figura 11. Entorno Big Data, IoT y Cloud)** es muy importante para la infraestructura de la nube que permite el almacenamiento de información de forma más eficiente, al igual que el procesamiento y el análisis en Big Data. La característica por destacar en Big Data es la escalabilidad con almacenamiento en la nube, independientemente de que sea un sistema de pago por el uso. [8]

Figura 11. Entorno Big Data, IoT y Cloud

La nube brinda la oportunidad para que los usuarios ingresen y analicen Big Data de manera más eficaz. IoT y Big data operan entre sí para compartir información debido a las características que comparten sobre gestión y conexiones múltiples de las redes IoT que manejan cantidades de datos grandes, dependiendo el tamaño de la red mientras ambos tienen un fin similar. Funciones en conjunto: Para la extracción de información de una empresa o una red domestica con un tamaño considerable, se tienen las redes IoT donde se puede conseguir una gran cantidad de información. El siguiente elemento (Big Data) que se encarga de analizar y clasificar los datos extraídos por relevancia hasta obtener la información que se requiere. [8]

Capítulo 3

Desarrollo del Trabajo

3.1 Introducción

En este capítulo se dará a conocer la tecnología LoRa y lo que conlleva a su utilización actual, además de que LoRaWAN es el protocolo MAC que se utiliza en las redes IoT. Así mismo, se abordarán temas tales como: arquitectura de la red LoRaWAN y sus componentes, administración y características de cada elemento de la red LoRaWAN, estructura de los paquetes de la red LoRaWAN, esquemas e indicaciones de seguridad para LoRaWAN, integridad de la nube para redes IoT y los proveedores Cloud para IoT.

La seguridad y los elementos que rodean el entorno, tienen un papel fundamental en la tecnología de las redes IoT LoRa/LoRaWAN con un potencial en aumento, en paralelo a las innovaciones por las características que la hacen flexible y segura para su implementación.

3.2 LoRa/LoRaWAN

3.2.1 LoRa

LoRa **(Figura 12. Logo LoRa)** se puede definir como la capa física o una tecnología de modulación que viene derivada de CSS. Se utiliza para las redes de baja potencia con una cobertura de red de largo alcance en referencia a su nombre “Long-Range”, con una utilidad para las redes que conocemos hoy en día como IoT. Una gran parte de los sistemas inalámbricos utilizan FSK que es la modulación por desplazamiento de frecuencia, por su

eficiente modulación para obtener una baja frecuencia. LoRa se basa en el espectro de chirp que no solo logra mantener las características de su baja potencia (modulación FSK), pero se obtiene un aumento en el alcance de las comunicaciones. [9]

Los dispositivos LoRa de tipo sensor son capaces de aplicarse a un amplio rango de aplicaciones por su transmisión de datos. LoRa es ideal para diferentes tipos de categorías como: servicios públicos, logística, ciudades inteligentes y agricultura por su flexibilidad para la implementación de las distintas necesidades de los usuarios. LoRa se encuentra bajo la administración de LoRa Alliance que es la encargada de certificar a los fabricantes que trabajan con esta tecnología, tiene un largo alcance de 10km hasta los 20km, una transferencia de datos baja de hasta 255 bytes, conexión punto a punto y una larga duración de la batería de hasta 10 años por su capacidad. Cuenta con la capacidad de demodular señales a 19.5 dB por debajo del ruido, mientras que los sistemas de manipulación por desplazamiento de frecuencia FSK en su mayoría requieren una potencia de 8 a 10 dB de señal por encima del ruido, con el objetivo de lograr una demodulación en buena forma. [10] [11]

3.2.2 LoRaWAN

LoRaWan es un protocolo de capa de acceso a medios basado en LoRa. Por su parte, tiene el protocolo de comunicaciones y la arquitectura del sistema **(Figura 13. Capas de uso de la tecnología LoRa/LoRaWAN)** en la capa física.

El protocolo de comunicaciones y la arquitectura tienen un papel fundamental para las características de LoRaWan como: Capacidad de la red, la seguridad, la vida útil en la batería de los dispositivos y el servicio de la red. Estas características son fundamentales para el funcionamiento de una red LoRaWAN y una buena administración para cambios de nuevos dispositivos o ajustes de la red a futuro. [6]

Figura 12. Logo LoRa

La primera especificación fue en 2015 y de ahí han surgido versiones de LoRaWAN que están especializadas para las redes de baja potencia y de área amplia como lo son las LPWAN. LoRaWAN se encarga de transmitir datos para comunicaciones y administración de los dispositivos de la red mediante este protocolo. Por este motivo es utilizado en distintas categorías de uso que vienen desde las pequeñas empresas hasta los hogares, debido a la modulación por parte de LoRa que le da un rango en comunicación mucho mayor con un ancho de banda bajo, lo que hace la diferencia con otros estándares IoT.

3.3 Arquitectura de red en sistemas LoRa/LoRaWAN

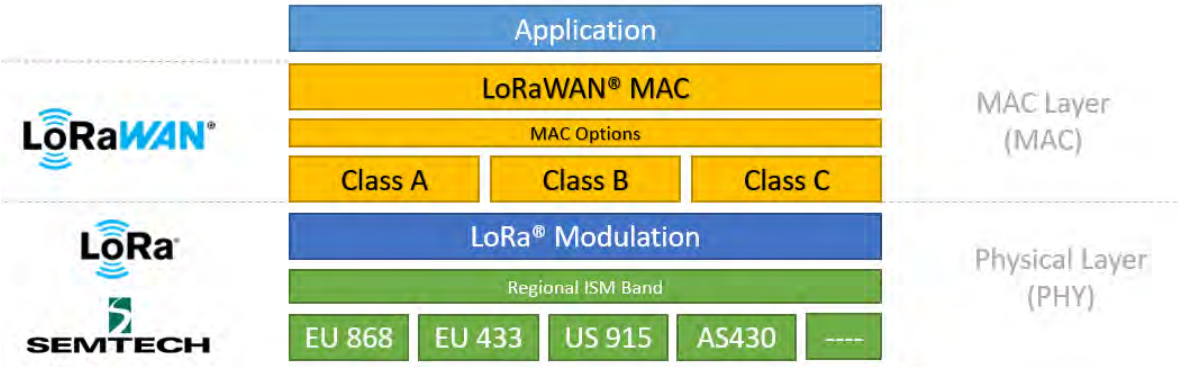

Figura 13. Capas de uso de la tecnología LoRa/LoRaWAN

El protocolo LoRaWAN tipo MAC **(Figura 14. Arquitectura de red LoRaWAN)** maneja una arquitectura, para una red de tipo estrella con un amplio rango y baja potencia. En la arquitectura de LoRaWAN, que es bidireccional, podemos encontrar distintos tipos de dispositivos IoT para verificar activos teniendo como dispositivos comunes, los sensores por su funcionalidad y bajo costo, aunque de igual forma al existir una amplia variedad de dispositivos, se manejan clases de nodos que son diferentes para la buena gestión de la red y obtener un equilibrio en la vida de las baterías de los dispositivos además de la latencia. [11]

En la red LoRaWAN se tiene una amplia variedad de dispositivos que se pueden conectar y al igual que otro tipo de redes, se encuentran diferencias y por este motivo LoRaWAN maneja 3 tipos de clases donde cada una se diferencia conforme a sus capacidades.

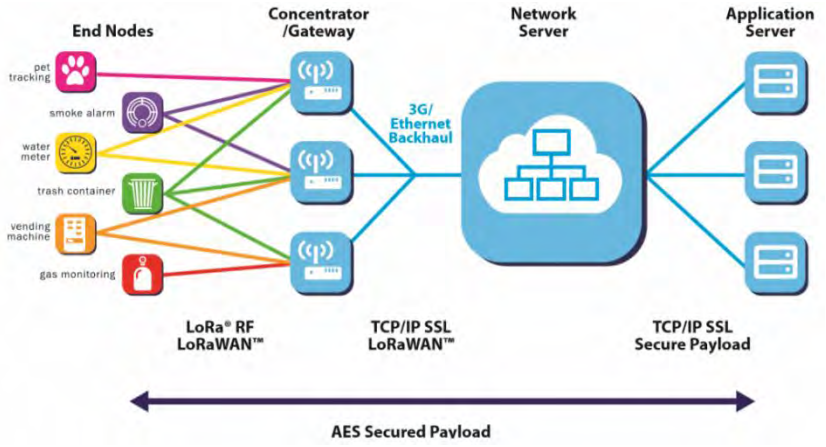

Figura 14. Arquitectura de red LoRaWAN

3.3.1 Clases de dispositivos LoRaWAN

Clase A: Dispositivos con un consumo bajo en energía.

En esta clase **(Figura 15. Clases de dispositivos LoRaWAN (MAC))** los dispositivos finales que se pueden encontrar son de bajo consumo en comparación con otros dispositivos de la red, esto se debe a que la mayor parte del tiempo se encuentran en estado “inactivo” y en espera de que cambie algo en su entorno para hacer una transición estado. Ante un cambio, el nodo o dispositivo de red entra en estado activo estableciendo un enlace de tipo ascendente con la finalidad de realizar una transmisión de datos en la red. Si en un tiempo determinado no se obtiene una respuesta, el dispositivo regresa a su estado original “inactivo”. El dispositivo en proceso de espera lo realiza mediante un enlace descendente, y maneja dos ventanas (Rx1) y (Rx2) donde cada uno de ellos es un momento de espera de respuesta. Cuando el dispositivo no obtiene respuesta entra a un modo “inactivo”. [6]

✓ Enlace descendente, se activa únicamente después de que el sensor transmita algo.
✓ Alta eficiencia en la duración de la batería.

Clase B: Dispositivos finales con ranuras de recepción programadas.

En esta clase **(Figura 15. Clases de dispositivos LoRaWAN (MAC))** se encuentran los dispositivos clase B que básicamente son una mejora de la clase A, para permitir más espacios para mensajes de enlace y como consecuencia, se tiene una menor latencia con un costo en la eficiencia en la batería. Los dispositivos de esta clase son eficientes dispositivos como los sensores para recibir enlaces descendentes en la red, además de que se obtiene ventanas de recepción programadas cuando se envían los enlaces.

✓ Espacios extra a la hora programada.
✓ Recibe una baliza sincronizada en el tiempo desde el Gateway.

Clase C: Dispositivos finales con ranuras de recepción máximas (Recepción continua).

En esta clase se encuentran ranuras de recepción continua que se cierran cuando el dispositivo manda un mensaje de enlace ascendente. Los dispositivos de esta clase siempre se encuentran a la espera de información y mensajes de enlace descendente que se transmiten en la red, por el estado activo en el que permanecen. Esta clase necesita una fuente de alimentación por su deficiencia en la energía, debido a que siempre se encuentra activa.

La clase C **(Figura 15. Clases de dispositivos LoRaWAN (MAC))** al igual que la clase A maneja las 2 ventanas conocidas como Rx1 y Rx2, pero a diferencia de la clase A que se cierra después del tiempo de Rx2, esta permanece hasta que se envía el siguiente mensaje al servidor de la red recordando que estas características se deben al estado activo que tienen esta clase de dispositivos. [6]

✓ Ventana de recepción abierta continua.
✓ Rx se encuentra cerrado solo cuando el dispositivo está transmitiendo.

Figura 15. Clases de dispositivos LoRaWAN (MAC)

Si se realiza una comparativa con otras redes IoT, podemos encontrar que en su mayoría usan una red de tipo malla lo que hace la diferencia con sistemas LoRa (tipo estrella). Al utilizar redes de tipo malla, se genera más trabajo y operaciones. En el diseño tipo malla se tienen que reenviar mensajes entre los nodos para que lleguen a su destino específico. Esto no solo vuelve más lento al proceso, sino que llega información innecesaria a nodos que no tienen relevancia o que requieren dicha información. Sin embargo, la información esta forzada a pasar para llegar a su destino. Esta diferencia es la que hace más eficiente a LoRaWAN sobre otras redes IoT por sus beneficios sobre el tipo de red estrella que también, ayuda a la gestión de la red para posibles modificaciones y nuevos dispositivos en la red.

Tiempo de vida de la batería

La duración del tiempo de vida las baterías y la efectividad de la red LoRaWAN, hacen referencia a la arquitectura y la distribución de las redes como la red de tipo malla en comparación a la red de estrella que es utilizada por LoRaWAN. La red tipo malla tiene un rango significativo, pero resulta compleja para los dispositivos y se refleja en la vida útil de la batería que sufre un decremento, por él envío de información nodo a nodo hasta su destino. La forma en la que funciona LoRaWAN da una idea de cómo funcionan las otras redes que usan el tipo malla y la sincronización constante para verificar la existencia de mensajes en espera.

LoRaWAN con su arquitectura tipo estrella tiene mejor rendimiento y envío de información, esto se debe a que los nodos de la red son asincrónicos y solo se comunican cuando tienen información para ser enviada. El tipo de protocolo que se utiliza en LoRaWAN también se le conoce como “Aloha” y teniendo la comparación con otras redes del tipo LPWAN, se muestra una clara ventaja en la vida útil de la batería que resulta de 3 a 5 veces mejor que otros sistemas IoT. [6]

Capacidad de la red

La capacidad de la red **(Figura 16. Capacidad global de la red LoRaWAN)** es un punto fundamental en la arquitectura de la red LoRaWAN, el cual necesita una serie de características para lograr el mayor rango y eficiencia en los nodos que se encuentran en el entorno de la red, como lo son: velocidad de datos, frecuencia para transmitir, canales concurrentes y la longitud de la carga.

Para tener una mayor capacidad de la red, se tienen que utilizar al máximo las características de LoRaWAN por su arquitectura en forma de estrella como punto principal. Con este tipo de red, una parte fundamental es el Gateway y lo más viable es tener una alta capacidad para recibir mensajes de los nodos. Cuando se tiene una capacidad elevada de la red, también entra en la velocidad de datos adaptativos (ADR) y un transmisor multicanal, para permitir mensajes de forma simultánea en canales múltiples.

ADR es el encargado de controlar y asignar los recursos a los dispositivos finales, utilizando una adaptación en el tiempo de la ejecución de los parámetros de comunicación, cuando la calidad de los enlaces cambia inevitablemente con el tiempo. [9] LoRa al ser una modulación de espectro extendido (o disperso), se entiende que las distintas señales son ortogonales unas de otras y cuando la dispersión cambia, la tasa de datos lo hace de igual manera.
De esta forma el Gateway aprovecha para recibir información en diferentes velocidades, diferentes datos, y todo esto al mismo momento, en un canal. Un nodo con un buen enlace nos indica que usará la menor velocidad de datos para no utilizar más de lo que se necesita. [9]

En el funcionamiento de una red LoRaWAN se pueden distinguir dos partes esenciales: los gateway y los nodos. El Gateway se encarga de recibir y enviar información a cualquier nodo de la red a internet, o el proceso solicitado, mientras que los dispositivos finales tienen la función de recibir o enviar información (siendo comúnmente sensores) hacia el Gateway.

Tomando todas las características anteriores de la arquitectura de una red LoRaWAN podemos encontrar:

- ✓ Bajo consumo de energía.
- ✓ Largo alcance.
- ✓ Transferencia de información baja.
- ✓ Soporte para 3 clases de nodos.
- ✓ Larga duración de las baterías.
- ✓ Red tipo estrella.
- ✓ Administración de los dispositivos de la red.

Todas las características anteriores, indican un entorno de red adecuado para redes privadas y redes públicas con una flexibilidad para el aumento y la gestión de la red con alta eficiencia en la transmisión de los datos.

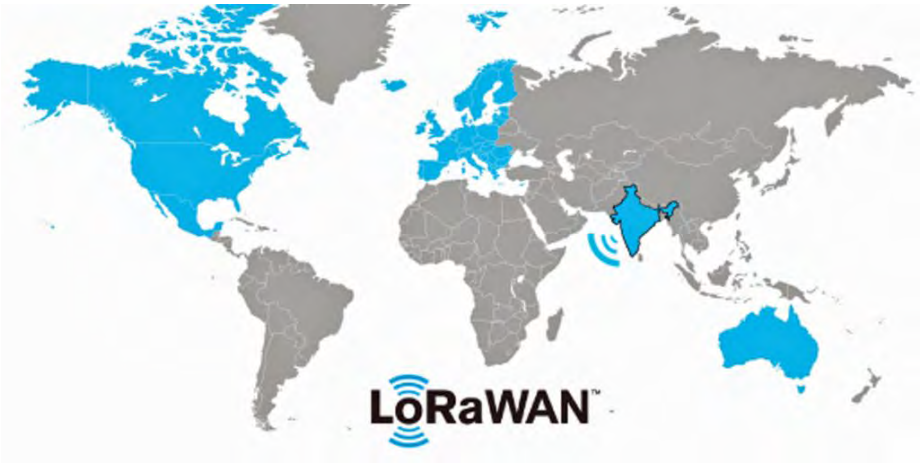

Figura 16. Capacidad global de la red LoRaWAN

3.3.3 Elementos que integran la red LoRa/LoRaWAN

En las redes LoRaWAN podemos encontrar elementos que la integran **(Figura 17. Elementos que integran la red LoRaWAN)** cada uno con sus funciones independientes, pero de igual manera tienen interacción para el funcionamiento de la red. Como primer elemento se encuentran los dispositivos finales que, en su mayoría, se componen de sensores o actuadores que a su vez forman los nodos que se conectan a otro elemento de la red conocido como Gateway o puerta de enlace que es el encargado de enviar información.

Los elementos que integran la red LoRaWAN son:

- ✓ Dispositivos finales/Nodos.
- ✓ Gateway/Puerta de enlace.
- ✓ Servidor de red.
- ✓ Servidores de aplicación

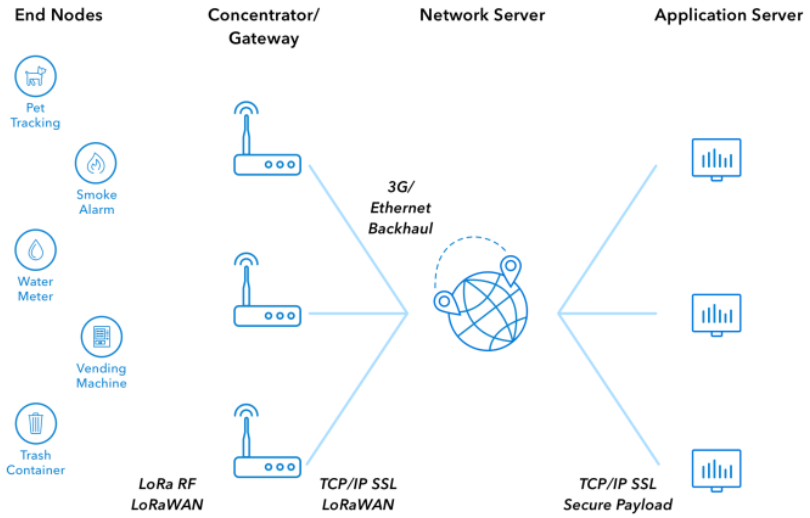

Figura 17. Elementos que integran la red LoRaWAN

Dispositivos finales

Los dispositivos finales **(Figura 18. Dispositivos finales LoRaWAN)** para una red LoRaWAN, son físicos y tienen la capacidad de conectarse a la red como los sensores o actuadores y en su mayoría estos mismos tienen una vida útil de batería por sus características. Su forma de conexión es simple debido a que están conectados de forma inalámbrica a la red LoRaWAN, por puertas de enlace (Gateway) con la modulación LoRa mencionada anteriormente. Las aplicaciones que tienen los dispositivos como los sensores, se encargan de medir en su mayoría condiciones en el medio ambiente como los sensores de temperatura o de presión, en cambio, los actuadores tienen otras funciones como el control de riego, alumbrado público, cerraduras, alarmas, etc. [12]

Existen tres clases de dispositivos con sus características como se menciona en la arquitectura de LoRa/LoRaWAN:

✓ Clase A: Dispositivos con un consumo bajo en energía.
✓ Clase B: Dispositivos finales con ranuras de recepción programadas.
✓ Clase C: Dispositivos finales con ranuras de recepción máximas.

En los dispositivos se manejan dos términos para los mensajes que se reciben de la puerta de enlace o los que se envían. Los enlaces ascendentes son cuando un dispositivo envía un mensaje a la puerta de enlace y un enlace descendente es cuando el dispositivo recibe un mensaje de la puerta de enlace. Un dispositivo puede aumentar su vida por varios años con la misma batería, dependiendo de su programación en la suspensión del dispositivo, con el objetivo de optimizar lo máximo posible y solo utilizarlo únicamente cuando la red lo requiera.

Puerta de enlace/Gateway

Figura 18. Dispositivos finales LoRaWAN

En una red LoRaWAN los nodos tienen una conexión directa con un Gateway en específico, a diferencia de otras tecnologías como la comunicación celular. No existe una conexión fija entre un dispositivo final y un Gateway en específico, con esto se entiende que los datos que son transmitidos desde los nodos de la red LoRaWAN, se envían a todos los Gateway de la red que a su vez es recibida por los Gateway y se tiene la función principal que es transmitir los datos recibidos a un servidor de red que se encuentre en la nube.

Con la conexión a los múltiples Gateway de la red, se reducen los errores en la perdida de paquetes teniendo de referencia, la existencia de otras puertas de enlace disponibles para recibir los datos y se reduce la sobrecarga de la batería de los dispositivos como consecuencia de la eficiencia de la red.

La conexión del Gateway a los servidores de red es mediante conexión a internet a través de IP, como enlaces de radio de telefonía móvil (3G, 4G, 5G), Wifi y Ethernet, para transmitir los datos que se reciben en el Gateway que se encuentra conectado a una fuente de alimentación para energía. [6]

Los Gateway LoRaWAN se pueden categorizar en dos tipos:

- ✓ **Gateway indoor:** Los Gateway de interiores **(Figura 19. Gateway indoor)** son los que se encargan de la cobertura como las casas y medianas empresas donde es muy difícil tener acceso.
- ✓ **Gateway outdoor:** Los Gateway de exteriores **(Figura 20. Gateway outdoor)** son los que se encargan de la cobertura en áreas abiertas y amplias por su posicionamiento en lugares como los techos de las casas y torres con una alta sensibilidad, beneficiando áreas rurales urbanas.

Figura 20. Gateway indoor

Figura 19. Gateway outdoor

Servidor de red

El servidor de una red LoRaWAN, tiene como función principal la administración de toda la red con una capacidad de controlar y adaptar dependiendo el uso de la red en forma dinámica, tomando como referencia las funciones que tiene con respecto a la información que recibe de los Gateway. [12] La conexión entre los Gateway y el servidor de red es mediante el protocolo IP. El manejo de los mensajes es fundamental para la recepción desde los Gateway como la eliminación de mensajes duplicados, por el envío a múltiples Gateway además de contar con características de enrutamiento en el reenvío de mensajes a la aplicación correcta.

En los Servidores de red LoRaWAN **(Figura 21. Red de dispositivos LoRaWAN)** se encuentran las siguientes características:

- ✓ Origen de los dispositivos.
- ✓ Reconocimiento de los mensajes.
- ✓ Adaptación de las velocidades con el protocolo ADR (Alternative Dispute Resolution).
- ✓ Gestión y autenticación de tramas.
- ✓ Descifrar mensajes desde nodos finales.

Figura 21. Red de dispositivos LoRaWAN

Servidores de aplicaciones

En los servidores de aplicación, se tienen procesos útiles **(Figura 22. Ruta de una red LoRaWAN)** como la recolección de datos de los dispositivos finales de la red. Los servidores comúnmente se ejecutan en la nube de forma privada o pública.

Las responsabilidades del servidor de aplicaciones son: Manipular, gestionar e interpretar los datos de las aplicaciones de los dispositivos finales, desde seguridad para el manejo de datos y generar enlaces descendentes de la capa de aplicaciones a los dispositivos finales de la red. La conexión de los servidores es en la nube y puede existir más de un servidor en la red. [12]

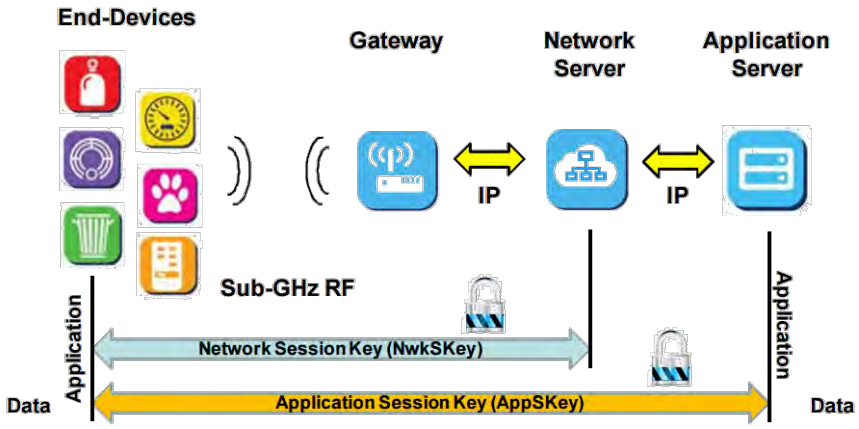

Figura 22. Ruta de una red LoRaWAN

Servidor de unión

El servidor de unión (join server) se encarga de administrar el proceso para añadir dispositivos en las redes LoRaWAN, conteniendo la información del procesamiento de las solicitudes de enlaces tipo ascendente, con la espera de la generación de tramas de aceptación de unión de forma descendente. El servidor de unión envía una acción al servidor de red, para saber cuál servidor de aplicaciones se conectará al dispositivo final y así se realizan las derivaciones del cifrado de la sesión. Al final la clave de sesión se comunica del dispositivo al servidor de red y la clave de la aplicación al servidor de aplicaciones.

- ✓ Clave de cifrado de aplicación (AppKey).
- ✓ Identificador del servidor de aplicaciones.
- ✓ Identificador único de serie del dispositivo final (DevEUI).
- ✓ Perfil de servicio del dispositivo final.
- ✓ Clave de cifrado de red (NwkKey).

3.3.4 Estructura de paquetes LoRa/LoRaWAN

En las redes LoRaWAN se utilizan dos tipos de mensajes que involucran la composición de los paquetes: Uplink y Downlink:

- ✓ **Uplink (Ascendente):** Los mensajes Uplink conocidos como enlaces ascendentes son los que se envían a partir de los dispositivos finales de la red, siguiendo la arquitectura de LoRaWAN con la utilización de uno o más Gateway en su camino. Este tipo de mensajes utilizan un modo explícito de radio con el encabezado LoRa, en el que la integridad de la carga se encuentra protegida por CRC. [3]

Preamble	PHDR	PHDR CRC	PHYPayload	CRC

Tabla 2. Mensajes Uplink

- ✓ **Downlink (Descendente):** Los mensajes Downlink conocidos como enlace descendente es el inverso de los Uplink debido a que los mensajes se mandan desde el servidor de red, siguiendo la arquitectura de la red LoRaWAN hasta llegar al dispositivo final pasando únicamente por un Gateway. Este tipo de mensajes utilizan el modo explícito con el encabezado LoRa y no cuenta con CRC. [3]

Preamble	PHDR	PHDR CRC	PHYPayload

Tabla 3. Mensajes Downlink

Capa física

En la trama de la capa física o PHY como se le conoce en inglés, se tiene la siguiente estructura:

- ✓ **Preamble:** Se empieza por el preámbulo con un tiempo estimado de 12,25Ts; que se encarga de definir el esquema de modulación del paquete, modulando con el mismo valor de ensanchamiento que el resto.
- ✓ **Header:** El Header que se conforma con el encabezado PHY y CRC. Cuenta con un valor total de 20 bits de tamaño, con una codificación más confiable que el resto del código que va con la tasa del encabezado.

- ✓ **Payload:** La trama de la capa física también contiene información de la longitud de Payload o carga útil **(Ver Tabla 6. Trama de la capa MAC)** que contiene la trama MAC.
- ✓ **Payload CRC:** La trama contiene carga útil CRC con una longitud de 16 bits que en una red LoRa con un mensaje de tipo ascendente, podemos encontrar esta parte de la estructura.

Preamble	Header + Header CRC (20 bits)	PHY Payload P bytes	Payload CRC 16 bits

Tabla 4. Trama capa física

Capa MAC

- ✓ **MAC Header:** El encabezado (Header) en la capa MAC, es el encargado de definir el tipo de mensaje (MType) y la versión del protocolo con la que se realizó la codificación. Esto para verificar la trama de datos o gestión y la forma del enlace que puede ser ascendente o descendente dependiendo su origen. En una red LoRaWAN podemos encontrar los siguientes tipos de MType:

MType	Descripción
000	Join Request
001	Join Accept
010	Unconfirmed Data Up
011	Unconfirmed Data Down
100	Confirmed Data Up
101	Confirmed Data Down
110	RFU
111	Proprietary

Tabla 5. Tipos de mensajes (MType)

- ✓ **MAC Payload:** La carga útil (MAC Payload) tiene la siguiente estructura: Encabezado (FHDR), Puerto opcional (FPort) y la carga útil de trama opcional (FRMPayload) **(Ver Tabla 7. Trama del Frame Header).** [3]
- ✓ **MIC:** El código de integridad del mensaje (MIC), se calcula en todos los campos del mensaje para obtener su valor, con una clave de sesión de red (App Session Key) para evitar falsificaciones y autenticar nodos.

MAC Header	MAC Payload	MIC
1 byte	M bytes	4 bytes

Tabla 6. Trama de la capa MAC

Capa de Aplicación

✓ **Frame Header:** El Frame Header cuenta con: Dirección del dispositivo (Device Address) de 4 bytes, Control de trama (Frame Control) de 1 byte, Contador de trama (Frame Counter) de 2 bytes y Opciones de trama (Frame Options) de hasta 15 bytes para transportar comandos MAC. [3]

Device Address	Frame Control	Frame Counter	Frame Options
4 bytes	1 byte	2 bytes	0… 15 bytes

Tabla 7. Trama del Frame Header

- **Device Address:** La dirección del dispositivo está conformada por los primeros 8 bits de identificación de la red y los otros bits son asignados de forma dinámica en la conexión de la red para identificar dispositivos.
- **Frame Control:** El Control de trama se encarga de la información del control de la red como las puertas de enlace, velocidad de datos, entre otra información.
- **Frame Counter:** Contador para números secuenciales.
- **Frame Options:** Las opciones de trama son utilizados con una longitud de hasta 15 bytes para la potencia de las transmisiones, transmisión de datos, etc.

✓ **Frame Port:** El puerto de trama es utilizado para indicar si la parte del Frame Payload tiene comandos MAC.

✓ **Frame Payload**: La trama de carga útil se encuentra encriptada antes del cálculo del MIC con un cifrado AES con longitud de 128 bits. [3]

Frame Header	Frame Port	Frame Payload
7 – 22 byte	1 bytes	N bytes

Tabla 8. Trama de la capa de aplicación

Finalmente, la estructura de los paquetes LoRa/LoRaWAN queda de la siguiente manera **(Figura 23. Estructura de paquetes LoRa)** referente a todas las capas de las estructuras explicadas anteriormente:

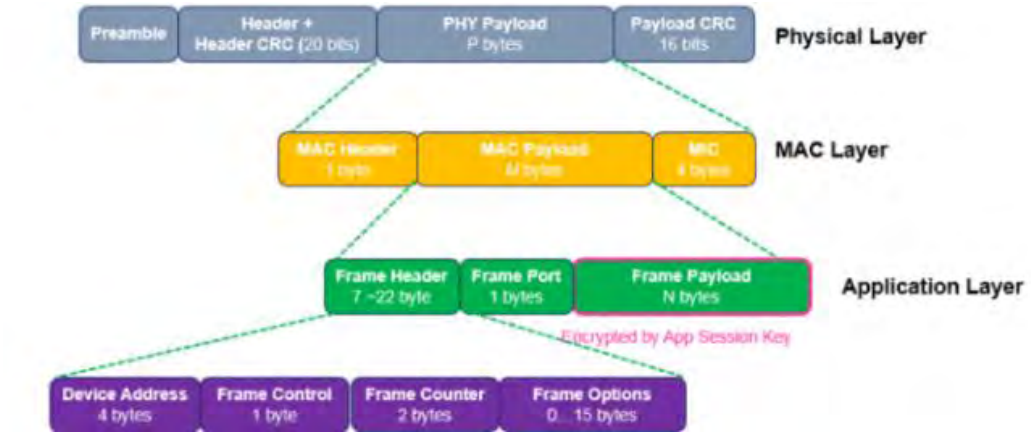

Figura 23. Estructura de paquetes LoRa

3.4 Esquemas de seguridad en redes IoT/LoRaWAN

3.4.1 Seguridad

El manejo de la seguridad en una red IoT como LoRaWAN se refiere a varios elementos que la conforman desde el inicio de la red como los errores humanos. Comúnmente se habla de seguridad como: Cifrados, control de accesos, entre otros métodos de seguridad. La seguridad se puede abordar con tres puntos fundamentales como los siguientes:

- ✓ **Red:** La seguridad de la red IoT es uno de los puntos fundamentales para su seguridad y control. Con un funcionamiento de forma remota, los dispositivos finales son un atractivo para los ataques dirigidos a los mismos y así intervenir en la información e ingresar a uno de los dispositivos de la red, con la consideración de que la seguridad tiene que ser tanto para los elementos físicos como los digitales. [13] Para su protección completa es necesario conocer cada parte de los elementos existentes en la red y sus funciones para asignar la seguridad correspondiente en cada caso, asegurando un control total de toda la red si se encuentra comprometida y responder de forma inmediata utilizando las herramientas de seguridad disponibles de acuerdo con la red y los servicios adicionales contratados.

- ✓ **Configuración:** Las configuraciones de los dispositivos de la red IoT cuentan con características y funcionalidades diferentes unos de otros que aportan a la seguridad de la red. La mayoría de los usuarios no cuentan con un conocimiento acerca de las configuraciones de los dispositivos y se puede volver una vulnerabilidad, si por algún error se cambia la configuración por defecto de los dispositivos. Es recomendable que antes de acceder a un entorno de red, conocer los dispositivos y evitar modificaciones que pueden tener un efecto en el filtrado de la información.
- ✓ **Usuarios:** En una red IoT como LoRaWAN se puede tener todo tipo de seguridad e implementaciones para asegurar la integridad de la red, además de que los usuarios tienen un papel fundamental que es la interacción con los dispositivos de este entorno. Gran parte de las filtraciones de información y vulnerabilidades, se generan por la mala interacción con la red debido a los conocidos errores humanos por carecer de conocimiento en el manejo de los dispositivos. En todo momento es recomendable tener conocimiento de lo que se realiza y el manejo responsable de todos los accesos del entorno, aportando a la seguridad de la red.

3.4.2 Privacidad

La privacidad en el entorno de las redes IoT tiene importancia, no solo para la utilización de estas redes que es la razón principal, si no de igual forma se requiere una atención y consideración especial para proteger la información de los usuarios que interactúen en estos entornos. A pesar de que cuentan con identificadores únicos y las comunicaciones de forma autónoma, los datos transmitidos por los puntos determinados de la red deben ser asegurados para evitar problemas con la privacidad. La múltiple cantidad de dispositivos y objetos que pueden existir en una red de pequeña y gran escala, tienen una transferencia de datos grande que es características de internet de las cosas. Los productos o dispositivos para estas redes no están principalmente diseñados para una seguridad alta y como consecuencia los dispositivos que se les denominan cotidianos son hasta cierto punto vulnerables. [13]

La mayoría de los usuarios no tienen interés en las políticas de privacidad de los dispositivos y entornos a los que acceden, creando un desconocimiento en el manejo de su información y como consecuencia los usuarios que no conocen la mayor parte de sus acciones.

Los usuarios de estas tecnologías se encuentran de forma gradual expuestos sin saber dónde se recopila su información y como es utilizada por terceros.

3.4.3 Vulnerabilidades

LoRaWAN está desarrollado con una serie de puntos de seguridad en distintas áreas de su estructura de red para protegerla de terceros, además de la seguridad cuando opera en conjunto con la nube. [14] A continuación, se presentan distintas vulnerabilidades de una red LoRaWAN:

- ✓ La generación de las claves de sesión y sus ciclos de vida son un problema importante debido a su almacenamiento en los dispositivos.
- ✓ En el cifrado de los mensajes se encuentra la misma longitud.
- ✓ El método de activación por personalización (ABP) maneja las mismas claves de sesión NwkSKey y AppSKey.

3.5 Tipos de ataques a redes LoRaWAN

3.5.1 Bit-Flipping

En la integridad de los mensajes LoRaWAN, podemos encontrar la protección del código de integridad del mensaje (MIC), el cual se encarga de evitar que la información sea manipulada de cualquier forma. Este proceso va desde los dispositivos hasta el servidor de aplicación, pasando por el servidor de red que es donde los mensajes son descifrados **(Figura 24. Cambio de bits)** para después enviarlos al servidor de aplicaciones generando un ataque potencial. [15]

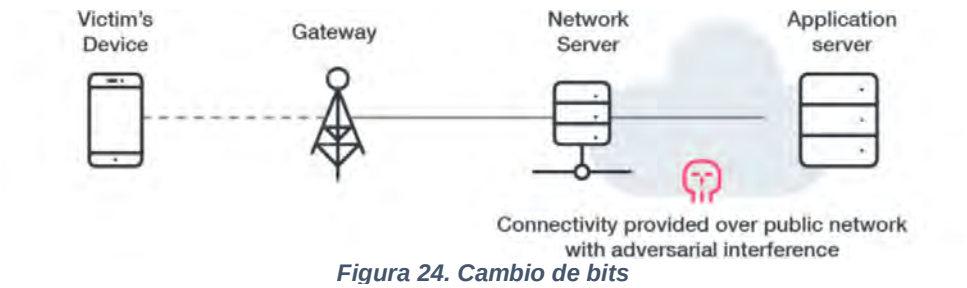

Figura 24. Cambio de bits

3.5.2 DoS en modo de activación ABP

Uno de los tipos de ataque a las redes LoRaWAN registrados, es por medio de denegación de servicios (DoS). Tomando en cuenta el FRMPayload con una longitud de 16 bits, se puede reproducir con un paquete capturado **(Figura 25. Denegación de servicios ABP)** hasta que el contador se desborde. Todo esto bajo las investigaciones realizadas en países bajos en el 2018. [15]

Este ataque es realizado debido a las claves de sesión que no cambian por el método APB, que suele ser el más vulnerable a un ataque en comparación a OTAA que en cada inicio de sesión, genera claves nuevas.

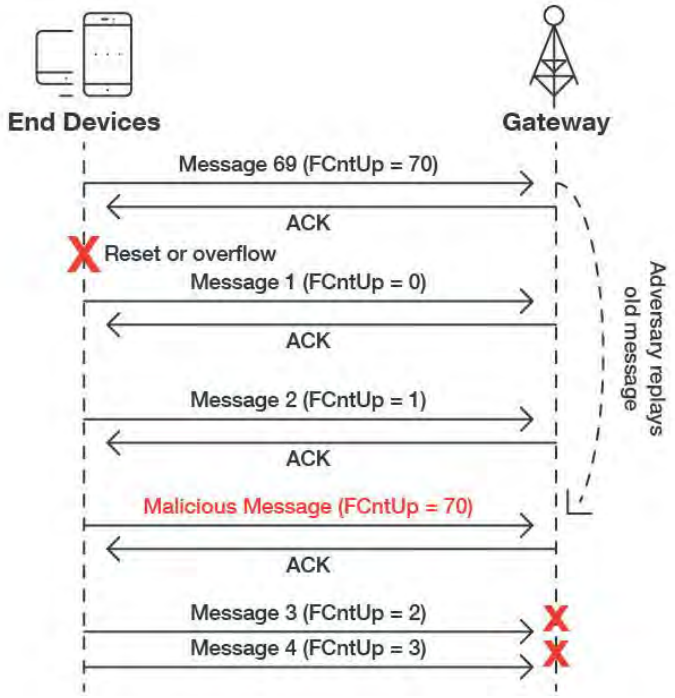

Figura 25. Denegación de servicios ABP

Gestión de claves raíz

En los dispositivos con el método de activación por aire (OTAA), es donde se utilizan las claves raíz y esto sucede cuando se generan las claves de sesión al ejecutarse la unión a la red LoRaWAN. [15]

Estas claves se encuentran potencialmente amenazadas por la exposición que tiene el backend a la red internet, en donde un tercero evalúa las posibles vulnerabilidades para crear paquetes, claves, lectura de información y hasta suplantación de identidad.

LoRaWAN

La seguridad en las redes IoT son parte fundamental de la elección por los elementos de seguridad que son la mayor influencia, para elegir entre una de las tecnologías disponibles en el mercado. En LoRaWAN se puede definir como dos capas correspondientes a su seguridad: La primera capa es a nivel de red y la otra a nivel de la capa aplicación, las cuales son importantes diferenciar como primera instancia. [13] Para la seguridad en la capa de red se aseguran y autentican los dispositivos o nodos de la red para otorgar un ambiente íntegro de acuerdo con la estructura de la red que va desde los dispositivos hasta el servidor de red. Por otro lado, la capa de aplicación es la encargada de verificar y garantizar la confidencialidad con ayuda de los cifrados (cifrado extremo a extremo), utilizados entre dispositivos además del servidor de red evitando vulnerabilidades que permiten la entrada a terceros en la red.

Llaves de seguridad

Las llaves de seguridad **(Tabla 9. Claves de sesión LoRaWAN.)** son la protección que utiliza LoRaWAN junto con el cifrado para proteger la información, con una serie de claves de longitud de 128 bits con el algoritmo de cifrado AES128 (Advanced Encryption Standard) para contener y proteger los datos que se transmiten en la red. [12]

Clave	Uso
Network Session Key (NwkSKey)	Clave de seguridad para la capa de red.
Application Session Key (AppSKey)	Clave de seguridad para la capa de aplicación
Application Key (AppKey)	Clave de seguridad para la capa de aplicación con activación por (OTTA)

Tabla 9. Claves de sesión LoRaWAN.

Claves de sesión

Después de conocer las llaves de seguridad **(Figura 26. Claves de sesión LoRaWAN)**, las tres claves antes mencionadas: NwkSKey, AppSKey y AppKey. Las claves tienen su función de generación ya que estas vienen desde una activación de un dispositivo a la red durante su sesión y ahí es donde se genera la AppSKey y la NwkSKey. Para la sesión de aplicación (AppSKey) se mantiene de forma privada y la NwkSKey se comparte con toda la red. [12]

- ✓ **Clave de sesión de red (NwkSKey):** La utilidad de NwkSKey son las validaciones de la integridad de los mensajes, que transitan debido al código MIC (Código de integración del mensaje) y es utilizada para la interacción existente en una red que va desde el nodo hasta el servidor de red.
- ✓ **Clave de sesión de aplicación (AppSKey**): La utilidad de la AppSKey está orientada a la carga útil de la red que va desde el nodo hasta el servidor de aplicación con el objetivo de cifrar y descifrar la carga útil, dando integridad a la carga para evitar que sea leída por terceros. [15]
- ✓ **Clave de aplicación (AppKey):** Esta última clave AppKey, es utilizada en la activación por aire (OTAA) donde solo el dispositivo y la aplicación conocen. Esta clave se utiliza para diferenciar de las claves anteriores mediante su proceso de activación.

Las claves mencionadas son únicas por sesión dependiendo el tipo de activación de dispositivo (OTAA y ABP). La activación de un dispositivo mediante la activación por aire (OTAA), causa la generación de la clave por activación mientras que en la activación por personalización (ABP) mantiene de forma estática la clave.

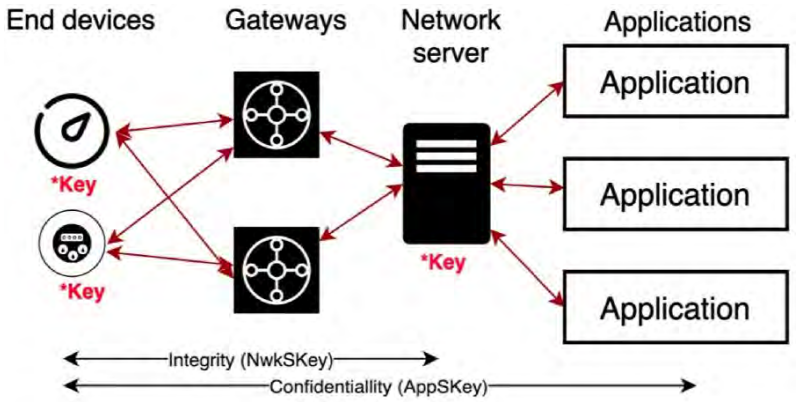

Figura 26. Claves de sesión LoRaWAN

3.5.3 Métodos de activación LoRaWAN

Los métodos de activación de dispositivos cuentan sus respectivas claves dependiendo el método y el identificador. Los métodos de activación existentes son: OTAA y ABP. Gracias a estos métodos antes mencionados, las claves y el identificador, se puede tener una red con un entorno integro.

Activación por aire (OTAA)

El método activación OTAA, **(Figura 27 Método de activación OTAA)** es uno de los métodos para conectarse a una red LoRaWAN de forma segura, con configuraciones de seguridad para resguardar la integridad de los dispositivos y la red. [16]

OTAA se encuentra compuesto de la siguiente manera:

- ✓ **Identificador de fabrica (DevEUI):** Es un identificador de fábrica único que se utiliza para diferenciar a los dispositivos con una semejanza a una dirección MAC en las computadoras, con una longitud de 64 bits.
- ✓ **Identificador de aplicación único (AppEUI):** Es un identificador que se utiliza para formar grupos de objetos o dispositivos, clasificándolos con una longitud de 64 bits.

También se maneja la clave de aplicación (AppKey) AES de 128 bits, que es compartida entre el dispositivo y la red para determinar las claves de la sesión de la red. Las características y el método de inicio de sesión en el aire generan más seguridad en cada inicio de sesión de un dispositivo por la generación de nuevas claves, correspondiente a una nueva conexión. [16]

1) Mensaje de solicitud de unión.
2) Autenticación y generación de claves de sesión.
3) Mensaje de aceptación.
4) Transferencia de AppSKey.
5) Generación de clave de sesión.

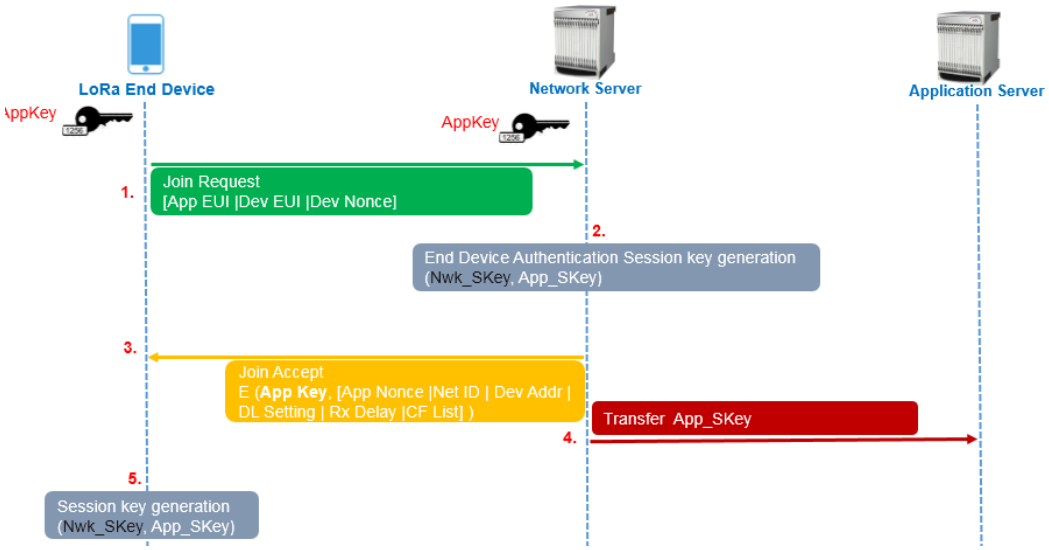

Figura 27 Método de activación OTAA

Activación por personalización (ABP)

El método activación por personalización **(Figura 28. Método de activación ABP),** forma parte de los métodos para conectarse a una red LoRaWAN enviando las claves de sesión (AppSKey y NwkSKey) que son componentes clave de los nodos, además de la dirección lógica (DevAddress). ABP cuenta con características diferentes al método de activación OTAA para resolver las conexiones de los dispositivos (nodos) y la red. [16]

ABP está compuesto con las siguientes características:

- ✓ **Dirección lógica (DevAddress):** DevAddress es la dirección del dispositivo con longitud de 32 bits y una semejanza a una dirección IP de un dispositivo de red, utilizada para la comunicación con la red.
- ✓ **Clave de sesión de red (NwkSKey):** La utilidad de la NwkSKey es para validaciones de la integridad de los mensajes que transitan, debido a su código MIC (Código de integridad del mensaje) y es utilizada para la interacción en la red desde el nodo hasta el servidor de red.
- ✓ **Clave de sesión de aplicación (AppSKey):** La AppSKey está orientada a la carga útil de la red que va desde el nodo, otorgando integridad a la carga para evitar su lectura por terceros.

Es el método de activación menos seguro para un dispositivo, con una vulnerabilidad respecto a su llave y una posible clonación de este si se extrae. Un tercero puede contar con la posibilidad extraer información, pero este método es efectivo para los dispositivos que se encuentran en movimiento constante, por no requerir un inicio de sesión nuevo en la red. [16]

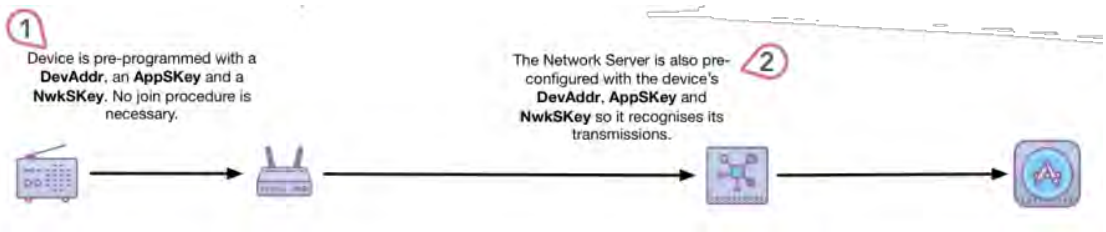

Figura 28. Método de activación ABP

1) Envío de datos al Gateway.
2) Validación de datos para el inicio de sesión.
3) Si la sesión es correcta, procede el inicio de sesión.

3.6 Integridad de IoT en la nube

Con la aparición de internet de las cosas, han surgido nuevas formas de interacción en los entornos domésticos y de trabajo con una variedad amplia de conexiones remotas y distanciamiento social. La composición de las redes IoT y la nube, abarcan una amplia variedad de aplicaciones **(Figura 29. Seguridad IoT - Cloud)** a bajo costo con una comodidad o control de acuerdo con las preferencias de los usuarios, respecto a las empresas que proporcionan estas tecnologías.

Figura 29. Seguridad IoT - Cloud

Cuando se menciona IoT y la nube, podemos decir que nos encontramos en una nueva frontera en cómo funcionan las empresas en su administración, por lo que es importante la seguridad y como referencia las posibles vulnerabilidades o riesgos, cuando estas tecnologías trabajan en conjunto. [7]

Para mencionar la integridad de las IoT en la nube, es necesario conocer el funcionamiento en conjunto. IoT tiene la capacidad de funcionar de distintas formas de acuerdo con las necesidades del usuario, para mejorar su ambiente y cumplir con las necesidades mientras que la nube es la herramienta que nos permite acceder a datos, herramientas y almacenar datos a través de internet. Con estas características, no existen limitaciones en la infraestructura debido a que sería un remplazo de servidores físicos entre otros dispositivos para redes y con esto lograr que los dispositivos físicos de una red IoT se conecten.

3.6.1 Características de IoT – Cloud:

- ✓ **Soporte:** Las diferentes empresas que existen actualmente ofrecen además de sus servicios de Cloud, esquemas de seguridad para la protección de datos y la buena administración. Estos sistemas de seguridad son diferentes unos de otros al igual que los servicios que ofrecen.
- ✓ **Procesamiento:** Los dispositivos y las aplicaciones tienen un sistema de procesamiento limitado para algunas de sus funciones principales y con la nube, la capacidad aumenta de forma virtual con la diferencia de cada tipo de servicio en la nube adquirido.
- ✓ **Mantenimiento remoto:** Con la integración de la nube a las redes IoT se realiza mejor soporte y mantenimiento por parte de los ingenieros y técnicos de forma remota.
- ✓ **Almacenamiento:** Esta es una de las características principales de las redes IoT por el manejo de grandes cantidades de datos, que provienen de distintos dispositivos finales de la red y con la nube un almacenamiento ilimitado para su análisis.

La seguridad de IoT y Cloud, no solo corresponde a los cifrados de la información y las contraseñas. Existen muchos factores que la componen empezando por el manejo de la información por parte de los usuarios que interactúan a diario con estas tecnologías. [7] Es de suma importancia saber los procesos que se realizan para tener un mejor manejo y control de los datos, además de aprender principios básicos como las contraseñas seguras. Con la

constante interacción a la red internet, se tienen muchas vulnerabilidades que son aprovechadas por ciber-delincuentes informáticos debido a un manejo inexistente en el seguimiento en los dispositivos, por este motivo es importante tener una red actualizada y con métodos de seguridad actualizados para evitar terceros en las redes y el robo de datos que se genera por tener sistemas o software obsoleto.

Diferentes empresas se encargan de proporcionar herramientas en la nube para redes IoT con diferentes protocolos y cifrados punto a punto fundamentales, con el fin de tener protocolos para todo tipo de situaciones de riesgo. Estas empresas se encargan de certificar y dar claves privadas a los usuarios para mejorar la operabilidad y sean más confiables.

3.6.2 Desafíos de seguridad

La unión de estas dos tecnologías presenta diferentes áreas de seguridad que son parte del complemento de la nube, pero de igual forma no termina de ser suficiente al tener varias brechas de seguridad que pueden ser consideradas debilidades para un entorno de red. [17]

Estas brechas se vuelven desafíos de seguridad como los siguientes:

- ✓ **Privacidad:** El tráfico de datos de los dispositivos finales en las redes IoT son confidenciales además de la seguridad que complementa con la nube. El manejo de esta información debe ser de alta prioridad para dirigirla a un lugar seguro con el soporte del proveedor de servicios.
- ✓ **Configuración inadecuada de la nube:** Una de las problemáticas que no se le da la importancia debida, es la correcta configuración de los componentes de la red. Una mala configuración puede causar posibles ataques o filtraciones en los datos para acceder a la nube e invadir el entorno seguro.
- ✓ **Centralización de la entrada en la infraestructura:** IoT y la nube en conjunto, cambia la estructura de la red por lo que el tráfico ascendente y descendente se concentra en una sola puerta de enlace en la nube. Esto significa que la puerta de enlace es la zona potencial a un ataque y de igual manera se reducen las posibilidades de un ataque en otra sección de la red por la atención dirigida. La opción más viable para este tipo de casos es un firewall de alta gama con las capacidades suficientes para solventar el problema antes mencionado.

- ✓ **Flujo de datos:** En las redes IoT el flujo de datos es de suma importancia para la comunicación segura. Si la seguridad que va desde los puntos finales o desde la nube no es la correcta, se tiene un riesgo muy grande en los controles de acceso que deriva hasta la integridad de los datos, por la falta de una autenticación adecuada y un cifrado de alto nivel para su protección.

3.6.3 Prácticas para garantizar la seguridad IoT – Cloud

Cifrado de datos en reposo

El cifrado es un método fundamental para garantizar la integridad en la nube mediante el proceso donde los datos pasan de un formato completamente legible, a una salida en texto completamente cifrado mediante un algoritmo para la conversión, sin la posibilidad de visualizar los datos debido a este proceso, aunque se tenga acceso a los dispositivos de la red. [17]

En datos con estado de reposo, el algoritmo de cifrado se utiliza para otorgar protección a los dispositivos que almacenan datos como unidades de estado sólido, mediante un principio de protección en capas donde ambas partes tanto dispositivos como la información se encuentren cifrados.

Cifrado de datos en tránsito

Los datos en tránsito son más vulnerables que los datos en reposo por el constante tráfico que existe en las redes. El objetivo principal es que estos datos lleguen a su destino sin ser intervenidos por terceros, aun con comunicaciones a través de internet con un método como el extremo a extremo. [17] Para estos casos se tienen conexiones cifradas como es el caso de HTTPS, SSL y TLS que son habilitados antes de su tránsito.

Identidad del dispositivo

En una red IoT es importante una identificación para cada parte de la estructura de la red, principalmente los dispositivos finales con una identidad única para su control en los inicios de sesión para autenticar y verificar que la comunicación sea segura.

Sistema de roles y políticas de usuario

Para el manejo de un entorno seguro se crean los roles, para gestionar el acceso de los usuarios con privilegios a una autenticación para que tener acceso a los datos de la red IoT. Las políticas son las que definen hasta qué punto son otorgados los permisos en base a un administrador.

Autenticación de dispositivos

Existen estándares para la autenticación de dispositivos con el objetivo de proteger el entorno de la red, como es el caso del estándar abierto OAuth 2.0 que tiene la función de la autenticación mediante tokens.

3.7. Proveedores de servicios Cloud para IoT

En la actualidad es posible encontrar una amplia gama de proveedores de Cloud en internet, cada uno con diferencias respecto a sus servicios de los distintos proveedores del mercado. El servicio de Cloud incluye la característica de almacenar y alojar los servicios empresariales o domésticos, sino también las herramientas que son otro factor importante de estos servicios para el soporte y buen funcionamiento del entorno dependiendo las necesidades del usuario. Los siguientes son los proveedores más populares del mercado con características atractivas, eficiencia de alto nivel y con sistemas de seguridad de alta fiabilidad.

3.7.1 Amazon Web Services (AWS)

Este servicio es el más popular del mercado y es propiedad de Amazon que parte de un servicio en la nube que forma una plataforma **(Figura 30 Servicios de AWS),** para manejo en la nube con acceso desde cualquier punto con conexión a internet respaldado por Amazon. Este servicio es utilizado por distintas empresas conocidas que lo posicionan en lo más alto a comparación de su competencia más directa que es Google Cloud y Azure. [18] Amazon maneja 5 puntos fundamentales para asegurar la integridad del entorno de sus usuarios en las distintas ramas y escenarios en los que se pueden ver afectados.

Protección de datos

La protección de datos para AWS está bajo un cifrado y administración de las llaves de acceso mediante detecciones de amenazas posibles, así como el monitoreo de las distintas cuentas de usuario para evitar alguna filtración en el entorno. Servicios de Amazon Web Services para protección de datos:

Casos de uso	Servicios de AWS
Descubrir y proteger datos confidenciales	Amazon Macie
Administración y almacenamiento clave	AWS Key Management Service (KMS)
Almacenamiento de claves en hardware a efectos de conformidad normativa	AWS CloudHSM
Aprovisionamiento, administración e implementación de certificados públicos y privados SSL/TLS	AWS Certificate Manager
Alternar, administrar y recuperar datos confidenciales	AWS Secrets Manager

Tabla 10. Protección de datos AWS

Gestión de identidad y acceso

AWS tiene la capacidad de la administración de las identidades y los permisos, mejorando la integridad del entorno con AWS Identity. [18] Los servicios de gestión están orientados a los clientes para mejorar y agilizar la carga de trabajo. Servicios de Amazon Web Services para gestión de identidad y acceso:

Casos de uso	Servicio AWS
Administrar de manera segura el acceso a los servicios y los recursos	AWS Identity & Access Management (IAM)
Servicio de inicio de sesión único (SSO) en la nube	Inicio de sesión único de AWS
Administración de identidades para las aplicaciones	Aprendizaje de Amazon

Tabla 11. Gestión de identidad y acceso

Protección de red y aplicación

La protección de la red y las aplicaciones de AWS para servicios IoT, ayudan al filtrado de la red y al análisis para la verificación de los servicios autorizados y aplicar los recursos a cada nivel. Servicios de Amazon Web Services para protección de red y aplicación:

Casos de uso	Servicios AWS
Seguridad de la red	AWS Network Firewall
Protección frente a ataques DDoS	AWS Shield
Filtrar el tráfico web malintencionado	AWS Web Application Firewall (WAF)
Administración de reglas de Firewall	AWS Firewall Manager

Tabla 12. Protección de red y aplicación AWS

Detección de amenazas y monitoreo continuo

AWS tiene la capacidad de monitorear de forma continua para detectar posibles amenazas de la red, así como los comportamientos de los usuarios en el entorno de la nube. [18] Servicios de Amazon Web Services para detección de amenazas y monitoreo continuo:

Casos de uso	Servicios de AWS
Centro unificado de seguridad y conformidad	AWS Security Hub
Servicio administrado de detección de amenazas	Amazon GuardDuty
Analizar la seguridad de las aplicaciones	Amazon Inspector
Registrar y evaluar las configuraciones de los recursos de AWS	AWS Config
Realizar un seguimiento de la actividad de los usuarios y el uso de las API	AWS CloudTrail
Administración de la seguridad para dispositivos compatibles con IoT	AWS IoT Device Defender

Tabla 13. Detección de amenazas y monitoreo AWS

Conformidad y privacidad de datos

AWS se encarga de ofrecer a los usuarios una vista previa de la integridad de la nube de forma continua y monitorizada de forma automática, para los estándares ya establecidos de la privacidad de los datos. Servicios de Amazon Web Services para conformidad y privacidad de datos:

Casos de uso	Servicios de AWS
Portal de autoservicio para el acceso bajo demanda a los informes de AWS	AWS Artifact
Auditorías del uso de AWS de forma continua para simplificar la forma en que evalúa el riesgo y la conformidad	AWS Audit Manager

Tabla 14.Conformidad y privacidad de datos AWS

Figura 30 Servicios de AWS

3.7.2 Google Cloud

Google Cloud es el servicio de la nube por parte de Google que se encarga de reunir todas sus aplicaciones para ofrecer soluciones en un entorno seguro. Esta plataforma es utilizada para dar soluciones de infraestructura en las empresas y hogares, con la capacidad de almacenar información y brindar una mayor escalabilidad por parte de las aplicaciones de uso

Google Cloud maneja una plataforma **(Figura 31. Google Cloud-IoT Core)** que se utiliza como espacio en la red para realizar actividades que antes requerían una infraestructura física. Con Google Cloud, la gestión de tareas, datos y los accesos cuentan un mejor control y se realizan en un entorno integro. [19]

Como en todas las aplicaciones y servicios de Google, en su plataforma se tiene una amplia variedad de herramientas que atribuyen al funcionamiento de su plataforma. Las características más destacadas de Google Cloud son las siguientes:

Procesamiento de archivos: Para procesamiento de archivos en tiempo real, Google maneja diferentes características que parten de Google Functions que se utiliza para procesar todo tipo de archivos como pueden ser imágenes, videos y datos, dependiendo el uso con capacidades de filtrado entre otros. Se utilizan para responder a los eventos las siguientes herramientas: [19]

Caso de uso	Servicio Google Cloud
Procesamiento de archivos	Cloud Storage
	Pub/Sub
	Cloud Firestore

Tabla 15. Procesamiento de archivos Google Cloud

Procesamiento de transmisión: El procesamiento de transmisión en tiempo real con Cloud Functions, tiene como objetivo el procesamiento de los datos de transmisión cómo pueden ser las transacciones o la telemetría de los dispositivos IoT, así como otras aplicaciones. [19] Se utilizan para responder a los eventos las siguientes herramientas:

Caso de uso	Servicio Google Cloud
Procesamiento de transmisión	Pub/Sub

Tabla 16. Procesamiento de transmisión Google Cloud

Backends de IoT sin servidores: Otra característica del uso de Cloud Functions es Backends de IoT para el procesamiento y análisis de datos en los dispositivos de una red IoT. [19] Se utilizan para responder a los eventos las siguientes herramientas:

Caso de uso	Servicio Google Cloud
Backends de IoT	Cloud IoT Core

Tabla 17. Back-ends de IoT Google Cloud

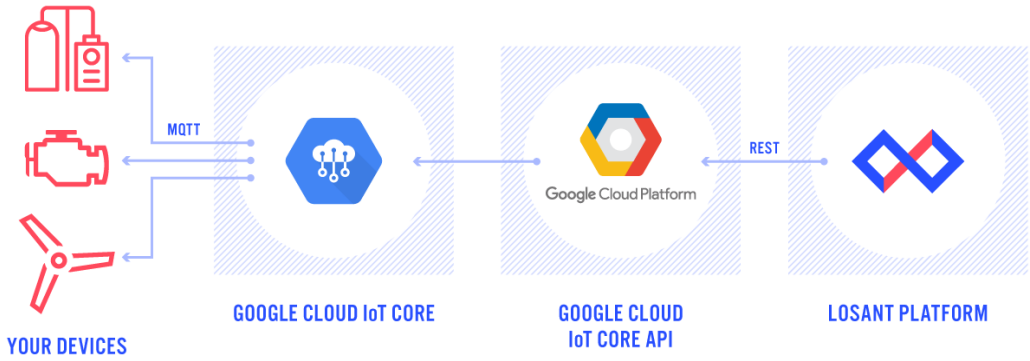

Figura 31. Google Cloud-IoT Core

3.7.3 Microsoft Azure

Azure es el nombre que se le otorgó al servicio de la nube parte de la empresa Microsoft, para entrar al mercado con un conjunto de servicios al igual que sus competidores en la actualidad. Azure **(Figura 32. Azure IoT tecnologías, servicios y soluciones)** tiene la capacidad de almacenar datos, crear y administrar los servicios de su entorno. Las capacidades de Azure dependen del pago de la licencia para la asignación de los servicios y las herramientas disponibles como todos los servicios de la nube actualmente, con diferencias en herramientas y la integridad del entorno. La Integridad de Azure cuenta con el soporte de Microsoft y su equipo de trabajo para una mayor confianza de los usuarios en la administración de sus espacios de trabajo y almacenamiento. En su enfoque hacia IoT, Azure tiene un énfasis en los servicios que se administran al igual que su plataforma en la red IoT y la nube. [20] Para contar con un buen enfoque hacia internet de las cosas con Azure IoT, se tienen los siguientes componentes:

- ✓ **Cosas:** Son los objetos físicos que se pueden encontrar en un entorno de trabajo, van desde los sensores en redes domesticas hasta los equipos industriales en fábricas que tienen una conexión a la nube intermitente o prolongada.
- ✓ **Perspectivas:** La perspectiva para Azure IoT es toda la información que se recopila de los diferentes dispositivos en un entorno IoT para su análisis y utilización.
- ✓ **Acciones:** Las acciones forman parte de la interacción que tienen los usuarios con los dispositivos, especialmente con los datos para realizar funciones con las herramientas disponibles.

La seguridad de Azure tiene un gran alcance en la interacción con los siguientes servicios y herramientas:

Protección de dispositivos: Para la protección de los dispositivos activos, no activos, administración, las vulnerabilidades y amenazas se realizan con la siguiente herramienta:

Casos de uso	Servicio Microsoft Azure
Protección de dispositivos	Azure Defender IoT

Tabla 18. Protección de dispositivos Microsoft Azure.

Reducción de riesgos: La reducción de los riesgos maneja un mejor estándar de seguridad y administración en este caso de una red IoT potencialmente vulnerable, con una postura de seguridad y reparación de vulnerabilidades con la siguiente herramienta:

Casos de uso	Servicio Microsoft Azure
Reducción de riesgos	Azure IoT Central

Tabla 19. Reducción de riesgos Microsoft Azure

Conexión de dispositivos: Para asegurar la conexión de los dispositivos, se debe determinar el tipo de software adecuado para la autorización de los dispositivos y las conexiones entre su entorno con la siguiente herramienta:

Casos de uso	Servicio Microsoft Azure
Conexión de dispositivos	Azure IoT Edge

Tabla 20. Conexión de dispositivos Microsoft Azure

Identidad y control de accesos: La administración y control de Microsoft Azure, ayuda con directorios de acceso para la protección de los usuarios con el siguiente servicio:

Casos de uso	Servicio Microsoft Azure
Administración de identidades y control de accesos	Azure Active Directory (AD)

Tabla 21. Identidades y controles de acceso Microsoft Azure

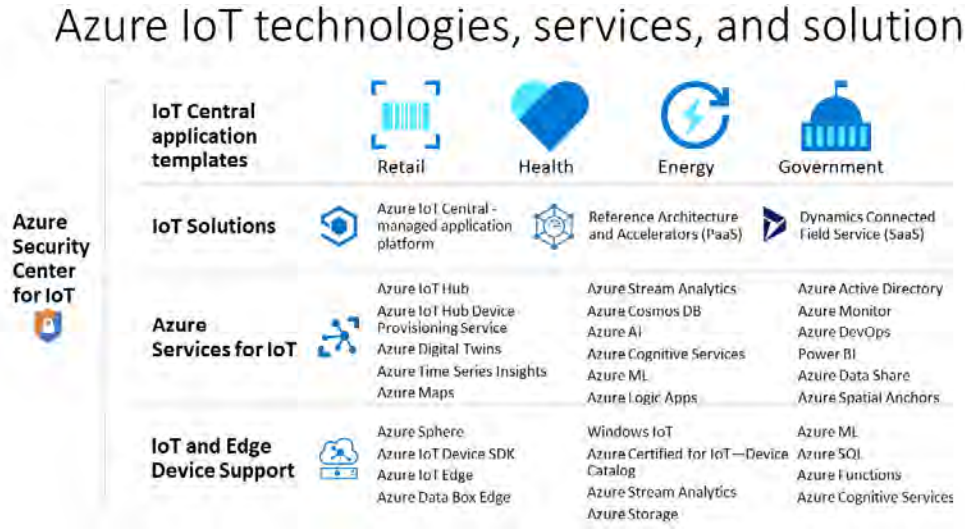

Figura 32. Azure IoT tecnologías, servicios y soluciones

Capítulo 4

Conclusiones

En el mundo actual, podemos observar la evolución de las comunicaciones en paralelo a los avances tecnológicos, para complementar la utilización de los dispositivos en entornos de trabajo o del hogar. Las redes IoT forman parte de las nuevas tecnologías y se perfilan para ser las más utilizadas en un futuro no muy lejano, tomando en cuenta que actualmente está generando popularidad por la capacidad de las múltiples aplicaciones y resoluciones de tareas. La mayor problemática en el entorno de las redes IoT es la seguridad, que involucra toda la arquitectura de la red, las configuraciones y la privacidad de los datos que se manejan en la red.

La seguridad en las redes IoT y específicamente LoRaWAN, cuentan con estándares para la implementación, esquemas, llaves y niveles de seguridad para la protección completa de estas redes. Analizando las características de la seguridad, se tiene conocimiento de que la seguridad en las redes IoT con todas sus características, no son el 100% seguras debido a que existen otros factores de suma importancia. Para tener un entorno seguro, es recomendable identificar y conocer el funcionamiento de la arquitectura de la red para la administración y la utilización de forma correcta.

Se reconocen tres puntos indispensables para aumentar la seguridad:

Errores humanos: La mayor parte de los errores se deben a errores humanos por falta de conocimiento en el funcionamiento de la red, lo que podría generar filtraciones a pesar de tener las configuraciones correspondientes.

Componentes de red: Es indispensable tener el conocimiento de los elementos de la red, para la asignación de la seguridad de cada caso en específico y obtener una respuesta inmediata en caso de riesgo.

Configuraciones adecuadas: La configuración de los dispositivos pueden variar dependiendo las características y el funcionamiento de cada dispositivo. Cuando la configuración no es la adecuada, los dispositivos son potencialmente vulnerables.

Es indispensable adaptarse a estas comunicaciones para tener un buen manejo de los datos personales que se ingresan en las redes IoT. Las configuraciones para cada dispositivo y las distintas llaves de seguridad que involucran los inicios de sesión, ayudan a la seguridad y privacidad de los datos, complementando la parte técnica de las configuraciones y la cultura del conocimiento del entorno mediante las recomendaciones de uso. Se cumplieron los objetivos de la investigación, conociendo los estándares actuales para las redes IoT y la importancia en los diferentes niveles de seguridad, así como la revisión y el estudio para proporcionar información desde el esquema de las tramas hasta las diferentes herramientas de seguridad como guía de uso.

Este trabajo me ayudó a adquirir conocimiento de la seguridad para redes y sistemas IoT, y más en específico, para LoRaWAN con la problemática que existe alrededor de todos los puntos clave abordados en el documento.

Referencias bibliográficas

[1] M. Gracia, «Deloitte,» 2021. [En línea]. Available: https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html.

[2] Sigfox, «Sigfox technical overview,» Labrège - Francia, 2006.

[3] LoRa Alliance, LoRaWAN 1.1 Specification, 2017.

[4] I-Scoop.eu, «I-Scoop,» 2019. [En línea]. Available: https://www.i-scoop.eu/internet-of-things-guide/lpwan/nb-iot-narrowband-iot/.

[5] avsystem, «avsystem,» 9 Junio 2020. [En línea]. Available: https://www.avsystem.com/blog/narrowband-iot/.

[6] LoRa-Developer.Semtech, «LoRa Developer portal,» 2018. [En línea]. Available: https://lora-developers.semtech.com/library/tech-papers-and-guides/lora-and-lorawan/.

[7] J. R. Vacca, «Cloud Computing Security,» 2016.

[8] N. McKenna, «Explaining the Relationship Between IoT, Big Data and Cloud Computing,» 5 Mayo 2021. [En línea]. Available: https://www.mckennaconsultants.com/relationship-between-iot-big-data-and-cloud-computing/.

[9] LoRa Alliance, Noviembre 2015. [En línea]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/what-is-lorawan.pdf.

[10] The things network, «What are LoRa LoRaWAN,» Octubre 20. [En línea]. Available: https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/.

[11] Semtech Corporation, LoRa FAQs, 2015.

[12] The things network, «The things network architecture,» 20. [En línea]. Available: https://www.thethingsnetwork.org/docs/lorawan/architecture/.

[13] LoRa Alliance, «LoRaWAN Security,» 2020. [En línea]. Available: https://pages.services/pages.lora-alliance.org/lorawan-security/.

[14] SmartMakers, «Seguridad en aplicaciones LoRaWAN,» 6 Febrero 2018. [En línea]. Available: https://smartmakers.io/en/security-in-lorawan-applications/.

[15] Trend Micro, «Trend micro. Bajo consumo y alto riesgo: posibles ataques a dispositivos LoRaWAN: Bajo consumo y alto riesgo: posibles ataques a dispositivos LoRaWAN,»

2020. [En línea]. Available: https://www.trendmicro.com/en_us/research/21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html.

[16] «Protocolo LoRa,» de *Redes de computadores*, 2018.

[17] Tren Micro, Diciembre 2010. [En línea]. Available: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/a-security-guide-to-iot-cloud-convergence.

[18] Amazon, «Amazon Web Services,» 2020. [En línea]. Available: https://aws.amazon.com/es/products/security/?nc=sn&loc=2.

[19] Google, «Google IoT Core,» 2020. [En línea]. Available: https://cloud.google.com/iot-core?hl=es-419.

[20] Microsoft, «Azure IoT,» 2020. [En línea]. Available: https://azure.microsoft.com/en-gb/overview/iot/security/.

Anexos

Acrónimos

IoT	**Internet de las cosas (Internet of things)**
LoRa	**Larco alcance (Long Range)**
LoRaWAN	**Red de área amplia de largo alcance (Long Range Wide Area Network)**
M2M	**Máquina a máquina (Machine to machine)**
UNB	**Banda ultra estrecha (Ultra Narrow Band)**
GPS	**Sistema de posicionamiento global (Global Positioning System)**
AES	**Estándar de cifrado avanzado (Advanced Encryption Standart)**
LPWAN	**Rede de área amplia de baja potencia (Low Power Wide Area Network)**
EPC	**Evolved Packet Core**