UNIVERSIDAD EAN

FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS

PROYECTO DE GRADO - INTEGRACIÓN – PREGRADO
ESCUELA DE FORMACIÓN EN INVESTIGACIÓN

MODELO INFORMÁTICO APLICADO A LA CIBERSEGURIDAD DE DISPOSITIVOS IOT

AUTORES:

JAVIER ALEXANDER CAÑAR CUEVAS
LUCAS ALEJANDRO PATIÑO DORADO

TUTOR:
JULIEN GWENDAL CHENET

BOGOTÁ, 2021

TABLA DE CONTENIDO

LISTA DE TABLAS

TABLA DE ILUSTRACIONES

Resumen

El siguiente documento contiene un proyecto de investigación referente a un modelo informático que permite mitigar el riesgo de sufrir un ataque cibernético a través de dispositivos IoT. El problema de investigación surge a partir del bajo nivel ciberseguridad ofrecido por los dispositivos IoT, debido a que estos han sido atacados y vulnerados en innumerables ocasiones por parte de diversos delincuentes cibernéticos en búsqueda de su propio beneficio. Adicionalmente, en este documento encontrará el marco teórico necesario para comprender este proyecto, los objetivos propuestos y una solución moderna que permite dar respuesta a este inconveniente que ha tenido lugar en los últimos 15 años.

Palabras clave: Dispositivos IoT, ciberseguridad, vulnerabilidad, delincuentes.

1. PROBLEMA DE INVESTIGACIÓN

La implementación de dispositivos inteligentes en los hogares está ocasionando incertidumbre entre sus usuarios puesto que la seguridad que estos ofrecen con respecto a la privacidad de sus datos personales es cuestionable. Por ejemplo, en octubre del año 2019, la compañía Kaspersky, líder mundial en ciberseguridad para hogares, detectó más de 100 millones de ataques a dispositivos y aplicaciones conectadas a Internet de las Cosas, provenientes de 276.000 direcciones IP públicas en los primeros 6 meses del año. Si bien es cierto que las políticas de tratamiento de datos dependen del gobierno de cada país, son los proveedores de los dispositivos IoT los responsables de garantizar altos niveles de ciberseguridad para así transmitir seguridad a sus clientes (Kaspersky, 2019).

Un ciberdelincuente puede obtener información privada y muy valiosa de todos los dispositivos conectados a la red que utiliza el dispositivo IoT atacado, es decir que un ciberataque puede afectar a todos los individuos que naveguen en internet utilizando esta misma red. Según el Instituto Nacional de Ciberseguridad (INCIBE) de España, un ciberdelincuente puede robar información como direcciones de correo electrónico, perfiles de usuario, información confidencial, recursos del sistema e incluso credenciales o contraseñas, es decir que pueden duplicar tarjetas de crédito, suplantar la identidad de la víctima, extorsionar al individuo o simplemente vender la información en el mercado negro (INCIBE, 2015).

Las oportunidades financieras que trae la explotación de las vulnerabilidades de los dispositivos IoT es uno de los mayores atractivos para los ciberdelincuentes en la actualidad, lo cual causa preocupación en muchos de los usuarios de este tipo de dispositivos puesto que nadie quisiera ser víctima de un ciberataque y menos de uno en el que puedan sufrir pérdidas económicas. Sin embargo, esta no es la única consecuencia de implementar dispositivos IoT con bajos niveles de seguridad en los hogares, el espionaje también es una de ellas. Un delincuente informático podría utilizar dispositivos como un Amazon Echo Dot para espiar y así conocer las rutinas diarias de su víctima, lo cual resulta bastante incómodo para cualquiera (Kaspersky, 2019). Es por esto que surge la siguiente pregunta: ¿Cómo mitigar el riesgo de sufrir un ciberataque por medio de dispositivos IoT?

2. OBJETIVOS

2.1. Objetivo general

Definir un modelo informático que facilite la implementación de un sistema capaz de brindar seguridad a la información presente en la red de los dispositivos conectados mediante IoT para mitigar el riesgo de que una vulnerabilidad sea explotada.

2.2. Objetivos específicos

- Identificar posibles soluciones informáticas que permitan mitigar el riesgo de explotación de una vulnerabilidad en dispositivos IoT.
- Comparar las diferentes características y condiciones de las soluciones identificadas.
- Seleccionar la solución o las soluciones más adecuada para reducir los ciberataques a dispositivos IoT.
- Diseñar y modelar la solución informática seleccionada.

3. ANÁLISIS DE REQUERIMIENTOS O ESPECIFICACIONES TÉCNICAS

Este proyecto será desarrollado dentro del campo de la Ingeniería de sistemas y tendrá un enfoque cualitativo, por lo cual será necesario acceder a diferentes fuentes de información reconocidas y especializadas en las temáticas relacionadas con la problemática a solucionar. Algunas de estas fuentes serán: Google Academic, ACM Digital Library, Accessengineering, Science Direct, entre otras. Estas facilitarán la recopilación de información de diferentes estudios realizados previamente sobre la ciberseguridad en dispositivos IoT, adicionalmente se partirá de otras soluciones ya propuestas y se definirá la trascendencia que estas tengan en el proyecto.

Luego será necesario comparar las características y condiciones de las diferentes soluciones encontradas. Los principales factores a tener en cuenta serán la viabilidad, factibilidad y rentabilidad de la solución junto con el nivel de seguridad ofrecido a los dispositivos IoT y la facilidad de su implementación. Esto permitirá elegir la mejor alternativa para comenzar a profundizar en el uso de las tecnologías asociadas a la solución informática seleccionada.

Una vez seleccionada la mejor alternativa se procederá a diseñar y modelar una solución que asegure los dispositivos IoT haciendo de uso de una herramienta especializada. La selección de esta herramienta dependerá de la naturaleza de la misma y las características que la componen. Esta deberá permitir la representación de un modelo informático a nivel técnico la cual facilite su implementación en un contexto tanto empresarial como doméstico, además de un diseño comprensible para un público con pocos conocimientos en el tema.

4. MARCO DE REFERENCIA

4.1. Marco conceptual

4.1.1. Internet of Things (IoT)

El término "IoT" ha tenido cada vez más popularidad en los últimos años debido a los avances tecnológicos que han permitido una mayor producción e implementación de estos dispositivos, pero a su vez ha impulsado el aumento de ataques informáticos. Por estas razones es importante definir algunos conceptos clave para la correcta compresión de esta investigación. Entre los cuales se encuentran el IoT y los dispositivos que lo conforman, la ciberseguridad, los ciberataques, ciberdelincuentes, securIT y las vulnerabilidades correspondientes a esta tecnología emergente.

El acrónimo "IoT" corresponde en inglés al término "Internet of Things", que en español significa "Internet de las Cosas". Esta frase tiene varias interpretaciones debido a que es bastante reciente, pero la más adecuada es para referirse a todos los dispositivos o "cosas" que tienen capacidades informáticas como comunicarse con otros dispositivos, almacenar información, ser controlados o supervisados de forma remota y la capacidad principal por la cual se le da este nombre, el poder establecer una conexión con la internet (Vinton, 2016).

4.1.2. Interconexión

La conectividad es un apartado importante a la hora de usar dispositivos IoT, según Oracle ven este apartado en como "Un conjunto de protocolos de red para Internet ha hecho que sea fácil conectar sensores a la nube y a otras 'cosas' para conseguir una transmisión de datos eficiente." (Oracle, 2020), es por eso que es necesario entender las diferentes maneras en las que

se puede conectar a una red cada persona. El primero es el Wi-Fi, que es una tecnología vital para el mundo hoy en día, este permite que todo usuario se pueda conectar de manera inalámbrica mediante dispositivos móviles, laptops u otros dispositivos que requieran ser compartidos por diferentes usuarios como impresoras o cámaras de circuito cerrado y de esta manera se estable una red mediante el uso de un router, todo esto es regulado mediante el estándar IEEE 802.11. Otro medio de conexión usado es el ethernet, que se refiere a toda conexión de red de área local (está cubierta por el estándar IEEE 802.3), que es el medio principal para que cualquier hogar o empresa disponga del servicio de internet el cual puede llegar por cable coaxial, fibra óptica o cable de par trenzado. (Cisco, 2020).

4.1.3. Dispositivos

El término IoT abre la posibilidad de clasificar algunos dispositivos gracias a su capacidad de conectarse a internet. Actualmente existen muchos dispositivos que podrían clasificarse como dispositivos IoT, algunos de estos son electrodomésticos como sistemas de calefacción, aire acondicionado, ventilación, tostadoras, neveras, cortadoras de césped, lavadoras, televisores, aspiradoras, entre otros. También existe una gran variedad de sensores y sistemas de alarmas de seguridad tanto para hogares como para empresas o automóviles (Vinton, 2016). Por otro lado, aunque los celulares, tabletas, relojes, reproductores de música y computadores portátiles podrían clasificarse como dispositivos IoT, esta investigación se enfoca en los niveles de ciberseguridad que ofrecen los primeros dispositivos mencionados.

4.1.4. Datos

Las bases de datos usadas para ciertos servicios generan gran accesibilidad desde diferentes dispositivos para que puedan ser controladas por sus usuarios y así lleven el control de los datos almacenados. De acuerdo a Amazon Web Services es “una recopilación de elementos de datos con relaciones predefinidas entre ellos. Estos elementos se organizan como un conjunto de tablas con columnas y filas. Las tablas se utilizan para guardar información sobre los objetos que se van a representar en la base de datos. Se puede obtener acceso a estos datos de muchas formas distintas sin reorganizar las propias tablas de la base de datos.” (AWS, 2020). En otras palabras, este servicio es el que hace posible que una empresa pueda disponer de sus datos en un

almacenamiento en la nube o local brindado por un tercero, generando confiabilidad, integridad y disponibilidad para esa información, además de pueden garantizar un backup de la misma.

"Las reglas de UE requieren que las organizaciones que traten datos personales en los sistemas IoT lleven a cabo evaluaciones de seguridad como así también hacer uso de las certificaciones de seguridad pertinentes y standards. Además, las compañías necesitan garantizarlo cuando utilicen proveedores de servicios externos para gestionar los dispositivos y los datos de IoT, en este sentido, aquellos proveedores también deben tomar razonables precauciones de seguridad." (Ministerio de modernización de Argentina, 2020).

En el mundo de hoy se evidencia en los diferentes dispositivos y redes una captura de datos masiva de datos personales, en tiempos de los sistemas IoT se puede mencionar la recopilación de estos datos en muchos lugares, además, la facilidad de la interconexión genera que nuestros datos sean compartidos a niveles nunca antes vistos, esta captura de datos va de la mano a la invasión de la privacidad (Ministerio de modernización de Argentina, 2020).

4.1.5. Seguridad informática

En lo que a ciberseguridad respecta, el Grupo de Trabajo Conjunto sobre Educación en Ciberseguridad, mejor conocido por su nombre original inglés Joint Task Force on Cybersecurity Education, define la ciberseguridad como una disciplina basada en la informática que involucra tecnología, personas, información y procesos para permitir operaciones aseguradas en el contexto de los adversarios. También afirman en una de sus publicaciones en el año 2018, que esta disciplina se basa en los campos fundamentales de la seguridad de la información y la garantía de la misma. Es por esto que surgen conceptos como los ciberataques y los ciberdelincuentes.

Al estar conectados a internet, estos dispositivos también son vulnerables a ser atacados. Un ciberataque es definido en la revista insignia de ACM (Association for Computing Machinery) "Communications of the ACM" como un ataque a una computadora y un sistema de red. Este ataque consiste en acciones que realiza la computadora como conexión remota o local, acceso a archivos de computadora o ejecución de un programa con la intención de comprometer la operación segura de la computadora y el sistema de red (Crawford, D., 2001).

Debido al aumento de la dependencia de las infraestructuras de información para respaldar operaciones críticas en defensa, banca, telecomunicaciones, transporte, energía eléctrica y muchos otros sistemas, los ciberataques se han convertido en una amenaza significativa para la sociedad con consecuencias potencialmente graves (Crawford, D., 2001). Como parte de los tipos de ciberataques que se mencionan en este documento, se encuentran el DOS, la implantación de malware como lo es un ransomware y los botnets. Adicionalmente, es importante diferenciar la seguridad física y virtual (ciber), donde la primera corresponde a toda la parte tangible del dispositivo, es decir, todo lo referente a la seguridad material o relacionada con la propiedad intelectual que comprende el diseño del dispositivo; mientras que la seguridad virtual se refiere a todo lo relacionado con la parte intangible, es decir todo tipo de información almacenada junto con todo el proceso de gestión y mantenimiento de datos.

4.1.5.1. Denial of Service (DOS)

Las siglas DOS significan Denial of Service, lo que traduce Denegación de Servicio y es se define como un tipo de ciberataque que tiene como objetivo anular la capacidad de un sitio web para atender y resolver las solicitudes de los clientes, saturando la computadora objetivo con paquetes de información enviados a través de internet. El objetivo se consigue principalmente inundando el sistema con un número exagerado de peticiones que exceda la capacidad de respuesta del servidor o la computadora objetivo de forma que el servidor no podrá responder más solicitudes. Por otra parte, también existe el término DDOS, el cual significa Distributed Denial of Service y se traduce como Denegación de Servicio Distribuido. Este tipo de ataque lo llevan a cabo varios agentes (a menudo cientos o miles de equipos cliente) que atacan el mismo sitio web al mismo tiempo. La mayoría de las veces son computadoras que son usadas en áreas educativas debido a la vulnerabilidad de manipulación a la que se encuentran (Singleton, 2002).

4.1.5.2. Implantación de malware

De igual forma se encuentran los ataques de implantación de malware. Para entender este tipo de ciberataque es necesario saber que es un malware. Este término abarca diferentes tipos de software malicioso diseñados para dañar o explotar cualquier dispositivo, servicio o red programable. Los ciberdelincuentes hacen uso de estos para extraer datos que pueden ser utilizados en un futuro para chantajear a las víctimas y así obtener ganancias financieras. Dentro de estos datos pueden estar datos financieros, hasta registros de atención médica, correos

electrónicos personales y contraseñas. La variedad de información que puede verse comprometida se ha vuelto ilimitada (McAfee, 2020). “El malware puede infectar computadoras y dispositivos de varias maneras y se presenta en diversas formas, algunas de las cuales incluyen virus, gusanos, troyanos, spyware y más.” (Kaspersky, 2020).

Dentro del término malware se encuentra uno de los softwares maliciosos más conocidos, el ransomware. Este es uno de los tipos de malware más rentables y, por ende, más populares entre los ciberdelincuentes. Este malware es instalado en el computador de la víctima, luego cifra sus archivos y finalmente se pide un rescate económico (normalmente en Bitcoins) para devolverle al usuario sus datos (McAfee, 2020).

4.1.5.3. Botnets

Asimismo, es necesario mencionar los botnets. Este nombre lo recibe un grupo de computadores infectados y controlados por un atacante de forma remota. Para esto, un hacker o un grupo de ellos crea un botnet usando un malware que infecta a una gran cantidad de computadores de varios usuarios al azar, en la gran mayoría de los casos, los dueños de estos computadores no tienen ni idea de que sus dispositivos están infectados y mucho menos que hacen parte de una botnet. Los ordenadores son parte del botnet, llamados “bots” o “zombies”. No existe un número mínimo de equipos para crear un botnet. Los botnets pequeños pueden incluir cientos de PCs infectados, mientras que los mayores utilizan millones de equipos (Kaspersky, 2020).

4.1.5.4. Ciberdelincuentes

Hasta este punto habrá leído la palabra “ciberdelincuentes” en diferentes oportunidades y podrá hacerse una idea de a lo que esta se refiere, pero ¿Qué son realmente los ciberdelincuentes? Los ciberdelincuentes pueden llegar a ser desde profesionales en áreas de la tecnología, estudiantes con experiencia o aficionados que utilizan internet. Todos ellos con la similitud de que buscan crear virus con el fin de infectar diferentes computadores, los fines de cada uno puede variar, desde el robo de información o espionaje. “Los ciberdelincuentes se están volviendo más ágiles, explotan las nuevas tecnologías a una velocidad de vértigo, adaptan sus ataques utilizando nuevos métodos y cooperan entre sí de manera nunca vista hasta ahora. Las

redes delictivas operan a escala planetaria, coordinando ataques complejos contra sus objetivos en cuestión de minutos.” (INTERPOL, 2020).

4.1.5.5. Medidas contra ciberataques

Luego de mencionar los ciberataques y los ciberdelincuentes, se hace importante mencionar las contramedidas, es decir la forma de contra restar los ciberataques o si es posible prevenirlos. Para esto se utilizan diferentes softwares especializados que realizan distintos procesos para evitar o combatir diferentes amenazas como puede serlo un virus informático o un malware. Estos aplicativos suelen ser instalados en un computador como cualquier otro programa y este se encarga de analizar todos los archivos que sean descargados o visitados en el caso de programas maliciosos que se encuentren directamente en la red (Kaspersky, 2021). Por otro lado, también se encuentran los honeypots, los cuales se definen como un sistema informático puesto en peligro para obtener información sobre los ciberdelincuentes. Un honeypot es como cualquier otro sistema informático que contiene directorios e información, los cuales se manejan como sistemas informáticos reales, pero su motivo es muy específico y diferente (Abhishek M., Debabrat B., Kanchan V., Debasish J., 2001).

4.1.6. Ciberseguridad en dispositivos IoT

Por otro lado, la seguridad en los dispositivos IoT es un apartado de gran importancia en un mundo donde se hace uso desde cámaras para monitorear a los bebes, elementos para el monitoreo de la salud de las personas, entre otros. Por esto, es vital que dichos aparatos electrónicos brinden la seguridad necesaria en cuanto a los datos, el funcionamiento de los mismos y la confiabilidad en su uso puesto que si un atacante aprovecha alguna vulnerabilidad de estos e infringe la privacidad de los usuarios manipulando algunos de los apartados anteriormente mencionados, este podría robar datos, interrumpir la entrega de servicios o cometer cualquier otro delito. Es por esto que las “Compañías de seguridad de IoT con gran experiencia recomiendan una estrategia de tres componentes para proteger los datos, los dispositivos y las conexiones que son: Protección del aprovisionamiento de los dispositivos, Protección de la conectividad entre los dispositivos y la nube, Protección de los datos en la nube durante su procesamiento y almacenamiento (Microsoft Azure, 2020).

4.1.7. Vulnerabilidades y amenazas

Adicionalmente, es necesario tener en cuenta las principales vulnerabilidades de los dispositivos IoT y para esto es indispensable entender que es una vulnerabilidad. El Instituto Nacional de Ciberseguridad (INCIBE) de España define una vulnerabilidad (en términos de informática) como una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que el INCIBE recomienda encontrarlas y eliminarlas lo antes posible.

Para entender un poco las amenazas de los dispositivos IoT se tendrá en cuenta los ataques a los que se pueden enfrentar clasificándolos en cinco categorías, la primera se trata de la suplantación de identidad en la que el atacante puede manipular el estado de un dispositivo anónimamente, también puede interceptar o invalidar parcialmente la difusión y con esto suplantar al autor y por último puede acceder a los datos que emite el dispositivo si el atacante puede acceder a la red luego de conocer la clave de acceso a la misma.

La segunda categoría trata de las alteraciones que se pueden generar en el software de los aparatos electrónicos con el fin de acceder a la configuración y manipular su funcionamiento. La tercera categoría es la revelación de información en la que el usuario se ve expuesto a que los delincuentes informáticos accedan a los datos privados que se encuentren almacenados sin la autorización pertinente para dicha acción o en algunos casos es posible que el acceso a la información sea denegado o se trate de información falsa.

Por último, la cuarta categoría trata de la denegación de servicios, para la cual se realizan interferencias en la comunicación de varios dispositivos haciendo uso de frecuencias de radio. Un ejemplo podría ser en el que una cámara de vigilancia deje de transmitir la información pertinente porque se le cortaron los cables intencionalmente. Por último, se tiene la elevación de privilegios en la que un dispositivo se puede ver afectado en su funcionamiento por los cambios en la configuración que realice el atacante, por ejemplo, si las compuertas de una presa normalmente se abren por completo para su correcto desempeño el delincuente puede variar esto y hacer que abran a mitad de su capacidad, consiguiendo afectar las labores de una empresa, así mismo podría suceder con algún dispositivo de un usuario en su hogar (Microsoft Azure, 2020).

4.1.8. Seguridad de la información

Por otra parte, es necesario aclarar la diferencia entre seguridad de la información y seguridad informática antes de explicar los diferentes mecanismos de seguridad que existen frente a las vulnerabilidades de los dispositivos IoT. Pese a tener cierta similitud, estos conceptos no significan lo mismo, la seguridad informática hace referencia a la protección de la infraestructura tecnológica incluyendo tanto software como hardware mientras que la seguridad de la información se refiere a la protección de la información independientemente del medio en el que se encuentre, bien sean documentos físicos, medios digitales o conocimiento propio de alguna persona. (Morales, Diaz y Leguizamón, 2019, p. 294).

Existen diferentes mecanismos de seguridad que permiten detectar o prevenir ataques relacionados con la seguridad de la información y la seguridad informática. Para la implementación de estos mecanismos en entornos IoT, es necesario tener en cuenta los cuatro pilares de la seguridad de las comunicaciones, los cuales son la disponibilidad, autenticación, integridad y confidencialidad, puesto que estos mecanismos incluyen diversos protocolos de seguridad inmersos en modelos de arquitectura de comunicación (Morales, Diaz y Leguizamón, 2019, p. 294).

4.1.9. Modelo de referencia de arquitectura IoT

Los modelos de referencia tienen como objetivo plantear una arquitectura que cumpla las necesidades que una organización tenga al momento de implementar IoT en sus negocios. Cada modelo de referencia se enfoca en un número distinto de capas de diferentes características y complejidades. Algunos de estos modelos son: las arquitecturas de referencia de IBM y de Azure las cuales manejan tres capas, el modelo ITU compuesto de cuatro capas, el IoT simple formado a partir de cinco capas, el modelo Intel IoT con seis capas y el modelo IoTWF de siete capas (Morales, Diaz y Leguizamón, 2019, p. 293).

4.1.9.1. Modelo de referencia IBM

La arquitectura de referencia de IBM se compone de tres capas las cuales son: la capa de dispositivos (devices), la capa de preprocesamiento (edge computing) y la capa de almacenamiento en la nube (cloud). Estas capas permiten que este modelo se enfoque en la reducción de la latencia y filtrado de datos que se dirigen a la nube gracias al uso de edge computing. Adicionalmente, el usuario interactúa con el modelo por medio de dispositivos

móviles gracias a la capa devices, la cual se centra en el control y análisis de los datos generados a través de las aplicaciones que recolectan la información de los distintos sensores o dispositivos. El único problema de este modelo es que solo está dirigido para dispositivos producidos por IBM (Vélez Pérez, 2019).

4.1.9.2. Modelo de referencia Azure

La arquitectura de referencia de Azure, de igual manera que IBM, se constituye de tres capas, la primera de ellas es things, esta se encarga de los dispositivos IoT que estén en el modelo además de pre procesar sus datos generados por medio de edge computing con el fin de mejorar las funcionalidades del modelo. Luego, por medio de un gateway se conecta de manera segura a la segunda capa llamada insights, su enfoque principal es el almacenamiento y transformación de la información recopilada anteriormente. La última capa se denomina action, donde el usuario interactúa con el modelo, se aplican los procesos o "acciones" al negocio y donde se analizan datos y acciones con machine learning. Es por eso que, este modelo permite una mejor toma de decisiones de acuerdo a los datos recopilados, no obstante, este modelo se centra únicamente a productos de Microsoft (Vélez Pérez, 2019).

4.1.9.3. Modelo de referencia ITU

El modelo ITU aumenta en una capa a diferencia de los otros modelos, dando como resultado de cuatro capas con capacidades transversales de gestión y seguridad de los datos. Una capa contiene la capacidad de gestión, la cual permite, como su nombre lo dice, la gestión de dispositivos, permitiendo la desactivación y activación de forma remota, además de gestionar la topología y el tráfico de la red. Por otro lado, las capacidades de la seguridad se encuentran en las otras tres capas del modelo, una de ellas es la de aplicación, esta capa define los límites del modelo por medio de la autenticación, autorización, integridad, privacidad, auditorias y antivirus. La capa de red comparte algunas características de la capa anterior, esas son la autenticación y autorización, pero se le añade la confidencialidad, con el fin de validar, permitir y asegurar el transporte de datos. Por último, está la capa de dispositivo, la cual también tiene autorización autenticación y confidencialidad, pero a diferencia de la capa de red, esta capa tiene control de acceso y protección de datos, además de estar enfocada a la interacción con los dispositivos del modelo y no de la conexión (Vélez Pérez, 2019).

4.1.9.4. Modelo de referencia IoT simple

IoT simple es un modelo de cinco capas, con una seguridad transversal en cada una de ellas, con un principio físico y lógico, cada capa integra autenticación, encriptación, protección y filtrado de datos. La capa uno son los dispositivos de tipo actuador o sensor, en la capa dos están los gateways, los cuales brindan un soporte a aquellos dispositivos que no tengan conexiones TCP IP. La capa tres se centra en el network, en esta capa se maneja la red empresarial en la que este el modelo. El management y analytics son los temas principales de la capa cuatro, en ella se administran los datos recolectados de los dispositivos. La última y quinta capa se enfoca en big data y data center, donde se define la capacidad de almacenamiento y se procesa la información (Vélez Pérez, 2019).

4.1.9.5. Modelo de referencia Intel

El modelo Intel IoT se compone de seis capas, cada una con un componente de seguridad transversal. Esas capas son: Business layer, application layer, control layer, management layer, data layer con analytics y communications/connectivity layer (Vélez Pérez, 2019). Del modelo se destacan las siguientes capas:

- Control layer: esta capa posee las políticas de seguridad y el control de acceso.
- Management layer: esta capa permite la gestión de los dispositivos y supervisión de las operaciones.
- Data layer: esta capa se enfoca en edge computing para el control de los datos y
- Communication/connectivity layer: esta es la capa permite la comunicación ya que utiliza varios protocolos entre distintos tipos de dispositivos conectados en una red PAN/LAN o WAN.

4.1.9.6. Modelo de referencia IoTWF

El modelo IoTWF es el de mayor número de capas a comparación de los demás modelos, este permite una mayor interacción entre los datos de una red, la cual brinda una mejor aplicación de estos antes de ser almacenados gracias al filtrado de datos que se realiza por medio de edge computing (Vélez Pérez, 2019). Las capas que lo componen son:

- Capa de dispositivos y controladores: en esta capa se encuentran todos los dispositivos físicos los cuales pueden enviar o recibir información.

- Capa de conectividad: esta capa se encarga de transmitir los datos según sea el medio necesario para la conexión con la capa uno.
- Capa de edge computing: es la capa que transforma los datos antes de ser depositados.
- Capa de almacenamiento de datos: se centra en el almacenamiento de toda la información generada.
- Capa de abstracción de datos: esta capa se enfoca en darle forma a los datos creados para facilitar su uso.
- Capa de aplicación: su finalidad es brindar la posibilidad de análisis de datos, reportes y monitoreo.
- Capa de procesos y colaboración: en esta capa se facilita la interacción entre dispositivos IoT y personas y/o negocios

4.1.10. Certificados digitales IoT

Las grandes compañías ofrecen diferentes servicios relacionados a la implementación de dispositivos IoT de forma segura. Una de estas compañías es Amazon a través de AWS (Amazon Web Services), la cual brinda la oportunidad de cifrar todo el tráfico de su infraestructura mediante una utilidad interna llamada transport layer security. Este servicio permite identificar los dispositivos conectados por medio de certificados X509 (formato estándar para certificados de clave pública). Este tipo de certificado digital utiliza un sistema de cifrado asimétrico que permite grabar las claves privadas de almacenamiento seguro de un dispositivo. Estos certificados son más seguros que otros sistemas de autenticación más comunes como los que utilizan nombre de usuario y contraseña o los tokens portables (Morales, Diaz y Leguizamón, 2019, p. 294).

Otra de las grandes empresas que ofrece certificados digitales IoT es Microsoft, quienes a través de la plataforma Azure IoT, brindan la posibilidad de utilizar un servicio llamado Azure IoT Hub, el cual permite conectar objetos de manera segura a internet. Adicionalmente, este servicio también soporta los certificados X509 para actividades de autenticación de los dispositivos conectados por medio de los protocolos HTTP, MQTT y/o AMQP. Esto significa que Azure IoT Hub crea los certificados y los asocia a los objetos conectados a internet con un identificador y la clave privada, mientras que, en AWS, el usuario debe crear el certificado y

asociarlo a un dispositivo IoT. Este tipo de certificado es validado y generado por una certificadora para que los dispositivos conectados puedan ser autenticados en IoT Hub. (Morales, Diaz y Leguizamón, 2019, p. 294).

4.1.11. Criptografía en entornos IoT

La criptografía proviene de la combinación de dos palabras en griego, “Kryptos”, la cual significa oculto y “graphia”, que significa escritura, y se define como: conjunto de técnicas que permiten alterar y modificar mensajes o archivos con la finalidad de que una persona o usuario no autorizado no pueda leer el contenido de dichos mensajes o archivos (NIC Argentina, 2018).

Esta es una herramienta muy utilizada en el sector de la ciberseguridad y actualmente se investiga en su aplicación para entornos IoT. Algunos de ellos son, por ejemplo, los protocolos WSN (red de sensores inalámbricos), se centra en la distribución de una red de sensores inalámbricos; esta solución se pensó para dos situaciones criptográficas: cuando se utiliza una topología tipo Mesh o red en malla, donde los nodos tiene una gran capacidad de procesamiento y para una topología de estrella, la cual trabaja una red de nodos de baja capacidad en comparación a al anterior (Morales, Diaz y Leguizamón, 2019, p. 294).

La finalidad de estos métodos de encriptación es el mantener un equilibrio entre los requerimientos y la seguridad de una red de sensores inalámbricos, en los cuales se emplea un árbol de nodos con función Hash. El Hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija, sin importar la longitud de los datos de entrada, el valor hash de salida siempre tendrá la misma longitud (Donohue, 2014). Los nodos finales de la red se encargan de enviar los hashes de información a los nodos enrutadores, una vez enviados, la información es validada con el fin de asegurar de que haya llegado completa dicha información, después, se transmite a cada nodo enrutador, usando la función HASH hasta llegar al último nodo del árbol (Morales, Diaz y Leguizamón, 2019, p. 295).

4.1.12. Blockchain aplicado en entornos IoT

Blockchain en los últimos años ha ganado bastante popularidad por su uso en las criptomonedas, pero este no es su única funcionalidad, y es que Blockchain es un sistema

descentralizado donde se realizan registros, en su mayoría de transacciones, de forma distribuida. Cada registro de información es incluido en un bloque, estos bloques forman una cadena mediante el uso de funciones matemáticas. Cada bloque contiene un hash criptográfico del bloque anterior, además, de almacenar los datos del registro o transacción y una marca de tiempo (Tudela, 2019). Con base a esas características, se forma un árbol Merkle (Becker,2008), el cual brinda beneficios como la verificación de información a gran velocidad o la resistencia a la modificación de datos. En pocas palabras, Blockchain es un registro público, descentralizado y capaz de almacenar registros entre dos partes de manera verificable, eficiente y permanente (Tudela, 2019).

Como se mencionó anteriormente, Blockchain tiene un enfoque al uso de criptomonedas inicialmente. Sin embargo, sus características ofrecen numerosos beneficios en sectores muy variados. En específico, su estructura distribuida y sus mecanismos de seguridad son aplicables a arquitecturas IoT. Es así como, uno de los novedosos métodos para la seguridad de sistema IoT se basa en Blockchain, este método se centra en contratos inteligentes permite gestionar recursos y aplicar sistemas de seguridad por medio de una red Ethereum. La red Ethereum permite hacer configuraciones de forma privada, facilitando la elección de las direcciones de la red que van a ser destinadas a cada dispositivo IoT, los cuales contaran con su respectiva cuenta en dicha red. Al aplicar contratos inteligentes con Blockchain el uso de métodos de seguridad es más sencillo, debido a que los métodos están incorporados en los contratos junto con la gestión de versiones y los registros de información, de esta manera se almacena en su mayoría la lógica del sistema (Tudela, 2019).

Otro método de seguridad similar al anterior pero que tiene una mayor escalabilidad es Amazon Managed Blockchain, es un servicio completamente administrado el cual facilita la creación y gestión de redes de Blockchain escalables por medio del uso de los marcos de código abierto Hyperledger Fabric y Ethereum. Su mejora se centra en eliminar la carga de creación de una red Blockchain, ya que un proceso normal conlleva a cada miembro de la red provisionar manualmente el hardware, instalar el software, crear y administrar los certificados para el control del acceso y configuración de los componentes de la red. Con el servicio de Amazon se facilita todo el proceso de la creación de una red óptima y segura, debido a que su escala se ajusta automáticamente a las solicitudes de miles de aplicaciones que ejecutan millones de registros en

los dispositivos IoT. Además, una vez la red está operando, se simplifica la tarea de mantener y administrar la red de Blockchain gracias a que el servicio permite invitar de forma sencilla a miembros nuevos a la red, adicionalmente, el servicio administra los certificados generados y ejecuta un seguimiento a las métricas operacionales de la red, tales como, el uso de memoria, almacenamiento y recursos informáticos. Es por estas características que, este servicio de Amazon tiene un gran potencial para simplificar y generar soluciones seguras de conexión a dispositivos IoT (AWS, 2021).

4.2. Estado del arte

4.2.1. Investigaciones Internacionales

4.2.1.1. Diseño de sistema IoT seguros y abiertos

Dentro de los antecedentes internacionales se considera importante destacar a Varshney, R.; Vogel, B. (2018) con su investigación titulada "*Towards Designing Open and Secure IoT Systems: Insights for Practitioners*", Association for Computing Machinery, Santa Barbara, Estados Unidos. La investigación estuvo basada en una metodología cualitativa cuyo objetivo fue proporcionar información para los profesionales de IoT con el fin de mejorar el diseño de seguridad y privacidad para sistemas de IoT abiertos y seguros. Los instrumentos utilizados para desarrollar la investigación fueron entrevistas cualitativas con profesionales en el campo de IoT. La muestra fue de unos 6 profesionales con una amplia experiencia y con cargos muy importantes en empresas enfocadas al desarrollo, diseño, instalación y mantenimiento en sistemas IoT. En los resultados obtenidos se identificaron varias tendencias y desafíos de seguridad además de unos diseños que deben de ser considerados por los profesionales de IoT. De igual manera los resultados apuntaron a que la seguridad no es solo un problema técnico, sino también una cuestión de conciencia, mentalidad y procesos realizados por las personas que los crean y/o utilizan. Por esa razón la conclusión que se concreto es que la seguridad no es la única cosa a tener en cuenta para el uso de IoT, sino que es más una característica obligatoria de los sistemas IoT. Sin embargo, no existen pautas generales que puedan proponerse para abordar la seguridad, debido a que la seguridad no es un problema técnico solo, sino también están los problemas de conciencia, mentalidad, personas y procesos. Es por eso que, se cree que el modelo conceptualizado en el

documento que enfatiza el aspecto humano en el bucle ayudaría a determinar los requisitos dinámicos y los principios de diseño de los sistemas IoT de una manera más abierta, común y segura. Además, de que las personas podrían participar activamente para dar forma a sus soluciones de IoT de una manera más transparente.

4.2.1.2. Dispositivos IoT como herramientas de ataques

Otra investigación de carácter internacional relevante es la del autor Alani, M (2018) en su investigación titulada "*IoT Lotto: Utilizing IoT Devices in Brute-Force Attacks*", Association for Computing Machinery, Nueva York, Estados Unidos. La investigación fue enfocada con una metodología cualitativa con el objetivo de presentar un diseño conceptual en el que los dispositivos de IoT se utilizan como herramientas en ataques de fuerza bruta para romper las claves de cifrado en cifrados en bloque. El resultado que arrojó la investigación es que el modelo conceptual que se propuso introduce un sistema en el cual un gran grupo de dispositivos de IoT pueden ser usados como máquinas de descifrado para encontrar una clave de cifrado mediante un ataque de fuerza bruta. Esto se apoya con el hecho de que se reduce el tiempo necesario para la búsqueda exhaustiva en el espacio clave debido a que una gran red de dispositivos de IoT está buscando de manera paralela en diferentes partes del espacio de búsqueda. Con esto se llegó a la conclusión de que el diseño conceptual que se propuso muestra que los dispositivos de IoT se pueden usar de manera colectiva para buscar la clave de cifrado de un cifrado de bloque en un ataque de fuerza bruta. Sin embargo, cuando el cifrado de bloques utilizado tiene un tamaño de clave grande con operaciones matemáticas complejas, el sistema propuesto puede ser lento, a menos que emplee una gran cantidad de dispositivos de IoT.

4.2.1.3. Diseño de sistema IoT con retos y barreras

La última investigación internacional destacable es de los autores Salazar, J.; Silvestre, S. (2019) cuyo título es "*Internet de las cosas*", Techpedia. České vysoké učení technické v Praze Fakulta elektrotechnická. Praga, Republica Checa. Centrada en una metodología cualitativa con el objetivo de ofrecer claridad en las diferentes etapas de desarrollo de tecnología IoT enfocándose en las posibles complicaciones al momento de aplicar esta tecnología, para que su implementación sea eficiente. Los resultados

obtenidos evidencian los puntos específicos como fiabilidad, rendimiento y gestión, los cuales son considerados vitales y que sin estos no se logra conseguir un buen abordaje a la tecnología IoT o en español (Internet de las cosas). La conclusión obtenida fue que los puntos como fiabilidad, rendimiento y gestión son relevantes a la hora de entrar en el ámbito de seguridad y privacidad, al momento de la implementación de la tecnología IoT en el usuario y en todos los datos que se manejan, con el fin de que el usuario al momento de hacer uso de esta tecnología se sienta seguro. El uso de estas tecnologías IoT deben ser adoptadas por los usuarios basándose en seguridad de transferencia de datos para su uso y no solo por adquirir nueva tecnología.

4.2.2. Investigaciones Nacionales

4.2.2.1. Diseño de sistemas IoT y ámbito organizacional

Dentro de los antecedentes nacionales se encuentra la notable investigación de Peña, E. (2018) titulada "*La seguridad del IoT desde una perspectiva de enfoque nacionalización*", Bogotá, Colombia. La cual está basada en una metodología cualitativa, cuyo objetivo fue la optimizar los procesos dentro de una organización establecida. En esta investigación los resultados identificaron algunas zonas de la organización en las cuales se logra una optimización debido a los sistemas IoT. Algunos de estos son: Mejora en la cadena de producción, mejora en análisis de inventario, impactos considerables en el modelo de distribución y mejor manejo en la relación organización-cliente. Lo anterior se logra identificando factores de riesgo en seguridad y trabajando para que no ocurran fallas, los factores son: suplantación de identidad, interrupción en algún servicio, manipulación de información entre otros. A partir de esta investigación, se concluyó que es necesario asegurar un alto nivel de seguridad en el ámbito organizacional debido a la sensibilidad de la información administrada, como pueden ser inventarios, datos privados, información de empleados, entre otros. Es por esto que la seguridad debe ser asegurada antes de implementar un sistema IoT, puesto que la mayoría de estos dispositivos no cuentan con la seguridad necesaria para ofrecer total privacidad sobre los datos tratados.

4.2.2.2. Diseño de sistemas IoT buenas prácticas entorno a seguridad

Otra investigación nacional a destacar es la del autor Perez, L. (2019) titulada "*Guía de buenas prácticas en torno a la seguridad de IoT para las smart house"* (Doctoral dissertation). Ocaña, Colombia. Con una metodología cualitativa se desarrolló el objetivo de dar a conocer los ítems de seguridad y las buenas prácticas para garantizar una buena práctica de los sistemas IoT en el hogar. Cuyos resultados establecen como factores importantes a la confidencialidad, el no repudio, la autorización, la disponibilidad, la autenticación y la privacidad, estos factores se deben de garantizar al momento de establecer una conexión con IoT, para asegurar el uso y el manejo correcto de esta tecnología, con el fin de disminuir el riesgo de exponer datos privados. La conclusión a la se llegó fue de que los pilares básicos de la seguridad o de la ciberseguridad, que son los que manejan los sistemas IoT son: la confidencialidad, la integridad y la disponibilidad, debido a que en cada uno de ellos se controlan aspectos como la disponibilidad de los datos y el manejo de estos, también la disponibilidad de las personas autorizadas para el acceso de los datos, el uso e información del sistema entre otros.

5. ANÁLISIS DE RESTRICCIONES

5.1. Restricciones éticas

Con respecto a las restricciones de esta investigación, es necesario tener en cuenta los aspectos éticos, puesto que todo aquello que se refiere a la seguridad de la información se relaciona con estos. La ética del uso y la gestión de la información componen un factor indispensable en lo que a una solución informática respecta, puesto que es fundamental velar por la privacidad de la información manejada, independientemente de quien sea el propietario.

Es por esto que la información que ingrese al modelo informático, es decir los datos recolectados por los dispositivos IoT, debe ser tratada de forma especial con el fin de garantizar su confidencialidad, integridad y disponibilidad. Estas consideraciones dependen principalmente de las indicaciones o restricciones propuestas por el cliente junto con las leyes relacionadas con el BigData y el Régimen General de Protección de Datos Personales cubierto por la Ley 1581 del año 2012 en Colombia (MinTIC, 2013). Adicionalmente es necesario restringir el acceso a los

elementos privados por parte de los autores de esta investigación una vez el modelo sea implementado.

5.1. Restricciones técnicas

Adicionalmente, el modelo debe cumplir las siguientes restricciones técnicas para ofrecer la mejor solución con respecto a seguridad y facilidad de implementación.

- Debe ser compatible con la mayoría de los dispositivos IoT.
- Debe asegurar y cifrar la conexión entre los dispositivos IoT y la red, con el fin de evitar el uso de estos dispositivos como puentes de acceso a la red para los ciberdelincuentes.
- Debe facilitar la autenticación y configuración de la conexión entre los dispositivos y la red.
- Debe ser escalable, es decir que pueda implementarse tanto en ambientes grandes como pequeños.

6. GENERACIÓN DE POSIBLES SOLUCIONES

A continuación, se describirán abreviadamente 8 posibles modelos informáticos que dan solución al problema planteado en este documento. Es importante mencionar que el orden en las que se encuentran estos modelos no tiene ninguna relación con su nivel de eficacia, dimensión, costo o cualquier otra característica similar.

6.1. Certificados Digitales

Existen dos opciones ofrecidas por diferentes proveedores que facilitan la implementación de este modelo:

- AWS brinda la oportunidad de cifrar todo el tráfico de su infraestructura mediante una utilidad interna llamada Transport Layer Security, la cual utiliza certificados X509, un formato estándar para certificados de clave pública. Este tipo de certificado es más seguro que otros sistemas de autenticación más comunes como los que utilizan nombre de usuario y contraseña o los tokens portables (Morales, Diaz y Leguizamón, 2019, p. 294).
- Microsoft ofrece la posibilidad de utilizar un servicio llamado Azure IoT Hub, el cual soporta los certificados X509 para actividades de autenticación de los dispositivos

conectados por medio de los protocolos HTTP, MQTT y/o AMQP (Morales, Diaz y Leguizamón, 2019, p. 294).

6.2. Contratos inteligentes con Blockchain

Este modelo implementa contratos inteligentes con Blockchain, lo cual permitiría gestionar recursos y aplicar sistemas de seguridad por medio de una red Ethereum. Esta red permite hacer configuraciones de forma privada, facilitando la elección de las direcciones de la red que van a ser destinadas a cada dispositivo IoT, los cuales contaran con su respectiva cuenta en dicha red. Al aplicar contratos inteligentes con Blockchain el uso de métodos de seguridad es más sencillo, debido a que los métodos están incorporados en los contratos junto con la gestión de versiones y los registros de información (Tudela, 2019).

6.3. Amazon Managed Blockchain

Este modelo utiliza un servicio completamente administrado que facilita la creación y gestión de redes escalables de Blockchain, por lo que ofrece un nivel de seguridad bastante alto. Este servicio recibe el nombre de Amazon Managed Blockchain en la plataforma de AWS y funciona dentro de los marcos de código abierto Hyperledger Fabric y Ethereum, lo cual le permite administrar los certificados generados y ejecuta un seguimiento a las métricas operacionales de la red, tales como, el uso de memoria, almacenamiento y recursos informáticos (AWS, 2021).

6.4. AWS IoT Core

AWS ofrece un servicio llamado AWS IoT Core, el cual permite conectar dispositivos de IoT a la nube de AWS sin la necesidad de aprovisionar o administrar servidores. Además, AWS IoT Core proporciona configuración y autenticación automatizadas en la primera conexión de un dispositivo a AWS IoT Core, así como el cifrado de extremo a extremo en todos los puntos de conexión, de modo que los datos nunca se intercambian entre dispositivos y AWS IoT Core sin identidad comprobada. Asimismo, puede proteger el acceso a los dispositivos y las aplicaciones mediante políticas con permisos pormenorizados (AWS, 2021).

6.5. Modelos Criptográficos

Los modelos que únicamente implementan técnicas criptográficas con algoritmos matemáticos de encriptación tanto simétricos como asimétricos también son modelos a tener en cuenta, debido a que estos ofrecen amplias opciones para asegurar la información de los dispositivos de una o varias redes. Uno de los más comunes es el HASH, el cual encripta los datos con valores matemáticos únicos, permitiendo de esta forma el uso de variadas topologías de red, dependiendo del número de dispositivos junto a sus características y sus correspondientes requerimientos respecto a la red a la cual se vayan a incorporar (Morales, Diaz y Leguizamón, 2019, p. 295).

6.6. Modelo Simple IoT

El modelo simple IoT es un notorio candidato por su propuesta de cinco capas, las cuales se componen de los dispositivos actuadores o de sensor, Gateways, Networks, herramientas de Managment y Analytics, y bases de datos escalables con Big Data y Data Centers. De esta forma el modelo brinda autenticación, protección, encriptación y filtrado a los datos que se generen en la red, generando una amplia variación de posibilidades IoT centradas a problemáticas empresariales o que sean significativamente complejas en número y distribución Morales, Diaz y Leguizamón, 2019, p. 295).

6.7. Modelo Intel IoT

Con seis capas y un componente transversal en cada una, el modelo IoT de Intel propone una arquitectura con múltiples variables compuestas en dos grandes grupos, en el primer grupo están los dispositivos junto a los Gateways, en el segundo grupo se encuentran los componentes cloud, en este último, se gestionan los datos de forma remota, además de centrarse en el análisis y almacenamiento de los datos junto a la gestión del servicio y seguridad. Esto es posible gracias a las capas de Business Layer, Application Layer, Control Layer, Management Layer, Data Layer con Analytics y Communications/Connectivity Layer, además, por su componente de Security que se encuentra en cada capa, brinda una seguridad robusta de principio a fin del modelo, aplicando distintas técnicas de seguridad respecto a la capa en que se encuentre. De esta forma los dispositivos con componentes Intel pueden tener una protección fiable y dinámica (Vélez Pérez, 2019).

6.8. Modelo IoTWF

El modelo IoTWTF también se considera como una posible solución debido a su gran capacidad de interacción de los datos en la red, compuesto por siete capas, el cual ofrece un flujo de información centrado en el desacoplamiento, análisis, interoperabilidad e integración de la empresa según la tecnología y dispositivos que posea. Esto se debe a que los dispositivos reciben y transmiten datos en una interacción constante en la red, donde los datos son normalizados y filtrados por medio de Edge computing previamente a su almacenamiento, es así como estos datos quedan disponibles para las aplicaciones, las cuales procesan los datos y proveen a las personas la capacidad de interactuar con el modelo (Vélez Pérez, 2019).

7. SELECCIÓN DE LA MEJOR ALTERNATIVA

Al seleccionar la mejor alternativa para cumplir el objetivo general es indispensable tener en cuenta los factores que se explican a continuación:

Grado de efectividad: Hace referencia al nivel de seguridad ofrecido por cada posible solución.

Facilidad de implementación: Se refiere al bajo nivel de complejidad para poner en marcha la solución.

Compatibilidad: Se refiere a la capacidad de establecer una conexión exitosa entre el modelo y los dispositivos IoT.

Escalable: Hace referencia a la capacidad de mejorar la disponibilidad y el comportamiento del modelo cuando sea necesario.

Teniendo en cuenta los factores mencionados anteriormente, se realizará un breve análisis para cada posible solución y finalmente se seleccionará la mejor alternativa.

Tabla 1

Tabla de comparación de soluciones

	Grado de efectividad	Facilidad de implementación	Compatibilidad	Escalable
Modelos criptográficos	En su mayoría dependen o son más eficientes junto a otro modelo, debido a que de	Cuando las técnicas son muy complejas, su implementación	Compatible con cualquier dispositivo.	No

	manera individual algunas de las técnicas criptográficas ya han sido vulneradas, provocando grandes consecuencias negativas por ello.	se dificulta en gran manera en comparación a otros modelos.		
Modelo Simple IoT	Eficiente y seguro gracias a su planteamiento de cinco capas que ofrece una buena seguridad transversal distribuida.	Enfocada en proyectos complejos, donde se debe realizar una estructura más intrincada y extensa, con el fin de cubrir todas las necesidades de la empresa en la cual se vaya a implementar.	Compatible con la mayoría de los dispositivos.	Si
Modelo Intel IoT	Proporciona una seguridad distribuida transversalmente en sus dos grupos principales, los cuales son mencionados de manera resumida como dispositivos y cloud, por lo que, a lo largo de sus seis capas, el modelo cuenta con una buena seguridad enfocada a cada una de ellas.	Solo permite el uso de este modelo exclusivamente a los dispositivos que cuenten con sus componentes o que sean propios de su marca, por lo que se limita en gran manera su alcance.	Compatible únicamente con dispositivos de Intel.	Si
Modelo IoTWF	Su implementación se enfoca en la distribución e incorporación del modelo a los dispositivos y componentes que posea una empresa con el objetivo de agilizar el envío, manejo y almacenamiento de los datos, pero sin preocuparse por aspectos de seguridad complejos.	Se evidencia la presencia de diversos inconvenientes para su implementación respecto a temas de seguridad, debido a que su punto fuerte es el flujo de la información por todas sus capas, por lo que su metodología para la seguridad solo se centra en roles y privilegios.	Compatible con la mayoría de los dispositivos.	Si
Certificados Digitales	Son una buena alternativa en cuanto a seguridad de la información, puesto que estos aseguran la confidencialidad y la integridad de la información gracias a su sistema de cifrado	Su implementación es sencilla gracias a las plataformas que los soportan como lo son AWS y Azure IoT Hub, quienes ofrecen una comunicación que	Compatible con la mayoría de los dispositivos.	No

	asimétrico que permite grabar las claves privadas de almacenamiento seguro de un dispositivo. Sin embargo, esta solución solamente se encarga de asegurar el flujo de la información dentro del sistema, pero no ofrece un modelo completo que permita administrar y gestionar la información.	implementa este tipo de certificados en sus servicios.		
Contratos inteligentes con Blockchain	Ofrecen una excelente seguridad de la información gracias a la implementación de esta tecnología, la cual, contiene los mejores aspectos de seguridad en el mercado actual.	Su implementación es compleja puesto que es imprescindible implementar la red Ethereum y adicionalmente configurarla, por lo que el proceso de construcción de esta solución puede llegar a ser bastante demorado y da lugar a la aparición de errores debido a que esta debe ser implementada sin ninguna base desde la cual iniciar.	Compatible con cualquier dispositivo.	Si
Amazon Managed Blockchain	Ofrece un nivel de seguridad de la información bastante alto en cuestión de minutos utilizando la tecnología con mejores referencias en relación a la seguridad de la información	Su implementación es bastante sencilla debido a que este es un servicio totalmente administrado por Amazon Web Services, lo cual permite acelerar el proceso de implementación de un modelo que utilice Blockchain.	Compatible con cualquier dispositivo.	Si
AWS IoT Core	Ofrece un alto nivel de seguridad gracias a su sistema de autenticación que utiliza un cifrado de extremo a extremo.	Su implementación es bastante sencilla puesto que también es un servicio totalmente administrado ofrecido por Amazon, el cual protege el acceso a los dispositivos y las aplicaciones	Compatible con cualquier dispositivo.	Si

		mediante políticas con permisos pormenorizados.		

Luego de realizar el análisis anterior, es posible afirmar que las soluciones con mayor grado de efectividad, mayor facilidad de implementación y mejores características de compatibilidad y escalabilidad son:

- Certificados Digitales
- Amazon Managed Blockchain
- AWS IoT Core

Estas tres soluciones pueden complementarse entre sí gracias a su naturaleza, por una parte, AWS IoT Core proporciona configuración y autenticación automatizadas entre la conexión de un dispositivo con la red, posteriormente Amazon Managed Blockchain podría implementarse para gestionar la información recolectada por los dispositivos IoT mientras que el certificado digital X509 se encarga de realizar un fuerte cifrado en todo el tráfico de la infraestructura gracias a una utilidad interna en AWS llamada Transport Layer Security. De esta forma se logra reducir drásticamente la posibilidad de que una vulnerabilidad de un dispositivo IoT sea explotada, además de facilitar la implementación de la solución gracias a las características y facilidades ofrecidas por los servicios de AWS. Es por esto que se decide integrar estas tres alternativas para dar solución al problema.

8. ESPECIFICACIONES DE INGENIERÍA PARA LA SOLUCIÓN

A continuación, se encuentran las especificaciones de la solución elegida, la cual corresponde a un modelo informático representado por una arquitectura de AWS que implementa Certificados Digitales y los servicios Amazon Managed Blockchain y AWS IoT Core.

- La arquitectura permite la conexión de dispositivos IoT con la nube de AWS de forma rápida y sencilla.
- La arquitectura asegura la confidencialidad, integridad y disponibilidad de la información recolectada por los dispositivos IoT aplicando Blockchain.

- La arquitectura cifra el flujo de la información en toda su infraestructura aplicando Certificados Digitales.
- La arquitectura gestiona y administra la información recolectada por los dispositivos IoT.
- La arquitectura es escalable y compatible con cualquier dispositivo IoT.

9. DIMENSIONAMIENTO DE LOS COMPONENTES

A continuación, se definen los componentes necesarios para realizar el diseño de la arquitectura AWS propuesta para dar solución al problema planteado inicialmente:

9.1. MQTT Protocol

El protocolo MQTT es el recomendado para conectar dispositivos IoT, puesto que es un protocolo de transporte de mensajería de publicación / suscripción de cliente-servidor, el cual permite una distribución de mensajes de una a muchos y un desacoplamiento de aplicaciones. Eso lo hace liviano, simple, abierto y fácil de implementar por su diseño. Gracias a estas características es el protocolo es ideal para implementar en comunicaciones de máquina a máquina (M2M) y en conexiones IoT, El protocolo se ejecuta sobre TCP / IP o sobre otros protocolos de red, los cuales brindan conexiones bidireccionales sin pérdidas y ordenadas (Banks y Gupta, 2014). Adicionalmente, la Transport Layer Security (TLS), cifra la conexión entre el dispositivo y el intermediario, garantizando así la confidencialidad del protocolo MQTT (AWS, 2021).

9.2. AWS IoT Core

AWS IoT Core es una plataforma en la nube completamente administrada la cual permite la conexión de dispositivos de manera fácil y segura con las aplicaciones en la nube y con otros dispositivos sin la necesidad de administrar o aprovisionar servidores. Gracias a AWS IoT Core, las aplicaciones tienen la capacidad de hacer un seguimiento de todos los dispositivos y comunicarse en todo momento, aun cuando no estén conectados. Además, AWS IoT Core facilita la utilización de los servicios de AWS, con el fin de crear aplicaciones de IoT que recopilen, analicen, procesen y utilicen los datos generados por los dispositivos conectados facilitando la administración de ninguna infraestructura (AWS, 2021).

9.3. Lambda Function

AWS Lambda es un servicio de informática sin servidor el cual ejecuta código como respuesta a eventos y que también administra de forma automática los recursos informáticos subyacentes. Este servicio de AWS permite ampliar la funcionalidad de otros productos de AWS con lógica personalizada o bien hacer servicios back-end propios que funcionen de manera adecuada con el rendimiento, nivel de seguridad y escala de AWS. AWS Lambda ejecuta código automáticamente en respuesta a varios eventos, como modificaciones realizadas en objetos en buckets de Amazon S3, actualizaciones de tablas de Amazon DynamoDB, transacciones de estado en AWS Step Functions y solicitudes HTTP las cuales permiten conectarse a Amazon API Gateway (AWS, 2021).

9.4. Amazon API Gateway

Amazon API Gateway es un servicio de AWS para la creación, publicación, mantenimiento, monitoreo y protección de API REST, HTTP y WebSocket a cualquier escala. Los desarrolladores pueden crear APIs que accedan a AWS o a otros servicios web, así como los datos almacenados en la nube de AWS, por lo que permite conectar diferentes servicios de AWS aunque se encuentren en redes distintas (Amazon, 2021).

9.5. Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) es un servicio que permite desplegar recursos de AWS en una red virtual aislada de forma lógica que el usuario define. Es posible controlar todos los aspectos del entorno de red virtual, como la selección del rango de direcciones IP, la creación de subredes y la configuración de tablas de enrutamiento y gateways de red. Es posible utilizar tanto IPv4 como IPv6 para la mayoría de los recursos de la nube virtual privada, lo que ayuda a garantizar el acceso seguro y fácil a los recursos y las aplicaciones (Amazon, 2021).

9.6. Application Load Balancer

Un Application Load Balancer es un servicio que distribuye automáticamente el tráfico entrante a través de múltiples destinos, como instancias EC2, contenedores y direcciones IP, en una o más zonas de disponibilidad. Este servicio funciona en la capa de aplicación, la séptima capa del modelo de interconexión de sistemas abiertos (OSI). Una vez que el equilibrador de carga recibe una solicitud, evalúa las reglas de escucha en orden de prioridad para determinar

qué regla aplicar y luego selecciona un objetivo del grupo objetivo para la acción de la regla. Puede configurar reglas de escucha para enrutar solicitudes a diferentes grupos de destino según el contenido del tráfico de la aplicación. También es posible configurar el algoritmo de enrutamiento utilizado en el nivel del grupo de destino. El algoritmo de enrutamiento predeterminado es Round Robin; como alternativa (Amazon, 2021).

9.7. Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona capacidad informática en la nube de forma segura y escalable. Está diseñado para simplificar el uso de la informática en la nube a escala web para los desarrolladores. La sencilla interfaz de servicios web de Amazon EC2 permite obtener y configurar capacidad con una fricción mínima. Proporciona un control completo sobre los recursos informáticos y puede ejecutarse en el entorno informático acreditado de Amazon (Amazon, 2021).

9.8. VPC Endpoint

Un VPC Endpoint es un servicio de AWS que permite establecer conexiones privadas entre una VPC y diferentes servicios de AWS compatibles y los servicios de VPC Endpoint con tecnología de AWS PrivateLink. El tráfico entre una VPC y otro otro servicio no sale de la red de Amazon (Amazon, 2021).

9.9. VPC PrivateLink

AWS PrivateLink es una tecnología que permite acceder a servicios de AWS de forma privada mediante el uso de direcciones IP privadas. Es decir que proporciona conectividad privada entre las VPC, los servicios de AWS y las redes en las instalaciones, sin exponer el tráfico a la internet pública. AWS PrivateLink facilita la conexión de servicios entre diferentes cuentas y las VPC a fin de simplificar radicalmente la arquitectura de la red (Amazon, 2021).

9.10. Amazon Managed Blockchain

Como fue mencionado anteriormente el servicio de Amazon Managed Blockchain también hace parte de los componentes del modelo informático propuesto debido a que su estructura y herramientas permite una implementación rápida y sencilla, además de permitir la creación de aplicaciones y redes donde distintas partes pueden ejecutar transacciones de forma

transparente, escalable y segura, además de compartir los datos sin la necesidad de una autoridad central (AWS, 2021).

10. ANÁLISIS DE COSTOS DEL DISEÑO

La estimación del costo de la gestión y administración del modelo es determinada por los precios que ofrece Amazon debido a que sus componentes son en su mayoría servicios de AWS. Es importante aclarar que AWS cobra solamente por lo que se usa mensualmente sin exigir tarifas mínimas ni uso obligatorio. Es por esto que el valor de la gestión y la administración dependen de lo que necesite el cliente en cuestión del número de dispositivos y la frecuencia de uso durante cada mes. Adicionalmente, es importante resaltar que el costo de implementación debe ser asumido por aquel que decida aplicar este modelo dentro de sus sistemas de información.

A continuación, se encuentran los costos presentados en la página oficial de Amazon en el año 2021 de los servicios de AWS que utiliza el modelo planteado, posteriormente, se presentará una tabla con la estimación total de tres posibles escenarios: el primero con pocos dispositivos, otro con un número medio y otro con muchos dispositivos asociados al modelo.

10.1. Costos AWS IoT Core

10.1.1. Conectividad

El servicio de conectividad de AWS IoT Core ofrece una conexión con autenticaciones y seguridad entre dispositivos y AWS IoT Core. La conectividad se mide en incrementos de 1 minuto y se basa en el tiempo total de conexión de los dispositivos a AWS IoT Core (AWS, 2021).

- El precio del servicio de conectividad es de: 0,08 USD (por millón de minutos de conexión).

10.1.2. Registro y sombra de dispositivos

AWS IoT Core ofrece la sombra de dispositivos, la cual almacena el estado deseado o real de un dispositivo, adicionalmente, el registro que se ofrece se utiliza para nombrar y administrar los dispositivos. El uso de ambos servicios se mide en función de la cantidad de operaciones que acceden a la sombra del dispositivo o a los datos del

registro o a los cambios. Las operaciones de sombra del dispositivo y registro se miden en incrementos de 1 KB del tamaño del registro de ambos servicios. Por ejemplo, una actualización a un registro de sombra de dispositivos de 1.5 KB se computa como dos operaciones (AWS, 2021).

- El precio del servicio registro y sombra del dispositivo es de: 1,25 USD (por millón de operaciones).

10.1.3. Motor de reglas

AWS IoT Core cuenta con un motor de reglas, el cual le permite transformar datos de dispositivos mediante el uso de operaciones aritméticas o funciones externas, como AWS Lambda y después direccionar los datos a un servicio de AWS como Amazon Kinesis, Amazon S3 o Amazon DynamoDB. El uso de este servicio se mide cada vez que se activa una regla y en función de la cantidad de acciones ejecutadas dentro de una regla, con un mínimo de una acción por regla. Las reglas y las acciones se miden en incrementos de 5 KB del tamaño de mensaje. Por ejemplo, una regla que procese un mensaje de 5 KB y no ejecute ninguna acción se computa como una regla y una acción, mientras que una regla que procese un mensaje de 8 KB y ejecute dos acciones se computa como dos reglas y cuatro acciones (AWS, 2021).

- Los precios del servicio de motor de reglas son:
  - Para reglas activadas: 0,15 USD (por millón de reglas activadas o de acciones ejecutadas).
  - Para acciones ejecutadas: 0,15 USD (por millón de reglas activadas o de acciones ejecutadas).

10.2. Costos AWS Lambda

AWS Lambda ofrece dos precios distintos:

- Precio por solicitudes: 0,20 USD por in millón de solicitudes.
- Precio por duración: 0,0000166667 USD por cada GB/segundo.

El precio para la duración se calcula según el volumen de memoria asignado a la función. A esta se le puede asignar cualquier volumen de memoria desde los 128 MB a los 10.240 MB en

incrementos de 1 MB. La tabla que se muestra a continuación contiene algunos ejemplos del precio por cada 1 ms asociado con distintos volúmenes de memoria (AWS, 2021).

Tabla 2

Costos AWS Lambda

Memoria (MB)	Precio por 1 MS
128	0,0000000021 USD
512	0,0000000083 USD
1024	0,0000000167 USD
1536	0,0000000250 USD
2048	0,0000000333 USD
3072	0,0000000500 USD
4096	0,0000000667 USD
5120	0,0000000833 USD
6144	0,0000001000 USD
7168	0,0000001167 USD
8192	0,0000001333 USD
9216	0,0000001500 USD
10240	0,0000001667 USD

10.3. Costos Amazon API Gateway (API REST)

De las opciones que ofrece API Gateway solo se usará el API REST para este modelo, el cual solo se tendrá que pagar por las llamadas que la API reciba y el volumen de datos de salida transferido, aunque las API privadas no producen cargos por la transferencia de datos salientes. No obstante, los cargos de AWS Private Link se aplican cuando se utilizan API privadas en API Gateway. API Gateway de igual forma proporciona un almacenamiento de datos en caché opcional, que se cobra de acuerdo con la tarifa por hora y en función del tamaño de la caché que se seleccione. En el caso de las API REST, la capa gratuita de API Gateway incluye un millón de llamadas a API al mes durante un máximo de 12 meses (AWS, 2021).

Tabla 3

Costos Amazon API Gateway

Número de solicitudes (por mes)	Precio (por millón)
Primeros 333 millones	3,50 USD
Próximos 667 millones	2,80 USD
Próximos 19 mil millones	2,38 USD
Más de 20 000 millones	1,51 USD

10.4. Costos de AWS Application load balancer

Para AWS Application load balancer el precio se cobra cada hora u hora parcial que se ejecute ALB y la cantidad de unidades de capacidad de balanceo de carga (LCU) usadas por hora (AWS, 2021).

- Los precios para los balanceadores de carga de aplicaciones de la región de AWS son:
    - 0,0225 USD por hora de balanceador de carga de aplicaciones (u hora parcial).
    - 0,008 USD por hora de LCU (u hora parcial).
- Los precios para los balanceadores de carga de aplicaciones de Outposts son:
    - 0,0225 USD por hora de balanceador de carga de aplicaciones (u hora parcial).
    - 0,00 USD por hora de LCU (u hora parcial).

10.5. Costos AWS PrivateLink

Con AWS PrivateLink se pueden crear puntos de enlace para habilitar la conectividad privada a un servicio que pertenezca a AWS o bien a un cliente o socio de AWS. El precio del costo se hará por cada hora que el punto de enlace de la VPC siga aprovisionado en cada zona de disponibilidad, independientemente del estado de su asociación con el servicio (AWS, 2021). AWS PrivateLink maneja los diferentes costos dependiendo de qué punto de enlace se usa, los cuales son:

Puntos de enlace de interfaz:

Los puntos de enlace de interfaz se pueden utilizar para acceder de manera privada y segura a servicios como los de AWS, los servicios de aplicaciones internas o los servicios SaaS que se desarrollen fuera de su VPC (AWS, 2021). Sus precios se manejan de la siguiente manera:

- Precio por punto de enlace de la VPC por zona de disponibilidad (USD/hora): 0,01 USD.
- Precio por GB de datos procesado (USD): 0,01 USD.

Puntos de enlace del balanceador de carga de portal:

Los puntos de enlace del balanceador de carga de portal se pueden utilizar para introducir de manera segura y privada servicios de red y seguridad, tales como cortafuegos, detectores de intrusos y sistemas de prevención, vigilancia, análisis y otros que se desarrollen fuera del flujo de tráfico de su VPC (AWS, 2021). Sus correspondientes precios son:

- Precio por punto de enlace de la VPC por zona de disponibilidad (USD/hora): 0,01 USD.
- Precio por GB de datos procesado (USB): 0,0035 USD.

Tabla 4

Costos AWS PrivateLink

Servicio	Precio por punto de enlace de la VPC por zona de disponibilidad (USD/hora)	Precio por GB de datos procesado (USD)
Puntos de enlace de interfaz	0,01 USD	0,01 USD
Puntos de enlace del balanceador de carga de portal	0,01 USD	0,0035 USD

10.6. Costos Amazon Managed Blockchain para Hyperledger Fabric

La red de Blockchain administrada para Hyperledger Fabric consta de uno o más miembros, y cada miembro tiene nodos pares con almacenamiento local, además de tener la capacidad de escribir datos en la red. Los aspectos que se cobran son: la membresía de la red, nodos bajo demanda, el almacenamiento del nodo y los datos escritos en la red. Los costos asociados con los componentes de red compartidos se incluyen en la tarifa de membresía de red por hora, que se factura por segundo (AWS, 2021). A continuación, se muestran los precios manejados en Amazon Managed Blockchain para Hyperledger Fabric.

10.6.1. Membresía

La membresía en una red Managed Blockchain para Hyperledger Fabric es equivalente a una organización Hyperledger Fabric. Esta organización autentica y autoriza las identidades individuales para la participación en la red. La tarifa de membresía incluye una autoridad de certificación (CA) de Hyperledger Fabric y otros

costos de red compartidos. Una sola cuenta de AWS puede crear varios miembros (AWS, 2021). El precio de la membresía en su edición estándar es:

- Tasa de membresía: 0,55 USD por hora.

10.6.2. Nodos bajo demanda (EC2)

Los precios bajo demanda permiten pagar por segundo por los nodos pares de Blockchain que se creen, con un mínimo de 1 minuto. Esto libera el costo y la complejidad de planificar y comprar capacidad de nodos pares por adelantado antes de sus necesidades. Los precios se manejan por horas y dependen del tipo de instancia que se use (AWS, 2021). Dichos precios son los siguientes:

Tabla 5

Instancias de EC2 para para Hyperledger Fabric

Tipo de instancia	Precio por hora (USD)
bc.c5.2xlarge	0,544 USD
bc.c5.4xlarge	1,088 USD
bc.c5.large	0,136 USD
bc.c5.xlarge	0,272 USD
bc.m5.2xlarge	0,617 USD
bc.m5.4xlarge	1,229 USD
bc.m5.large	0,154 USD
bc.m5.xlarge	0,307 USD
bc.t3.large	0,134 USD
bc.t3.medium	0,067 USD
bc.t3.small	0,034 USD
bc.t3.xlarge	0,267 USD

10.6.3. Almacenamiento de nodos de pares

El almacenamiento de nodos de pares se escala elásticamente para almacenar el libro mayor de la cadena de bloques y las aplicaciones de código de cadena. El almacenamiento del nodo del mismo nivel se cobra en incrementos de GB por mes (AWS, 2021). El precio de la tasa de almacenamiento es el siguiente:

- Tasa de almacenamiento: 0,10 USD por GB al mes.

10.6.4. Datos escritos

Los datos escritos es la cantidad de datos que el usuario (por ejemplo, una membresía) ha escrito en la red Hyperledger Fabric. Esto incluye el tamaño completo de la carga útil de cada transacción que se crea en la red (AWS, 2021). El precio de la tasa de almacenamiento es el siguiente:

- Tasa de almacenamiento: 0,10 USD por GB al mes.

A continuación se encuentra una tabla correspondiente a los costos estimados para cada uno de los servicios de AWS en tres diferentes escenarios determinados por rangos específicos en relación a la cantidad de dispositivos activos que se incluyan dentro de la implementación del modelo, debido a la metodología de cobro de AWS. Para determinar estos costos, se utilizó la herramienta ofrecida por AWS, que permite calcular y simular el costo de sus servicios según el número de dispositivos vinculados y la cantidad de peticiones y acciones que se realicen durante un mes. En el caso de las peticiones, se utilizó una estimación estándar, en la que cada dispositivo realiza en promedio 1 petición cada hora durante el día y 1 petición cada 2 horas durante la noche, por lo que se mantiene conexión con el modelo de forma segura durante las 24 horas del día los 30/31 días del mes.

Tabla 6

Costos por posibles escenarios

Cantidad	Servicio	De 5 a 25 dispositivos	De 25 a 50 dispositivos	De 50 a 100 dispositivos
1	**AWS IoT Core**	0,50 USD a 2,53 USD	2,53 USD a 5,04 USD	5,04 USD a 10,07 USD
2	**AWS Lambda Function**	0 USD a 6,83 USD	6,83 USD a 20,45 USD	20,45 USD a 47,78 USD
1	**Amazon API Gateway**	0,57 USD a 2,83 USD	2,83 USD a 5,67 USD	5,67 USD a 11,34 USD
1	**Application Load Balancer**	22,27 USD	22,27 USD	22,27 USD
1	**EC2 y Amazon Managed Blockchain**	30,61 USD	35,72 USD	40,06 USD
1	**Virtual Private Cloud (VPC, VPC Endpoint y VPC Private Link)**	21,90 USD	21,90 USD	21,90 USD

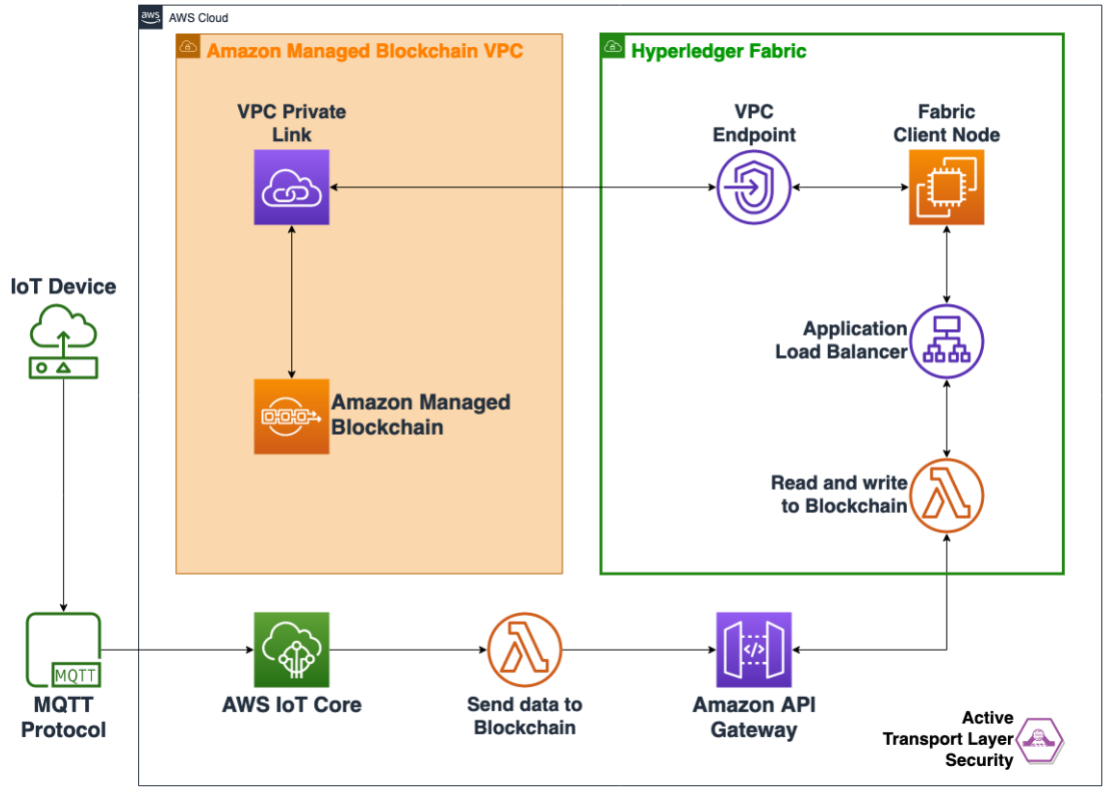
TOTAL	***75,85 USD a 90,97 USD***	***98,91 USD a 131,5 USD***	***135,84 USD a 201,2 USD***

11. PROTOTIPADO O DISEÑO CONCEPTUAL

A continuación, se encuentra el modelo que integra las tres soluciones escogidas anteriormente, representado por el diseño de una arquitectura de AWS:

Ilustración 1

Modelo informático



El flujo de este modelo es el siguiente:

1	El dispositivo IoT (***IoT Device***) obtiene los datos correspondientes.	
2	Luego, los datos recolectados por el dispositivo IoT son enviados a AWS a través del protocolo MQTT (***MQTT Protocol***).	
3	Posteriormente, el servicio ***AWS IoT Core*** recibe los datos del dispositivo IoT de forma segura.	
4	Después, la ***Función Lambda*** "*Send data to Blockchain*" ejecuta un código que serializa los datos y los envía hacia la VPC llamada Hyperledger Fabric mediante una Amazon API Gateway.	

5	Luego, el servicio ***Amazon API Gateway*** permite la creación, publicación, mantenimiento y monitoreo de la API RESTful que permite la comunicación con la VPC Hyperledger Fabric.	
6	Posteriormente, la ***Función Lambda*** "*Read and write to Blockchain*" ejecuta un código que lee la información enviada por el Amazon API Gateway y lo envía a un balanceador de cargas para efectuar la creación del nuevo nodo de la cadena de bloques.	
7	Después, el ***Application Load Balancer*** se encarga de distribuir el tráfico de la aplicación para aumentar la disponibilidad de la aplicación.	
8	Luego, en la instancia del ***EC2***, se ejecuta la creación del nuevo nodo que se unirá a la red de bloques.	
9	Seguido a esto, desde la instancia del EC2 se envían los datos correspondientes al nodo creado hacia la VPC donde se encuentra la red de Blockchain a través de una conexión privada establecida mediante un ***VPC Endpoint***.	
10	Posteriormente, el servicio de ***VPC Private Link*** se encarga de leer los datos del nuevo nodo de la red de forma segura.	
11	Finalmente, el servicio de ***Amazon Managed Blockchain*** obtiene los datos del nuevo nodo a partir del VPC Private Link y lo incluye dentro de la red de bloques.	
12	Durante todo el flujo, AWS se encarga de realizar el cifrado de los datos en tránsito mediante el ***Transport Layer Security***, el cual utiliza un certificado digital.	

12. CONCLUSIONES

En conclusión, es posible afirmar que algunas de las soluciones informáticas planteadas en este proyecto, presentaban dificultades en su implementación debido a su alta complejidad mientras que otras no ofrecían un nivel de seguridad óptimo, sin embargo, otras soluciones ofrecían altos niveles de seguridad al utilizar el Blockchain como componente principal, la

tecnología con mejor fama en el mercado sobre su efectividad en cuanto a ciberseguridad respecta.

Es por esto que se seleccionaron las tres mejores alternativas, en las que se incluye el Blockchain, para dar solución al problema, además, gracias a su compatibilidad y capacidad de componer una mejor solución, fue posible integrar estas tres soluciones en un solo modelo informático escalable, fácil de implementar y capaz de proporcionar un alto nivel de seguridad de la información presente en la red de los dispositivos conectados mediante el internet de las cosas (IoT).

No obstante, la ciberdelincuencia ha sido un problema que ha aumentado durante los últimos años, al igual que las soluciones de ciberseguridad, por lo que, además de seguir mejorando este modelo propuesto, es necesario continuar investigando acerca de la seguridad en los dispositivos IoT para fortalecer progresivamente los nuevos sistemas y tecnologías modernas.

13. RECOMENDACIONES

Las recomendaciones a tomar en cuenta respecto a este proyecto son:

- Por limitaciones de tiempo y dificultades vividas en el momento de desarrollo de este proyecto (año 2021) el modelo no fue probado y se limita únicamente a un planteamiento que debe ser simulado y analizado.
- Este modelo es solamente un planteamiento, por lo que no está cerrado a cambios o actualizaciones, si se identifica una posibilidad de mejora o expansión se puede hacer libremente.
- Como se mencionó en el análisis de costos, el valor del mismo depende de las necesidades del cliente, por lo que es necesario hacer un análisis previo de los dispositivos IoT y red a implementar antes de aplicar este modelo.

14. LISTA DE REFERENCIAS

Abhishek Mairh, Debabrat Barik, Kanchan Verma, and Debasish Jena. (2011). *Honeypot in network security: a survey. In Proceedings of the 2011 International Conference on Communication*, Computing & Security. Association for Computing Machinery, New York, NY, USA, 600–605. Recuperado de https://doi.org/10.1145/1947940.1948065

A. Calvo. (2018). *Seguridad en internet de las cosas: firmwares, vulnerabilidades y riesgos en la rapidez del desarrollo y consumo de internet of things*. Recuperado de http://hdl.handle.net/10609/89625

Mohammed M. Alani. (2018). *IoT Lotto: Utilizing IoT Devices in Brute-Force Attacks. In Proceedings of the 6th International Conference on Information Technology: IoT and Smart CityAssociation for Computing Machinery,* New York, NY, USA, 140–144. Recuperado de https://doi.org/10.1145/3301551.3301606

AWS. (2020). *Amazon IoT Core*. Recuperado de https://aws.amazon.com/es/iot-core/

AWS. (2020). *Amazon Managed Blockchain*. Recuperado de https://aws.amazon.com/es/managed-blockchain/

AWS. (2020). *Blockchain en AWS*. Recuperado de https://aws.amazon.com/es/blockchain/

AWS. (2021). *Precios de AWS IoT Core*. Recuperado de https://aws.amazon.com/es/iot-core/pricing/

AWS. (2021). *Precios de AWS Lambda*. Recuperado de https://aws.amazon.com/es/lambda/pricing/

AWS. (2021). *Precios de Amazon API Gateway*. Recuperado de https://aws.amazon.com/es/api-gateway/pricing/

AWS. (2021). *Precios de Elastic Load Balancing*. Recuperado de https://aws.amazon.com/es/elasticloadbalancing/pricing/

AWS. (2021). *Precios de AWS PrivateLink*. Recuperado de https://aws.amazon.com/es/privatelink/pricing/

AWS. (2021). *Precios de Amazon Managed Blockchain para Hyperledger Fabric*. Recuperado de https://aws.amazon.com/es/managed-blockchain/pricing/hyperledger/

AWS. (2021). *Características de AWS Lambda*. Recuperado de https://aws.amazon.com/es/lambda/features/

AWS. (2021), *Documentación de AWS IoT Core.* Recuperado de https://docs.aws.amazon.com/es_es/iot/?id=d

AWS. (2020). *¿Qué es una base de datos relacional?*. Recuperado de https://aws.amazon.com/es/relational-database/

AWS. (2021), *Amazon API Gateway Guía del desarrollador*. Recuperado de https://docs.aws.amazon.com/es_es/apigateway/latest/developerguide/welcome.html

AWS. (2021), *AWS IoT Core*. Recuperado de https://aws.amazon.com/es/iot-core/

AWS. (2021), *Amazon Virtual Private Cloud.* Recuperado de https://aws.amazon.com/es/vpc/?vpc-blogs.sort-by=item.additionalFields.createdDate&vpc-blogs.sort-order=desc

AWS. (2021), *MQTT*. Recuperado de https://docs.aws.amazon.com/iot/latest/developerguide/mqtt.html

AWS. (2021), *Elastic Load Balancing Application Load Balancers*. Recuperado de https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html

AWS. (2021), *Amazon EC2.* Recuperado de https://aws.amazon.com/es/ec2/

AWS. (2021), *Amazon VPC Endpoint.* Recuperado de *https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints.html*

AWS. (2021), *Amazon PrivateLink.* Recuperado de https://aws.amazon.com/es/privatelink/

Cisco. (2020). *¿Qué es Wi-Fi?*. Recuperado de https://www.cisco.com/c/es_mx/products/wireless/what-is-wifi.html

Cisco. (2020). *Ethernet.* Recuperado de https://www.cisco.com/c/en/us/tech/lan-switching/ethernet/index.html

Crawford, D. (2001) *A process control approach to cyber attack detection*. 44, 8, Communications of the ACM, 76–82. Recuperado de https://doi.org/10.1145/381641.381662

Donohue, B (2014). *¿Qué es un Hash y cómo funciona?*. Recuperado de https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/#:~:text=10%20Abr%202014-,Una%20funci%C3%B3n%20criptogr%C3%A1fica%20hash%2D%20usualmente%20conocida%20como%20%E2%80%9Chash%E2%80%9D%2D,tendr%C3%A1%20siempre%20la%20misma%20longitud.

G. Becker. (2018). *Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis*. Recuperado de https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/becker_1.pdf

Google Cloud. (2021). *Cloud IoT Core*. Recuperado de https://cloud.google.com/iot-core/?&utm_source=google&utm_

INCIBE. (2015). *¿Qué hacen los ciberdelincuentes con los datos robados?*. Recuperado de https://www.incibe.es/protege-tu-empresa/blog/que-hacen-los-ciberdelincuentes-con-los-datos-robados

INTERPOL. (2020). *Los ataques cibernéticos no conocen fronteras y evolucionan a gran velocidad.* Recuperado de https://www.interpol.int/es/Delitos/Ciberdelincuencia

Joint Task Force on Cybersecurity Education. (2018). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Association for Computing Machinery, New York, NY, USA.

Kaspersky. (2019). *Kaspersky detecta más de 100 millones de ataques a dispositivos inteligentes en el primer semestre de 2019*. Recuperado de https://latam.kaspersky.com/about/press-releases/2019_kaspersky-detecta-ms-de-100-millones-de-ataques-a-dispositivos-inteligentes-en-el-primer-semestre-de-2019

Kaspersky. (2020). *Más información sobre el malware y cómo proteger todos tus dispositivos*. Recuperado de https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

Kaspersky. (2020). *¿Qué es un botnet?*. Recuperado de https://www.kaspersky.es/blog/que-es-un-botnet/755/

Kaspersky. (2021). *Detección de malware y exploits*. Recuperado de https://latam.kaspersky.com/resource-center/preemptive-safety/antivirus-malware-detection

L. Tudela (2019), *Arquitectura blockchain para la securización de dispositivos iot mediante smart contracts*. Tesis de grado, Universidad de Vigo. Pontevedra.

McAfee. (2020). *¿Qué es malware?*. Recuperado de https://www.mcafee.com/es-co/antivirus/malware.html

Microsoft Azure. (2020). *Introducción a la seguridad de IoT*. Recuperado de https://azure.microsoft.com/es-es/overview/internet-of-things-iot/iot-security-cybersecurity/

Ministerio de modernización de Argentina. (2020). *Internet de las Cosas.* Recuperado de https://www.argentina.gob.ar/sites/default/files/paperbenchmarkinternacional-iot.pdf

MinTIC. (2013). *Decreto número 1377 de 2013*. Recuperado de https://www.mintic.gov.co/arquitecturati/630/articles-9011_documento.pdf

Morales Suárez, A., Díaz Ávila, S. and Leguizamón Páez, M., 2019. Mecanismos de seguridad en el internet de las cosas. Revista vínculos, 16(2), pp.288-297.

Oracle. (2020). *¿Qué es IoT?* Recuperado de https://www.oracle.com/co/internet-of-things/what-is-iot.html

Peña, E. (2018). *La seguridad del IoT desde una perspectiva de enfoque nacionalización*. Bogotá, Colombia. Recuperado de https://repository.unimilitar.edu.co/bitstream/handle/10654/32074/Pe%c3%b1aOrtizEdgarAlberto2019.pdf?sequence=2&isAllowed=y

Perez L. (2019). *Guía de buenas prácticas en torno a la seguridad de IoT para las smart house* (Doctoral dissertation). Recuperado de http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/2473/1/32696.pd

R. Gupta and A. Banks (2014). Estándar OASIS MQTT Versión 3.1.1. Recuperado de http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

Salazar, J.; Silvestre, S. (2019) *Internet de las cosas*. Techpedia. České vysoké učení technické v Praze Fakulta elektrotechnická. Recuperado de https://upcommons.upc.edu/bitstream/handle/2117/100921/LM08_R_ES.pdf

Singleton, T. (2002). *Managing Distributed Denial-Of-Service Attacks*, EDPACS, 30:5, 7-20. Recuperado de 10.1201/1079/43288.30.5.20021101/39237.2

Tudela Díaz, L (2019). *Arquitectura Blockchain para la securización de dispositivos IoT mediante Smart Contracts*. Recuperado de http://castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/345/TFG%20Iago%20Tudela%20D%C3%ADaz.pdf?sequence=1&isAllowed=y

Varshney, R.; Vogel, B. (2018) *Towards Designing Open and Secure IoT Systems: Insights for Practitioners*, Association for Computing Machinery, Santa Barbara, Estados Unidos.

Vélez Pérez, A (2019). *Arquitecturas de referencia para IoT con transferencia segura de información*. Recuperado de https://repository.unad.edu.co/bitstream/handle/10596/27648/avelezpe.pdf?sequence=4&isAllowed=y

Vinton G. Cerf. (2016). *Prospects for the internet of things*. 22, 2 (Winter 2015), 28–31. Recuperado de https://doi.org/10.1145/2845145