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:

DISEÑO DE UNA ARQUITECTURA PARA SEGURIDAD DE DATOS EN LAS COMUNICACIONES EN REDES BASADO EN INDUSTRIAL IOT

AUTORES:

MARCO ANTONIO LÓPEZ REINOSO
PAÚL ANDRÉS MONTESDEOCA MÉNDEZ

DIRECTOR:

JUAN CARLOS DOMÍNGUEZ AYALA

CUENCA – ECUADOR
2023

Autor:

Marco Antonio López Reinoso
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
mlopezre@est.ups.edu.ec

Paúl Andrés Montesdeoca Méndez
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
pmontesdeoca@est.ups.edu.ec

Dirigido por:

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

Todos los derechos reservados.

Queda prohibida, salvo excepción prevista en la Ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra para fines comerciales, sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual. Se permite la libre difusión de este texto con fines académicos investigativos por cualquier medio, con la debida notificación a los autores.

DERECHOS RESERVADOS
2023 © Universidad Politécnica Salesiana.
CUENCA – ECUADOR – SUDAMÉRICA
MARCO ANTONIO LÓPEZ REINOSO
PAÚL ANDRÉS MONTESDEOCA MENDEZ
Diseño de una arquitectura para seguridad de datos en las comunicaciones en redes basado en Industrial IoT

DEDICATORIA

Este trabajo lo dedico con mucho cariño a mi querido e inolvidable hermano Santiago quien debido a los planes de Dios se nos adelantó, pero se siente vivo en nuestros corazones y su espíritu luchador ha sido un impulso en mi vida que me ha permitido no decaer y esforzarme más para conseguir este objetivo y sé que de seguro el estaría muy orgulloso de mi.

También dedico a mis padres, hermano y mi querida esposa quienes son mi fuente de motivación e inspiración para superarme cada día, los cuales con su amor, paciencia y esfuerzo no me han dejado de caer en llegar a cumplir este objetivo, inculcando en mí el ejemplo de constancia, perseverancia y trabajo para poder alcanzar nuestros sueños.

Paúl Andrés Montesdeoca Méndez

AGRADECIMIENTO

Agradezco a Dios por haberme permitido dar este paso muy esencial en mi vida y poder cumplir uno de mis objetivos más importantes de mi preparación académica.

Agradezco a mi esposa por ser un pilar muy importante en mi vida por su apoyo y confianza incondicional desde el inicio de la maestría, así como a mis padres y hermanos que siempre me supieron apoyar, aconsejarme y sobretodo animarme a sobresalir y ser mejor cada día.

Agradezco de manera muy particular a mi compañero de tesis Marco López quien es más que un compañero es un amigo de confianza ya que desde el inicio de nuestra amistad siempre ha confiado en mí y ahora es un logro más juntos que hemos podido alcanzar; también agradezco a nuestro tutor Magister Juan Carlos Domínguez quien con sus consejos y empatía nos ha guiado a alcanzar este objetivo, sin él no hubiera sido posible.

Paúl Andrés Montesdeoca Méndez

DEDICATORIA

Dedico este trabajo de titulación primeramente a mis hijos Santiago y Paul que son mi inspiración en mi vida, la razón para cada día seguir adelante, seguir creciendo, ser una mejor persona y un mejor profesional, los que más amo en este mundo y espero que algún día comprendan que lo que soy hoy se los debo a ustedes y que este logro sirva de ejemplo y herramienta para guiar cada uno de sus pasos , a mi esposa, amiga y compañera de vida que con cada detalle ha demostrado su amor incondicional hacia mi persona que ha estado a mi lado en todo momento a pesar de las circunstancias, a mis padres quienes a lo largo de mi vida han estado guiándome, apoyándome y cuidando por mi bienestar y por no dejarme rendir en ningún momento, a mi hermana por su cariño y apoyo incondicional.

Marco Antonio López Reinoso

AGRADECIMIENTO

En primer lugar, agradezco a dios por haberme permitido llegar hasta este momento tan importante de mi formación profesional.

Agradezco a mi esposa por su apoyo incondicional siendo el pilar más importante, de igual manera a mi hijo Santiago por su comprensión y apoyo en este proceso, a mis padres por poner su confianza en mí para cumplir esta meta.

Agradezco a mi amigo y compañero de tesis Paul Montesdeoca que con su apoyo pudimos sacar este trabajo adelante, también agradezco a nuestro tutor Magister Juan Carlos Domínguez que sin su ayuda no hubiera sido posible sacar adelante este trabajo por ultimo gracias a la Universidad por permitirme convertirme en profesional en lo que me apasiona, gracias a cada maestro que hizo parte de este proceso de formación.

Marco Antonio López Reinoso

Tabla de Contenido

Diseño de una arquitectura para seguridad de datos en las comunicaciones en redes basado en Industrial IoT

Autor(es):

Marco Antonio López Reinoso
Paúl Andrés Montesdeoca Méndez

Resumen

Se revisaron artículos científicos sobre Industrial Internet of Things (IIoT) en diferentes dominios para conocer el entorno actual. Esta investigación se justifica porque para minimizar los riesgos es necesario responder con un nivel adecuado de seguridad en IIoT, que debe ser informativo y funcional. El aporte que se pretende entregar es una arquitectura IIoT dirigida a la seguridad de datos y que pueda ser modelo general para futuras implementaciones. El objetivo general es diseñar una arquitectura para robustecer el nivel de seguridad de datos en las comunicaciones de redes basado en IIoT. Los objetivos específicos son: analizar modelos IIoT en artículos científicos, diseñar una arquitectura para robustecer el nivel de seguridad basada en IIoT, y evaluar la arquitectura teórica para identificar el rendimiento y seguridad. Como metodologías, se utiliza el enfoque cuantitativo, el enfoque cualitativo, el diseño experimental, el alcance exploratorio, el alcance descriptivo, Revisión Sistemática de la Literatura y modelo PRIMA. Entre los resultados se obtuvo 45 artículos tabulados que responden a las preguntas de investigación; se conoció que el principal objetivo en IIoT es Seguridad, el entorno más utilizado es Industria, el protocolo más utilizado es MQTT, la herramienta tecnológica más utilizada es Fog-Edge, los dispositivos más utilizados para capturar datos son los sensores, y el mayor desafío son los ataques. Se diseñó una arquitectura de 4 capas: Dispositivos, Comunicación, Cloud Computing y Aplicaciones informáticas. En la evaluación de la arquitectura en software NODE RED se utiliza el protocolo MQTT sin seguridad y con seguridad, este protocolo aplica encriptación y autenticación para mantener la seguridad y privacidad, esto demuestra su eficacia.

Palabras clave:

IoT, IoT Industrial, Seguridad de la Información, Seguridad en IIoT, Protocolos IoT.

ABSTRACT

Scientific articles on Industrial Internet of Things (IIoT) in different domains were reviewed to know the current environment. This research is justified because to minimize risks it is necessary to respond with an adequate level of security in IIoT, which must be informative and functional. The intended contribution is an IIoT architecture aimed at data security and that can be a general model for future implementations. The overall objective is to design an architecture to strengthen the level of data security in IIoT-based network communications. The specific objectives are: to analyze IIoT models in scientific articles, to design an architecture to strengthen the level of security based on IIoT, and to evaluate the theoretical architecture to identify performance and security. As methodologies, the quantitative approach, the qualitative approach, the experimental design, the exploratory scope, the descriptive scope, the Systematic Review of the Literature and the PRIMA model are used. Among the results, 45 tabulated articles were obtained that answer the research questions; It was known that the main objective in IIoT is Security, the most used environment is Industry, the most used protocol is MQTT, the most used technological tool is Fog-Edge, the most used devices to capture data are sensors, and the biggest challenge is attacks. A 4-layer architecture was designed: Devices, Communication, Cloud Computing and Computer Applications. In the evaluation of the NODE RED software architecture, the MQTT protocol is used without security and with security, this protocol applies encryption and authentication to maintain security and privacy, this demonstrates its effectiveness.

Palabras clave:

IoT, Industrial IoT, Security of the Information, Security on IIoT, IoT protocols.

1. Introducción

Durante la pandemia de Covid-19 las amenazas cibernéticas crecieron y afectaron los datos e industrias de infraestructuras críticas (Buja et al., 2022), es así que existe un claro desafío para aumentar el nivel de seguridad de datos en la infraestructura industrial y además en sus componentes, debido a que los ataques cibernéticos a esta clase de infraestructura cada vez son mayores y supone fuertes pérdidas (Panchal, 2018); otra consecuencia de ataques cibernéticos durante la pandemia fue la falla en cadenas de suministro centralizadas que produjo escases, esto se convirtió en la oportunidad de crecimiento acelerado y mejoras de "redes de dispositivos interconectados", este tipo de red es un pilar descentralizado en las industrias conocido como Industrial Internet of Things IIoT (Darwish et al., 2020).

La seguridad cibernética es un tema importante y crítico para la adopción de IIoT, además, este tema es analizado por universidades e industrias a nivel mundial porque IIoT hereda algunos retos de confianza/seguridad de IoT, algunos intereses apuntan a: seguridad de datos, la integridad de las aplicaciones informáticas, validación de dispositivos y gestión de dispositivos. Es posible adoptar prácticas de seguridad de IoT para superar los problemas, aunque en IIoT la seguridad se enfatiza en la no intervención de personas y en las actividades autónomas de dispositivos/máquinas; los modelos IIoT brindan conectividad con dispositivos, escalabilidad en infraestructura e inteligencia en línea para los procesos industriales y tienen el riesgo de sufrir ataques. Por ejemplo, existen entornos industriales que son independientes de la infraestructura TI y su diseño no considera la ciberseguridad, la cantidad de dispositivos interconectados se incrementa en estos entornos, y, en consecuencia, aumentan las vulnerabilidades. Los nuevos diseños IIoT deben considerar la seguridad que se presenta a las industrias o fábricas (Yu & Yuira-staredusg, 2019).

IIoT es la utilización específica de IoT en las fábricas o industrias, existen dispositivos interconectados y sistemas de gestión para alcanzar un propósito, ésta

interconexión dentro de las industrias no es nueva, pero si está dirigida a zonas en la empresa industrial; los sensores recolectan datos desde lugares remotos y se envían a lugares de supervisión y control para aumentar la productividad (Panchal, 2018).

Se estima que el mercado de IIoT en 2019 es $87 mil millones y en 2023 será $310 mil millones. Se afirma que este impulso es por la producción en equipos de fabricación para optimizar las industrias (Knezevic & Kasunic, 2020).

IIoT se compone de dispositivos livianos (sensores/actuadores) con procesadores y conexión a red, estos dispositivos inteligentes utilizan diferentes protocolos de comunicación como Bluetooth, LoRa, WiFi, Zwave o ZigBee para el intercambio de datos entre ellos o envío a un servidor en la nube al entrar por puertas de enlace; los dispositivos brindan un entorno inteligente para seguimiento de condiciones y responder de acuerdo a las circunstancias o parámetros, lo que puede significar reducción de tiempos y reducción de costos en la gestión; IIoT integra dispositivos inteligentes con sistemas de control para aumentar la seguridad de personas o procesos, esto deriva en servicios o actividades inteligentes que fomentan la toma de decisiones o gestión dinámica (Koroniotis et al., 2021).

IIoT se utiliza en varias áreas industriales como refinerías de petróleo y gas, producción, manufactura, ciudades inteligentes, agricultura, infraestructura de agua e infraestructura de energía; ésta tecnología recopila datos, realiza monitoreo y genera datos remotos, tiene beneficios y potencial que agregan valor a una empresa industrial; IIoT también es llamada Industria 4.0 por sus extensiones de IoT que se enfocan a entornos industriales que conectan máquinas y sensores industriales basados en IoT (Buja et al., 2022). Otras áreas que utiliza IIoT son aeropuertos, hospitales, marítima, transporte inteligente (Koroniotis et al., 2021), salud en recolectar datos de covid-19 y diagnóstico remoto (M. Zhang et al., 2021), robótica, automatización de industria y vehículos autónomos (Puri, 2020).

Cabe resaltar que IoT se diseña para el área comercial, mientras IIoT se diseña para el área industrial. IIoT genera datos capturados por sensores y entrega respuestas

en línea, ésta tecnología está asociada con Industria 4.0 que reúne tecnologías en empresas y apoya la cadena de valor; se utiliza en ensamble de producción, gestión, control de calidad, existe un fuerte impacto en plataformas de automatización y se espera que los activos inteligentes estén interconectados a "empresas de fabricación inteligente". Algunos componentes de un modelo IIoT son: dispositivos, datos transitorios, procesadores, aplicaciones informáticas, canales de comunicación, gateways, procesos, almacenamiento permanente, modelo de análisis de datos, cloud computing (Karmakar, 2019).

IIoT trabaja con otras tecnologías como Machine Learning, Big Data (Karmakar, 2019), Realidad Extendida (XR), Cloud Computing, Inteligencia Artificial, Blockchain, Hiper Automatización (Buja et al., 2022).

En Ecuador, algunos artículos sobre IIoT realizados son: en industria 4.0 (Mora-sánchez & Guerrero-marín, 2020), control de baterías (Pablo et al., 2021), operaciones en Gas/Petróleo (Montalvo et al., 2020), arquitecturas industriales para minimizar el consumo de energía (Lozada et al., 2020), comunicaciones en las industrias (Caiza et al., 2019), robótica en campos de petróleo (C. A. Garcia et al., 2018), protocolos de comunicación (Espín et al., 2018), control mediante software (Minchala et al., 2020), arquitectura para control industrial (Ambato et al., 2018), entrenamiento en máquinas industriales mediante realidad aumentada (V. Garcia, 2020).

El objetivo general es diseñar una arquitectura para robustecer el nivel de seguridad de datos en las comunicaciones de redes basado en Industrial Internet of Things (IIoT)

Los objetivos específicos son: a) Analizar modelos en artículos científicos para conocer la seguridad aplicada a IIoT en diferentes entornos mediante la revisión sistemática de la literatura. b) Diseñar una arquitectura para robustecer el nivel de seguridad de datos en las comunicaciones de redes basado en Industrial Internet of Things (IIoT). c) Evaluar la arquitectura teórica para identificar el nivel de rendimiento y seguridad mediante la simulación virtual en software.

2. Determinación del Problema

De acuerdo a (Buja et al., 2022), la seguridad conocida como CIA (confidencialidad, integridad, disponibilidad), triple AAA, antivirus, firewalls y otros programas son tradicionales, y es necesario “reconsiderar el modelo de seguridad” de las empresas industriales porque IIoT recopila datos de infraestructuras críticas.

De acuerdo a (Koroniotis et al., 2021) es primordial garantizar la ciberseguridad y la estabilidad de los sistemas industriales, a pesar que existen vulnerabilidades inherentes en los dispositivos inteligentes y esto genera problemas en las operaciones industriales.

IIoT es sinónimo de Industria 4.0, aunque otros autores consideran que son diferentes, Industria 4.0 trata el “desarrollo de la industria” para que las actividades de fabricación sean más inteligentes, aquí existen dispositivos como sensores/actuadores y monitoreo sistemático de las instalaciones de red. IIoT e Industry 4.0 tienen desafíos iguales en seguridad, algunas amenazas existentes son: Hurto de datos, Corrupción a los datos, Averías a los componentes del sistema, Deterioros a la comunicación del sistema (Wadsworth et al., 2020).

Algunas prácticas de seguridad recomendadas son: actualizar firmware, utilizar cifrado, control de autenticación para dispositivos, control para aplicaciones móviles, utilizar firewall y seguridad física (Knezevic & Kasunic, 2020). Aunque estas recomendaciones no inciden en un diseño de arquitectura o modelo, solo sirven en modelos ya implementados.

Los países actualizan sus leyes en exigir conexiones seguras para los ciudadanos y empresas, la conectividad a Internet es más amplia y accesible con más dispositivos; las empresas utilizan dispositivos inteligentes para control y gestión diaria, se considera un desafío mantener una IIoT segura para los datos que generan sus dispositivos y fluyen a través de la red, las necesidades de conexiones en la industria a nivel global han generado una explosión tecnológica y aumento de ataques

(Conference et al., 2020); esto se convierte en otra oportunidad para proponer seguridad de datos en el diseño de entornos IIoT.

Los entornos IIoT deben cumplir niveles de confiabilidad, seguridad y privacidad, los niveles de seguridad se aplican de acuerdo al caso del entorno IIoT porque un ataque a sus componentes causa alto impacto; un caso puede ser los fabricantes de sensores/actuadores que deben aplicar controles, y otro caso son los proveedores de servicios que deben utilizar los dispositivos con seguridades mínimas (Nakamura, 2018).

Los entornos IIoT con dispositivos heredados no consideraron la seguridad en el diseño de sus arquitecturas y ni en la conectividad, además, los dispositivos se conectan con otras tecnologías emergentes y utilizan protocolos de comunicación (Al-hawawreh, 2021), esta es otra razón para proponer la seguridad en la fase de diseño de entornos IIoT.

Las amenazas a la seguridad de la información a las que se enfrenta el IIoT se derivan principalmente de otras tecnologías introducidas y de sus características estructurales.

Una arquitectura básica de IIoT está formada por otras tecnologías básicas como: adquisición de datos, transmisión de datos y procesamiento de datos, éstas tecnologías tienen sus protecciones de seguridad (Chen et al., 2019).

La amenaza informática que se materializa acarrea costos económicos y afecta la imagen de la empresa que sufre el ataque. Entonces para minimizar los riesgos es necesario responder con un nivel adecuado de seguridad en IIoT, que debe ser informativo y funcional.

Para la justificación social de este anteproyecto resalta la importancia de minimizar las vulnerabilidades, riesgos y amenazas en entornos IIoT como es caso de salud, fábrica de alimentos, industria automotriz y aeropuertos que ofrecen servicios directos a la sociedad.

La justificación legal de este anteproyecto está basada en la Constitución de la República del Ecuador en el Art 334 que promueve la democratización y acceso equitativo a los factores de producción como conocimiento y tecnologías, además el Art 350 expresa que una de las finalidades de la educación superior es la investigación científica y tecnológica.

El aporte que se pretende entregar es una arquitectura IIoT dirigida a la seguridad de datos que pueda ser modelo general para futuras implementaciones.

3. Marco teórico referencial

3.1 Industrial Internet Of Things

Concepto de IoT: Se conoce como IoT a la tecnología que captura datos mediante la interconexión de dispositivos físicos en redes, los datos son enviados en su estado original a Internet y se guardan en almacenes de la nube (Karmakar, 2019).

Concepto de IIoT: es un subconjunto base de IoT que recolecta datos de extremidades robóticas, dispositivos de salud y los despacha a un sistema de información (Buja et al., 2022). Es la IoT que se aplica al campo industrial y conecta actuadores, microcontroladores, sensores, computadoras, artefactos, entre otros, esto hace que las actividades industriales sean eficientes (Hou et al., 2019). Otros denominan IIoT como unificación de TI y OT (tecnología operativa), en esta integración TI es la red empresarial y OT es la red de la fábrica, aunque estos dos elementos tienen distintos requisitos de seguridad; otros componentes de IIoT son el análisis de datos y sistemas de mecanismos inteligentes que trabajan en un entorno escalable, eficiente e interoperable para automatizar una infraestructura crítica y aumentar la productividad de la empresa (Panchal, 2018).

3.2 Ataques en IIoT

Existen ataques en diferentes niveles en una IIoT: a nivel de sensores/actuadores los ataques son ingeniería inversa, software malicioso, introducción de paquetes, pesquisa, búsqueda impulsada; a nivel de controladores programables los ataques son repetición, sniffing, previsión de contraseñas; a nivel de estación de operaciones los ataques son reemplazo de IP, rastreo de datos, maniobra de datos; a nivel aplicaciones informáticas los ataques son phishing, introducciones de SQL, malware, corrupción de DNS, actuación remota de código, fuerza bruta, ataques a las aplicaciones web; a nivel de nube los ataques son denegación de servicios, ataques de canal adyacente, introducción de malware, autenticación falsa, Man-in-the-Middle, agresiones a dispositivos móviles (Panchal, 2018).

3.3 SEGURIDAD DE ARQUITECTURAS IIoT

En (P. Zhang et al., 2020) se propone una arquitectura como un esquema abierto y escalable que mantenga las conexiones entre IIoT y usuarios; los ingenieros pueden utilizar este modelo para satisfacer determinadas demandas de manera eficiente, y formada por instalaciones de software/hardware; se puede ajustar a otras funciones y optimizar el rendimiento IIoT mediante la implementación de aplicaciones web/móviles; los autores confirman que es flexible, confiable y eficiente; la arquitectura básica presenta servicio de software, servicio de plataforma, servicio de negocios, dispositivos inteligentes, tecnologías de visualización, en cuanto a seguridad de la información esta arquitectura aplica Blockchain con algoritmos basado en créditos.

En (Abuhasel & Khan, 2020) se presenta una red neuronal profunda y utiliza algoritmos de encriptación optimizados para transmitir los datos para industria, además agrupan los sensores que utilizan los algoritmos de cifrado, el algoritmo clasifica de acuerdo a almacenamiento-computación-ancho de banda; el algoritmo es bajo en latencia, consumo de energía, concesión eficiente de recursos y alta seguridad; la arquitectura está organizada en capas como sensores, conexión, fog y nube, las simulaciones se realizan en software y miden la latencia, consumo de energía y tiempo de cifrado.

En el proyecto de (Gaba et al., 2021) se utiliza el protocolo AMQP que se fundamenta en la pauta de publicación/suscripción y desarrolla mensajes de intercambio, este protocolo se utiliza en seguridad porque genera una clave única por cola de mensajes, y además se asegura en la capa de transporte, aquí los datos se cifran con clave pública y se descifran con una clave privada; el proyecto asegura que AMQP se utiliza en industrias pequeñas o económicas, además es confiable y seguro.

El análisis de (Iglesias-Urkia et al., 2018) especifica que CoAP se utiliza redes restringidas, es apropiado para operar en dispositivos IoT en bajo consumo de energía, se fundamenta en modelos cliente-servidor; el servidor CoAP es quien responde las solicitudes, el cliente CoAP realiza las solicitudes; la seguridad se centra en la conexión de servidor generada en el transporte de datos, el protocolo es escalable y flexible, por lo general se utiliza en viviendas y edificios.

En (Liu et al., 2020) se propone un esquema optimizado en una red de distribución inalámbrica con una comunicación terminal que es segura, confiable y flexible basada en MQTT; este protocolo es una base teórica de la tecnología inalámbrica y compensa las necesidades en comunicación IoT, los mensajes son jerárquicos, por ejemplo Industria/Área/Focos/Estado; además el protocolo se ejecuta sobre TCP en la transportación de datos entonces la seguridad se amplía en la capa de transporte.

En (Ferrera et al., 2018) se propone una plataforma IoT con servicio de gestión de red e implementación, la plataforma se basa en XMPP para gestión de la red IoT; la arquitectura consta de 3 niveles, el primer nivel es gestión, el segundo nivel es core y tercer nivel es control, el último nivel combina XMPP, MQTT y HTTP Rest; en la seguridad de datos se utiliza cifrado y autenticación que están integradas a XMPP.

En (Paliwal, 2019) se propone un protocolo ligero para autenticación que protege la privacidad y optimiza la seguridad, el esquema utiliza hash y secuencia de números que mejoran el proceso mediante claves dinámicas generadas por dispositivo o usuario, y usa seudónimos para ocultar al nodo sensor o usuario.

De acuerdo a (Gebremichael et al., 2020) en servicios de seguridad en una IIoT se aplican protocolos de seguridad en las distintas capas de un modelo o arquitectura, de modo general: en la capa de red se aplica bluetooth, ZigBee, ieee 802.15.4, NB-IoT, wlan, LoRaWAN, data link o 6LoWPAN; en la capa plataforma se aplica CoAP, MQTT, TCP o UDP; mientras para las conexiones se debe aplicar autenticación, control para accesos, claves, cifrado de datos o filtros.

En (Makrakis et al., 2021) se analiza una arquitectura de seis capas y se cubren las vulnerabilidades con un sistema de ataque, la seguridad se aplica mediante sistemas de control y estándares americanos que utilizan mejores prácticas.

En (Kasongo, 2021) se describe una arquitectura de tres capas como red, perceptual y aplicación; para la seguridad en la capa de red utiliza protocolos, aunque para reforzar la seguridad utilizan como elemento adicional algoritmos de Machine Learning para detectar comportamientos de posibles intrusos, utiliza tres algoritmos de ML como RF, Decision Tree (DT) y Extra Tree (ET); las simulaciones se realizaron en una herramienta libre Python.

En (Almadani & Mostafa, 2021) los autores proponen un modelo de comunicación de datos para control y seguimiento de la producción agrícola en línea, el modelo se compone de sensores, actuadores, controladores de zona y controladores de cada granja; se capturan datos como temperatura, humedad, dióxido, luz, sonidos, y los actuadores trabajan sobre ventilación, irrigación, cultivo, focos; se nombra seguridad como cifrado, autenticación, mecanismos de seguridad y claves públicas, aunque no se utiliza ninguno de estos en seguridad; la simulación es en un jardín y dispositivos que miden el rendimiento del modelo.

En (Gao et al., 2021) utilizan Blockchain para la seguridad y privacidad de la información a una arquitectura IIoT, aquí la cadena de bloques permite a los dispositivos que puedan almacenar los datos, además utilizan otro esquema para dar mayor seguridad a los dispositivos en su comunicación, la arquitectura contiene capa de dispositivos, red y nube, y la red blockchain es privada en Hyperledger.

Otra manera de seguridad en una IIoT es un modelo para detectar ransomware en las líneas perimetrales, utiliza Deep Learning para detectar al intruso, una parte del modelo filtra los datos y elimina ruidos, otra parte identifica al intruso objetivo; la propuesta presenta una arquitectura de tres capas: dispositivos, gateways y plataforma empresarial; la capa dispositivos contiene sensores, actuadores y PLC, la capa gateways contiene entrenamiento y agregación de los datos; la tercera capa contiene el almacenamiento, aplicaciones informáticas, mantenimiento y usuarios;

la capa gateways se encuentra el algoritmo de entrenamiento con los datos que consigue de la red para identificación del intruso (Al-Hawawreh et al., 2021).

En (Ferrag et al., 2022) se propone una arquitectura IIoT formada por cuatro capas como física, fog, blockchain y nube. La capa física contiene sensores de sonido, fuego, nivel de agua, temperatura, pH, humedad, frecuencia; en la capa fog se utiliza protocolo MQTT para la seguridad en los dispositivos; en la capa blockchain se utiliza hyperledger para aumentar la seguridad mediante gestión del almacenamiento, consenso, estados y accesos controlados; la capa cloud está el almacenamiento, aplicaciones informáticas de acceso, dashboard, análisis de datos; mientras que para las pruebas del modelo utilizaron un banco de datos en un simulador.

Los protocolos MQTT, CoAP, AMQP, RestAPI y HTTP son utilizados por los dispositivos IoT para la comunicación de datos. Un estudio combina MQTT y CoAP para generar un modelo seguridad integrado que minimiza la tasa de error y maximiza el uso del cifrado en MQTT y el uso de datagramas en CoAP; las pruebas las realizaron sobre una plataforma virtual y midieron los paquetes perdidos y performance (Dave et al., 2020).

De acuerdo a (Gebremichael et al., 2020) los servicios de seguridad en una IIoT son: autenticación, no repudio, confidencialidad de datos, confidencialidad del tráfico, control de acceso, cifrado de datos, protocolos de comunicación, aislamiento de datos y segmentación. Los objetivos de seguridad son Confidencialidad, Integridad y Disponibilidad (CIA), los servicios de seguridad nombrados anteriormente cubren uno o varios objetivos. En esta investigación se aplica Protocolos de Comunicación porque cubre los tres objetivos de seguridad y se puede utilizar varios protocolos, en cambio el Aislamiento de Datos y Segmentación utilizan hardware como firewall o contenedores.

El marco teórico desarrollado se utiliza para integrar la teoría o conceptos con la propuesta de esta investigación, las definiciones encontradas son utilizadas durante el desarrollo de esta propuesta; los conceptos de IoT y IIoT nos amplía la visión, los

ataques en IIoT nos demuestra ciertas vulnerabilidades, la seguridad en arquitecturas IIoT nos demuestran diferentes modelos o medidas utilizadas para minimizar los riesgos.

4. MATERIALES Y METODOLOGÍA

De (Hernández-Sampieri; Fernández-Collado; Baptista-Lucio, 2010) se utilizan varios métodos que se describen a continuación:

Se utiliza el enfoque cuantitativo para determinar los artículos científicos que pueden ser útiles en esta investigación, contestar las preguntas de investigación con valores numéricos, ver la generalización de los resultados, se utiliza el proceso deductivo para determinar las características generales, conocer la precisión de otras arquitecturas, hacer la replicación de los componentes de otras arquitecturas IIoT.

Se utiliza el enfoque cualitativo para explorar las características de las arquitecturas encontradas en los artículos científicos, extraer los significados de los modelos, se utiliza el proceso inductivo para determinar características únicas, se analiza las realidades aplicadas por los artículos científicos, interpretar las bondades de otras arquitecturas IIoT.

El tipo de investigación en función del diseño es experimental porque se utiliza una herramienta de software para simular la arquitectura que se propone en esta investigación.

El alcance del artículo está de acuerdo a los objetivos específicos descritos en la introducción: alcance exploratorio para revisar los contenidos de los artículos científicos obtenidos en la revisión sistemática; alcance descriptivo para describir la arquitectura que se propone en este documento; alcance correlacional para describir las relaciones entre los componentes de la arquitectura.

Se utiliza la Revisión Sistemática de la Literatura de (Bertolino et al., 2019) para determinar la confiabilidad, validez y objetividad los artículos seleccionados.

4.1 Analizar modelos en artículos científicos para conocer la seguridad aplicada a IIoT.

En la planificación del primer objetivo, se adopta de (Bertolino et al., 2019) las fases de la Revisión Sistemática de la Literatura (RSL) que identifica y categoriza investigaciones relevantes sobre Seguridad aplicada a IIoT o Arquitecturas IIoT. El análisis cubre modelos de seguridad en entornos IIoT en cualquier dominio o área. La búsqueda incluye 4 bibliotecas digitales: ACM, IEEE, Science Direct y Springer.

La metodología de investigación RSL tiene 3 fases: Planificación de la revisión, Realización de la revisión e Informe de la revisión. Cabe destacar que aquí se presentan los métodos o proyección de los pasos, y los resultados de estas fases se presentan en el capítulo 5.

Fase 1) Planificación de la revisión: Aquí se entenderá el estado del arte de modelos IIoT y enfoques de seguridad sobre IIoT. Se proponen las siguientes preguntas de investigación (PI):

PI1: ¿Cuáles son los principales objetivos de seguridad de datos en IIoT?

PI2: ¿Cuáles son los entornos o dominios o áreas que utilizan IIoT?

PI3: ¿Cuáles son los protocolos utilizados para seguridad de datos en IIoT?

PI4: ¿Qué otras herramientas o métodos o técnicas se utilizan para seguridad de datos en IIoT?

PI5: ¿Cuáles son los dispositivos más utilizados en IIoT?

PI6: ¿Cuáles son los desafíos más comunes en seguridad de datos en IIoT?

Fase 2) Realización de la revisión: Aquí se inicia con la identificación de los artículos primarios, la búsqueda se centra en 4 bibliotecas digitales: ACM Digital Library, IEEE Xplore, Science Direct, y Springer Link. En esta fase existen 5 pasos:

2.1 Búsqueda en las Bibliotecas Digitales. Se busca por título o palabras clave mediante una cadena de búsqueda: "Industrial Internet of Thing OR IIoT OR Security Industrial Internet of Thing OR Security IIoT".

2.2 Selección con criterios de inclusión/exclusión. La selección es sobre el título y resumen de los artículos y se filtra de acuerdo a la Inclusión/Exclusión:

Tabla 1. Criterios

Criterio de inclusión	Artículos desde año 2017
	Artículos en idioma inglés
	Artículos que presenten arquitecturas IIoT
	Artículos que presenten seguridad en IIoT
Criterio de exclusión:	Artículos resumen
	Documentos de tesis o monografías o libros

Fuente: Autores.

2.3 Selección con evaluación de la calidad. Aquí se realiza una lectura completa del artículo para evaluar la calidad en cinco puntos:

Tabla 2. Evaluación

	Evaluación de calidad
EC1	¿Está claro el problema del estudio?
EC2	¿Está claro el modelo IIoT?,
EC3	¿Está clara la seguridad en IIoT?,
EC4	¿Están claras las limitaciones?,.
EC5	¿Está claro el enfoque de IIoT?
Respuestas No = 0, Parcialmente = 0.5 y Si = 1	

Fuente: Autores.

Cada artículo se basa en suma de los puntos individuales I_K con la siguiente ecuación Puntuación de calidad:

$$\sum_{k=1}^{K=5} I_k$$

Si un artículo tiene 2 o más puntos es aceptable.

2.4 Búsqueda Snowballing. Ésta búsqueda complementa las consultas, se adopta la "bola de nieve" con una sola interacción hacia atrás y hacia adelante para confirmar artículos que en la primera búsqueda se pasa por alto; en cada artículo seleccionado se analiza la lista de referencias y luego se verifica la referencia específica.

2.5 Evaluación de la metodología. Se realiza una búsqueda para confirmar los artículos primarios y relevantes. Se realiza otra búsqueda en las diferentes bibliotecas.

Los datos obtenidos serán tabulados en una hoja electrónica, para responder a las preguntas de investigación.

Fase 3) Informe de la revisión: Se desarrolla en la sección 5 de este documento, con los datos obtenidos en las 2 primeras fases. Se presentan resultados numéricos, análisis cuantitativos y respuestas a las preguntas de investigación.

4.2 Diseñar una arquitectura para robustecer el nivel en seguridad de datos en las comunicaciones de redes basado en IIoT.

En la observación de diseños en modelos IIoT que se encuentran en las referencias, se distingue ciertos aspectos clave en los desarrollos como niveles, dispositivos, protocolos, herramientas y comunicaciones.

Para planificar el segundo objetivo, se define un modelo en niveles para diferenciar los componentes en grupos, se verifica y se adopta los dispositivos (sensores/actuadores) para la adquisición de datos que se pueden utilizar, se verifica y se adoptan los dispositivos para el transporte de datos que se pueden utilizar, se adoptan dispositivos para almacenamiento de los datos, se adoptan dispositivos para el procesamiento de datos, se adoptan herramientas para el análisis de datos, se verifica y se adoptan protocolos/herramientas para seguridad en cada nivel, se describen las herramientas

necesarias para gestión de la información procesada. Se describen las responsabilidades o funciones en cada nivel.

4.3 Evaluar la arquitectura teórica para identificar el nivel de rendimiento y seguridad

Para planificar el tercer objetivo, se emplea la herramienta de programación visual NODE RED. Con NODE RED, es posible agregar o suprimir nodos y establecer conexiones entre ellos para facilitar la comunicación. Esta utilidad se muestra especialmente beneficiosa para equipos involucrados en labores industriales o para el desarrollo y ensayo de soluciones destinadas a equipos de planta que requieren interconectarse. NODE RED funciona como un motor de flujos con un enfoque en Internet de las cosas (IoT), lo que habilita la definición de flujos de servicios a través de protocolos como MQTT.

5. Resultados y discusión

En esta fase, los resultados son las respuestas a los objetivos específicos planteados en esta investigación.

5.1 Análisis de modelos en artículos científicos para conocer la seguridad aplicada a IIoT.

Para llegar a este primer resultado se ejecutaron los pasos de la Revisión Sistemática de la Literatura propuestas en el capítulo anterior, la Planificación de la Revisión que presenta las preguntas de investigación son respondidas en este capítulo; la Realización de la Revisión se desarrolló de acuerdo a las fases presentadas en el capítulo anterior, luego de la búsqueda y selección se obtuvieron 45 artículos, la realización se plasma en la figura 1 que utiliza un diagrama PRISMA. Estos 45 artículos fueron tabulados en una hoja electrónica, la hoja contiene las siguientes características: Nombre del artículo, país, año, objetivos (Confidencialidad, Integridad, Disponibilidad, Confiabilidad, Privacidad, Protección, Transparencia, Seguridad), Dominios (Industria, Salud, Ciudad, Inteligente, Agricultura, Energía), Protocolos (Algoritmos Cifrado, HTTP, ZigBee, WiFi, Bluetooth, CoAp, AMQP, MQTT, SSH, XMPP, LoRaWAN), Otras herramientas (Blockchain, Fog O Edge, Inteligencia Artificial, Big Data, 5G), Dispositivos (Sensores, Actuadores, Microcontroladores), Desafíos (Reducir latencia, Reducir sobrecarga, Emparejar, Tolerancia a fallos, Ataques, Resiliencia, Amenazas, Vulnerabilidades, Riesgos), Otras características (Arquitectura, Framework, Modelo, No específica, Capas).

Estos 45 artículos tabulados responden las preguntas de investigación y se obtienen gráficos que ayudan a entender las respuestas, luego a continuación se describe las respuestas de acuerdo a los hallazgos.

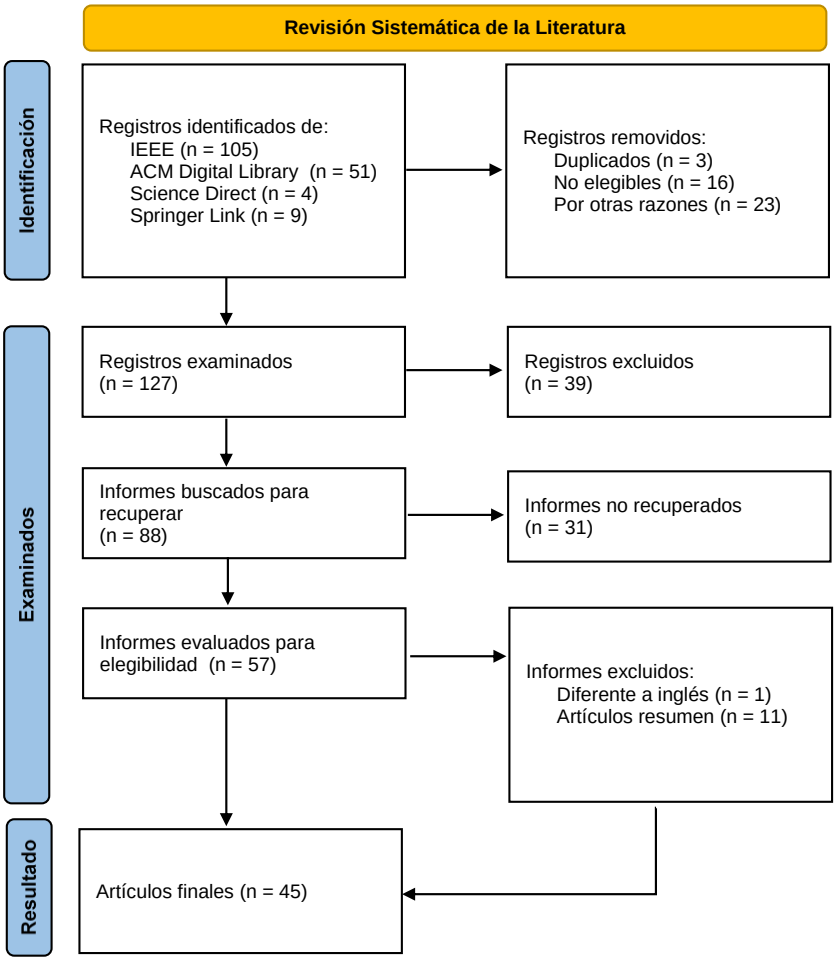

Figura 1. PRISMA.

Entre los 45 artículos, el 49% presenta arquitecturas, 24% presenta modelos, 18% no especifica, y 9% presenta framework, ver figura 2. Las arquitecturas son diseños detallados de las propuestas que presentan en capas, componentes, herramientas utilizadas, tecnologías utilizadas, procesos y flujos de información. Los modelos son diseños más generales, no todo modelo se presenta las capas o componentes. Las arquitecturas y modelos son propuestas para empresas o entornos específicos. Los framework son propuestas que se pueden adaptar a cualquier tipo de entono o dominio. El 58% de los artículos (26 documentos) presenta su propuesta en capas, la mínima cantidad de capas utilizada es 3, la máxima es 7, el promedio de capas es 4.

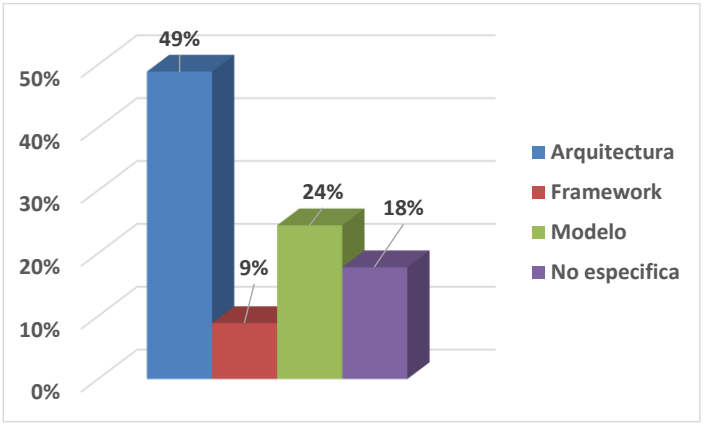

Figura 2. Características.

A continuación, en la tabla 3 se presentan los artículos científicos agrupados por regiones, se resalta que se encontró 7 artículos de Ecuador.

Tabla 3. Artículos científicos

China: (Hou et al., 2019), (Gao et al., 2021), (Liu et al., 2020), (P. Zhang et al., 2020), (Chen et al., 2019), (M. Zhang et al., 2021), (Li et al., 2018).
India: (Karmakar, 2019), (Gaba et al., 2021), (Paliwal, 2019), (Dave et al., 2020), (Panchal, 2018), (Wu et al., 2019).
Brasil: (Nakamura, 2018), (Ferrera et al., 2018).
Ecuador: (Minchala et al., 2020), (Lozada et al., 2020), (Espín et al., 2018), (C. A. Garcia et al., 2018), (Caiza et al., 2019), (Montalvo et al., 2020), (Pablo et al., 2021).
Otras regiones: (Abuhasel & Khan, 2020), (Yu & Yuira-staredusg, 2019), (Puri, 2020), (Buja et al., 2022), (Al-hawawreh, 2021), (Wadsworth et al., 2020), (Drăgulinescu et al., 2022), (Conference et al., 2020), (Almadani & Mostafa, 2021), (Gebremichael et al., 2020), (Kasongo, 2021), (Makrakis et al., 2021), (Al-Hawawreh et al., 2021), (Ferrag et al., 2022), (Farooq et al., 2022), (Munoz et al., 2019), (Saksonov et al., 2019), (Knezevic & Kasunic, 2020), (Koroniotis et al., 2021), (Darwish et al., 2020), (Alsaedi, Moustafa, Tari, Mahmood, & Anwar, 2020), (Hafeez et al., 2021), (Genge et al., 2019).

Fuente: Autores.

PI1: ¿Cuáles son los principales objetivos de seguridad de datos en IIoT?

Entre los 45 artículos, 38% aplica o nombra la palabra Seguridad, 15% nombran la Integridad, 13% nombran la Privacidad, 11% nombran la Confidencialidad, 11% nombran la Disponibilidad, 4% nombran la Transparencia, 3% nombran la Protección, 3% nombran la Confiabilidad, ver figura 3. Se resalta que 18% de los artículos (8 documentos) aplican la combinación Confidencialidad-Integridad-Disponibilidad (CIA). Otro 18% de los artículos (8 documentos) no aplica ni nombra ninguna de los objetivos de seguridad, solo presentan la propuesta de modelo en IIoT sin ninguna medida de

seguridad. Otro 13% de los artículos (12 documentos) aplica Privacidad en combinación con Seguridad.

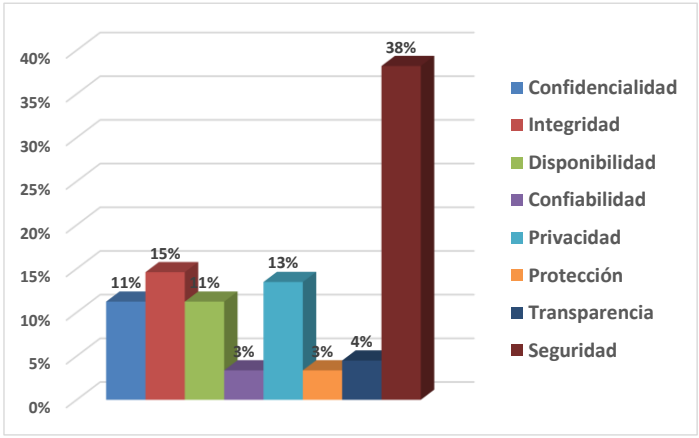

Figura 3. Objetivos en seguridad de datos IIoT.

PI2: ¿Cuáles son los entornos o dominios o áreas que utilizan IIoT?

Entre los 45 artículos, cada artículo aplica IIoT a un solo entorno, el entorno más utilizado es Industria con 56%, luego Energía como gas o electricidad con 18%, luego Salud con 13%, luego Ciudad Inteligente con 8%, y Agricultura con 5%, ver figura 4. Se resalta que IIoT no solo se utiliza en Industria también en las otras áreas que se nombran, en Salud se utiliza robot o conexiones de dispositivos médicos a gran escala o diagnóstico de Covid-19 en grandes volúmenes de datos. En energía se utiliza robots en petróleo o monitoreo de gas o mantenimiento predictivo de instalaciones. En ciudad inteligente se utiliza IIoT para sistema de comunicaciones a mayor escala.

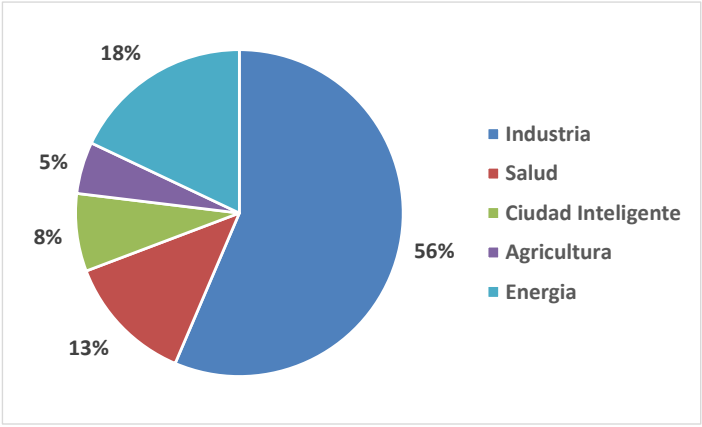

Figura 4. Entornos que se utilizan en IIoT.

PI3: ¿Cuáles son los protocolos utilizados para seguridad de datos en IIoT?

Entre los 45 artículos, los protocolos más utilizados son MQTT en 19%, luego Algoritmos Cifrados en 18%, WiFi en 18%, luego LoRaWAN en 9%, luego HTTP en 8%, luego ZigBee en 7%, CoAp en 7%, luego Bluetooth en 6%, luego AMQP en 4%, XMPP en 4%, y SSH en 1%, ver figura 5. Se resalta que algunos modelos utilizan varios protocolos a la vez. Los Algoritmos Cifrados son adaptaciones de algoritmos de encriptación como AES. Wifi es utilizado en combinación con ZigBee o Bluetooth en 9% de los artículos (4 documentos). CoAp y MQTT se utilizan en combinación en 11% de los artículos (5 documentos). El Algoritmo Cifrado se utiliza de manea única en 11% de los artículos (5 documentos), en los demás artículos (10 documentos) se utiliza en combinación con varios protocolos.

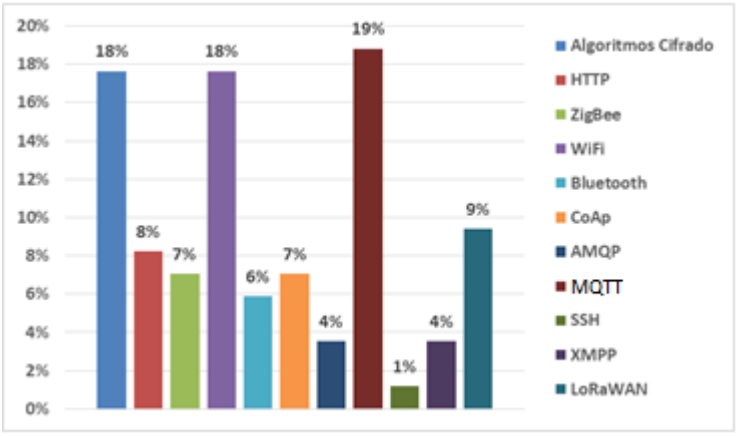

Figura 5. Protocolos en IIoT.

PI4: ¿Qué otras herramientas o métodos o técnicas se utilizan para seguridad de datos en IIoT?

Entre los 45 artículos, otras herramientas tecnológicas que se utilizan en combinación con IIoT son: Fog-Edge en 33%, Inteligencia Artificial en 27%, Blockchain en 18%, tecnología 5G en 18%, y Big Data en 3%, ver figura 6. Se resalta que Inteligencia Artificial se utiliza para obtener tendencias de posibles ataques a las infraestructuras IIoT y tomar acciones preventivas. Inteligencia Artificial se utiliza en combinación con otras tecnologías como blockchain/Fog/5G en 13% de los artículos (6 documentos). Otro grupo solo utiliza Inteligencia Artificial en 7% de los artículos (3 documentos). Las propuestas en Blockchain se utilizan para un almacenamiento seguro y distribuido de la información recolectada. Fog se utiliza en 18% de los artículos (8 documentos) para preparación de los datos recolectados en centros descentralizados. Big Data se utiliza

para conversión de diferentes tipos de datos recolectados por los sensores, y luego se aplica para análisis de datos.

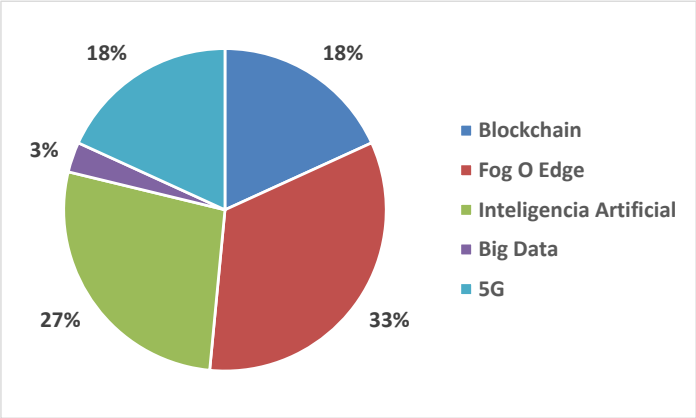

Figura 6. Otras herramientas en IIoT.

PI5: ¿Cuáles son los dispositivos más utilizados en IIoT?

Entre los 45 artículos, los dispositivos se clasificaron en: los Sensores son los dispositivos que capturan los datos en 51%, los Actuadores son los dispositivos que emiten señales de órdenes a las maquinarias en 28%, los Microcontroladores están incluidos PLC o Raspberry u otros dispositivos en 21%, ver figura 7. Se resalta que un grupo de investigaciones utiliza la combinación Sensores-Actuadores-Microcontroladores en 33% de los artículos (15 documentos). Otro grupo utiliza solo Sensores en 33% de los artículos (15 documentos). Otro grupo utiliza Sensores en combinación con Actuadores en 11% de los artículos (5 documentos). Todas las propuestas que utilizan Microcontroladores se basan en los Sensores que capturaron datos.

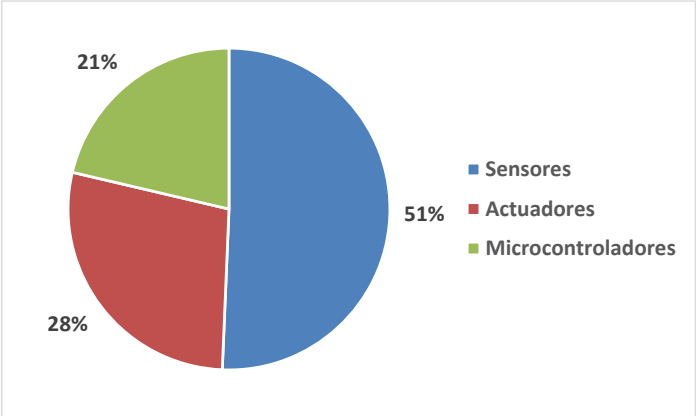

Figura 7. Dispositivos en IIoT.

PI6: ¿Cuáles son los desafíos más comunes en seguridad de datos en IIoT?

Entre los 45 artículos, los desafíos encontrados están: Ataques en 28%, Reducir Latencia en 16%, Amenazas en 16%, Vulnerabilidades en 15%, Riesgos en 9%, Tolerancia a Fallos en 8%, Reducir Sobrecarga en 2%, Resiliencia en 2%, Emparejar en 1%, ver figura 8. Se resalta que los Ataques es cualquier suceso contra el modelo IIoT como virus, malware, denegación de acceso u otros. Los desafíos Amenazas-Vulnerabilidades-Riesgos se nombran en 18% de los artículos (8 documentos). La Tolerancia a Fallos se nombra con Reducir Latencia en 13% de los artículos (6 documentos). Reducir Latencia en nombrada de manera única en 11% de los artículos (5 documentos). Ataque en nombrada de manera única en 9% de los artículos (4 documentos). Reducir Latencia es nombrada con Reducir Sobrecarga en 4% de los artículos (2 documentos).

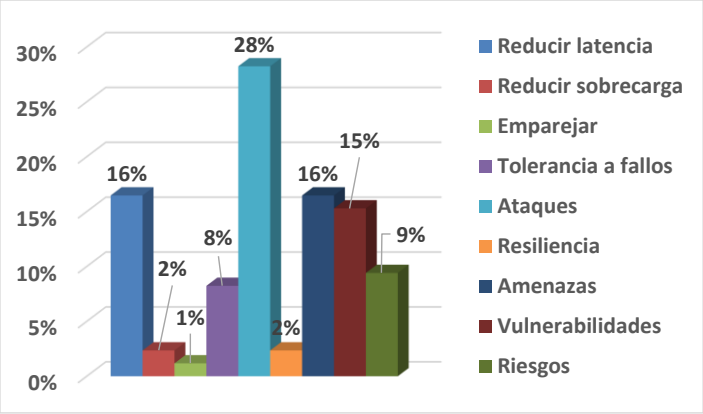

Figura 8. Desafíos en IIoT.

5.2 Diseño de una arquitectura para robustecer el nivel en seguridad de datos en las comunicaciones de redes basado en IIoT.

Para el diseño de la arquitectura se adopta de (Chen et al., 2019) una "estrategia de protección" para aumentar el nivel de seguridad en diferentes entornos IIoT, el marco de protección de seguridad actúa en los niveles o capas de Adquisición de datos, Transporte de datos y Procesamiento de datos. De (Saksonov et al., 2019) se adoptan

las recomendaciones en protocolos para minimizar los problemas de seguridad de datos en entornos IIoT.

La arquitectura se propone en capas porque es entendible a los diseñadores e implementadores (Abuhasel & Khan, 2020), (Al-Hawawreh et al., 2021), (Wadsworth et al., 2020), (Drăgulinescu et al., 2022). Se propone una arquitectura IIoT con un alto nivel de seguridad de los datos, la arquitectura se la presenta en capas para mejor entendimiento, ver figura 9; a continuación, se describe las capas de la arquitectura.

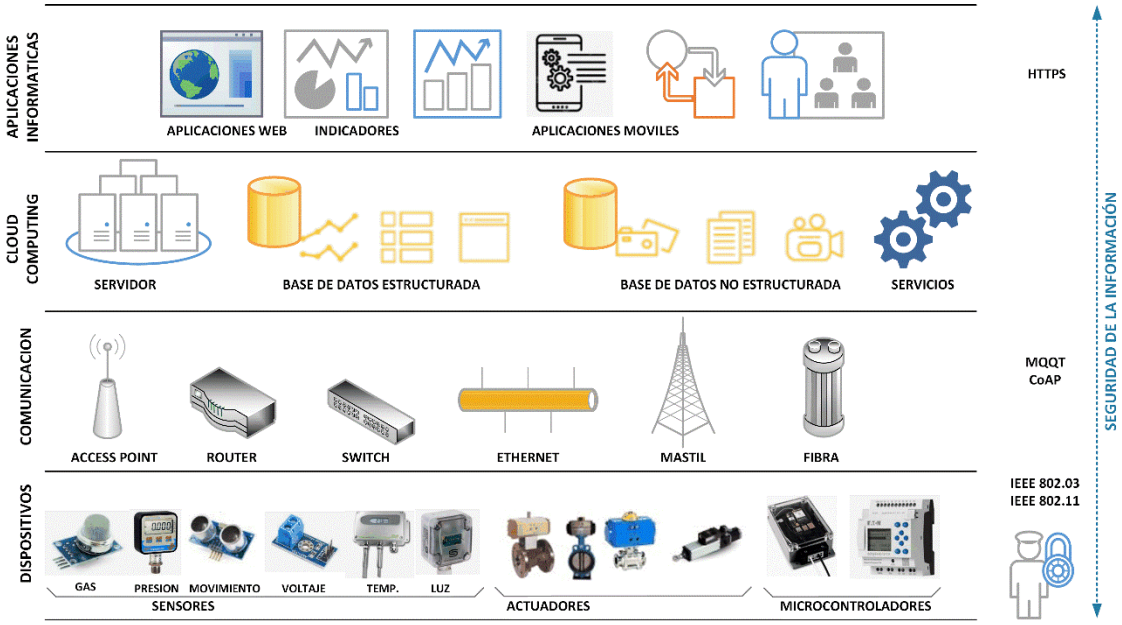

Figura 9. Arquitectura para seguridad de datos en IIoT.

Capa Dispositivos: Esta capa se encarga del seguimiento de cualquier tipo de dato y su entorno, captura los datos del mundo físico y los almacena en el mundo digital; se utilizan Sensores que son dispositivos heterogéneos para capturar datos, existen distintos tipos de sensores como infrarrojo, vibración, brújula, huno, inductivo, voltaje eléctrico, circuitos, movimientos, sonido, presión, gas, temperatura, caudal, humedad, peso, red, distancia, iluminación, funcionamiento, entre otros. También se pueden utilizar Actuadores que reciben una señal y la convierten en movimiento, los Actuadores se activan de acuerdo a las órdenes enviadas por los Microcontroladores o los servicios de la nube, los actuadores pueden ser eléctricos, hidráulicos o neumáticos. También se pueden utilizar Microcontroladores como PLC o Raspberry o Arduino. Los dispositivos se conectan a la red mediante Gateway. Como medida de Seguridad para evitar el acceso no autorizado se debe registrar el dispositivo y el inicio de sesión a la red. Se

adoptan sensores basados en las referencias (Minchala et al., 2020), (Lozada et al., 2020) y (Hou et al., 2019).

Capa Comunicación: Se encarga de la agregación y conectividad para la comunicación de los dispositivos hacia el Internet, aquí se realiza la interoperabilidad entre diversos estándares-protocolos-sistemas; se utilizan Access point, router, switch, antenas de comunicación, cableado físico, unidades de corriente continua, mástiles de comunicación. En esta capa se ejecutan todas las funciones de comunicación y transmisión de datos, aquí se conectan todos los dispositivos. Se adoptan componentes de comunicación basados en las referencias (Karmakar, 2019), (Almadani & Mostafa, 2021) y (Gao et al., 2021).

Como medida de Seguridad las conexiones físicas deben utilizar el protocolo Ethernet IEEE 802.3 (Puri, 2020); las conexiones inalámbricas deben utilizar el protocolo IEEE 802.11; el protocolo HTTP se utiliza para acceso desde redes externas, además para envío-recibo de notificaciones (Hou et al., 2019); el protocolo MQTT se utiliza para publicación de datos en el servidor de la nube y se utiliza en dispositivos con pocos recursos (Ferrag et al., 2022), (Farooq et al., 2022).

Capa Cloud Computing: Esta capa recibe los datos o medidas o estados del entorno desde la capa de comunicación para almacenar y procesar los datos; esta capa es fuerte con sólidas características de computación y almacenamiento, y está formada por servidores de alto rendimiento; los datos en la nube pueden ser procesados en tiempo real y ser presentados por las aplicaciones informáticas para análisis y toma de decisiones. En esta capa también se encuentran los Servicios para procesamiento de datos, generación de gráficos, almacenamiento, consultas de información y posibles actualizaciones. También se encuentra la base de datos estructurada que se propone para guardar información resumida de la jornada industrial; la base de datos no estructurada se propone para guardar datos de los sensores heterogéneos porque los datos son distintos en tipo y volumen. También se encuentra el Servidor que contiene el sistema operativo y gestiona el almacenamiento y procesamiento de los datos. Se adopta los componentes de la nube basados en las referencias (Li et al., 2018) y (Alsaedi, Moustafa, Tari, Mahmood, & Adna N Anwar, 2020).

Capa Aplicaciones Informáticas: En esta capa se definen las interfaces gráficas de usuario para conectar la información IIoT, las interfaces definen los resultados analíticos y los gráficos estadísticos de información que son obtenidos de los servicios de la nube; en esta capa se realiza el desarrollo, implementación y operación de las aplicaciones IIoT, esta capa es flexible por los cambios de las interfaces de acuerdo a las necesidades de la empresa. En esta capa se definen los indicadores que ayudan en la mejor toma de decisiones para realizar acciones preventivas o correctivas, se propone indicadores generales como: caudal, presión, temperatura, humedad, ciclos de operación, energía. Se adoptan los componentes de las aplicaciones basados en las referencias (Hafeez et al., 2021), (Koroniotis et al., 2021) y (Knezevic & Kasunic, 2020).

5.3 Evaluación de la arquitectura teórica para identificar el nivel de rendimiento y seguridad

Para evaluar la arquitectura de seguridad se realiza un caso en software en NODE RED para la seguridad se utiliza el protocolo MQTT. Se utiliza MQTT porque se basa en comunicación de publicación-suscripción, el cliente sensor publica mensajes en un intermediario, se utiliza en sistemas inalámbricos que minimicen la latencia; en caso de perder la conexión de suscripción, el intermediario mantiene el mensaje y lo envía al suscriptor al restablecerse la conexión, además tiene rendimiento en velocidad (Espín et al., 2018).

A continuación, se presenta diagramas del flujo de información en el protocolo MQTT que establece las etapas de comunicación para el envío de información, tanto para una arquitectura sin seguridad y con seguridad, ver figura 10 y figura 11.

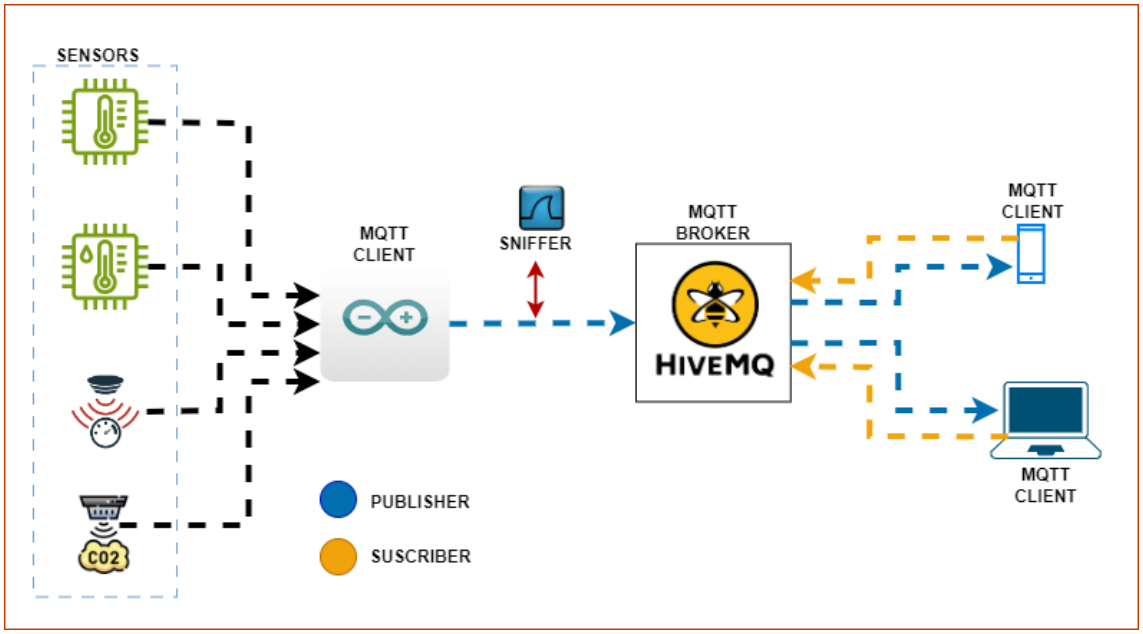

Figura 10. Flujo de envío de información en protocolo MQTT sin Seguridad.

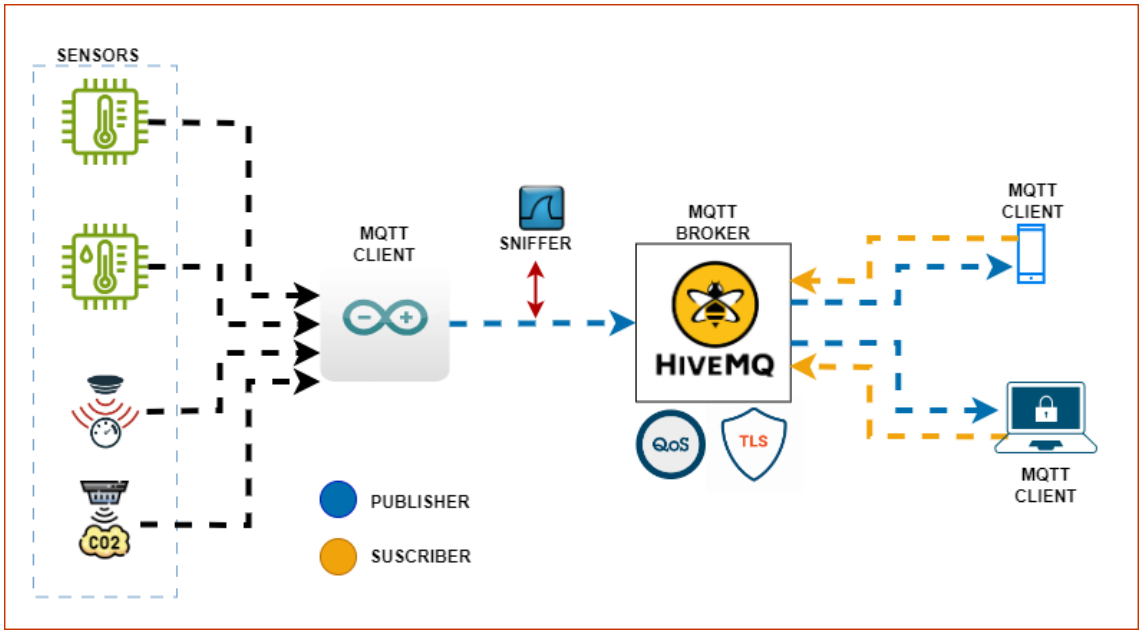

Figura 11. Flujo de envío de información en protocolo MQTT con Seguridad.

El protocolo MQTT tiene el siguiente flujo:

1. Conexión entre Servidor MQTT (Broker) y el Cliente MQTT (Publisher).
2. Recolección de información por parte de los sensores (temperatura, humedad, presión de aire y concentración de CO2).
3. Visualización de resultados recolectados y almacenados en el servidor MQTT desde el Cliente MQTT (Subscriber).

La arquitectura ejemplo está formada por el protocolo MQTT. Contiene sensores de humedad, sensor de temperatura, sensor de presión de aire y sensor de concentración de CO2 que están conectados a un SBC board (MQTT Client Publisher); los datos que son receptados por los sensores son enviados al MQTT BROKER (server) y finalmente los datos pueden ser presentados en dispositivos finales como smartphones, laptops, mediante dashboards de visualización (MQTT Client SUSCRIBER) Ver figura 12.

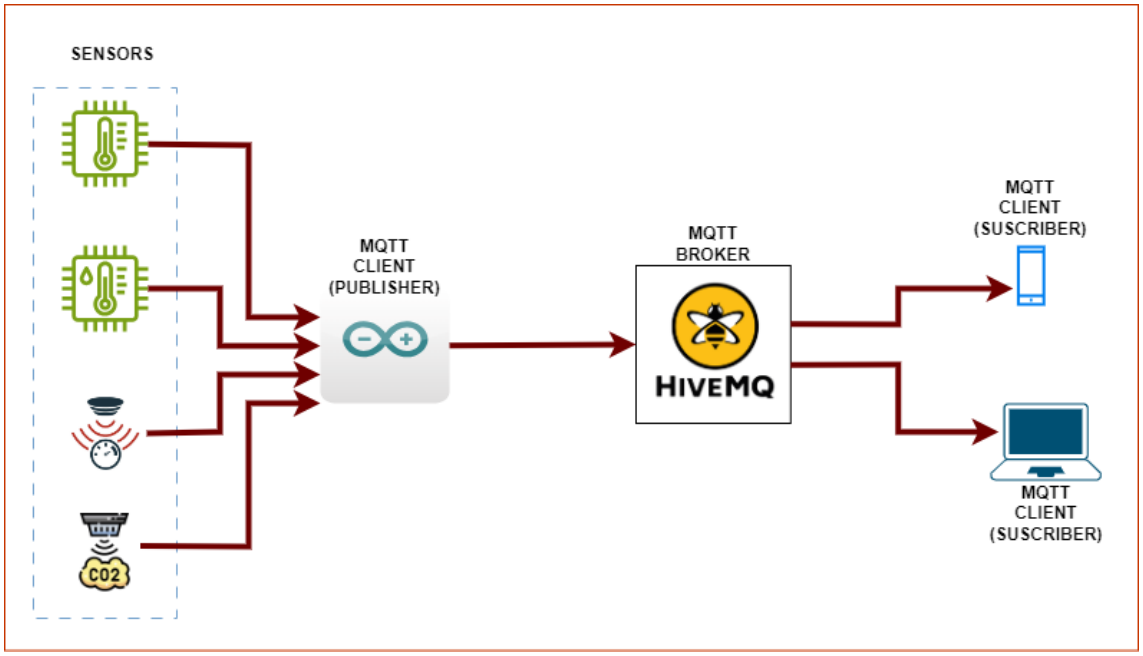

Figura 12. Arquitectura teórica

Para la evaluación de MQTT se proponen dos escenarios:

Escenario 1, Arquitectura Sin Seguridad: Envío de paquetes en texto plano que permite obtener la información enviada es leíble.

Escenario 2, Arquitectura con Seguridad: Se aplica MQTT con TLSv1.2, permite que la información enviada sea cifrada y no sea leíble ni vulnerada, y es más seguro para la transmisión de información.

La tabla 4 presenta las configuraciones de los dos escenarios, el tiempo de envío de paquetes es cada milisegundo por cada minuto, la diferencia está en el uso del protocolo MQTT.

Tabla 4. Escenarios de simulación en la arquitectura

	Sin seguridad	**Con Seguridad**
Server	ServerMqtt	ServerMqtt
Action	Subcribe to single topic	Subcribe to single topic
Topic	Sensors	Sensors
QoS	2	2
Output	Auto-detect	Auto-detect
Name	Broker	Broker
Connection	Broker.hivemq.com	Broker.hivemq.com
Port	1883	8883
Connect auto	Yes	Yes
Use TLS	No	Yes
Protocol	-	MQTT v3.1.1
Keep Ailve	60	60
Use clean session	Yes	Yes
Loop Every	0.001 Seconds	0.001 Seconds
Max Timeout	1 Minute	1 Minute
Source	52.29.97.85	192.168.18.42
Destination	192.168.18.42	3.77.247.6
Longitud	362 bytes	399 bytes
Capturados	362 bytes	54 bytes
Legible	Si	No

Fuente: Autores.

Dentro de las simulaciones se verifican las variables:

1. Sniffing de paquetes sobre la Arquitectura sin seguridad y con seguridad: el "sniffing" es un problema de seguridad recurrente que se presenta en la actualidad como la intersección del tráfico de red, con el uso de herramientas, los datos pueden ser leídos fácilmente y vulnerados, comprometiendo la seguridad de la red que puede

ser aprovechada por hackers para sus ataques cibernéticos. Para las simulaciones se utiliza un sniffer “Wireshark” que permite capturar los paquetes que se transmiten en la red. La figura 12, muestra los datos capturados por el “sniffing” como temperatura, humedad, presión, estado de luz y otros datos, que están resaltados en color amarillo. Los 362 bytes que se transmitieron fueron capturados y son leíbles en 100%.

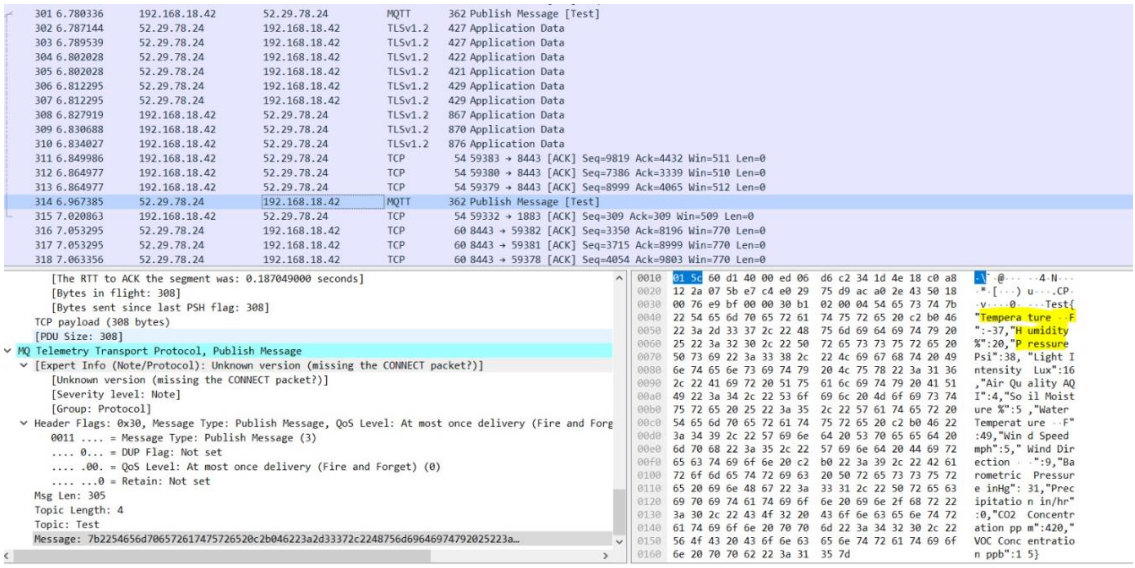

Figura 13. Prueba sin seguridad

La figura 13, muestra los datos capturados por el “sniffing”, estos datos de la dirección enviada 192.168.18.42 están resaltados en color azul. Los 399 bytes que se transmitieron fueron capturados 54 bytes de ida, y capturados 66 bytes de regreso y son leíbles en 0%.

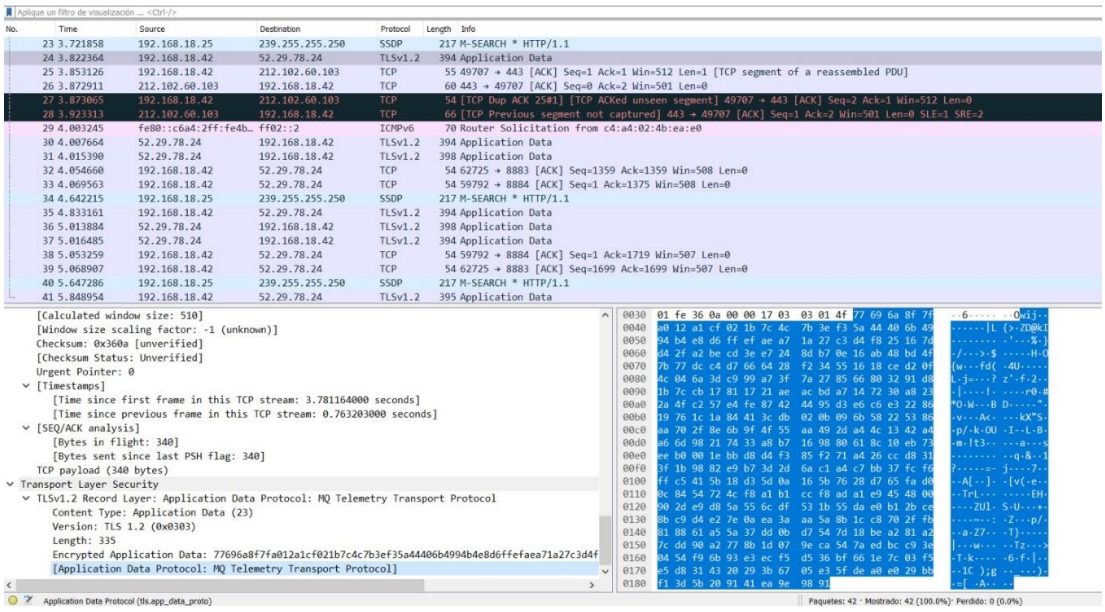

Figura 14. Prueba con seguridad

2. Análisis de paquetes enviados y recibidos sobre la Arquitectura sin seguridad y con seguridad y verificación de paquetes perdidos, aquí se conoce la cantidad de paquetes enviados y recibidos de extremo a extremo, así como los paquetes perdidos, se presenta la cantidad de paquetes enviados y recibidos por 1 minuto, ver tabla 5.

Tabla 5. Paquetes en los escenarios

Escenario	Paquetes Enviados	Paquetes Recibidos	Paquetes Perdidos
Sin seguridad			
Prueba 1	13543	13543	0
Prueba 2	13845	5957	7888
Prueba 3	14769	2309	12463
Con seguridad			
Prueba 1	16817	16817	0
Prueba 2	12247	5549	6698
Prueba 3	11728	1551	10177

Fuente: Autores.

3. Tasa de entrega y pérdida de publicaciones: Los resultados de la tasa de entrega-pérdida de publicaciones sobre el mecanismo de confiabilidad QoS en función de la cantidad de sensores que generan publicaciones. Se tiene una tasa de entrega promedio del 99.38% y una tasa de pérdida promedio del 0.62% en la recepción de publicaciones al momento que el mecanismo utiliza seguridad. El mecanismo de confianza CERO del protocolo MQTT tiene un 100% de tasa de entrega en cualquiera de los dos escenarios.

Tabla 6. Mecanismos de confianza en los escenarios

Mecanismo de confiabilidad	Entrega	Pérdida
Sin seguridad		
QoS 0	100%	0%
QoS 1	43.03%	56.97%
QoS 2	15.62%	84.38%
Promedio	52.88%	47.12%
Con seguridad		
QoS 0	100%	0%
QoS 1	98.47%	1.53%
QoS 2	99.68%	0.32%
Promedio	99.38%	0.62%

Fuente: Autores.

Tabla 7. Niveles de QoS en MQTT

Nivel	Entrega
QoS 0 (QoS At Most Once)	En este nivel, el mensaje se entrega una vez o no se entrega en absoluto. No hay garantía de que el mensaje se entregue con éxito, ya que no se realizan intentos de reenvío. Esto hace que el nivel de QoS 0 sea el más eficiente en términos de ancho de banda y latencia, pero con el riesgo de pérdida de mensajes.
QoS 1 (QoS At Least Once)	En este nivel, se garantiza que el mensaje se entregue al menos una vez al destinatario, lo que implica un proceso de confirmación. Si el cliente no recibe un acuse de recibo del servidor, se realizará un reenvío. Esto garantiza que el mensaje se entregue al menos una vez, pero puede provocar duplicaciones de mensajes si hay interrupciones en la red.
QoS 2 (QoS Exactly Once)	En este nivel, se garantiza que el mensaje se entregue exactamente una vez al destinatario. Utiliza un proceso de intercambio de mensajes más complejo, que implica un intercambio de cuatro etapas entre el cliente y el servidor para garantizar que el mensaje se entregue solo una vez. Este nivel es el más fiable, pero puede introducir mayor latencia y sobrecarga en la red.

Fuente: Autores.

Sobre la seguridad del protocolo MQTT, se aplica en el nivel de red que genera conexión fiable para envíos entre servidor y clientes; a nivel de transporte se aplica la encriptación para dar confidencialidad, es decir la información cifrada no es leíble en el envío, porque el cliente utiliza mecanismos de autenticación para validar su identidad en ambos extremos; a nivel de aplicación el protocolo genera una identificación de cliente que certifica al dispositivo ante la aplicación, además el protocolo encripta la carga útil que aumenta la seguridad de los datos.

En base al análisis de la arquitectura evaluada, podemos enfatizar que el protocolo MQTT mantiene buenas características, debido a que MQTT dispone de una variación de autenticación como el uso de identificador de cliente, usuario/contraseña, además el broker MQTT tiene la capacidad de controlar quiénes pueden subscribirse o publicar en determinados topics. Otra característica a resaltar es, que por naturaleza MQTT es capaz de establecer tres niveles de QoS diferentes, garantizando la entrega de información.

Como características adicionales, podemos indicar que MQTT es óptimo para aquellos dispositivos que tienen memoria y batería limitadas, para redes con entornos restringidos e inseguros y redes con ancho de banda reducido y alta latencia, además de ser un protocolo abierto y fácil de implementar.

6. Conclusiones

Se concluye que cada modelo IIoT, revisado y obtenidos de la revisión sistemática, tiene su propia dinámica y características que requieren sus enfoques en evaluación de riesgos y se debe considerar el marco de seguridad, la interacción físico-digital y sus límites; entre los 45 artículos obtenidos los porcentajes más altos son: el 49% de todos presenta arquitecturas, el 38% de todos apuntan principalmente a la Seguridad, el 56% de todos son dirigidos a Industria y el 19% de todos utilizan el protocolo MQTT. En base al resultado de la revisión sistemática, se concluye que el protocolo más recomendable para seguridad de información es MQTT.

Esta arquitectura que se propone en este documento debe ser seleccionada porque se basa en una “estrategia de protección” que aumenta el nivel de seguridad y en recomendaciones del protocolo MQTT para minimizar los problemas de seguridad de datos, en base a los resultados de la evaluación con MQTT, los datos son cifrados en 100%, son leíbles en 0%, el mecanismo de confiabilidad propio de MQTT presenta una tasa de entrega promedio de 99.38% y una tasa de pérdida promedio de 0.62%; esto afianza esta propuesta.

La arquitectura propuesta es entendible porque se presenta en capas y los componentes se adoptaron de la investigación científica; las cuatro capas Dispositivos, Comunicación, Cloud Computing y Aplicaciones Informáticas están dirigidas a la industria y diseñadores-implementadores.

Se concluye que el protocolo MQTT utilizado en esta propuesta mantiene excelentes características porque dispone de una variación de autenticación como el uso de identificador, control de subscriptor-publicador y servicio de calidad que garantizan el cifrado-entrega de datos; esto lo convierte en óptimo para aquellos dispositivos que tienen memoria y batería limitadas, además es un protocolo abierto y fácil de implementar; las pruebas del prototipo con el protocolo MQTT certifica que la entrega en 99.38% y transmisión del tráfico de red se encuentra cifrada durante el envío en 100%.

Referencias

Abuhasel, K. A., & Khan, M. A. (2020). A Secure Industrial Internet of Things (IIoT) Framework for Resource Management in Smart Manufacturing. *IEEE Access*, *8*, 117354–117364. https://doi.org/10.1109/ACCESS.2020.3004711

Al-hawawreh, M. (2021). Developing a Security Testbed for Industrial Internet of Things. *IEEE Internet of Things Journal*, *8*(7), 5558–5573. https://doi.org/10.1109/JIOT.2020.3032093

Al-Hawawreh, M., Sitnikova, E., & Aboutorab, N. (2021). Asynchronous peer-to-peer federated capability-based targeted ransomware detection model for industrial IoT. *IEEE Access*, *9*, 148738–148755. https://doi.org/10.1109/ACCESS.2021.3124634

Almadani, B., & Mostafa, S. M. (2021). IIoT based multimodal communication model for agriculture and agro-industries. *IEEE Access*, *9*, 10070–10088. https://doi.org/10.1109/ACCESS.2021.3050391

Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Adna N Anwar. (2020). TON-IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *IEEE Access*, *8*, 165130–165150. https://doi.org/10.1109/ACCESS.2020.3022862

Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. *IEEE Access*, *8*, 165130–165150. https://doi.org/10.1109/ACCESS.2020.3022862

Ambato, T. De, Irisarri, E., & Pérez, F. (2018). Flexible Container Platform Architecture for Industrial Robot Control. *IEEE*, 1056–1059. https://doi.org/10.1109/ETFA.2018.8502496

Bertolino, A., Rey, U., & Carlos, J. (2019). A Systematic Review on Cloud Testing. *ACM Computing Surveys*, *52*(5), 1–42. https://doi.org/https://doi.org/10.1145/3331447

Buja, A., Apostolova, M., & Luma, A. (2022). Cyber Security standards for the Industrial Internet of Things (IIoT)– A Systematic Review. *International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 4–9. https://doi.org/10.1109/HORA55278.2022.9799870

Caiza, G., Alvarez-m, E., Remache, E., & Ortiz, A. (2019). Comparación de AMQP y CoAP para la integración de las comunicaciones en el área de producción. *Iberian Journal of Information Systems and Technologies*, 652–667.

Chen, H., Hu, M., Yan, H., & Yu, P. (2019). *Research on Industrial Internet of Things Security Architecture and Protection Strategy*. 5–8. https://doi.org/10.1109/ICVRIS.2019.00095

Conference, I., Intelligence, C., Venugopal, V., Gudlur, R., & Raju, V. (2020). IIoT Digital Forensics and Major Security issues. *INSPEC*, *October*, 8–9. https://doi.org/10.1109/ICCI51257.2020.9247685

Darwish, L. R., Farag, M. M., & El-wakad, M. T. (2020). Towards Reinforcing Healthcare 4 . 0 : A Green Real-Time IIoT Scheduling and Nesting Architecture for COVID-19 Large-Scale 3D Printing Tasks. *IEEE Access*, *8*, 1–12. https://doi.org/10.1109/ACCESS.2020.3040544

Dave, M., Doshi, J., & Arolkar, H. (2020). MQTT- CoAP Interconnector: IoT

interoperability solution for application layer protocols. *Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020*, 122–127. https://doi.org/10.1109/I-SMAC49090.2020.9243377

Drăgulinescu, A. M. C., Manea, A. F., Fratu, O., & Drăgulinescu, A. (2022). LoRa-Based Medical IoT System Architecture and Testbed. *Wireless Personal Communications*, *126*(1), 25–47. https://doi.org/10.1007/s11277-020-07235-z

Espín, H. I., García, V., José, E., Lozada, C., Carlos, A., García, A., Marcelo, V., & García, V. (2018). Flexible Architecture for Transparency of a Bilateral Tele-Operation System implemented Transparency of of Robots Industry. *IFAC-PapersOnLine*, *51*(8), 239–244. https://doi.org/10.1016/j.ifacol.2018.06.383

Farooq, M. S., Sohail, O. O., Abid, A., & Rasheed, S. (2022). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Livestock Environment. *IEEE Access*, *10*, 9483–9505. https://doi.org/10.1109/ACCESS.2022.3142848

Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access*, *10*, 40281–40306. https://doi.org/10.1109/ACCESS.2022.3165809

Ferrera, E., Conzon, D., Brizzi, P., Rossini, R., Pastrone, C., Jentsch, M., Kool, P., Kamienski, C., & Sadok, D. (2018). XMPP-based infrastructure for IoT network management and rapid services and applications development. *Annales Des Telecommunications/Annals of Telecommunications*, *72*(7–8), 443–457. https://doi.org/10.1007/s12243-017-0586-3

Gaba, G. S., Kumar, G., Kim, T. H., Monga, H., & Kumar, P. (2021). Secure Device-to-Device communications for 5G enabled Internet of Things applications. *Computer Communications*, *169*(October 2020), 114–128. https://doi.org/10.1016/j.comcom.2021.01.010

Gao, Y., Chen, Y., Hu, X., Lin, H., Liu, Y., & Nie, L. (2021). Blockchain Based IIoT Data Sharing Framework for SDN-Enabled Pervasive Edge Computing. *IEEE Transactions on Industrial Informatics*, *17*(7), 5041–5049. https://doi.org/10.1109/TII.2020.3012508

Garcia, C. A., Naranjo, J. E., Ambato, U. T. De, Castro, M., Beltran, C., Ambato, U. T. De, & Iec-, A. S. (2018). Flexible Robotic Teleoperation Architecture Under IEC 61499 Standard for Oil & Gas Process. *International Conference on Emerging Technologies and Factory Automation (ETFA)*, 1269–1272. https://doi.org/10.1109/ETFA.2018.8502520

Garcia, V. (2020). An Augmented Reality Platform for training in the industrial context. *IFAC PapersOnLine*, *53*(3), 197–202. https://doi.org/10.1016/j.ifacol.2020.11.032

Gebremichael, T., Ledwaba, L. P. I., Eldefrawy, M. H., Hancke, G. P., Pereira, N., Gidlund, M., & Akerberg, J. (2020). Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. *IEEE Access*, *8*, 152351–152366. https://doi.org/10.1109/ACCESS.2020.3016937

Genge, B., Haller, P., & Enachescu, C. (2019). Anomaly Detection in Aging Industrial Internet of Things. *IEEE Access*, *7*, 74217–74230. https://doi.org/10.1109/ACCESS.2019.2920699

Hafeez, T., Xu, L., & Mcardle, G. (2021). Edge Intelligence for Data Handling and Predictive Maintenance in IIOT. *IEEE Access*, *9*, 49355–49371. https://doi.org/10.1109/ACCESS.2021.3069137

Hernández-Sampieri; Fernández-Collado; Baptista-Lucio. (2010). *Metodología de la Investigación*. McGraw-Hill Interamericana.

Hou, X., Ren, Z., Yang, K., Chen, C., Zhang, H., & Xiao, Y. (2019). IIoT-MEC : A Novel Mobile Edge Computing Framework for 5G-enabled IIoT. *IEEE Wireless Communications and Networking Conference (WCNC)*. https://doi.org/10.1109/WCNC.2019.8885703

Iglesias-Urkia, M., Orive, A., & Urbieta, A. (2018). Analysis of CoAP Implementations for Industrial Internet of Things: A Survey. *Procedia Computer Science*, *109*(2018), 188–195. https://doi.org/10.1016/j.procs.2017.05.323

Karmakar, A. (2019). Industrial Internet of Things : A Review. *International Conference on Opto-Electronics and Applied Optics (Optronix)*, 0–5. https://doi.org/10.1109/OPTRONIX.2019.8862436

Kasongo, S. M. (2021). An advanced intrusion detection system for IIoT Based on GA and tree based algorithms. *IEEE Access*, *9*, 113199–113212. https://doi.org/10.1109/ACCESS.2021.3104113

Kato, A., Maeno, T., Owada, Y., Sato, G., Temma, K., Kuri, T., Takai, M., & Ishihara, S. (2021). Link Setup Time Reduction by FILS on IEEE 802.11-Based Inter-Vehicular Communications. *IEEE Access*, *9*, 159796–159808. https://doi.org/10.1109/ACCESS.2021.3128974

Knezevic, D. B., & Kasunic, N. (2020). Security challenges of Wi-Fi connected beer cooler and serving IIoT device. *International Conference on Smart and Sustainable Technologies (SpliTech)*. https://doi.org/10.23919/SpliTech49282.2020.9243787

Koroniotis, N., Moustafa, N., Member, S., Schiliro, F., Gauravaram, P., & Janicke, H. (2021). The SAir-IIoT Cyber Testbed as a Service : A Novel Cybertwins Architecture in IIoT-Based Smart Airports. *IEEE Transactions on Intelligent Transportation Systems (Early Access)*, 1–14. https://doi.org/10.1109/TITS.2021.3106378

Li, G., Wu, J., Li, J., Wang, K., & Ye, T. (2018). Service Popularity-Based Smart Resources Partitioning for Fog Computing-Enabled Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *14*(10), 4702–4711. https://doi.org/10.1109/TII.2018.2845844

Liu, X., Zhang, T., Hu, N., Zhang, P., & Zhang, Y. (2020). The method of Internet of Things access and network communication based on MQTT. *Computer Communications*, *153*(January), 169–176. https://doi.org/10.1016/j.comcom.2020.01.044

Lozada, J. D., Bautista, A. D., & Rioja, L. (2020). *Diseño de arquitectura tecnológica de ciudadela inteligente Tecnipetrol , basado en industria 4 . 0 en Esmeraldas-Ecuador*. 1–16.

Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents. *IEEE Access*, *9*, 165295–165325. https://doi.org/10.1109/ACCESS.2021.3133348

Minchala, L. I., Peralta, J., & Mata-quevedo, P. (2020). An Approach to Industrial Automation Based on Low-Cost Embedded Platforms and Open Software. *Applied Sciences*, *10*, 2–15. https://doi.org/10.3390/app10144696

Montalvo, W., Garcia, C. A., Naranjo, J. E., & Ortiz, A. (2020). Sistema de Tele-operación para Robots Móviles en la industria del Petróleo y Gas. *Iberian Journal of Information Systems and Technologies Recebido/Submission:*, *February*.

Mora-sánchez, D., & Guerrero-marín, L. (2020). Industria 4.0: el reto en la ruta hacia las

organizaciones digitales. *Estudios de La Gestión*, *8*(8), 191–214. https://doi.org/https://doi.org/10.32719/25506641.2020.8.7

Munoz, J., Rincon, F., Chang, T., Vilajosana, X., Munoz, J., Rincon, F., Chang, T., Vilajosana, X., Vermeulen, B., Mu, J., Rincon, F., Chang, T., Vilajosana, X., & Vermeulen, B. (2019). *OpenTestBed : Poor Man ' s IoT Testbed To cite this version : HAL Id : hal-02266558 OpenTestBed : Poor Man ' s IoT Testbed*.

Nakamura, E. T. (2018). A Privacy , Security , Safety , Resilience and Reliability Focused Risk Assessment Methodology for IIoT Systems. *Global Internet of Things Summit (GIoTS)*. https://doi.org/10.1109/GIOTS.2018.8534521

Pablo, P., Henry, E., & Luis, N. (2021). MEASUREMENT AND REMOTE MONITORING OF HYDROGEN SULFIDE GAS GENERATED BY BATTERIES USING. *IEEE Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*. https://doi.org/10.1109

Paliwal, S. (2019). Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial internet of things. *IEEE Access*, *7*, 136073–136093. https://doi.org/10.1109/ACCESS.2019.2941701

Panchal, A. C. (2018). Security Issues in IIoT : A Comprehensive Survey of Attacks on IIoT and Its Countermeasures. *IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, 124–130. https://doi.org/10.1109/GCWCN.2018.8668630

Puri, V. (2020). Blockchain meets IIoT : An architecture for privacy preservation and security in IIoT. *International Conference on Computer Science, Engineering and Applications (ICCSEA)*. https://doi.org/10.1109/ICCSEA49143.2020.9132860

Saksonov, E. A., Leokhin, Y. L., & Azarov, V. N. (2019). Organization of Information Security in Industrial Internet of Things Systems. *Quality Management, Transport and Information Security, Information Technologies*, 3–7. https://doi.org/10.1109/ITQMIS.2019.8928442

Wadsworth, A., Thanoon, M. I., Mccurry, C., & Sabatto, S. Z. (2020). Development of IIoT Monitoring and Control Security Scheme for Cyber Physical Systems. *SoutheastCon*, 6–10. https://doi.org/10.1109/SoutheastCon42311.2019.9020516

Wu, T.-Y., Chen, C.-M., Wang, K.-H., & Wu, J. M.-T. (2019). Security Analysis and Enhancement of a Certificateless Searchable Public Key Encryption Scheme for IIoT Environments. *IEEE Access*, *7*, 49232–49239. https://doi.org/10.1109/ACCESS.2019.2909040

Yu, X., & Yuira-staredusg, S. (2019). A Survey on IIoT Security. *IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*. https://doi.org/10.1109/VTS-APWCS.2019.8851679

Zhang, M., Chu, R., Dong, C., Wei, J., Lu, W., Xiong, N., & Member, S. (2021). Residual Learning Diagnosis Detection : An Advanced Residual Learning Diagnosis Detection System for COVID-19 in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *17*(9), 6510–6518. https://doi.org/10.1109/TII.2021.3051952

Zhang, P., Wu, Y., & Zhu, H. (2020). Open ecosystem for future industrial internet of things (IIoT): Architecture and application. *CSEE Journal of Power and Energy Systems*, *6*(1), 1–11. https://doi.org/10.17775/CSEEJPES.2019.01810

Anexos

Dentro de la simulación llevada a cabo en NODE RED, se simula el envío de información de varios sensores de los cuales para esta práctica se hace uso de 4 sensores como son Temperatura, Humedad, Presión de Aire y Concentración de CO2. En la siguiente imagen podemos ver al lado izquierdo la configuración del MQTT CLIENT (Publisher), en el cual cuenta con un timmer para el envío de paquetes por 1 minuto, un contador de envío de paquetes, funciones para obtener la información de los sensores y gráfica de los mismos; mientras que al lado derecho se cuenta con la configuración del MQTT Broker, en donde se tiene un contador de recepción de paquetes, la conexión con el Broker MQTT (HiveMQ) y un debug que muestra la información de los paquetes que se recibieron (ver figura 16)

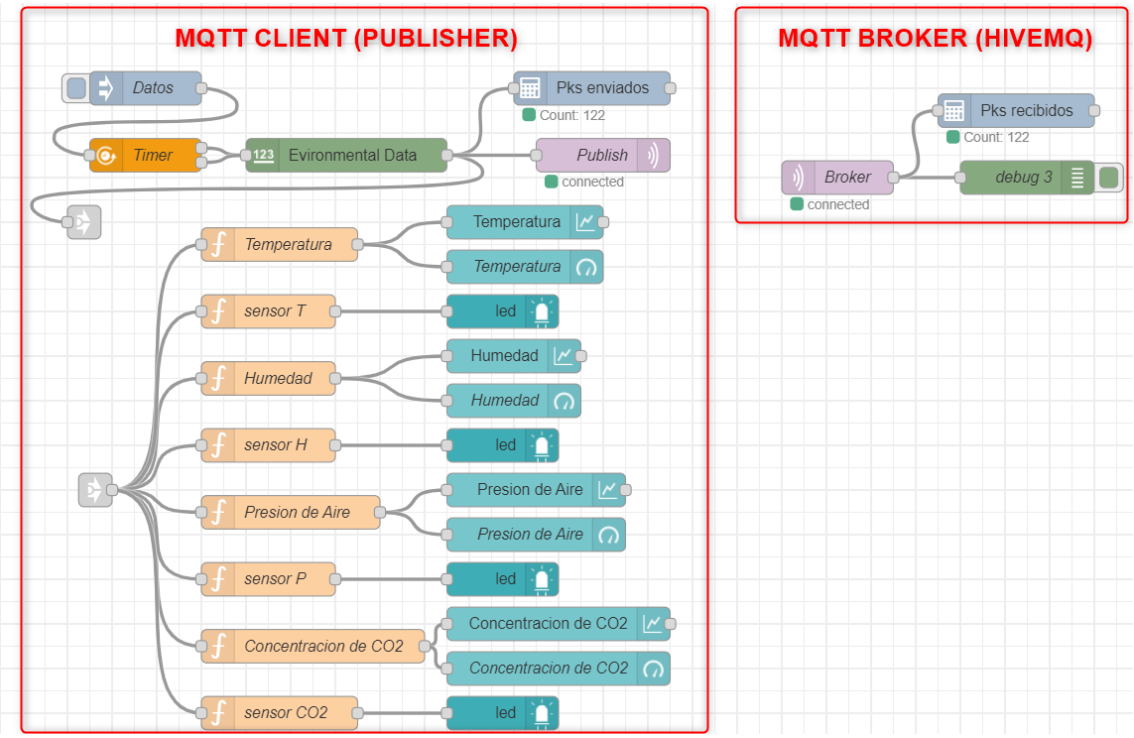

Figura 15. Componentes en Node-Red

Figura 16. Información recibida por parte del Broker MQTT

La siguiente imagen da a conocer el Dashboard de información enviada por parte de los sensores, en los cuales se cuenta con umbrales, manejando 3 estados alto, medio y bajo; cada uno de ellos representados por los colores rojo, amarillo y verde respectivamente tal como se visualiza en la tabla 8

Tabla 8. Umbrales de medición de sensores

Sensor	Umbral	Valor	Estado	Color
Temperatura	0°C a 100°C	0°C a 39°C	Bajo	
		40°C a 74°C	Medio	
		75°C a 100°C	Alto	
Humedad	0% a 100%	0% a 39%	Bajo	
		40% a 74%	Medio	
		75% a 100%	Alto	
Presión de Aire	10psi a 500psi	10psi a 174psi	Bajo	
		175psi a 329psi	Medio	
		330psi a 500psi	Alto	
Concentración de CO2	400ppm a 1000ppm	400ppm a 599ppm	Bajo	
		600ppm a 799ppm	Medio	
		800ppm a 1000ppm	Alto	

Fuente: Autores.

Figura 17. Dashboard MQTT

A medida que se recolecte la información enviada por los sensores, en el dashboard se representaran de colores los gráficos de acuerdo a los umbrales establecidos anteriormente; esto nos ayuda a identificar el estado de los sensores y el poder llevar a cabo acciones que nos permitan corregir o prevenir incidentes en el ámbito industrial.