UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:
ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:
ESTUDIO DE MECANISMOS DE CIBERSEGURIDAD PARA ASEGURAR LAS COMUNICACIONES EN INTERNET DE LAS COSAS INDUSTRIAL IOT.

AUTORES:
ANDERSON SEBASTIÁN GARZÓN POZO
KELLY VIVIANA REYES ROSAS

DIRECTOR:
JUAN CARLOS DOMÍNGUEZ AYALA

CUENCA – ECUADOR
2023

Autores:

Anderson Sebastián Garzón Pozo
Ingeniero Electrónico.
Candidato a Magíster en Seguridad de la Información por laUniversidad Politécnica Salesiana – Sede Cuenca.
agarzonp@est.ups.edu.ec

Kelly Viviana Reyes Rosas
Ingeniera en Sistemas, mención Telemática.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
kreyesr3@est.ups.edu.ec

Dirigido por:

Juan Carlos Domínguez Ayala
Ingeniero en Sistemas.
Magister en Redes de Comunicaciones.
jdominguez@ups.edu.ec

Estudio de mecanismos de ciberseguridad para asegurar las comunicaciones en internet de las cosas industrial IoT.

DEDICATORIA

Dedicado a mi madre Carmen Alicia Pozo Chamorro, porque su apoyo siempre será primordial para cada meta lograda.

Y a los investigadores afines a encontrar modelos, servicios y productos que contribuyen al a fortalecer la seguridad de las comunicaciones y que a través de este aporte se pueda aterrizar en sistemas sólidos de protección prácticos.

Anderson Sebastian Garzón Pozo

AGRADECIMIENTO

Agradezco a mi madre y padre por su apoyo incondicional para alcanzar un objetivo más en la vida, que, con sabiduría, enfoque y en compañía de Dios se culmina satisfactoriamente este proceso.

También a las personas que ha formado parte en el desarrollo de este artículo Docentes, tutor, dirección de la maestría y mi compañera y colega Kelly Reyes que han contribuido con sus conocimientos, consejos y premisas que han sido un aporte valioso para alcanzar los resultados esperados.

Anderson Sebastian Garzón Pozo

AGRADECIMIENTO

Con este trabajo quiero agradecer principalmente a Dios por permitirme haber llegado hasta este momento tan importante de mi formación, a toda mi familia y de manera muy especial a mi madre y mis abuelitos por el cariño y apoyo brindado en todo momento.

A los docentes quienes conforman la Maestría en Seguridad de la Información de la Universidad Politécnica Salesiana.

Y de manera especial, al Mgtr.Juan Carlos Domínguez Ayala director de Tesis por la guía en el desarrollo de este artículo de titulación, por su tiempo, dedicación y predisposición para ayudar en la elaboración del presente proyecto.

Kelly Viviana Reyes Rosas.

Tabla de Contenido

Estudio de mecanismos de Ciberseguridad para asegurar las comunicaciones en Internet de las cosas Industrial IoT.

Autor(es):

Anderson Sebastian Garzón Pozo

Kelly Viviana Reyes Rosas

Resumen

Teniendo en cuenta los ecosistemas que existen en IoT, los cuales permiten la integración e interconexión de múltiples dispositivos, que se encargan de recopilar, procesar información y emitir órdenes para la automatización de tareas programadas por los usuarios, a través de una red de datos.

Generalmente, estas implementaciones no cumplen con todos los estándares o mecanismos de seguridad necesarios en sus dispositivos que distribuyen para su consumo; por lo que esto aumenta significativamente el umbral de riesgo de seguridad, creando una puerta de acceso a la información a personas no autorizadas.

El objetivo principal de este trabajo es estudiar los diversos Mecanismos y estrategias de Ciberseguridad para asegurar las comunicaciones en Internet de las cosas Industrial IoT existentes. Con base en los análisis realizados, se pretende presentar una propuesta de uno de estos mecanismos.

Toda la información recopilada de diversos medios contribuyó a establecer una propuesta de un mecanismo de ciberseguridad para la industria agrícola.

Palabras clave:

Mecanismos, blockchain, ciberseguridad, Edge computing, internet de las cosas (IOT), industria 4.0

Abstract

Considering the ecosystems that exist in IoT, which allow for the integration and interconnection of multiple devices, that collect, process information, and issue orders for the automation of tasks programmed by users, through a data network.

These implementations do not comply with all the necessary security standards or mechanisms in the devices they distribute for consumption, which significantly increases the security risk threshold, creating a gateway for unauthorized access to information.

The main objective of this work is to study the various mechanisms and cybersecurity strategies to ensure communications in existing Industrial IoT systems. Based on the analyses conducted, the aim is to present a proposal for oneof these mechanisms.

All the information collected from various sources contributed to establishing a proposal for a cybersecurity mechanism for the agricultural industry.

Palabras clave:

Mechanisms, blockchain, cybersecurity, edge computing, Internet of Things (IoT), Industry 4.0.

1. Introducción

El internet ha logrado una gran revolución en cuanto a las comunicaciones hasta el punto de llegar a convertirse en un medio de comunicación global, ya que diversos dispositivos electrónicos se conectan, recopilan y comparten todo tipo de información a través de él, en la actualidad el internet de las cosas (IoT), ha cobrado gran fuerza dentro del mundo de la tecnología, ya que brinda la facilidad para que la mayoría de dispositivos electrónicos cuenten con la capacidad de conectarse a internet, establecer un medio de comunicación entre dispositivos conectados y permitir a los usuarios el acceso a ellos desde cualquier parte.

En el transcurso de las últimas décadas, las redes IoT han marcado un nuevo paradigma dentro de la computación y la ciberseguridad, debido a su rápida integración con la infraestructura de los diferentes sectores industriales, como lo es el caso de la agroindustria que día a día incorpora nuevas soluciones para el tratado de sus datos, con lo cual se crean nuevas oportunidades para accesos maliciosos hacia los mismos, todo esto con el fin de poder obtener información de los datos de producción, lo cual puede llegar a generarles a los ciberdelincuentes ganancias significativas, ya que este es un sector sumamente importante dentro de la economía.

Por lo que, a la hora de implementar técnicas inteligentes dentro de este entorno se debe contemplar varios aspectos en cuanto a definir o establecer mecanismos para poder mitigar los riesgos existentes que conlleva dicho desarrollo, que va desde la implantación de políticas que se incorpora la ciberseguridad hasta contar con tecnologías avanzadas para el área.

2. Determinación del Problema

En la actualidad, el internet de las cosas (IoT) ha cobrado especial importancia ya que esta tecnología ofrece varios beneficios. Dentro de ella, se puede observar el impacto que tiene dentro del área industrial con la proliferación de dispositivos integrados en este entorno, en el cual existen una gran cantidad de soluciones para automatizar los procedimientos como lo menciona [1].

Es por ello por lo que al hablar de IoT no solo se refiere a la captura de datos mediante los diferentes tipos de sensores conectados, los cuales se encargan de la captura, transmisión y el manejo de datos para así poder darles un valor, de tal manera que dentro del proceso de la toma de decisiones se realice de forma automática y ágil.

Hoy en día, Ecuador ha implementado IoT para las industrias ya sea dentro del área agrícola, ganadera, entretenimiento, industria 4.0, entre otras, las cuales utilizan miles de dispositivos inteligentes y sensores para la automatización de sus procesos, con los que se pueden controlar aspectos dentro del proceso de fabricación, desde la línea de producción hasta la protección del entorno operativo, al usar esta tecnología los fabricantes pueden llegar a reducir de forma considerable los costos de operación.

Sin embargo, IoT presenta algunos desafíos como las múltiples amenazas en cuanto a seguridad, por lo que se debe contar con una infraestructura de seguridad bien diseñada que permita mitigar las vulnerabilidades y amenazas que podrían ocasionar daños considerables a los activos e información de las organizaciones.

3. Marco teórico referencial

Ante el aumento de componentes IoT conectados a internet también aumenta los problemas de ciberseguridad para las empresas, donde la violación a la seguridad evoluciona y el reto para los departamentos de seguridades (SOC) es prepararse para enfrentar los ciberataques.

Los dispositivos y su comunicación son un elemento vulnerable en la seguridad por tener desventajas como: interfaces inseguras, capacidades de seguridad débiles, servicios de red inseguros, heterogeneidad. Esto implica la manipulación de dispositivos, robo o alteración de datos, secuestro del dispositivo y ataques DDoS (denegación de servicios distribuidos) logrando afectar la infraestructura de la cual forman parte dichos componentes como lo indica [1].

De acuerdo con [2], entre los medios utilizados para la comunicación existe LoRaWAN, RFID, Wi-Fi, Zigbee, bluetooth, etc. En el caso del primero tiene operativos 100 millones en el mundo y se espera al 2023 alcancen a los 730 millones de dispositivos LoRaWAN conectados, donde su principio de funcionamiento es empleando puertas de enlace por medio de LoRaWAN y estas a su vez se comunican con un servidor de red con protocolos TCP/UDP.

Los servidores de red son los enrutadores y responsables de autenticación y autorización, sin embargo, el rol de estos se encuentra propenso a ataques de denegación de servicio (DoS (denegación de servicio)) contra dispositivos y servidores de red.

3.1 Medios de transmisión inalámbrica

Como lo señala [3], los medios de comunicación inalámbricos son aquellos que emplean ondas electromagnéticas para enviar la información por medio del aire, usando transmisión y recepción por medio de antenas, es un método único para cubrir interconexiones en grandes extensiones como cultivos, zonas de difícil acceso con cableado, entre otras.

Sin embargo, este medio es susceptible a cambios climáticos y a la falta de seguridad durante el proceso de comunicación entre los elementos que conforman la red.

Existen diferentes medios de transmisión inalámbrica los cuales se pueden clasificar según su cobertura, estándares y tecnologías que manejan sus marcas, como se observa la figura 3.

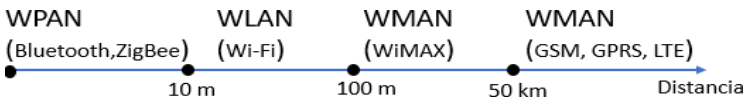

Figura 1 Tipos de redes inalámbricas [4]

3.1.1 Mecanismos de autenticación

Para el proceso de autenticación en los dispositivos IoT, tanto para la capa de negocio como la de red pueden llegar a estar de una u otra forma ligada entre sí, todo esto dependerá del diseño para lo cual puede basarse en el nivel de sensibilidad de la seguridad o en el proveedor de servicios.

3.1.2 Mecanismos en cifrado en IoT

Usualmente la capa de red emplea el mecanismo de encriptación salto a salto, el cual asegura que la información este encriptada en el transcurso de la transmisión, dicha información se encuentra en texto plano en cada nodo, por lo que continuamente requiere ser encriptada y descifrada dentro de cada nodo.

Mientras que el mecanismo end-to-end encryption (E2EE (end to end encryption)) en la capa de servicio garantiza que la información se encuentra en texto cifrado a lo largo de toda la transmisión y en los nodos de reenvío.

3.1.3 Protocolos de conexiones

Como indica [5], durante los últimos años no ha existido una restricción en cuanto al uso de un único protocolo, o su vez en una reducción del grupo de protocolos empleados, por lo contrario, existen en la actualidad una gran cantidad de protocolos que son utilizados para la automatización industrial.

Con la llegada de IoT los protocolos como fieldbus que eran usados para la implementación de sistemas complejos como el caso de SCADA, el cual involucra tanto conexiones PLCs (Programable LogicControllers), PIV (Proportional Integral-Derivative) como actuadores y actuadores que se encuentran conectados mediante el fieldbus.

3.2 Seguridad en IoT

Los componentes de IoT, se encuentran en constante recolección de datos y a su vez se intercambia la información hacia internet, donde participan 3 elementos como son:

3.2.1 Seguridad de dispositivos

Según [6], la ocupación de los componentes conectados en internet cada vez va en aumento, siendo millones de estos quienes captan información por medio de portales web, aplicativos o servicios, por lo que incrementa los puntos de ataques tanto desde su origen hasta el destino.

3.2.2 Seguridad en la nube

Los datos que se almacenan en la nube requieren de cierta seguridad al ser información crítica y a su vez se procesa un gran volumen de información, que, recibida de los componentes conectados hacia estas bases de datos, se ven susceptibles ante posibles amenazas internas de la organización y su entorno.

3.2.3 Seguridad en las redes inalámbricas

Otro de los medios expuestos a los ciberataques son los medios de transmisión, que a pesar de existir diferentes protocolos de seguridad y sistemas de detección de intrusos (IDS); como lo indica [7], esto no garantiza una seguridad total, sin embargo, puede reducir el impacto al definir correctamente su aplicación.

3.3 Tecnologías empleadas para IIoT

3.3.1 Tecnología bluetooth

Como plantea [8], esta tecnología en la actualidad es una de las más empleadas para las comunicaciones inalámbricas entre dispositivos como: sensores, Gateway, módulos de

transferencia de datos, aplicaciones de corto alcance y pequeños proyectos que requieran trabajar en la banda de ISM 2.4 GHz, ya que al no requerir de licencia para su libre uso y ser considerada segura, debido a que cuenta con un enlace codificado y protegido ante pérdidas e interferencias.

3.3.2 Tecnología Zigbee

Citando a [9], Zigbee Alliance fue creada para aplicaciones en edificaciones y su automatización, en las que están la medicina, recolección de datos en invernaderos, automatización industrial, lectura de instrumentos de servicios, sistemas de riego, control de iluminación, etc. Por lo que se podría definir como una tecnología de corto alcance y de bajo uso de energía.

3.3.3 Tecnología LoRaWAN

De acuerdo con [10], este protocolo de red de largo alcance y bajo consumo, es utilizado por la tecnología Lora, lo que faculta la interconexión con dispositivos inteligentes sin que exista la exigencia de instalaciones a nivel local, adicionalmente brinda una mayor libertad de uso para los usuarios finales.

LoRa Alliance está compuesto por las siguientes capas del modelo, dentro de ellas la empresa Semtech, es la encargada en cuanto a los elementos físicos de LoRaWAN, para los dispositivos lógicos se encuentra a cargo de LoRa Alliance, estos integran tanto la estructura de varios protocolos de comunicación, los cuales sirven de soporte para aplicaciones en la capa final del usuario [11].

3.3.4 Tecnología Wi-Fi

Como expresa [12], esta es una tecnología basada en IEEE 802.11, estándares que inicialmente fueron creados para una red de área local inalámbrica (WLAN), también es muy utilizada para conexiones peer-to-peer, conexiones de área personal (WPAN), esta tecnología proporciona un nivel de confianza, confiablidad y conectividad inalámbrica, por lo que comúnmente Wi-Fi es utilizado para conectar dispositivos electrónicos entre sí, este tipo de redes operan dentro de una banda 2.4GHz y 5GHz, sin embargo algunos dispositivos pueden llegar a funcionar en ambas bandas.

3.3.5 Tecnología LTE-M (Long Term Evolution Category M1)

Por otro lado, existe la tecnología LTE-M (Long Term Evolution Category M1) o EPS (Envolved Packet System) que contribuye a la reducción de costos y largo plazo de duración de batería, adicional LTE-M acapara la mayoría de las especificaciones de redes LTE, acerca de seguridad y confidencialidad de información aprovechando la red 4G.

En la actualidad empresas de telecomunicaciones como Orange S.A en Francia han implementado esta tecnología específica para IoT sin aun tener mayor expansión, no obstante, para determinar la mejor opción se debe considerar el tipo de proyecto.

4. Materiales y metodología

4.1 Análisis de tecnologías de comunicación

Los componentes antes detallados ZigBee, Bluetooth, Wi-Fi, son utilizados para soluciones de corto alcance, donde su mercado apuntaba a brindar servicios de IoT a hogares, soluciones en agroindustria, monitoreo, fabricas, edificaciones, etc. Sin embargo, por la limitante de su alcance incorporan las redes de área amplia LPWAN llegando así a ampliar su área de cobertura.

De acuerdo con [13], la seguridad sobre las tecnologías LPWAN son empleadas por LoRaWAN, Sigfox y NB-IoT, donde el mercado se ha inclinado por el uso de estas por su enfoque en la seguridad que ofrecen en la transferencia de datos, en las diferentes pruebas controladas que han realizado se ha determinado las características de seguridad, vulnerabilidades y respuesta de ataques.

Las pruebas que se han aplicado son: ataques de repetición que aterriza en DOS (denegación de servicio) (denegación de servicio) sobre componentes IoT específicos, alteración de mensajes maliciosos, modificación al proporcionar la información y un ataque de uso excesivo del suministro de energía. Estos estudios han permitido definir las características de seguridad de los dispositivos LoRaWAN versus otros productos, determinando así las brechas de seguridad.

Por otro lado, la definición de los correctos protocolos y arquitecturas de comunicación permite tener una red segura que brinda garantías y confianza al usuario, donde diferentes artículos precisan la necesidad del despliegue de estas herramientas con esquemas de integridad, autenticación y cifrado de datos mediante esquemas como AES CCM, AES STR, etc., los cuales se debe considerar como protección para evitar ataques externos, no obstante, al implementar estas medidas de seguridad también involucra consumo de recursos energéticos de los dispositivos inalámbricos, factor importante al diseñar los dispositivos a utilizar.

A continuación, se presenta las diferentes características de seguridad de los protocolos de los diferentes módulos empleados para IIoT.

Protocolo	Estándar	Autenticación	Encriptación	Alcance	Velocidad	Consumo Energético
BLE	IEEE 802.15.1	AES-CCM	AES-CCM	100m	1Mbps	10 mW
ZigBee	IEEE 802.15.4	AES-CCM	AES-CCM	100m	20, 40, 250 Kbps	36.9 mW
LoRa	IEEE 802.15.4g	AES-CTR	AES-CTR	Urbano 2Km, rural 15 Km	50 Kbps	100 mW
NB-IoT	3Gpp release 13	DTLS APN	DTLS APN	Urbano 1 – 8 Km Rural 25 Km	200 Kbps	106mW

Figura 1 Descripción técnica de seguridad de diferentes protocolos [14]

El aporte de este documento será el análisis sobre diferentes tecnologías en cuanto a la seguridad y comunicación sobre el campo de la agricultura, y los mecanismos de ciberseguridad que estos elementos prestan para asegurar la informacióncontemplando las características principales: Disponibilidad, Confidencialidad e Integridad.

Hoy en día, existen diferentes plataformas de IoT, donde cada uno cuenta con distintas soluciones, para el caso de la agricultura se tiene el monitoreo constante del desarrollo de la planta, riego, humedad, análisis de PH, y demás variables necesarias para el sector agrícola lo que permite incrementar la productividad de las plantaciones a través de diferentes dispositivos inalámbricos ubicados en el sitio, esto permite aprovechar mejor los recursos hídricos, fertilizantes, abonos, etc. Esto ayuda a las industrias agrícolas en la toma de decisiones en base a la información recopilada [15].

4.2 Amenazas de Ciberseguridad en IIoT

Tomando en cuenta el incremento de los diferentes componentes electrónicos conectados a internet, el intercambio de información, así como el aumento en el número de ciberataques dirigidos específicamente a estos dispositivos inalámbricos, en donde sus esfuerzos se encuentran enfocados en alterar y robar la información a fin de cumplir su propósito.

Entre los incidentes más reiterados están DDoS, Rasomware, vigilancia y espionaje. Teniendo en cuenta [16], DDos también es empleado por empresas para definir el correcto funcionamiento de sus dispositivos, por otro lado, los atacantes usan este método por su efectividad para causar daño en la red, alteración de la información y robo de la misma; ya que consiste en generar grandes volúmenes de flujo de información desde distintas ubicaciones hacia un solo punto mediante Bots, que es un programa que ejecuta automáticamente actividades reiterativas, a través de internet [17].

Rasomware, es considerado el ataque más peligroso al obstruir el acceso a la información, según [18] se traduce al secuestro sea de máquinas virtuales, Sistemas operativos, servicios y aplicaciones, donde para poder recuperar la información solicitan un pago por su rescate en bitcoin o transferencias, no obstante, el cancelar estos valores no ofrece garantías de recuperar la información.

4.3 Brechas de seguridad en IoT

Como plantea [19], algunas brechas de seguridad en IoT se pueden presentar a menudo en portales web no seguros o sin sistemas de bloqueo, lo que genera oportunidades de ataque, ya que de esta forma tendrían acceso a la información, lo mismo ocurre con la autenticación al no tener una complejidad alta, al igual que ocurre con el cifrado de datos en las comunicaciones, todo esto con el fin de tener el control de la red.

Las empresas destinadas a la fabricación y asistencia de servicios de IoT han implementado distintas estrategias y metodologías de seguridad para salvaguardar la información, esto debido a las constantes amenazas, vulnerabilidades y ataques del ecosistema de IoT, sin embargo, como menciona [20], estos elementos son inalámbricos e intercambian información de forma constante con un muestreo y este a su vez a la nube, lo que se ha vuelto un reto proteger los dispositivos, en la siguiente sección se tratará sobre los mecanismos de seguridad existentes para asegurar las comunicaciones en la industria.

4.4 Mecanismos de ciberseguridad en IoT

En la actualidad la protección de la información consta de aplicación de normas, protocolos que coadyuvan a salvaguardar la información proveniente de los dispositivos de IoT, donde los proveedores de servicios de IoT ofrecen el diseño, implementación y puesta en marcha de la solución, a esto le agregan un soporte ante eventos e incidentes, aunque, de acuerdo con [21], estas acciones no aseguran del todo las comunicaciones.

Actualización de parches de seguridad: El plan de mantenimientos a pesar de involucrar costos, asegura las actualizaciones a tiempo, de acuerdo con lo recomendado con el fabricante, la mejor practica es aplicar estas actualizaciones de forma automática sin intervención del usuario final y a su vez esto notificar periódicamente para su registro.

Análisis de vulnerabilidades: Realizar pruebas de penetración sobre la plataforma y/o herramientas permite detectar vulnerabilidades en el software, al ser encontrado se podrá reducir el riesgo de ataque, los métodos para ejecutar puede ser un análisis de código estático combinado con revisiones dinámicas para detectar más brechas de seguridad ocultas.

Protección a la información: Implementar cifrado de datos en la memoria no volátil del dispositivo es una forma de asegurar los datos, además de suministrar la eliminación de elementos utilizados sin exponer la información confidencial. Se ha de destacar que estos procesos consumen energía, por lo que el buen rendimiento del dispositivo IoT debe asegurar la disponibilidad, y proporcionar alta potencia de procesamiento que se asegure la encriptación de datos y conectividad.

4.5 Arquitecturas de seguridad para IoT

Existen varios modelos de arquitectura como lo señala [22], que son utilizados en las industrias que se ajustan a las recomendaciones de las organizaciones y proveedores de servicios de seguridad, que permanecen constantemente en el estudio e implementación de productos con sus modelos como Intel IoT, ITU, Azure par IoT, IoT simple y IoTWF (Internet of Things World Forum).

En [23], se muestra las conexiones correctas entre los componentes del ecosistema de IoT mediante sus 7 capas que son: Componentes físicos, Driver/Controller, conectividad, almacenamiento de información, procesos, abstracción de datos, aplicación, colaboración y computación perimetral. Este modelo contribuye más a la interacción de la data, sobre la red junto con un modelo de filtrado con Edge Computingpara enriquecer el análisis en la información transmitida previo a su almacenamiento.

En tanto el modelo de Intel IoT destaca un elemento transversal de seguridad, su arquitectura se compone de las siguientes capas: Bussiness, Data y Analytics, Application, Control, Management, Communications and Connectivity. Estos elementos incrementan la integración de la seguridad de los componentes inteligentes a través de software y hardware.

El modelo IoT simple [24], consta en su arquitectura de 5 capas: actuador/sensor, puerta de enlace, red, management/analitycs y Big Data/Data Center, de la misma forma que en IoT Intel, este modelo emplea elementos físicos y lógicos que centraliza los diversos mecanismos de seguridad ya sea filtrado, autenticación, protección y encriptación de datos.

En base al modelo ITU, el cual consta de 4 etapas, con 2 elementos que consiste en la gestión de los dispositivos, activación/desactivación vía remota, esto más el diagnóstico y las actualizaciones del software (firmware, versión, drives, etc.), topología y tráfico de red. Mientras que el otro componente es la seguridad que se enfoca en tres capas: integridad, autenticación, privacidad, autorización, antivirus y auditoría. En cuanto a la capa de red se basa en la protección de los datos, confidencialidad, control de accesos, autorización a dispositivos y autenticación.

Finalmente se presenta el modelo de seguridad de IBM [25], el cual se puede usar para distintas topologías, las capas que utiliza son: Devices, Cloud y Edge, lo que permite captar la mayor interacción entre los dispositivos, esto es posible por medio de dispositivos que permiten monitorear, controlar y analizar los datos.

Como se han descrito los modelos y sus capas para los elementos de IoT, los proveedores de servicios, marcas o fabricantes ofrece sus propias arquitecturas que operan con sus plataformas, por lo que no se presentan modelos estándar y como se ha visto no todos los modelos cuentan con componentes de seguridad.

Para la aplicación de estos modelos en específico, se debe tomar en cuenta los protocolos de comunicación los cuales se utilizan para IoT, por lo que ambos trabajan en conjunto para el mecanismo de seguridad a utilizar. Por otro lado, los modelos antes descritos no son suficientes para reducir las vulnerabilidades por lo que existen varios proveedores de este servicio que proponen soluciones a la operación.

4.6 Certificados digitales para soluciones IoT

Microsoft Azure [26], servicio de computación en la nube, ofrece aplicaciones de IoT, mejor conocido como Azure IoT Hub, que asegura la comunicación de componentes alámbricos e inalámbricos, en la red emplea certificados X.509 para autenticación de dispositivos que se encuentran conectados a través de los protocolos HTTP y MQTT, se diferencia de otros proveedores similares, donde ahí se debe crear el certificado y vincularlo al objeto, en tanto Azure facilita este proceso gracias a Hub IoT que lo hace de forma automática más una credencial privada. Estos certificados son homologados y difundidos por una entidad certificadora con el objetivo de que los componentes enlazados se autentiquen por medio de este servicio de Azure.

Por otro lado, también existe Amazon Web Service, como lo expresa [27], en su colección de servicios de computación, incorpora metodologías de autenticación y seguridad para los componentes de IoT, que al transportar el tráfico por su plataforma aplica el cifrado en la capa de seguridad de transporte, lo cual precisa los elementos conectados que usan certificados X509 por seguridad que estos brindan para la navegación web autenticada y encriptada, rubrica de documentos, autenticación del cliente e identificación electrónica, entre otros.

4.7 Criptografía en dispositivos IoT

Este mecanismo es uno de los más imprescindibles para entornos IoT de red de sensores inalámbricos, según [28], este método se ha propuesto para una topología estrella que pueda trabajar con nodos de bajo consumo de CPU, de igual forma para topología malla donde los nodos alcanzan más procesamiento, la finalidad de este método es equilibrar la seguridad y peticiones de la red de sensores, a través de un árbol de nodos en función del conjunto de caracteres alfanumérico (HASH), para después validar la información y asegurar que este correcta, seguido será transferida a cada uno de los nodos del árbol.

4.8 IoT basado en Blockchain

Este método se ha convertido en el más confiable debido a lo novedoso en su tecnología, Blockchain se le define como una "cadena de Bloques", cada información almacenada se une en grupos llamados bloques, donde realiza la validación y almacenamiento seguro y descentralizado.

Este método admite aplicar configuraciones de forma privada e indicar las direcciones que serían parte de la red y con esto se puede crear un identificador para cada objeto IoT. Esto permite generar un mecanismo más seguro puesto que están embebidos en los contratos con registros, donde se verifica en la base el historial de todas las transacciones asociadas al mismo [29], mediante un algoritmo en el que todos los nodos o usuarios dentro de la red Blockchain tienen acceso a la información para poder realizar consultas y verificar la validez de coincidencia.

Todos los mecanismos que se han descrito se pueden adherir a las soluciones de IoT permitiendo mayor protección a los dispositivos de la red, a su vez estos se perfeccionan con los modelos de referencia antes descritos lo que mejora el diseño de seguridad.

5. Análisis comparativo y recomendaciones

5.1 Análisis comparativo de mecanismos

A continuación, en la tabla 1 se resume el análisis comparativo de mecanismos y modelos de referencia, donde estos se emplean, en el cual resalta la empresa privada con mayor inversión en infraestructura AWS (Amazon Web Services), al tener más reducida la latencia que ofrecen sus servicios, a esto se suma por ser el de mayor presencia a nivel mundial, seguido de Microsoft Azure y Google Cloud Plataform, donde sus servicios están disponibles para grandes, medianas y pequeñas empresas [30].

Tabla 1 Análisis comparativo de mecanismos

Análisis comparativo de mecanismos			
Mecanismos	**Modelo de referencia**	**Característica**	**Descripción**
Encriptación, protección, autenticación, filtrado, criptografía	Modelo IoTWF	Trabaja en siete capas: dispositivos físicos y controladores, conectividad, EdgeComputing, almacenamiento de datos, abstracción de datos, aplicación, procesos y colaboración	Crea mayor interacción de los datos en la red con EdgeComputing para mejorar análisis de la información transmitida
Autenticación, filtrado, criptografía en hardware	Modelo Intel IoT	Emplea 6 capas con un componente transversal de seguridad, las seis capas que trabaja en esta arquitectura son capas de Application, Control, Management, Data and Analytics, Communications and Connectivity y Security	Esta arquitectura tiene como enfoque asegurar los componentes a través de software y hardware
Autenticación, filtrado, encriptación y protección	IoT Simple	Utiliza cinco capas sensor o actuador, Gateway, network, management /analitycs y Big Data/data center	Su arquitectura tiene como objetivo garantizar la seguridad e integración de los objetos a través de elementos físicos y lógicos
Autenticación y autorización, integridad, control de acceso	ITU	Trabaja con tres capas Aplicación, red, dispositivos de autorización	Esta arquitectura está basada en dos componentes transversales como son la gestión y seguridad.
IoT basado en Blockchain		Emplea cadena de bloques	La cadena de bloques almacena información en cada bloque y realiza la validación, almacenamiento seguro y descentralizado
Certificados digitales para soluciones IoT	Azure IoT Hub	Emplea certificados X-509 para autenticación de dispositivos que se conectan con protocolos HTTP y MQTT	Ofrece aplicaciones con tecnología propia de la marca para asegurar las comunicaciones

5.2 Análisis de las tecnologías

A continuación, se reflejan los datos técnicos de cada una de las tecnologías anteriormente descritas, donde se resalta Zigbee como los componentes inteligentes más implementados, de acuerdo con el análisis de los diferentes artículos, donde su hardware requiere de emplear un HUB para el control de red de dispositivos. Bluetooth sigue en la cadena de elementos el cual por su trayectoria se encuentra establecido en el mercado. Finalmente es seguido por la nueva tecnología LoRaWAN que se encuentra en crecimiento constante con nuevas funcionalidades de alcance, seguridad y calidad, bien aceptado por la industria.

Tabla 2 Análisis comparativo de tecnologías de comunicación

Análisis comparativo de las tecnologías de comunicación					
Tecnologías	**Topología**	**Alcance**	**Velocidad**	**Consumo Energético**	**Estándar**
LoRaWAN	Start	Urbano 2 Km y rural 15 Km	250 kbps	Very Low	IEEE 802.15.4g
RFID	P2P	5 m	500 kbps	Very Low	ISO/EPC
Wi-Fi	Start	1 km	150-780 Kbps	Low-High	IEEE 02.11 ah
Zigbee	Mesh, Start, Tree	100 m	20- 250 Kbps	Very Low	IEEE 802.15.4
Bluetooth	Start	50 m	1 Mbps	Low	IEEE 802.15.1 IOT InterConnect
LTE-M	Basado Red LTE	100m	384 kbps	Low+10 años de duración	LPWAN

Se presenta una tabla comparativa entre las dos tecnologías que contribuyen con más mecanismos de seguridad.

Tabla 3 Análisis comparativo de LoRaWAN y LTE-M

Análisis comparativo de seguridad entre las tecnologías LoRaWAN y LTE-M		
Mecanismo	**LTE-M**	**LoRaWAN**
Identificador global único	IMSI	Opcional
Autenticación del dispositivo	UICC	Dispositivo o suscripción
Autenticación de la red	LTE	Opcional
Protección de identidad	TMSI	Parcial
Confidencialidad de datos	Si	Si
Seguridad End-to-Middle	No	Si
Integridad de los datos	Opcional	Variable
Protección frente a ataques de reinyección	Opcional	Si
Reliable Delivery	Si	No
Clasificación de infraestructura critica	11-15	No
Actualizaciones del hardware	Si	No
Monitorización de la red y filtering	Si	Limitada
Provision del key	Si por RSP	Si por OTAA
Negicion del algoritmo	Si	No

6. Resultados y discusión

6.1 Mecanismo propuesto como resultado de los análisis realizados.

Este artículo permitió examinar varios mecanismos de seguridad disponibles en la actualidad. Basándose en la información recopilada y el análisis de los diferentes métodos, se puede afirmar que todos estos mecanismos buscan principalmente determinar el método más apropiado para aplicar en diferentes situaciones, con el fin de reducir las vulnerabilidades de seguridad de los datos informáticos y fortalecer los sistemas en un ambiente IoT determinado, en los cuales se plantean diferentes modelos de seguridad adaptadas al contexto agrícola.

Finalmente, en este trabajo se propone una metodología para mejorar la seguridad en un sistema IoT en el área agrícola, con el fin de alcanzar un nivel de seguridad alto.

Para este entorno se plantea implementar medidas en cuanto a la seguridad, los mismos que permitan solventar o mitigar algunos de los problemas relacionados con los dispositivos IoT en cuanto a la ciberseguridad tales como:

- Mantener las aplicaciones actualizadas de los dispositivos.
- Contar con canales de comunicación seguros mediante el uso de criptografía.
- Uso de conexiones VPN.
- Implementar políticas de control para endpoints o firewalls, evitando accesos no autorizados hacia los dispositivos del entorno IoT.
- Diseño e implementación de planes para la gestión de incidentes.
- Configurar o limitar los servicios dentro del dispositivo para prevenir una exposición innecesaria con los accesos externos.
- Realizar una correcta segmentación de la red.

Se deberá considerar también para su implementación el modelo IoT basado en Blockchain, ya que este presenta un avance significativo en la ciberseguridad, puesto que ayuda a prevenir ciberataques, filtración de datos, entre otras.

Mejora la seguridad gracias a su modelo descentralizado, el mismo que ofrece alta disponibilidad, por lo que cada uno de sus nodos se encuentran conectados a la red y además, cuenta con una copia inalterable de su cadena de bloques, permitiendo así que la gestión de los datos sea mucho más fácil de poder controlar, también dificulta la manipulación de las transacciones realizadas ya que, para lograr penetrar una cadena de bloques con éxito, el atacante deberá contar con acceso a la mayor parte de la cadena de bloques, lo que es imposible debido a la gran cantidad de bloques que forman parte de la misma cadena.

7. Conclusiones

En las tecnologías que se han presentado como opciones para comunicarse entre los dispositivos con mayor trayectoria esta ZigBee, sin embargo, para coberturas más extensas aparece LoRaWAN que otorga mayor alcance de 15 km con velocidades de 250 kbps, y otra tecnología en el mercado es LTE-M con alcances de 100m y velocidades de 384 kbps, sin embargo, aún continúa integrándose al mercado de la agroindustria.

No obstante, enfocándose en mecanismos de seguridad robustos, LTE-M cuenta con mecanismos de seguridad más sólidos frente a LoRaWAN que permite a los desarrolladores definir configuraciones de seguridad, lo que podría dar cabida a configuraciones débiles durante el despliegue del sistema.

Este estudio determina que los mecanismos de ciberseguridad que tiene soporte en la nube y sus elementos que trabajan con la misma marca, contribuyen a cerrar brechas de seguridad, disponibilidad y asegurar la sincronización de toda la red de dispositivos, sin embargo ninguno de los mecanismos, modelos, protocolos y tecnologías garantizan en su totalidad la seguridad, esto ante el constante crecimiento de metodologías aplicadas por los ciberdelincuentes por lo que, la seguridad siempre debe estar en constante actualización y adaptación en cuanto al ecosistema IoT en la agricultura.

El mecanismo propuesto para asegurar las comunicaciones en las redes de IoT para la agroindustria se define como el producto y servicio que se complementa con soportes para brindar actualizaciones de sus componentes, criptografía, uso de conexiones seguras como VPN, configuración de endpoints, seguridades perimetrales (firewall), para finalmente adecuar el mecanismo a un modelo basado en Blockchain.

8. Referencias

[1] J. Pérez Bedmar y D. Purón, «LA CIBERSEGURIDAD EN EL IOT INDUSTRIAL,» 2020, pp. 6,7.

[2] C. Cerrudo, F. Martinez y M. Sequeira, «LoRaWAN Networks Susceptible to Hacking: Common Cyber Security Problems, How to Detect and Prevent Them,» pp. 6,7, 2020.

[3] J. SALAZAR, «REDES INALÁMBRICAS,» TechPedia - European Virtual Learning Platform for Electrical and Information Engineering, p. 40, 2017.

[4] Camara Valencia, «Infraestructuras (I) Redes Inalámbricas,» 2017. [En línea]. Available: https://ticnegocios.camaravalencia.com/servicios/tendencias/caminar-con-exito-hacia-la-industria-4-0-capitulo-11-infraestructuras-i-redes-inalambricas/.

[5] C. Cisneros, «Estudio de mecanismos de aseguramiento de la información para internet de,» 24 abril 2021. [En línea]. Available: http://repositorio.puce.edu.ec/bitstream/handle/22000/18891/Proyecto%20de%20Titulaci%c3%b3n%20Maestr%c3%ada%20Tic%c2%b4s%20Christian%20Cisneros.pdf?sequence=1&isAllowed=y.

[6] CyberArk, «Seguridad en la Nube,» Massachusetts, 2021.

[7] KASPERSKY, «Protección de las redes inalámbricas,» 2020. [En línea]. Available: https://www.kaspersky.es/resource-center/preemptive-safety/protecting-wireless-networks.

[8] SoftwareLab, «¿Qué es el Bluetooth y para qué sirve?,» Florida, 2020.

[9] . E. A. OCAS INFANTE, «ENLACE INALÁMBRICO ZIGBEE PARA UN SISTEMA DE ALUMBRADO LED AUTÓNOMO,» 2018. [En línea]. Available: https://repositorio.unp.edu.pe/bitstream/handle/UNP/1759/CIE-SIF-JIM-19.pdf?sequence=1&isAllowed=y.

[10] A. Heredia, P. Lucero, F. Astudillo y A. Vázquez, «Design and implementation of wireless sensor network with LoRa technology for industrial monitoring,» LATIN-AMERICAN JOURNAL OF COMPUTING (LAJC), pp. 50-52, 2020.

[11] M. Manrique, L. Buitrago y J. Hernández, «Redes LoRaWAN. Revisión de componentes funcionales en aplicaciones IoT.,» 02 Diciembre 2019. [En línea]. Available: https://repository.udistrital.edu.co/bitstream/handle/11349/22411/LeidyMarcelaBuitragoMarquez2019.pdf?sequence=1&isAllowed=y.

[12] S. Cheruvu, A. Kumar, N. Smith y D. Wheeler, Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment, New York: Open Access, 2020.

[13] C. A. González González, F. Arévalo Tapias y J. Hernández Gutiérrez, «Análisis de seguridad en redes LPWAN para dispositivos IoT,» 12 07 2018. [En línea]. Available: https://oaji.net/articles/2020/3374-1597336649.pdf.

[14] C. P. Chuchico Arcos, «N odos sensores y protocolos de comunicación del internet de las cosas aplicados a la agricultura inteligente,» 22 NOVIEMBRE 2021. [En línea]. Available: http://repositorio.espe.edu.ec/bitstream/21000/27321/1/T-ESPEL-MEI-0009.pdf.

[15] . J. A. Tomalá Puero y H. A. Valenzuela Cornejo, «Investigación y análisis del ecosistema para el internet of the things en las áreas de smart cities, home automation, smart energy, connected vehicle, industria 4.0 y smart health.,» 15 ABRIL 2019. [En línea]. Available: http://repositorio.ug.edu.ec/handle/redug/40119.

[16] J. E. Martínez-Lozano y P. S. Atencio-Ortiz, «Creation of a DDOS attack using HTTP-GET Flood with the Cyber Kill Chain methodology,» 19 06 2019. [En línea]. Available: https://doi.org/10.15332/.v16i1.2160.

[17] MALWAREBYTES, «Ransomware,» Ireland, 2022.

[18] IOT SECURITY FOUNDATION, «IOT SECURITY FOUNDATION,» 14 11 2022. [En línea]. Available: https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/.

[19] Á. Calvo del Olmo, «Seguridad en internet de las cosas: firmwares, vulnerabilidades y riesgos en la rapidez del desarrollo y consumo de internet of things,» 31 12 2018. [En línea]. Available: http://hdl.handle.net/10609/89625.

[20] J. C. Najar-Pacheco, J. A. Bohada-Jaime y W. Y. Rojas-Moreno, «Vulnerabilities in the internet of things,» REVISTA VISIÓN ELECTRÓNICA, p. 15, 05 MAYO 2019.

[21] Specialized Software Development Company, «Internet of Things (IoT) Security: Challenges and Best Practices,» 17 febrero 2022. [En línea]. Available: https://www.apriorit.com/white-papers/513-iot-security.

[22] A. Vélez Pérez, «Repositorio de la Universidad Nacional Abierta y a Distancia,» 03 09 2019. [En línea]. Available: https://repository.unad.edu.co/handle/10596/27648.

[23] Telecom Reseller, «Internet of Things World Forum (IoTWF) leaders announce new IoT Reference Model and IoTWF Talent Consortium,» 2014. [En línea]. Available: https://telecomreseller.com/2014/10/14/internet-of-things-world-forum-iotwf-leaders-announce-new-iot-reference-model-and-iotwf-talent-consortium/.

[24] J. S. Rueda y J. M. Talavera, «Similarities and differences between Wireless Sensor Networks and the Internet of Things: Towards a clarifying position,» 20 abril 2017. [En línea]. Available: http://www.iotsimple.com/que-es-iot.

[25] IBM, «Arquitectura de IoT CE on Cloud,» 03 03 2021. [En línea]. Available: https://www.ibm.com/docs/es/elm/6.0.6?topic=offerings-architecture.

[26] Azure IoT Hub, «Azure IoT Hub,» 26 09 2022. [En línea]. Available: https://azure.microsoft.com/es-mx/products/iot-hub/?&ef_id=CjwKCAiAjs2bBhACEiwALTBWZePQnsVugYCnNHqw359y8bySDwpG0XvKjEz5iuKAEGIP6iaLwSOOxhoCf-gQAvD_BwE:G:s&OCID=AIDcmmvcssag76_SEM_CjwKCAiAjs2bBhACEiwALTBWZePQnsVugYCnNHqw359y8bySDwpG0XvKjEz5iuKAEGIP6iaLwSOO.

[27] AWS IoT Core, «AWS,» 2022. [En línea]. Available: https://docs.aws.amazon.com/es_es/iot/latest/developerguide/x509-client-certs.html.

[28] M. Salinas Rosales y G. Duchén Sánchez, «Identity based authentication protocol for wireless sensor networks,» Revista Facultad de Ingeniería Universidad de Antioquia, p. 4, 2010.

[29] J. Sanz Peláez, «REPOSITORIO DE LA UNIVERSIDAD DE VALLADOLID,» 14 Junio 2018. [En línea]. Available: https://uvadoc.uva.es/bitstream/handle/10324/33006/TFG-G3417.pdf?sequence=1&isAllowed=y.

[30] . F. Prieta Pintado y E. Pascual Corral, «Repositorio de la Universidad de DSALAMANCA,» JULIO 2021. [En línea]. Available: https://gredos.usal.es/bitstream/handle/10366/150066/Jaime%20de%20la%20Pe%C3%B1a%20Ramos_memoria%20tfg_GII.pdf?sequence=1&isAllowed=y.

[31] J. Calles-García y P. González-Pérez, La Biblia del Footprinting, 2011.

[32] www.elhacker.net, «www.elhacker.net,» [En línea]. Available: https://www.elhacker.net/trucos_google.html.

[33] F. De La Prieta Pintado y E. Pascual Corral, «IoT Aplicado a la Agricultura y Ganadería,» JULIO 2021. [En línea]. Available: https://gredos.usal.es/bitstream/handle/10366/150066/Jaime%20de%20la%20Pe%C3%B1a%20Ramos_memoria%20tfg_GII.pdf?sequence=1&isAllowed=y. [Último acceso: 26 12 2022.