UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA DE INGENIERÍA DE SISTEMAS

COMPARACIÓN DE PROTOCOLOS DE COMUNICACIÓN PARA INTERNET DE LAS COSAS (IOT)

Trabajo de titulación previo a la obtención del
Título de Ingenieros de Sistemas

AUTORES: EVELYN JOSETTE GUANANGA NARVÁEZ

WILMER RICARDO VIVAS DÍAZ

TUTOR: MANUEL RAFAEL JAYA DUCHE

Quito-Ecuador
2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Evelyn Josette Guananga Narváez con documento de identificación N° 1723305650 y Wilmer Ricardo Vivas Díaz, y N° 1715832000; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 08 de septiembre de 2022

Atentamente,

Evelyn Josette Guananga Narváez

1723305650

Wilmer Ricardo Vivas Díaz

1715832000

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, Evelyn Josette Guananga Narváez y Wilmer Ricardo Vivas Díaz con documento de identificación N.º 1723305650, y N.º 1715832000, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Artículo Académico: " Comparación de Protocolos de Comunicación para Internet de las Cosas (IOT)", el cual ha sido desarrollado para optar por el título de: Ingenieros de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 08 de septiembre de 2022

Atentamente,

Evelyn Josette Guananga Narváez

1723305650

Wilmer Ricardo Vivas Díaz

1715832000

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Manuel Rafael Jaya Duche con documento de identificación N° 1710631035, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: COMPARACIÓN DE PROTOCOLOS DE COMUNICACIÓN PARA INTERNET DE LAS COSAS (IOT), realizado por Evelyn Josette Guananga Narváez, con documento de identificación N.º 1723305650 y Wilmer Ricardo Vivas Díaz, y N.º 1715832000 , obteniendo como resultado final el trabajo de titulación bajo la opción de Articulo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 08 de septiembre de 2022

Atentamente,

Ing. Manuel Rafael Jaya Duche, Msc.

1710631035

DEDICATORIA

Dedico este trabajo a mi querida madre Rosario Díaz y a mi padre que siempre estuvieron en los momentos más difíciles y siempre me apoyaron rotundamente a lo largo de mi carrera y al resto de mi familia y aunque mi madre ya no se encuentre, esto va dedicado especialmente a ella a quien tengo presente cada día y cada instante de mi vida con sus enseñanzas y valores, a mis hijos y a las personas que por a o b motivo me han dado una palabra de aliento o cualquier tipo de apoyo en esta larga carrera que se convirtió en algo inalcanzable, pero sobre todo a la persona que estuvo atrás de este proyecto a mi lado dándome consejos, aliento y acompañándome hasta dar por concluso el mismo.

DEDICATORIA

Dedico este trabajo a Dios, a mis padres Wilma Narváez Y Julio Guananga por todo el apoyo que me han brindado a lo largo de este camino.

A mi hija Doménica Bahamonde por darme las fuerzas necesarias para continuar en este proceso de llegar a cumplir una de mis metas más deseadas.

.

AGRADECIMIENTO

Primero quiero agradecer a Dios por ser mi guía y acompañarme en el transcurso de mi vida, brindándome paciencia y sabiduría para culminar con éxito esta etapa de mi vida.

A mis padres y a mi hija por ser mi pilar fundamental y haberme apoyado incondicionalmente, pese a las adversidades e inconvenientes que se presentaron.

AGRADECIMIENTO

Agradezco a Dios y a mí por tener la constancia, la fuerza y convicción para seguir adelante después de cada traba y dificultad que tuve a lo largo de esta carrera y agradezco nunca haberme rendido, solo Dios sabe todo mi suplicio a lo largo de este camino.

COMPARACIÓN DE PROTOCOLOS DE COMUNICACIÓN PARA INTERNET DE LAS COSAS (IOT)

COMPARISON OF COMMUNICATION PROTOCOLS FOR INTHERNET OF THINGSD (IOT)

Evelyn Josette Guananga Narváez[1], Wilmer Ricardo Vivas Díaz [2], Manuel Rafael Jaya Duche [3]

Resumen

La finalidad del presente artículo es contrastar los protocolos de comunicación para Internet de las Cosas (IoT), para esto, se aplica el Estudio de Mapeo Sistemático por medio del cual se realizan búsquedas en plataformas como IEEE Xplore y Scopus, así también con el Método AHP (Proceso Analítico Jerárquico) de esta forma se extraen las características más relevantes como seguridad, calidad de servicio, eficiencia energética, banda ancha y latencia de los protocolos de comunicación (HTTP, MQTT,DDS,XMPP,AMQP y CoAP). Posteriormente se utilizan estos criterios para el Método AHP obteniendo como resultado que el protocolo CoAP ofrece un 26% de seguridad, 24% de latencia, 21% de efectividad energética mayor a los demás protocolos y un 22% y 19% de ancho de banda y calidad de servicio respectivamente, seguido del protocolo MQTT con 24% de seguridad,14% de latencia,14% de efectividad energética,12% de ancho de banda y un 24% de calidad de servicio mayor a los demás protocolos sin dejar de lado a AMQP con 16% de seguridad,17% de latencia,19% de efectividad energética,12 % de ancho de banda y 15% de calidad de servicio, este protocolo a pesar de tener porcentajes aceptables para IoT requiere de más recursos físicos con los que se deben trabajar, tal es el caso de HTTP y MQTT.

Palabras clave: IoT, Protocolos de Comunicación, seguridad, calidad de servicio, eficiencia energética, banda ancha y latencia.

Abstract

The purpose of this article is to contrast the communication protocols for the Internet of Things (IoT), for this, the Systematic Mapping Study is applied through which searches are made in platforms such as IEEE Xplore and Scopus, as well as with the AHP Method (Hierarchical Analytical Process) in this way the most relevant characteristics such as security are extracted, quality of service, energy efficiency, broadband and latency of communication protocols (HTTP, MQTT, DDS, XMPP, AMQP and CoAP). Subsequently, these criteria are used for the AHP Method obtaining as a result that the CoAP protocol offers 26% security, 24% latency, 21% of energy effectiveness greater than the other protocols and 22% and 19% of bandwidth and quality of service respectively, followed by the MQTT protocol with 24% security, 14% latency, 14% of energy effectiveness, 12% of bandwidth and 24% of quality of service greater than the other protocols without neglecting AMQP with 16% security, 17% of latency, 19% of energy effectiveness, 12% of bandwidth and 15% of quality of service, this protocol despite having acceptable percentages for IoT requires more physical resources with which to work, such is the case with HTTP and MQTT. ***Keywords:*** IoT, Communication Protocols, Stability, Security, Maturity, Availability, Speed.

[1]Estudiante de Ingeniería de Sistemas – Universidad Politécnica Salesiana, Egresado – UPS – sede Quito. Autor para correspondencia: eguananga@est.ups.edu.ec

[2]Estudiante de Ingeniería de Sistemas – Universidad Politécnica Salesiana, Egresado – UPS – sede Quito. Autor para correspondencia: wvivas@est.ups.edu.ec

[3]Magister en Redes de Información y Conectividad, Ingeniero de Electrónica y Telecomunicaciones, Profesor de Ingeniería de Sistemas – UPS – sede Quito

Email: mjaya@ups.edu.ec

1. Introducción

La Internet de las cosas (IoT) es la red de elementos físicos equipados de electrónica los cuales permiten a estos objetos recolectar y permutar datos [1].

En muchos aspectos, la IoT puede parecer inicialmente lo mismo que la comunicación machine-to-machine (M2M) que conecta sensores y otros dispositivos a los sistemas TIC (Tecnologías de la Información y la Comunicación) a través de redes alámbricas o inalámbricas. Sin embargo, a diferencia de la M2M, la IoT también hace alusión a la conexión de estos sistemas y sensores así también al uso de tecnologías generales de Internet [2].

Las continuas innovaciones en hardware, software y soluciones de conexión en la última década han llevado a la expansión del IoT, con un número de dispositivos conectados que crece día a día. La alta demanda de cantidad de datos generados por estos dispositivos exige encontrar una arquitectura de sistema adecuada la cual pueda de procesar y reunir todos los datos [3].

Una década después de su concepción, el Internet de las cosas es una tecnología emergente que aún no ha alcanzado la conciencia de las masas. Y, sin embargo, tiene una historia sorprendentemente larga, incluso ilustre. Además, es una parte integral de

dispositivos envían datos sin procesar a la nube que luego se comparten con otros dispositivos/sistemas que se suscriben a esta gran cantidad de datos (ya sean datos en bruto o procesados por el servidor), lo que hace que la comunicación entre estos dispositivos sea un aspecto importante del IoT [8].

Los protocolos de comunicación desempeñan un papel fundamental para que la comunicación sea eficiente [7]. Los protocolos de comunicación son

su vida [4]. En 2016 existieron 5.000 millones de objetos inteligentes conectados a Internet, mientras que para 2020 hubo 25.000 millones. La integración de los "objetos" en Internet es un reto porque pueden tener características como memoria, capacidad de procesamiento y recursos energéticos limitados [5].

Además, el IoT tiene ahora un amplio abanico de aplicaciones en la vida cotidiana, como la industria, el transporte, la logística, la sanidad, el medio ambiente inteligente, así como la información personal, la de los juegos sociales y la de las ciudades. Los dispositivos inteligentes pueden tener conexión por cable o inalámbrica. En cuanto al IOT inalámbrico, se pueden utilizar muchas tecnologías y protocolos de comunicación inalámbricos diferentes para conectar el dispositivo inteligente.

El IoT hace posible enviar información recopilada a través de Internet en tiempo real [6]. Los dispositivos que se comunican en la IoT, al estar limitados en términos de memoria y energía, tienen que acordar diferentes aspectos de los datos intercambiados para una transmisión eficaz basada en ciertos protocolos [7].

Los nodos finales del IoT suelen ser sensores o pequeños dispositivos que tienen una capacidad de procesamiento limitada y poca memoria. En estos casos, los

parte integral del omnipresente IoT [8]. Con el tiempo, se han ido añadiendo más y más protocolos al IoT, ya que los anteriores se consideraron inadecuados para satisfacer los requisitos del IoT.

En general, los protocolos de comunicación candidatos difieren en sus modelos de interacción, es decir, petición-respuesta y publicación-suscripción. El modelo de comunicación petición-respuesta es uno de los paradigmas de comunicación más básicos. Representa un patrón de

intercambio de mensajes especialmente común en las arquitecturas cliente/servidor. Permite a un cliente solicitar información a un servidor que recibe el mensaje de solicitud, lo procesa y devuelve un mensaje de respuesta. Este tipo de información suele gestionarse e intercambiarse de forma centralizada [3].

Los dispositivos IoT utilizan diferentes protocolos de comunicación porque, de momento, no existe un único protocolo estándar. Varias implementaciones de código abierto para estándares como CoAP y MQTT están muy extendidas entre las comunidades, pero cada productor tiene sus propios estándares y arquitecturas. El CoAP es un medio de transferencia destinado a los nodos y redes restringidas. Emplea el estilo arquitectónico Representational State Transfer (REST) usando su propio protocolo que es mucho más ligero que el protocolo clásico Hyper Text Transfer Protocol (HTTP) [9].

No obstante, hay ciertos criterios que los protocolos tienen que tratar para su idoneidad en los entornos del IoT. Estos parámetros son la escalabilidad, la comunicación, la gestión, la seguridad, etc [7]. Así, la necesidad de comprender correctamente la aplicabilidad de estos protocolos es imperiosa.

Muchos dispositivos IoT suelen tener un bajo coste y recursos restringidos, como una baja conexión de red, energía y limitación de procesamiento. Los protocolos de comunicación son muy críticos para organizar los flujos de datos y determinar cómo el IoT interactúa entre sí. El IoT requiere nuevos protocolos flexibles para los dispositivos heterogéneos y limitados, a diferencia de los protocolos de comunicación comunes [10].

De esta forma, es posible aseverar que el objetivo final del IoT es mantener la eficacia de la comunicación entre los objetos y también fortalecer la relación entre ellos a través de sus diferentes aplicaciones.

2. Métodos y materiales

2.1 Mapeo Sistemático

Se implementa el Systematic Mapping Studio (Estudio de Mapeo Sistemático), el cual consiste en filtrar información tomando en cuenta parámetros como antigüedad de publicaciones en este caso desde el año 2019 hasta el año presente 2022, así también las fuentes confiables como Artículos de investigación, libros, artículos para conferencias y artículos para revistas, utilizando las siguientes palabras clave y cadena de búsqueda**.** Fuente: Propia, Adaptado de [13].

Todos estos documentos publicados son fuentes confiables de las cuales se extrae información verídica puesto que son previamente revisados por lectores especializado de la plataforma IEEE Xplore. Y para comparar el contenido de estos documentos se recolectan datos de la plataforma SCOPUS la cual realiza un análisis de los protocolos más usados en varios países con mayor desarrollo en Ingeniería de Telecomunicaciones bajo estos criterios se realizan tablas comparativas, tomando en cuenta puntos importantes de cada protocolo como la seguridad, calidad de servicio y eficiencia energética así también las características de cada uno de ellos como la arquitectura, protocolo de transporte, conectividad, latencia, consumo de banda ancha, formato de codificación , estándares y aplicaciones.

Se debe tener en cuenta que los estudios de mapeo son revisiones documentales, pero estos no discuten los resultados, únicamente se basan en los conceptos publicados en artículos, los mismos que no son hallazgos, sino

que se encuentran de manera indirecta al estudio.

En la **¡Error! No se encuentra el origen de la referencia.** se presenta los pasos de esta metodología:

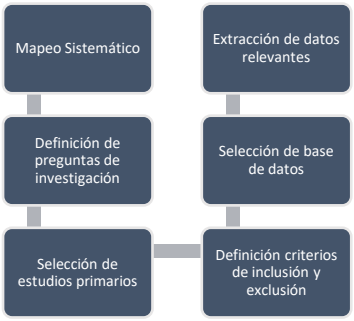


Figura 1. Proceso de Estudio de Mapeo Sistemático. Fuente: Propia

2.1.1 Definición de preguntas de Investigación

1. ¿Cuántos artículos se han anunciado en los últimos cuatro años?
2. ¿Cuáles son las bases de datos más utilizadas en los últimos cuatro años?
3. ¿Cuáles son los países que han aportado más de un artículo en los últimos cuatro años?
4. ¿En qué idiomas se produce la investigación sobre Protocolos IoT?
5. ¿Cuáles son los protocolos de comunicación más empleados?
6. ¿Cuáles son las características y funcionamiento de estos protocolos?
7. ¿Identificar los sistemas de seguridad más empleados?
8. ¿Cuáles son los modelos de protocolos empleados?

2.1.2 Selección de estudios primarios

En la **Tabla 1** se describen los resultados de la búsqueda, posteriormente se aplican los siguientes filtros de revisión:

a) Primer filtro presentado en la Tabla 1 en la sección C_1 bajo los siguientes criterios.

a. Título: se revisan los títulos de las publicaciones arrojadas en las bases de datos.
b. Resumen o Abstract: De los títulos seleccionados, se somete a revisión y lectura del Abstract.

b) Segundo Filtro presentado en la Tabla 1 en la sección C_2 bajo los siguientes criterios.

a. Texto Completo: Finalmente las publicaciones que pasaron el primer filtro se verifican si se dispone del texto completo.

En la **Tabla 1** en la sección de Filtros se presenta la cantidad de estudios obtenidos para cada una de las palabras clave y resultados luego de aplicar el primer y segundo filtro.

Tabla 1. Resultado de búsqueda con filtros aplicados para las plataformas IEEE Xplore y SCOPUS

BASE	CADENA DE BÚSQUEDA	RES	C_1	C_2	Filtros
IEEE Xplore	("Abstract": "Internet of Things" OR "Abstract": IoT) AND ("Abstract": Protocol OR "Abstract": technology) AND ("Abstract": HTTP OR "Abstract": MQTT OR "Abstract": DDS OR "Abstract": XMPP OR "Abstract": AMQP OR "Abstract": CoAP)	75637	1126	54	23
SCOPUS	TITLE-ABS-KEY ((“Internet of Things” OR IoT) AND (protocol OR technology) AND (HTTP OR MQTT OR DDS OR XMPP OR AMQP OR CoAP))	139589	78	65	30
:*Total:		215226	1204	119	53

Fuente: Propia

2.2 Criterios de inclusión y exclusión.

2.2.1 Criterios de inclusión

Se definen los siguientes criterios de inclusión y exclusión para la elección de estudios. Es necesario mencionar que no se excluyeron los artículos cortos (es decir, de menos de cuatro páginas).

I1: Estudio que investiguen los protocolos de comunicación del IoT.

I2: Estudios revisados por pares y disponibles en texto completo.

I3: Estudio que estén escritos en español.

I4: Estudios publicados desde 2019 en adelante.

2.1.2 Criterios de exclusión

Se contemplan los siguientes criterios:

E1: Si dos estudios sobre el mismo trabajo están publicados en diferentes lugares (por ejemplo, taller y conferencia), se excluye el menos reciente.

E2: Si un estudio utiliza un enfoque que emplea protocolos de investigación, pero este enfoque no se utiliza para el IoT, se excluye este estudio.

E3: Si un estudio utiliza un enfoque que se aplicó en el IoT, pero este enfoque no emplea protocolos de investigación, se excluye este estudio.

E4: Si un estudio no está revisado por pares, por ejemplo, un informe técnico, se excluye este estudio.

E5: Si un estudio fue publicado antes de 2019 se excluye de este estudio.

En la **¡Error! No se encuentra el origen de la referencia.¡Error! No se encuentra el origen de la referencia.** se detalla el flujograma para la selección de los estudios a analizar bajo los Criterios de inclusión y exclusión.

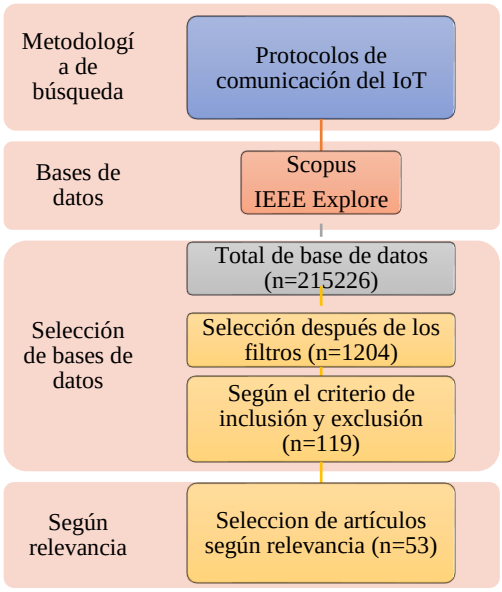


Figura 2. Flujograma de resultados de Estudio de Mapeo Sistemático. Fuente: Propia

2.3 Método de Proceso de Jerarquía Analítico (AHP)

En la **¡Error! No se encuentra el origen de la referencia.** se presenta el análisis cuantitativo según criterios definidos permitiendo generar escalas de prioridad a través de la comparación de pares destinada a la toma de decisiones.

Tabla 2. Escala de importancia según método AHP.

Criterio numérico	Significado Lingüístico
1	Igual de importante
3	Sensato
5	Imprescindible
7	Decisivo
9	Primordial
2,4,6,8	Valores intermedios de importancia

Fuente: Propia

Mediante la escala de la **¡Error! No se encuentra el origen de la referencia.**

presentada previamente se realizan tres tablas (**Tabla 5**, **Tabla 8**,**Tabla 9**) expuestas en esta investigación, las cuales inician con la comparación entre las características de cada protocolo de comunicación como: Arquitectura, Tamaño de encabezado, Calidad de servicio (QoS)/Confiabilidad, Protocolo de transporte, Energía de consumo, Seguridad, Conectividad, Latencia y Banda ancha.

3. Resultados y discusión

En el siguiente apartado se muestra las respuestas a las preguntas de investigación formuladas mediante la metodología de Estudio de Mapeo Sistemático.

1. ¿Cuántos artículos se han anunciado en los últimos cuatro años?

Posteriormente se realizan los cálculos respectivos para la matriz comparativa y de esta manera identificar los protocolos de comunicación que se adecuan de una manera eficiente e ideal para el Internet de las cosas (IoT) de acuerdo a las aplicaciones dispuestas por el área y el usuario donde estos son utilizados.

En la **¡Error! No se encuentra el origen de la referencia.** se observa un decremento para el año 2022, siendo los años 2020 y 2021 los picos para la investigación acerca de los protocolos de comunicación para Internet de las Cosas presentados según la plataforma de Scopus.

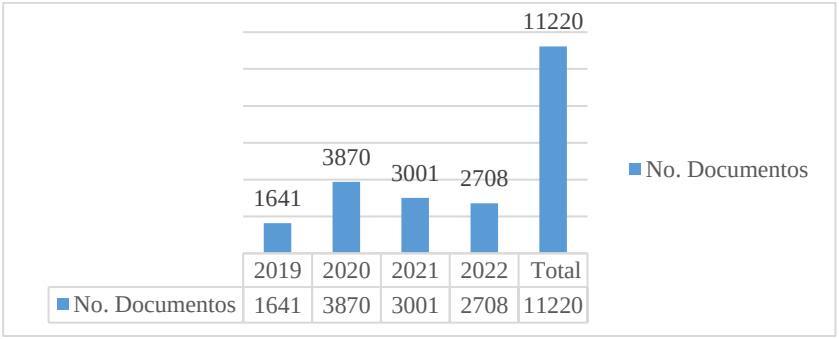


Figura 3. Número de artículos publicados los últimos cuatro años según SCOPUS. Fuente: Propia

En la **¡Error! No se encuentra el origen de la referencia.** se observa que en el año 2022 versus 2021 ,2020 y 2019 disminuyeron las investigaciones acerca de los protocolos de comunicación IoT en la plataforma de IEEE Xplore, siendo el año 2020 el de mayor recolección de información, año en el cual inicio la Pandemia Covid-19, por ende incremento el uso de plataformas en tiempo real

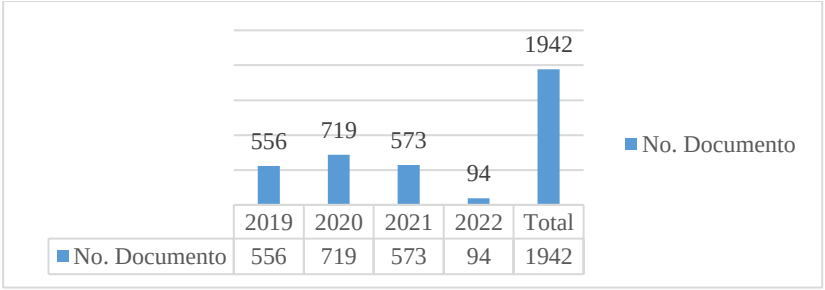


Figura 4. Número de artículos publicados los últimos cuatro años según IEEE Xplore. Fuente: Propia

2. ¿Cuáles son las bases de datos más utilizadas en los últimos cuatro años?

Las bases de datos se distribuyen a razón de la búsqueda y la aplicación de los filtros, criterios de inclusión y exclusión, se puede evidenciar que la base de datos que tienen más información respecto al tema es SCOPUS, concentrando el 85% de las investigaciones con 739.450 documentos expuestos seguido por IEEE Xplore concentrando un 15% con 135.441 documentos complementándose para llegar al 100% expuestos en la **¡Error! No se encuentra el origen de la referencia.**.

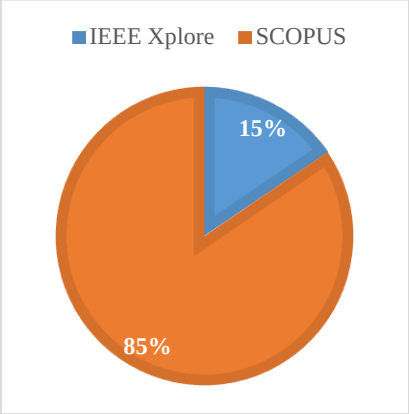


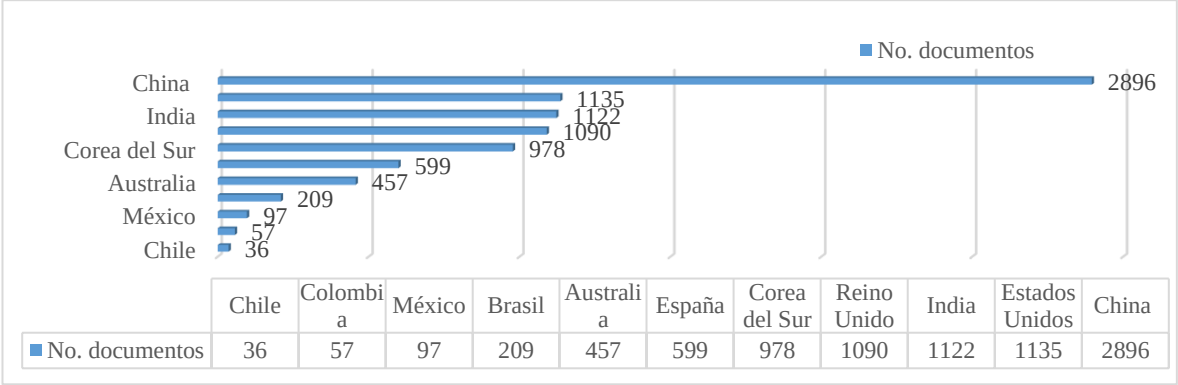
Figura 5. Bases de datos más utilizadas los últimos cuatro años según IEEE Xplore y Scopus. Fuente: Propia

3. ¿Cuáles son los países que han aportado más de un artículo en los últimos cuatro años?

De la **¡Error! No se encuentra el origen de la referencia.** a la **¡Error! No se encuentra el origen de la referencia.** se detallan los países con más aportaciones para protocolos de comunicación para protocolos IoT donde se evidencia que los países que se involucran más son China, India, Estados Unidos, Reino Unido y Corea del Sur

Según la plataforma de SCOPUS cabe recalcar que países latinoamericanos como Ecuador, Colombia, Brasil y Argentina también tienen su aporte a nivel internacional con artículos de investigación, esto demuestra un avance en la ingeniería sistemática para América del Sur.

En la **¡Error! No se encuentra el origen de la referencia.** según la extracción de datos mediante el Mapeo Sistemático, China es el país donde se aplica en mayor cantidad el uso de Internet de las Cosas (IoT) seguido por Estados Unidos e India con 1122 documentos, cabe recalcar que América del Sur no se queda atrás representado por Colombia y Chile; siendo estos, los países que están en contacto mayormente con aplicaciones en tiempo real.



	Chile	Colombia	México	Brasil	Australia	España	Corea del Sur	Reino Unido	India	Estados Unidos	China
No. documentos	36	57	97	209	457	599	978	1090	1122	1135	2896

Figura 6. Número de documentos publicados en diferentes países acerca de Protocolos IoT. Fuente: Propia

En la **¡Error! No se encuentra el origen de la referencia.** se puede enfatizar en la disminución de la cantidad de investigaciones expuestas para el protocolo de comunicación AMQP siendo participe en esta ocasión Ecuador con 1 documento presentado a nivel internacional en los últimos cuatro años.

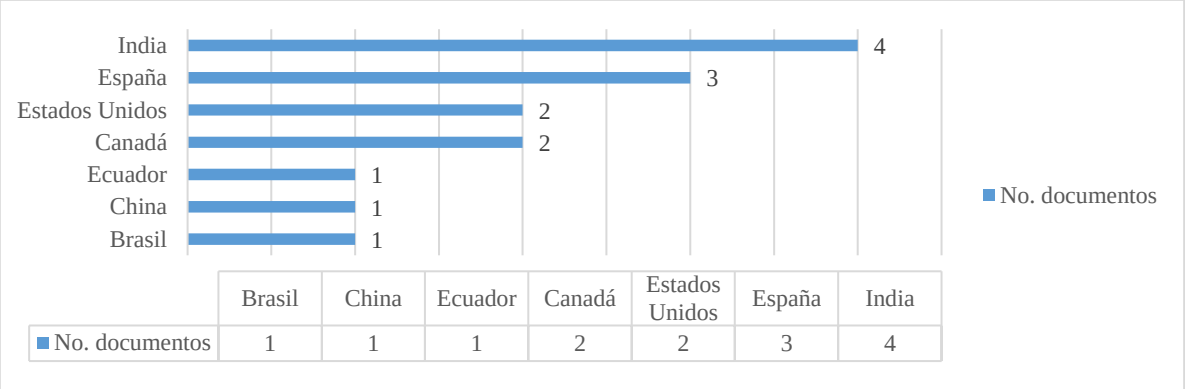


Figura 7. No. de documentos publicados en diferentes países acerca del Protocolo AMQP para IoT. Fuente: Propia

En la **¡Error! No se encuentra el origen de la referencia.** se puede observar liderando se encuentra India en el primer puesto de investigaciones respecto al protocolo de comunicación DDS con 10 documentos en los últimos cuatro años sin quedarse fuera Ecuador, demostrando el interés por desarrollar de nuevas aplicaciones para IoT mediante DDS y mayor participación en el mundo de la Telecomunicación y Sistemas.

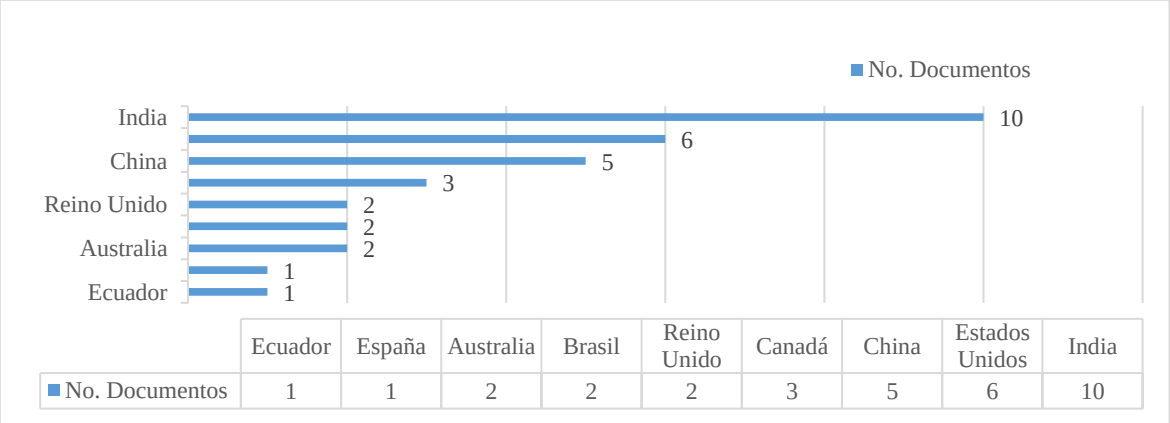
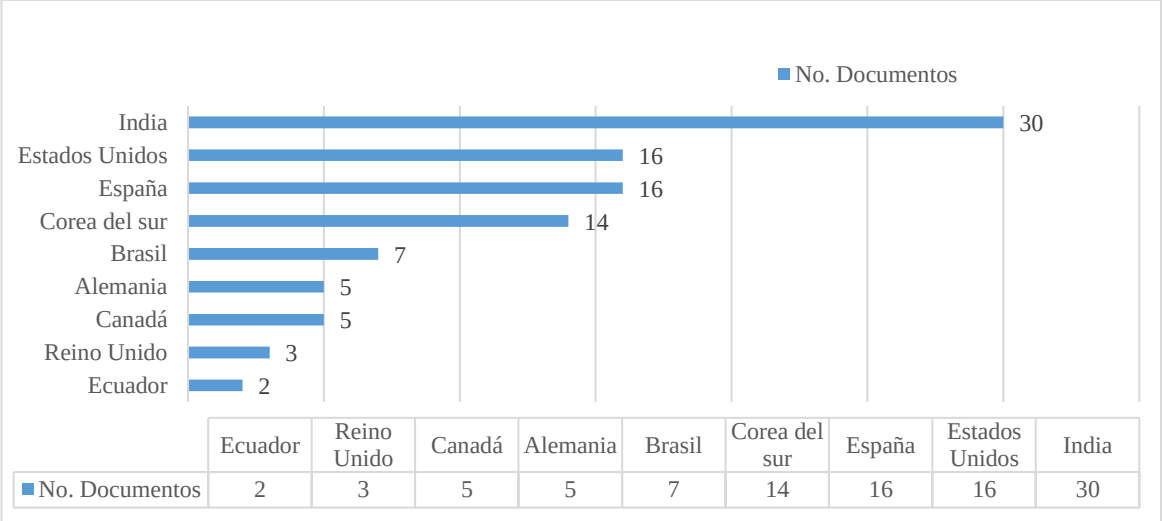


Figura 8. Número de documentos publicados en diferentes países acerca del Protocolo DDS para IoT. Fuente: Propia

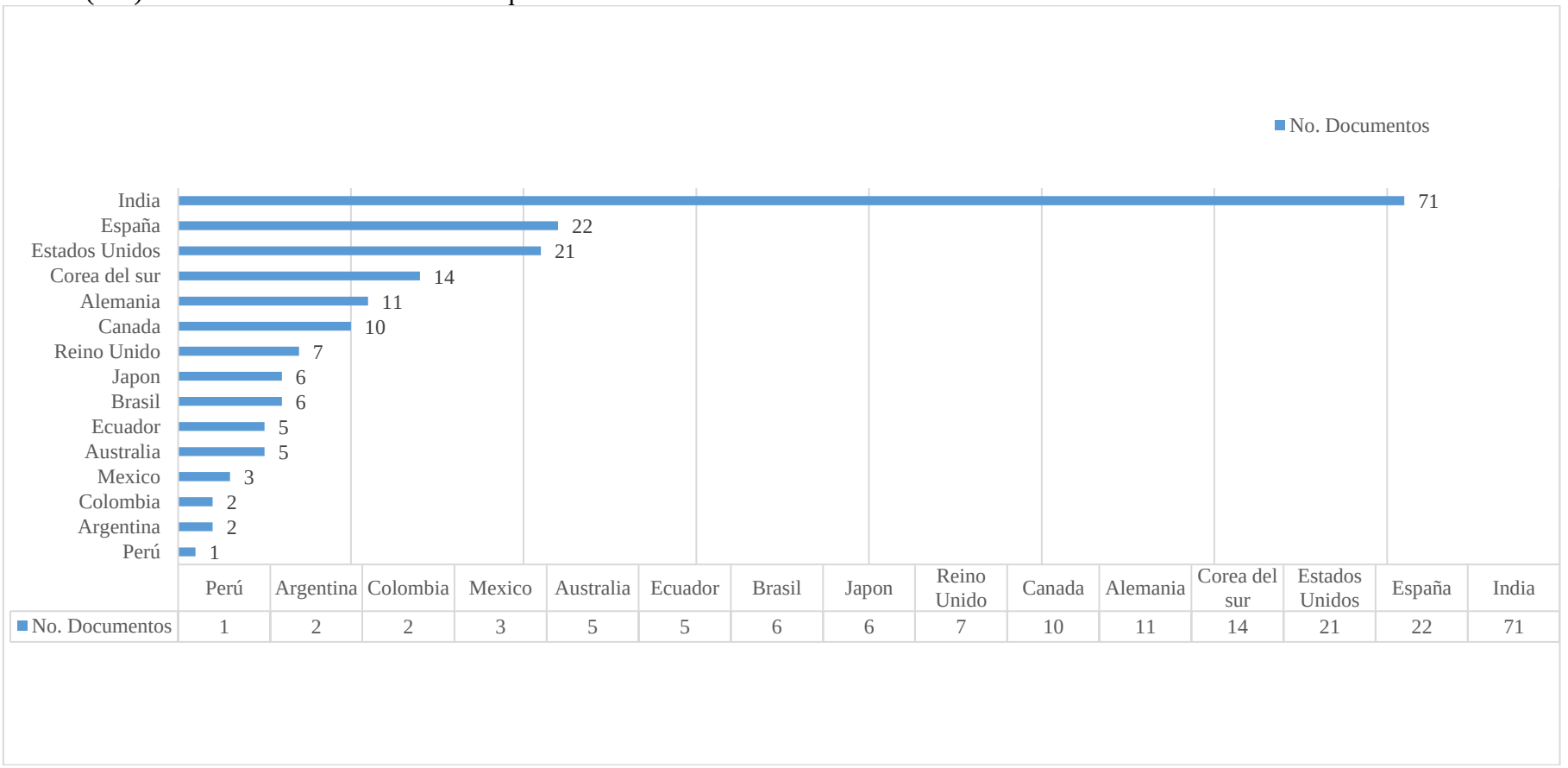
En la **¡Error! No se encuentra el origen de la referencia.**, India sigue demostrando que día a día investiga nuevas aplicaciones para la aplicación de CoAP respecto a Internet de las Cosas sin quedar fuera Ecuador con dos documentos presentados en los últimos cuatro años, tomando en cuenta que existen más documentos acerca de este protocolo extraídos de Scopus e IEEE XPLORE



	Ecuador	Reino Unido	Canadá	Alemania	Brasil	Corea del sur	España	Estados Unidos	India
No. Documentos	2	3	5	5	7	14	16	16	30

Figura 9. Número de documentos publicados en diferentes países acerca del Protocolo CoAP para IoT. Fuente: Propia

Finalmente, en la **¡Error! No se encuentra el origen de la referencia.** se puede observar un incremento de documentos de investigación para el protocolo de MQTT para Internet de las Cosas (IoT) deduciendo de esta manera que es uno de los protocolos mayormente aplicado en países Asiáticos, Europeos y Americanos.



	Perú	Argentina	Colombia	Mexico	Australia	Ecuador	Brasil	Japon	Reino Unido	Canada	Alemania	Corea del sur	Estados Unidos	España	India
No. Documentos	1	2	2	3	5	5	6	6	7	10	11	14	21	22	71

Figura 10. Número de documentos publicados en diferentes países acerca del Protocolo MQTT para IoT. Fuente: Propia

4. ¿En qué idiomas se produce la investigación sobre Protocolos IoT?

El total de la información fue recabada de artículos de investigación y libros en idioma inglés y español en la plataforma de
SCOPUS así también un porcentaje de revistas y conferencias mayormente en inglés presentadas en IEEE Xplore.

5. ¿Cuáles son los protocolos de comunicación más empleados?
En la **Tabla 3** se presentan un resumen de los resultados de los protocolos hallados en las plataformas IEEE Xplore y Scopus después de aplicar los filtros.

Tabla 3. Protocolos hallados según IEEE Xplore y SCOPUS

Protocolo	Número	Referencias
HTTP	12	[14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25]
MQTT	10	[26], [27], [28], [29], [30], [1], [31], [32], [33], [34]
DDS	8	[35], [36], [37], [38], [39], [40], [41], [42]
XMPP	7	[43], [44], [45], [6], [46], [47], [48]
AMQP	9	[49], [50], [51], [52], [53], [54], [55], [56], [57]
CoAP	7	[58], [59], [60], [61], [62], [63], [64]
Total	**53**	

Fuente: Propia

6. ¿Cuáles son las características y funcionamiento de estos protocolos?

En la **Tabla 4** se presentan las características técnicas más relevantes de cada protocolo de comunicación para Internet de las Cosas (IoT) después del método de Estudio de Mapeo Sistemático realizado en las plataformas de Scopus e IEEE Xplore.

Tabla 4. Características más relevantes de los protocolos de comunicación para IoT según el Estudio de Mapeo Sistemático

Protocolo	Características más relevantes
HTTP	• HTTP usa el Identificador de recursos universal (URI) • HTTP que se integra con REST se ha utilizado en la arquitectura IoT. • Utiliza cuatro modos, como POST, GET, PUT y DELETE eficientes para IoT [8]. • Utiliza muchos anchos de banda del modelo de solicitud y respuesta. Por lo tanto; es difícil adaptar HTTP a los protocolos IoT. • Envío de archivos de gran tamaño para IoT.
MQTT	• Según [13], el protocolo MQTT se utiliza como un protocolo de comunicación apropiado para IoT y M2M. • Ideal para dispositivos de recursos comprimidos los cuales ocupan enlaces con menor confiabilidad y de bajo ancho de banda. • Uno de los requisitos clave del IoT es la idea de utilizar un ancho de banda bajo para enviar datos y requisitos para un recurso de dispositivo pequeño.
DDS	• Es un middleware separado de plataforma y de código abierto estándar • Arquitectura de publicación/suscripción sin intermediarios. • Es altamente confiable y proporciona conexiones seguras SSL y DTLS. • Su arquitectura define dos capas: Data-Centric Publish Subscribe (DCPS) y Data-Local Reconstruction layer (DLRL). • DCPS es responsable de proporcionar la información a sus suscriptores. • DLRL es una capa opcional y actúa como una interfaz para el uso de DCPS. Permite compartir datos distribuidos entre objetos distribuidos [18].
XMPP	• Solución adaptable para el intercambio asíncrono de extremo a extremo de datos organizados [20]. • Incorpora métodos TLS, que proporcionan una forma fiable, la cual garantiza privacidad e integridad de los datos. • Según [21] admite mejor los mensajes pequeños de baja latencia. • Los mensajes XML producen la mayor parte de la sobrecarga debido a los diversos encabezados y formatos de etiquetas que aumentan el consumo de energía.
AMQP	• Es la base de un protocolo de IoT ligero de código abierto creado para redes orientadas a la mensajería. • Con los editores y los suscriptores, hay dos componentes adicionales, las colas de intercambio y de mensajes [18]. • El componente de intercambio es responsable de obtener los mensajes del editor y entregarlos en colas siguiendo roles predeterminados; • Los suscriptores se conectan a esas colas, que básicamente representan temas, y obtienen detalles para escuchar siempre que estén disponibles[21].
CoAP	• Para lograr la transmisión de datos, CoAP mantiene el tamaño del mensaje lo más pequeño posible y admite el mecanismo de retorno de la espera. • Utiliza (URI) en lugar de encabezados, sin embargo, los utiliza según el servidor web o la tecnología de la aplicación. • Utiliza mensajes "válidos" o "inciertos" para proveer dos niveles diferentes de calidad de servicio. Allí, los mensajes verificados son recibidos por el destinatario mediante el paquete ACK y los mensajes no verificados no. • Se considera un reemplazo de HTTP para las redes de IoT.[23].

Fuente: Propia

7. ¿Identificar los sistemas de seguridad más empleados?

En la **Tabla 5** se identifican los sistemas de seguridad empleados mayormente para protocolos de comunicación basados en IoT como TLS, DTLS y DDS.

Tabla 5. Sistemas de seguridad

Sistemas	Referencias
TLS	[18], [19], [39], [40], [63], [64], [6], [46]
DTLS	[43], [44], [33], [34], [28], [29]
DDS	[20], [22], [48], [59], [60]

Fuente: Propia

8. ¿Cuáles son los modelos de protocolos empleados?

En la **Tabla 6** se presentan los modelos empelados para cada uno de los protocolos indagados con sus respectivas referencias resultantes del Estudios de Mapeo Sistemático

Tabla 6. Modelos de protocolos empelados

Modelos	Referencias
Intercambio punto a punto	[28], [19], [22], [11], [41], [44], [62], [64]
Petición / Respuesta	[26], [33], [35], [17], [27]
Publicación / Subscripción	[36], [42], [30], [34]

Fuente: Propia

En la **Tabla 7** se realiza un análisis comparativo entre los protocolos HTTP, MQTT y CoAP, tomando en cuenta la Arquitectura, Calidad de servicio (QoS)/Confiabilidad, Protocolo de transporte, Energía de consumo, Seguridad, Conectividad y Latencia donde se incluye

el número de la escala AHP y más adelante esto servirá para aplicar el método como tal, con el fin de seleccionar el protocolo que se ajusta a Internet de las cosas (IoT).

Tabla 7. Comparación entre protocolos HTTP, MQTT y CoAP según la extracción de datos mediante mapeo sistemático.

Características	HTTP (1)	MQTT (5)	CoAP (9)
Arquitectura	Cliente /Servidor	Cliente/Broker	Solicitud/Respuesta o Publicar/Suscribirse
Calidad de servicio (QoS)/Confiabilidad	Limitado (a través de Protocolo de transporte- TCP)	QoS 0 QoS 1 QoS 2	Mensaje Confirmable Mensaje no Confirmable
Protocolo de transporte	TCP	TCP (MQTT-SN puede aplicarse UDP)	UDP
Consumo de Energía	Requiere la mayor potencia/energía consumida por HTTP fue mucho mayor que con MQTT	MQTT es energéticamente más eficiente	CoAP es más eficiente en términos de energía
Seguridad	TLS/SSL	TLS/SSL tiene el nivel más bajo	DTLS, IPSec garantizar la autenticación, integridad y encriptación
Conectividad	Uno-a-uno	Uno-a-uno, uno-a-muchos y muchos-a-muchos	Uno a uno y muchos a muchos
Latencia	Implica mayor latencia, HTTP tiene el más alto latencia que otros	MQTT tiene más baja latencia que HTTP	CoAP tiene latencia más baja que todos los protocolos
Consumo de Banda ancha	Implica mayor ancho de banda	Consume más banda ancha	Implica el ancho de banda más bajo
Aplicaciones	Web	Automatización del hogar, aplicaciones de nivel empresarial	Casas inteligentes, red inteligente y automatización de edificios

Fuente: Propia

En la **Tabla 8** se presenta un análisis comparativo entre los protocolos HTTP, MQTT y CoAP, tomando en cuenta la Arquitectura, Calidad de servicio (QoS)/Confiabilidad, Protocolo de transporte, Energía de consumo, Seguridad, Conectividad y Latencia donde se incluye el número de la escala AHP y más adelante esto servirá para aplicar el método como tal, con el fin de seleccionar el protocolo que se ajusta a Internet de las cosas (IoT).

Tabla 8. Comparación entre protocolos DDS, XMPP y AMQP según la extracción de datos mediante mapeo sistemático.

Características	DDS (3)	XMPP (1)	AMQP (5)
Arquitectura	Sin Intermediario	Cliente/ servidor	Cliente/Broker (Cliente/Servidor)
Calidad de servicio (QoS)/Confiabilidad	23 pólizas: Seguridad,fiabilidad,durabilidad , prioridad,etc	Sin soporte para QoS	Settle Format (similar a Como máximo una vez) o Unsettle Format (similar a Al menos una vez)
Protocolo de transporte	UDP	TCP	TCP, SCTP
Consumo de Energía	NA	Incrementa la energía de consumo	Requiere levemente mayor potencia
Seguridad	TLS/ SSL, DTL	TLS/SSL	TLS/SSL, 1Psec, SASL Seguridad más fuerte
Conectividad	peer-to-peer, uno-a-uno,uno-a-muchos, muchos-a-muchos, y muchos-a-uno	Uno-a-uno	Punto-a-punto
Latencia	Baja latencia	Baja latencia	AMQP tiene la más baja latencia que MQTT
Consumo de ancho de Banda	Bajo	Bajo	Alto consumo de ancho de banda
Aplicaciones	Imágenes médicas, sistemas militares	Mensajería instantánea , Chat en grupo, juegos en línea, Monitores de vehículos	Negocio de mensajería e Industria Bancaria

Fuente: Propia

3.1 Aplicación de método de proceso analítico jerárquico

En la **Tabla 9** se aplica el método de proceso de jerarquía analítico mediante los siguientes pasos:

Etapa 1: Seleccionar los criterios más importantes para el proceso jerárquico, estos son: seguridad, latencia, efectividad energética, acho de banda y calidad de servicio (QoS).

Etapa 2: Se emplean valores pares de 1 al 9 basado en el método AHP siendo así : HTTP (1),MQTT(5),DDS(3),XMPP(1), AMQP(5) , CoAP(9).

Etapa 3: Finalmente en la **Tabla 9** se la matriz de comparación debe ser normalizada por lo cual se toman valores de la columna y cada valor se divide por la sumatoria total de la columna;

Tabla 9. Pesos para criterios según AHP

CRITERIOS	SEGURIDAD	LATENCIA	EFECTIVIDAD ENERGETICA	ANCHO DE BANDA	QOS
SEGURIDAD	1	9	5	5	1/3
LATENCIA	1/9	1	3	3	3
EFECTIVIDAD ENERGETICA	1/5	1/3	1	1/3	1/3
ANCHO DE BANDA	1/5	1/3	3	1	1/3
QoS	3	1/3	3	3	1
TOTAL	4.51	11.00	15.00	12.33	5.00

Fuente: Propia

En la finalmente se debe tomar en cuenta que la sumatoria final debe dar como resultado 1.00 equivalente al 100%. Se calculan los vectores de peso para el criterio.

Tabla 10. Matriz normalizada según pesos de criterios

MATRIZ NORMALIZADA				
0.22	0.82	0.33	0.41	0.07
0.02	0.09	0.20	0.24	0.60
0.04	0.03	0.07	0.03	0.07
0.04	0.03	0.20	0.08	0.07
0.67	0.03	0.20	0.24	0.20
1.00	1.00	1.00	1.00	1.00

Fuente: Propia

Etapa 4: Se calcula la ponderación mediante el promedio de la matriz normalizada por filas siendo la ponderación:

(0,22+0,82+0,33+0,41+0,07)/5=0,37

(0,02+0,09+0,20+0,24+0,60)/5=0,23

(0,04+0,03+0,07+0,03+0,07)/5=0,05

(0,04+0,03+0,20+0,08+0,07)/5=0,08

(0,67+0,03+0,20+0,24+0,20)/5=0,27

Etapa 5: Para calcular λmax la cual es la sumatoria de los valores del peso de criterio total por la ponderación de cada uno de los criterios. Se deben tomar los siguientes valores:

λmax=(4,51*0,37)+(11*0,23)+(15*0,05)+ (12,33*0,08)+(5*0,27)

λmax= 7,2996

Etapa 6: Las medidas del tomador de decisiones son bilateralmente consistentes. Se calcula el índice de consistencia (IC)

Donde (n) es el número de criterios a comparar en este caso (5).

IC=λmax- n/ (n-1)

IC=7,2996-5/(5-1)

IC=0,5749

Etapa 7: Se obtiene una razón de consistencia (RC) que es la razón de IC. En este caso CA es un factor . Donde:

RC=IC/CA

RC= 0,5749/1,24

RC=0,4636

En la **¡Error! No se encuentra el origen de la referencia.** posterior a la correcta Aplicación de método de proceso analítico jerárquico se obtienen los siguientes resultados.

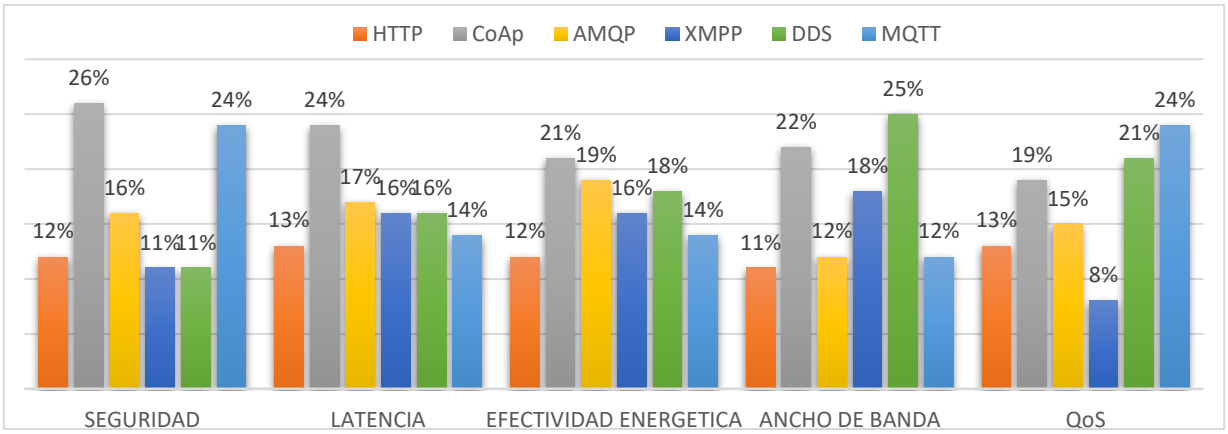


Figura 11. Análisis Comparativo AHP de Protocolos de Comunicación para IoT .Fuente: Propia

En la **¡Error! No se encuentra el origen de la referencia.** según los datos obtenidos se tiene como resultado la relevancia de criterios a considerar en primera instancia, empezando con el criterio de seguridad con un 26% seguido del ancho de banda con el 25%, la calidad de servicio con un 24%, la latencia con un 24% y finalmente la efectividad energética con un 21%.

Estos valores demuestran que la efectividad energética es importante sin embargo se deben tomar en cuenta los cuatro criterios antes mencionados, previo a la elección del protocolo de comunicación que funciona de manera efectiva para IoT tomando en cuenta factores como el área y aplicación destinados por el usuario.

Por medio de los resultados alcanzados en el análisis de las características de los protocolos de comunicación IoT se destacan los siguientes aspectos a discusión.

- CoAp ofrece seguridad mediante DTLS e IPSec garantizando la autenticación, integridad y encriptación además de un ancho de banda más bajo y eficiencia energética, todos estos aspectos lo hacen ideal para IoT siendo aplicado en la automatización de edificios y, redes inteligentes a mayor escala.

- MQTT cuenta con una calidad de servicio (QoS) aceptable, con niveles bajos de consumo de ancho de banda y consumo energético adicionalmente la seguridad que ofrece es aceptable. Considerado perfecto para IoT a menor escala como automatizar una casa, sin embargo, no tiene una buena acogida a escalas Industriales.

- AMQP es uno de los mejores protocolos para IoT puesto que su prioridad es la seguridad utilizando SAS O TLS de manera rápida y eficiente para la trasmisión de datos, por otro requiere de mayor ancho de banda y consumo energético estos aspectos lo hacen inadaptable para dispositivos móviles por estos criterios requiere de otros protocolos (MQTT y HTTP) para un buen funcionamiento sin dejar de lado que es un protocolo muy utilizado en mensajería y en la industria bancaria.

- DDS cuenta con una calidad de servicio aceptable sin embargo es levemente seguro, en cuanto a HTTP requiere mayor ancho de banda por otro lado es el más efectivo con un alto nivel de latencia en comparación a los demás protocolos, por último, en el ámbito energético HTTP, XMPP y DDS consumen altos niveles energéticos no favorables para IoT.

4. Conclusiones

En el presente trabajo se identifica que para el mejoramiento de aplicaciones que funcionan en tiempo real y sistemas automatizados es necesario identificar una infraestructura que permita converger diferentes protocolos funcionando de manera efectiva con IoT.

Por esta razón después del análisis realizado en este artículo se deduce que el protocolo CoAP ofrece mayor seguridad con (26%) en comparación a los demás protocolos; este se ejecuta con UDP siendo adecuado para aplicaciones IoT que requieren una alta carga de recursos con bajo consumo de energía (21%) además de un alto porcentaje (24%) en latencia , en cambio el protocolo MQTT se basa en el estándar TCP que sigue los procedimientos de protocolo de enlace y se comunica a través de conexiones establecidas mediante Publisher/suscriber, por lo que MQTT es preferido por las aplicaciones de IoT que crean un entorno de comunicación seguro y envían mensajes a múltiples suscriptores al mismo tiempo, así también ofrece un alto porcentaje (24%) en calidad de servicio (QoS).

Sin olvidar al protocolo AMQP logrando ser eficiente al fusionarse con MQTT y HTTP el cual se sabe que no puede trabajar solo, requiriendo de IpSec y TLS para elevar el nivel de seguridad. Para el ancho de banda el protocolo que ofrece el mayor porcentaje es DDS con un 25% de ventaja ante los otros protocolos sin embargo se requiere de un sistema cableado para su funcionamiento siendo utilizado en proyectos militares.

Finalmente, cada protocolo mencionado en este artículo está expuesto a condiciones y limitaciones propias, dependientes del área y la aplicación que el usuario destine, ya sea en casa o en una industria, se debe tener en cuenta sobre todo el criterio más importante de la presente investigación, la seguridad, donde CoAP es el mejor protocolo para Internet de las Cosas (IoT).

5. Referencias

1 P. Gokhale, O. Bhat y S. Bhat, «Introduction to IOT,» *International Advanced Research Journal in Science, Engineering and Technology*, pp. 41-44, 2018.

2 A. H. Raheem, «An integrated security Protocol communication scheme for Internet of Things using the Locator/ID Separation Protocol Network,» Doctoral dissertation, Middlesex University, 2017.

3 J. Dizdarević, F. Carpio, A. Jukan y X. Masip-Bruin, «A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration,» *ACM Computing Surveys (CSUR)*, vol. 51, nº 6, pp. 1-29, 2019.

4 R. Van Kranenburg y A. Bassi, «IoT Challenges,» *Nature Carrers*, pp. 1-9, 2012.

5 D. Dragonir, L. Gheorghe, S. Costea y A. Radovici, «A Survey on Secure Communication Protocols for IoT Systems,» *International Workshop on Secure Internet of Things (SIoT),* pp. 47-62, 2016.

6 J. Guerrero, F. Estrada y M. Medina, «SGreenH-IoT: Plataforma IoT para Agricultura de Precisión,» *SISTEMAS, CIBERNÉTICA E INFORMÁTICA,* pp. 53-58, 2017.

7 C. Sharma y N. K. Gondhi, «Communication Protocol Stack for Constrained IoT Systems,» *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU),* 2018.

8 M. Diwan y M. D'Souza, «A framework for modeling and verifying

IoT communication protocols,» *International Symposium on Dependable Software Engineering: Theories, Tools, and Applications*, pp. 266-280, 2017.

9 A. F. Santamaria, F. De Rango, A. Serianni y P. Raimondo, «A real IoT device deployment for e-Health applications under lightweight communication protocols, activity classifier and edge data filtering,» *Computer Communications*, vol. 128, pp. 60-73, 2018.

10 B. H. Çorak, F. Y. Okay, M. Güzel, Ş. Murt y S. Ozdemir, «Comparative analysis of IoT communication protocols,» *2018 International symposium on networks, computers and communications (ISNCC)*, pp. 1-6, 2018.

11 K. Petersen, R. Feldt, S. Mujtaba y M. Mattsson, 2008. [En línea]. Available: https://www.researchgate.net/publication/228350426_Systematic_Mapping_Studies_in_Software_Engineering. [Último acceso: diciembre 2021].

12 S. Luján, «Mapeo sistemático,» 2018. [En línea]. Available: http://desarrolloweb.dlsi.ua.es/cursos/2015/i-d-i/mapeo-sistematico.

13 T. Bi, P. Liang, A. Tang y C. Yang, «A systematic mapping study on text analysis techniques in software architecture,» *Journal of Systems and Software*, pp. 533-558, 2018.

14 C. Cheik Goh, E. Kanagaraj, L. Munirah Kamarudin y A. Zakaria, «IV-AQMS: HTTP and MQTT Protocol from a Realistic Testbed,» *2019 IEEE International Conference on Sensors and Nanotechnology*, 2019.

15 C. Gemirter, Ç. Şenturca y Ş. Baydere, «A Comparative Evaluation of AMQP, MQTT and HTTP Protocols Using Real-Time Public Smart City Data,» *2021 6th International Conference on Computer Science and Engineering (UBMK)*, 2021.

16 MDN Web Docs, «Generalidades del protocolo HTTP,» 2021. [En línea]. Available: https://developer.mozilla.org/es/docs/Web/HTTP/Overview.

17 A. A. Zaida, B. B. Zaidan, M. Qahtan, O. Albahri, A. Albahri, M. Alaa, M. Jumaah, M. Talal, K. Tan, K. Shir y C. Lim, «A survey on communication components for IoT-based technologies in smart homes,» *Telecommunication Systems*, nº 69, pp. 1-25, 2018.

18 M. Husnain, K. Hayat, E. Cambiaso, U. Fayyaz y M. Mongelli, «Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System,» *Sensors*, vol. 22, nº 2, p. 567, 2022.

19 J. Baek, M. Kanampiu y C. Kim, «A Secure Internet of Things Smart Home Network: Design and Configuration,» *Applied Sciences*, vol. 11, nº 14, p. 6280, 2021.

20 K. Khalil, K. Elgazzar, M. Selim y M. Bayoumi, «Resource discovery techniques in the internet of things: A review,» *Internet of Things*, vol. 12, p. 100293, 2020.

21 A. P. Haripriya y K. Kulothungan, «Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things,» *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, nº 1, pp. 1-15, 2019.

22 A. Kondoro y I. Dhaou, «Real time performance analysis of secure IoT protocols for microgrid communication,» *Future Generation Computer Systems*, vol. 116, pp. 1-12, 2021.

23 A. K. Muhammad, M. Khan, S. U. Jan, J. Ahmad y S. Jamal, «A Deep Learning-Based Intrusion Detection System for MQTT Enabled IoT,» *Sensors*, vol. 21, nº 21, p. 7016, 2021.

24 P. Jun-Hong, K. Hyeong-Su y K. Won-Tae, «DM-MQTT: An Efficient

MQTT Based on SDN Multicast for Massive IoT Communications,» *Sensors,* vol. 18, nº 9, 2018.

25 M. Yassein, M. Shatnawi, S. Aljwarneh y R. Al-Hatmi, «Internet of Things: Survey and open issues of MQTT protocol,» *2017 International Conference on Engineering & MIS (ICEMIS),* 2017.

26 E. Adi, A. Anwar, Z. Baig y S. Zeadally, «Machine learning and data analytics for the IoT,» *Neural Computing and Applications,* nº 32, pp. 16205-16233, 2020.

27 I. Ahammad, A. Rahman Khan y Z. Salehin, «Software-Defined Dew, Roof, Fog and Cloud (SD-DRFC) Framework for IoT Ecosystem: The Journey, Novel Framework Architecture, Simulation, and Use Cases,» *SN Computer Science,* vol. 2, nº 159, 2021.

28 M. Baig y T. Iqbal, «Design and implementation of an open-Source IoT and blockchain-based peer-to-peer energy trading platform using ESP32-S2, Node-Red and, MQTT protocol,» *Energy Reports,* vol. 7, pp. 5733-5746, 2021.

29 A. Chaudhary, S. Peddoju y K. Kadarla, «Study of Internet-of-Things Messaging Protocols Used for Exchanging Data with External Sources,» *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS),* 2017.

30 A. Larmo, A. Ratilainen y J. Saarinen, «Impact of CoAP and MQTT on NB-IoT System Performance,» *Sensors,* vol. 19, nº 1, 2019.

31 V. Gupta, S. Kher y N. Turk, «MQTT protocol employing IOT based home safety system with ABE encryption,» *Multimedia Tools and Applications,* vol. 80, nº 2, pp. 2931-2949, 2021.

32 A. Zainudi, M. Fahmi Syaifudin y N. Syahroni, «Design and Implementation of Node Gateway with MQTT and CoAP Protocol for IoT Applications,» *2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE),* 2019.

33 M. Yuan, «Conozca MQTT,» 2017. [En línea]. Available: https://developer.ibm.com/es/articles/iot-mqtt-why-good-for-iot/.

34 F. Viel, L. Silva, Q. L. Valderi Reis y J. F. De Paz Santana, «An Efficient Interface for the Integration of IoT Devices with Smart Grids,» *Sensors,* vol. 20, nº 10, p. 2849, 2020.

35 M. Kashyap, V. Sharma y G. Verma, «Implementation and Analysis of IoT Based Automation Using MQTT,» *2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON),* 2021.

36 Z. Ali y H. Ali , «Towards sustainable smart IoT applications architectural elements and design: opportunities, challenges, and open directions,» *The Journal of Supercomputing,* vol. 77, pp. 5668-5725, 2021.

37 Arrow Electronics, «Descripción general de los protocolos web,» 2015. [En línea]. Available: https://www.arrow.com/es-mx/research-and-events/articles/overview-of-web-protocols.

38 DITEL, «Protocolo MQTT,» 2021. [En línea]. Available: https://www.ditel.es/protocolo-mqtt/.

39 M. Cruz, J. Rodriguez, P. Lorenz, P. Solic, J. Muhtali y H. Albuqierque, «A proposal for bridging application layer protocols to HTTP on IoT solutions,» *Future Generation Computer Systems,* vol. 97, pp. 145-152, 2019.

40 S. Hernández Ramos, T. Villalba y R. Lacuesta, «MQTT Security: A Novel Fuzzing Approach,» *Wireless*

Communications & Mobile Computing, vol. 2018, 2018.

41 S. Jaloudi, «Communication Protocols of an Industrial Internet of Things Environment: A Comparative Study,» *Future Internet*, vol. 11, nº 3, 2019.

42 IONOS, «¿Qué es el HTTP?,» 2020. [En línea]. Available: https://www.ionos.es/digitalguide/hosting/cuestiones-tecnicas/protocolo-http/.

43 V. Seoane, C. Garcia-Rubio, F. Almendares y C. Campo, «Performance evaluation of CoAP and MQTT with security support for IoT environments,» *Computer Networks*, vol. 197, nº 9, p. 108338, 2021.

44 A. Kumar y S. Sharad, «Secure and energy-efficient smart building architecture with emerging technology IoT,» *Computer Communications*, vol. 176, nº 1, pp. 207-217, 2021.

45 C. R. Cisneros, «"Estudio de mecanismos de aseguramiento de la información para internet de las cosas IoT en Smart home".,» 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.

46 T. Lee Scott y A. Eleyan, «CoAP based IoT data transfer from a Raspberry Pi to Cloud,» *2019 International Symposium on Networks, Computers and Communications (ISNCC)*, 2019.

47 L. Llamas, «¿Qué Es Mqtt? Su Importancia Como Protocolo Iot?,» 2019. [En línea]. Available: https://www.luisllamas.es/que-es-mqtt-su-importancia-como-protocolo-iot/.

48 A. Felfernig, S. Polat-Erdeniz, C. Uran, S. Reiterer y M. Atas, «An overview of recommender systems in the internet of things,» *Journal of Intelligent Information Systems*, nº 52, pp. 285-309, 2019.

49 F. Luthfi, E. A. Juanda y I. Kustiawan, «Optimization of Data Communication on Air Control Device Based on Internet of Things with Application of HTTP and MQTT Protocols,» *IOP Conference Series. Materials Science and Engineering*, vol. 384, nº 1, 2018.

50 A. Makkad, «Security in Application Layer Protocols for IoT: A focus on CoAP,» *International Journal of Advanced Research in Computer Science*, vol. 8, nº 5, pp. 2653-2656, 2017.

51 M. E. Ouadghiri, B. Aghoutane y N. E. Farissi, «Communication model in the Internet Of Things,» *Procedia Computer Science*, vol. 177, pp. 72-77, 2020.

52 G. De Oliveira, O. De Faria Oliveira y S. De Abreu, «Opportunities and accessibility challenges for open-source general-purpose home automation mobile applications for visually disabled users,» *Multimedia Tools and Applications*, vol. 81, pp. 10695-10722, 2022.

53 M. Poh, J. Kubela, S. Bosse y K. Turowski, «Performance Evaluation of Application Layer Protocols for the Internet-of-Things,» *2018 Sixth International Conference on Enterprise Systems (ES)*, 2018.

54 G. Poonam y P. Indhra Om , «A Survey of Application Layer Protocols for Internet of Things,» *2021 International Conference on Communication information and Computing Technology (ICCICT)*, 2021.

55 Programadorclick, «Programador clic,» 2019. [En línea]. Available: https://programmerclick.com/article/90602231214/.

56 C. Sanaboina y T. Eluri, «Performance Evaluation of Advanced Congestion Control Mechanisms for COAP,» *i-Manager's Journal on Wireless*

Communication Networks, vol. 7, nº 1, p. 17, 2018.

57 D. Silva, L. Carvalho, J. Soares y R. Sofia, «A Performance Analysis of Internet of Things Networking Protocols: Evaluating MQTT, CoAP, OPC UA,» *Applied Sciences,* vol. 11, nº 11, p. 4879, 2021.

58 N. F. Syed, Z. Baig, A. Ibrahim y C. Valli, «Denial of service attack detection through machine learning for the IoT,» *ournal of Information and Telecommunication,* vol. 4, nº 4, pp. 482-503, 2020.

59 I. P. Sáez, «IoT: protocolos de comunicación, ataques y recomendaciones,» 2019. [En línea]. Available: https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones.

60 R. Tamri y S. Rakrak, «The MI-SDN System to Manage MQTT Data in an Interoperable IoT Wireless Network,» *Turkish Journal of Computer and Mathematics Education,* vol. 15, nº 5, pp. 1031-1036, 2021.

61 F. Tortoriello y I. Veronesi, «Internet of things to protect the environment: a technological transdisciplinary project to develop mathematics with ethical effects,» *Soft Computing,* vol. 25, pp. 8159-8168, 2021.

62 G. Uddin, F. Sabir, Y.-G. Guéhéneuc, O. Alam y F. Khomh, «An empirical study of IoT topics in IoT developer discussions on Stack Overflow,» *Empirical Software Engineering,* vol. 26, 2021.

63 M.-C. Chen y P. Hung Ho, «Exploring technology opportunities and evolution of IoT-related logistics services with text mining,» *Complex & Intelligent Systems,* vol. 7, pp. 2577-2595, 2021.

64 H. Hamid, R. Noor, O. Syaril Nizam , I. Ahmedy y S. Anjum, «IoT-based botnet attacks systematic mapping study of literature,» *Scientometrics*, vol. 126, pp. 2759-2800, 2021.

65 D. I. Dikiy y V. D. Artemeva, «MQTT DATA PROTOCOL IN REMOTE ACCESS CONTROL MANAGEMENT MODEL FOR INTERNET NETWORKS,» *Nauchno-Tekhnicheskii Vestnik Informatsionnykh Tekhnologii, Mekhaniki i Optiki*, vol. 19, nº 1, pp. 109-117, 2019.