REVISIÓN SISTEMÁTICA DE LITERATURA DE MIDDLEWARE PARA AUMENTAR LA EFECTIVIDAD EN LA IMPLEMENTACIÓN DEL INTERNET DE LAS COSAS (IOT)

ANDRÉS MAURICIO PUERTA VÉLEZ

CRISTHIAN ANDRES SALDARRIAGA GOMEZ

DIRECTOR:

SEBASTIAN GOMEZ JARAMILLO

Tecnológico de Antioquia

Institución Universitaria

Ingeniería en Software

Medellín, Colombia.

2019

DEDICATORIA

El presente trabajo investigativo lo dedicamos principalmente a Dios, por ser el inspirador y darnos fuerza para continuar en este proceso de obtener uno de los anhelos más deseados.

A nuestros padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes hemos logrado llegar hasta aquí y convertirnos en lo que somos. Ha sido el orgullo y el privilegio de ser sus hijos, son los mejores padres.

A nuestros hermanos (as) por estar siempre presentes, acompañándonos y por el apoyo moral, que nos brindaron a lo largo de esta etapa de nuestras vidas.

A todas las personas que nos han apoyado y han hecho que el trabajo se realice con éxito en especial a aquellos que nos abrieron las puertas y compartieron sus conocimientos.

AGRADECIMIENTOS

Agradecemos a Dios por bendecirnos la vida, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a nuestros padres: Luz Aida y Henry; Angela y Alberto, por ser los principales promotores de nuestros sueños, por confiar y creer en nuestras expectativas, por los consejos, valores y principios que nos han inculcado.

Agradecemos a nuestros docentes de la institución universitaria Tecnológico de Antioquia, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión, de manera especial, al Doctor Sebastián Gómez Jaramillo tutor de nuestro proyecto de investigación quien ha guiado con su paciencia, así como también a Raúl Andres Castañeda Quintero docente de física quien hoy, se encuentra en los Estados Unidos. Al docente Leonardo Ceballos Urrego docente de Matemáticas y Calculo.

Quiero agradecer y resaltar la dedicación, entusiasmo, amistad y guia de Juan Carlos Muñoz maestro del Club de Taekwondo de la institución, este hombre invierte su tiempo y su vida en el bienestar de sus alumnos, formándolos y apoyándolos para superar sus sueños, metas y objetivos, fue y seguirá siendo una gran inspiración de integridad, perseverancia y honestidad.

RESUMEN

El internet de las cosas es la tecnología emergente que plantea la revolución del internet como lo conocemos, debido a que promete la interconexión de aproximadamente 50.000 millones de objetos para el 2020, esto plantea la solución a muchos procesos que requieren tener una disponibilidad de información completa, pero tambien tiene unas vulnerabilidades significativas que ponen en peligro la seguridad e integridad de la información, por lo anterior se plantea la implementación del Middleware para mitigar estas vulnerabilidades y darle a los usuarios de esta tecnología la confianza requerida para su implementación.

En el presente trabajo se hace una revisión sistemática de literatura para identificar el estado actual del uso del Middleware en aplicaciones de IOT, conociendo sus usos, fortalezas y áreas en donde más se ha utilizado.

PALABRAS CLAVE

IoT, Middleware, Intertnet of things, Seguridad, Integridad, Disponibilidad, Plataformas, Dispositivos, Interconexión, Interoperabilidad, 5g, LoRa, BLE.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En la actualidad, la ciudad de Medellín está implementado diferentes tecnologías emergentes enfocadas a la mejora continua en la calidad de vida de las personas, buscando siempre optimizar actividades y disminuir el tiempo que tarda realizar cada proceso. Teniendo en cuenta las ventajas de internet, como las conexiones globales que hacen posible la existencia de la navegación web, los medios sociales y los dispositivos móviles inteligentes, se ha trabajado en la integración de más aplicaciones, plataformas y dispositivos, que puedan cumplir su funcion dentro de la red eficazmente, al día hoy, se predice que Internet interconectará 50.000 millones de objetos para el año 2020 (Corporación Ruta N 2015). La tecnología para la interconexion de dispositivos se denomina IoT, logrando una conexión e integración de diferentes dispositivos y objetos de la vida cotidiana a través de los diferentes medios de conexión Wlan, Lan, 4G, Bluetooth, Wireless Sensor Network, entre otros (McKinsey Global Institute, 2014).

Para mejorar la interconexión es necesario comprender el lenguaje, método o formato de comunicación y así, obtener un control, monitoreo y optimización de las actividades realizadas en los campos donde se desarrolla el IoT, como la Manufactura (Candia et al. 2018), Salud (Senthil Kumaran, Nallakaruppan, and Senthil Kumar 2016), Transporte (Cristian Valencia R. 2018), Servicios publicos (Balcells J., Romeral 2015), entre otras. Por lo tanto, el mayor reto de esta tecnología es mitigar las fallas de dicha interconexión entre los diferentes dispositivos, interpretar su lenguaje, lograr una comunicación efectiva y homogénea entre las aplicaciones. Lo anterior se traduce en que la información sea confiable, conserve su integridad, disminuyan los tiempos de envío y recepción aumentando la seguridad de la información. Debido a esto existen proyectos basados IoT enfocados en suplir o lograr solucionar la problemática descrita, implementando el Middleware como posible solución. (Fremantle and Scott 2017). Ya que es un Software de conectividad el cual consiste en un conjunto de servicios que permiten interactuar a múltiples procesos que se ejecutan en distintas máquinas a través de una red, brindando la capacidad de recopilar, analizar e interpretar datos (Mendoza et al. 2016), ocultando la heterogeneidad, abstrayendo la complejidad subyacente y de esta manera, se provee un modelo de programación conveniente para los desarrolladores de software. (Sosa 2014).

El IoT es una tecnología emergente y en la ciudad Medellín es muy reciente aún, de modo que, requiere mucha más investigación, estudio, laboratorios y/o pruebas que ayuden a comprender mejor su aplicación en las diferentes ramas de la ciencia. En los últimos años, en el sector de las telecomunicaciones se ha propuesto la implementación de IoT en ambientes residenciales y empresariales, como es el caso de Claro (IoT Claro 2015) y Tigo (Tigo Business 2015), quienes designaron un equipo para el estudio de este nuevo mercado creciente y su aplicación en el

medio, la Alcaldía y EPM con su proyecto de integración de los medios de transporte TPM llamado Ciudades inteligentes (EPM 2019) también ha tenido participación en el tema, EPM además busca implementar un sistema de monitoreo más eficiente de sus redes eléctricas Smart Grid o redes Electricas inteligentes (EPM 2017), además de los entes de investigación e innovación como Ruta N que en apoyo de varias compañías ha velado por profundizar más en el tema y lograr tener unas bases fundamentadas en dicha tecnología, hecho que se resalta con la selección de Medellín como la 5ta sede de la 4ta Revolución Industrial situada en el Complejo Ruta N, es aquí donde se recopilaran, analizarán e implementaran diversos proyectos en las ramas que comprende dicha revolución, como el IoT. Lo anterior crea una base fundamental para profundizar en el IoT como la tecnología que revolucionará las comunicaciones, aclarando que requiera una investigación muy exhaustiva en pro de garantizar la comunicación y la seguridad de las diferentes plataformas, dispositivos, leguajes y procesos con la intervención del Middleware. Esto también ha de generar un impacto positivo en las diferentes universidades y sus semilleros de investigación, ampliando el conocimiento, preparando profesionales más preparados y aumentando la calidad de la enseñanza no solo en la ciudad, sino en el país.

2. DEFINICIÓN DEL PROBLEMA

Las redes de datos, la interconexión de dispositivos y la transferencia de información han dado como fruto una de las nuevas tecnologias que revolucionará la conexión a internet, el IoT ha tenido en los últimos años un crecimiento significativo en pro de cumplir un objetivo en específico el interconectar más y más dispositivos, controlar sus diferentes funcionalidades y características, además de monitorear el estado de las actividades ejecutadas por cada uno, y es aquí donde surge el reto más grande hasta el momento de esta tecnología, lograr traducir los diferentes lenguajes de comunicación de cada fabricante de acuerdo al sistema operativo, aplicación y programa ejecutado, estableciendo una comunicación segura y continua para garantizar la confiabilidad de la información, generando un ambiente donde la heterogeneidad sea mitigada de tal forma que la recolección de datos sea mucho más optima. Los fabricantes enfrentan a menudo desafíos económicos y técnicos cuando construyen y mantienen características de seguridad sólidas en los dispositivos de la IoT. Sin embargo, los dispositivos y servicios con seguridad débil son vulnerables a ataques cibernéticos y pueden exponer los datos del usuario a robo. Esto es un desafío clave en la IoT porque un número mayor de dispositivos de la IoT en línea aumenta la cantidad de posibles vulnerabilidades de seguridad. En principio, los desarrolladores, los usuarios de dispositivos y sistemas de la IoT tienen una obligación colectiva de asegurar que no exponen a sus usuarios ni a la misma Internet a un posible daño. (Manyika et al. 2016)

Un ejemplo de esta problemática mencionada ocurrio en 2016, más de 100.000 dispositivos de IoT se unieron en una botnet hostil llamada Mirai que atacó los servidores DNS de la costa este de los Estados Unidos. Por lo tanto, hay una fuerte motivación para encontrar enfoques para mejorar y aumentar la seguridad y privacidad de la IoT. (Fremantle and Scott 2017)

Los dispositivos de la IoT tocarán probablemente la mayor parte de aspectos de nuestras vidas, incluidos los dispositivos en nuestros hogares, lugares de trabajo, hospitales y otros espacios públicos. Así, es posible que afecten las políticas sobre privacidad, seguridad de datos, la atención médica, el transporte y la tecnología. Esta clase de amplio alcance sugiere que quienes crean los entes regulatorios necesitarán considerar las amplias implicaciones sobre las políticas a lo largo de un gran campo de objetivos e iniciativas de protección de la información que se transmiten a través del IoT, por ende profundizar en la tecnologia del Middleware aplicado en la IoT como la solución propuesta a la vulnerabilidad de integración de las diferentes aplicaciones y dispositivos reduciendo el porcentaje de colapso en la red, perdida en la comunicación, errores en el envío de la información y fallas en la operatividad de cada dispositivo, además de que proporciona un

mayor nivel de seguridad y/o confiabilidad en el envío y recepción de los datos, lo que permitira proteger más eficazmente la informaciòn de los usuarios que utilizan esta tecnología, este punto es clave de la IoT porque cada vez habràn más dispositivos en línea, lo que aumenta la cantidad de posibles vulnerabilidades de seguridad. (Fremantle and Scott 2017)

3. MARCO TEÓRICO

El **«Internet de las Cosas»** (IoT) hace referencia, como se ha adelantado, a una tecnología basada en la conexión de objetos cotidianos a Internet que intercambian, agregan y procesan información sobre su entorno físico para proporcionar servicios de valor añadido a los usuarios finales. También reconoce eventos o cambios, y tales sistemas pueden reaccionar de forma autónoma y adecuada. Su finalidad es, por tanto, brindar una infraestructura que supere la barrera entre los objetos en el mundo físico y su representación en los sistemas de información. El Internet de las Cosas se equipara a menudo con electrodomésticos y bienes de consumo, como las ropas tecnológicas (wearables) o los coches inteligentes. Por lo tanto, muchas de las preocupaciones iniciales se han centrado en los productos de consumo (Andrés M. 2018).

La seguridad: Los términos seguridad de la información, seguridad informática y garantía de la información son utilizados con bastante frecuencia. El significado de dichas palabras es diferente, pero todos persiguen la misma finalidad que es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización. Entre dichos términos existen pequeñas diferencias, dichas diferencias proceden del enfoque que le dé, las metodologías usadas y las zonas de concentración.

La Seguridad de la Información, según ISO27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan (SGSI-ISO 2015).

La Privacidad: La protección de datos, también llamada privacidad de información, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros (Rouse 2014).

La interoperabilidad: La interoperabilidad es la capacidad de dos o más sistemas o componentes para intercambiar información y usar la información que se ha intercambiado. La interoperabilidad típica se lleva a cabo en dos niveles; semántico y técnico. La interoperabilidad semántica permite a las partes involucradas describir los requisitos sin considerar la implementación técnica. Con respecto al software, el término interoperabilidad se usa para describir la capacidad técnica de distintos programas para intercambiar los datos a través de un conjunto común de formatos de intercambio, para leer y escribir los mismos formatos de archivo, y para usar los mismos protocolos (Naciones Unidas 2012).

IPv6: IPv6 es la versión actualizada del protocolo de Internet. En gran parte de Internet se utiliza IPv4, un protocolo fiable y elástico que viene utilizándose desde hace más de 20 años. Sin embargo, IPv4 tiene limitaciones que podrían causar problemas a medida que Internet crece. IPv6

es la versión actualizada de IPv4 y está sustituyendo gradualmente a IPv4 como estándar de Internet (Madakam, Ramaswamy, and Tripathi 2015).

Red 5G: Es la próxima (quinta) generación de tecnología celular que promete mejorar enormemente la velocidad, cobertura y capacidad de respuesta de las redes inalámbricas. ¿De qué tan rápido estamos hablando? Piensa en unas 10 a 100 veces más rápida que tu conexión celular actual, y aún más rápida que cualquier cosa que puedas obtener con un cable de fibra óptica en tu casa (CHENG 2018).

LoRa: LoRa está pensado para aplicaciones de baja potencia, de red de área amplia (LPWAN). Tiene un rango de más de 15 kilómetros y una capacidad de hasta 1 millones de nodos. La combinación de baja potencia y largo alcance limita la velocidad de datos máxima a 50 kilobits por segundo (Kbps).

LoRa es una tecnología exclusiva y patentada de propiedad de Semtech Corporation, que funciona en la banda ISM. La asignación de frecuencias y los requisitos reglamentarios para ISM varían por región Dos de las más populares son las frecuencias de 868 megahercios (MHz) utilizada en Europa y 915 MHz utilizada en América del Norte (Pickering 2017).

Bluetooth BLE: La tecnología BLE (Bluetooth low Energy) se basa en el estándar Bluetooth 4.0, funciona en las frecuencias de 2,4 GHz y fue creada por razones de marketing para dispositivos smartphone y tablet, casi en contraste con la tecnología NFC, cuya principal diferencia es la distancia de lectura, que en el caso de la tecnología BLE puede llegar hasta 100 metros.

El potencial de esta tecnología, sin embargo, va allá de los utilizos en el campo del marketing a travès de los dispositivos móviles, y van a comprender aplicaciones que hasta hoy se implementaban con la tecnología RFID activa (Global Tag Srl 2016).

Middleware: Software de conectividad que consiste en un conjunto de servicios que permiten interactuar a múltiples procesos que se ejecutan en distintas máquinas a través de una red. Ocultan la heterogeneidad, abstrae la complejidad subyacente y proveen de un modelo de programación conveniente para los desarrolladores de aplicaciones. Es un software que puede incrementar significativamente la reusabilidad mediante soluciones utilizables rápidamente y basadas en estándares aplicables a problemas y tareas comunes en programación. Permite concentrarse en asuntos propios de la aplicación y olvidarse de problemas comunes, estructurales o no, ya resueltos previamente de forma elegante y satisfactoria (Sosa 2014).

4. OBJETIVOS

4.1. Objetivo General

Analizar la efectividad del Middleware para optimizar la implementación de IoT por medio de una revisión sistemática de la literatura.

4.2. Objetivos Específico

- Diseñar un proceso de planeación de la revisión de literatura según el protocolo de Kitchenham
- Realizar el análisis de los artículos identificados que cumplan con el proceso de planeación.
- Reportar los resultados obtenidos en la revisión de literatura

5. METODOLOGÍA

Para logar cumplir exitosamente los objetivos propuestos se desarrolló una revisión sistemática y exhaustiva de los estándares, fundamentos y proyectos basados en IoT y el Middleware siguiendo el protocolo definido por Kitchenham, se analizan los procesos realizados, sus resultados y que conclusiones se obtuvieron, se ha de realizar una tabla comparativa que evalúe los puntos más importantes de la implementación del IoT, de ahí se tomaron unas métricas y conclusiones requeridas para continuar con la investigación. Todo esto buscando resolver la vulnerabilidad de la seguridad de la información, la intercomunicación de dispositivos, plataformas y lenguajes en pro de aumentar la efectividad de la tecnología.

Posteriormente se realizó un análisis, clasificación y validación del middleware haciendo énfasis en las ventajas que puede otorgar a los procesos del IoT, debido a que esta tecnología tiene un campo de acción bastante amplio es necesario que la clasificación realizada se adapte a cada rama en la que se aplique dicha tecnología como la Salud, Transporte, Telecomunicaciones, Manufactura y Educación entre otras, además tener en cuenta las aplicaciones que ya ha tenido, y como podría implementarse en los proyectos de la ciudad de Medellín como una de las sedes de la 4ta revolución industrial, por consiguiente permite tener un acceso mucho más amplio a la información de las investigaciones realizadas y el impacto que estas generan.

Por ultimo unas conclusiones con base en los resultados obtenidos en esta investigación, se hará de forma minuciosa la explicación de cada aspecto encontrado en este proceso y se resaltará el porcentaje de efectividad en la disminución de la problemática propuesta.

6. DESARROLLO DEL PROYECTO

7.1. Diseñar proceso de planeación

Para hacerlo se siguió el protocolo de revisión Kitchenham, el cual está enfocado en el contexto de ingeniería de software a través de un método para identificar, analizar e interpretar los artículos relacionados con el objetivo de la investigación. Este protocolo permite apoyar de forma sistemática, repetible y sin sesgos la realización de una revisión de literatura distribuido en las fases de planificación, ejecución y de conclusiones.

La primera etapa, denominada planificación, se refiere a las actividades previas a la revisión y tiene como objetivo establecer los criterios del protocolo de revisión definiendo las preguntas de investigación, los criterios de inclusión y de exclusión, las fuentes de información, la cadena de búsqueda y los procedimientos de categorización.

Las preguntas de investigación presentadas a continuación permiten identificar cómo ha sido la aplicación del Middleware en IoT. En la Tabla 1 están desglosadas cada una de las preguntas junto con su respectiva justificación.

Preguntas de investigación

Pregunta	Justificación
¿La implementación de IoT analizada fue utilizada en qué rama de la ciencia y/o la tecnología? (Movilidad y transporte, salud, telecomunicaciones, energía, monitoreo ambiental, entre otros)	Permite conocer el estado actual de las áreas de conocimiento en dónde más se ha utilizado el IOT y poder planificar en qué áreas del conocimiento se pueden realizar trabajos futuros.
¿Cómo influyen estas implementaciones de middleware para optimizar el IoT?	Se pretende identificar el aporte del Middleware para el proceso del IOT

Pregunta	Justificación
¿ Cuáles fueron los resultados obtenidos que demuestran la efectividad del middleware para optimizar el IoT?	Se busca analizar las fortalezas dadas por el Middleware y poder justificar su uso en futuras aplicaciones
¿Qué tipo de conexiones utilizan dichas implementaciones? (F.O, 4G, 5G, Wifi, Bluetooth, LoRa, Bluetooth Ble, etc)	Conocer las conexiones donde se ha implementado y las futuras a implementar.

Se definieron seis criterios de inclusión y tres de exclusión para poder identificar la viabilidad de usar los artículos dentro de la revisión sistemática de literatura. Estos criterios están descritos en la siguiente tabla.

Criterios de inclusión y de exclusión

Inclusión	Exclusión
El artículo aplica elementos de Middleware e IOT	No es un resumen o el artículo no se encuentra completo
Artículos en inglés y español	El artículo no tiene bien definido el proceso de implementación de IOT
El artículo tiene las palabras de la cadena de búsqueda	El foco del artículo no es el IOT o el Middleware
El artículo es de una fuente de buena calidad	

La estrategia de búsqueda se hizo con fuentes de información primarias de bases de datos académicas reconocidas dentro del campo de aplicación de la búsqueda. Las cuales tienen artículos netamente académicos que han pasado por revisión de pares realizadas por expertos, correspondientes a artículos de revista, capítulos de libros y memorias de eventos académicos. Los criterios de búsqueda fueron aplicados al título, el resumen y las palabras claves, con artículos

publicados en inglés o en español hasta el año 2017. El resumen de la estrategia de búsqueda se observa en la Tabla III.

EEstrategia de búsqueda

Bases de Datos	Science Direct
	IEEExplore
	Springer
Tipo de Publicación	Artículos de revista
	Memorias de Conferencias
	Workshops
	Libros
Búsqueda aplicada a	Titulo
	Resumen
	Palabras claves
Idioma	Inglés
	Español
Periodo de publicación	Hasta noviembre de 2017

La búsqueda de los estudios se realizó teniendo en cuenta principalmente el uso de IOT y en segunda medida Middleware junto con otros términos de interés. Por eso se definieron dos términos principales para la cadena de búsqueda. Posteriormente se agregaron términos alternativos con el booleano OR que permite relacionar sinónimos, términos similares o expresiones semejantes al término principal. Asimismo, cada grupo de términos fue asociado con

el booleano AND para que la búsqueda arrojara artículos que contuviera los tres grandes términos de la cadena de búsqueda. Esta cadena se describe en la Tabla IV..

Cadena de Búsqueda

Término principal	Término alternativo
IOT	Internet of Things
	IoT
Middleware	Middleware
	Services
	Interlogical
Otros	Implementation
	Effect*
	Security
	Plattforms
	Devices

7.2. Análisis de los artículos identificados

Siguiendo el protocolo de Kitchenham y después de hacer un criterio de inclusión y de exclusión quedaron los siguientes artículos

#	Nombre_Artículo	Referencia	Año	Tipo publicación
1	A Qualitative Evaluation of IPv6 for the Industrial Internet of Things	(Feldner and Herber 2018)	2018	Evento

2	A middleware architecture for adaptive devices	(Cereda and Neto 2017)	2017	Evento
3	A survey on Internet of Things architectures	(Ray 2018)	2016	Artículo
4	An Overview of Security in Internet of Things	(Al-Turjman 2020)	2019	Artículo
5	Analysis of identifiers on IoT platforms	(Aftab et al. 2019)	2019	Artículo
6	An agile and effective network function virtualization infrastructure for the Internet of Things	(Mattos, Velloso, and Duarte 2019)	2019	Capítulo de libro
7	Security Testbed for Internet of Things Devices	(Siboni et al. 2019)	2019	Evento
8	A method of NC machine tools intelligent monitoring system in Smart factories"	(W. Liu et al. 2020)	2019	Artículo
9	A semantic-based discovery service for the Internet of Things	(Gomes et al. 2019)	2019	Artículo
10	A telehealth system framework for assessing knee-joint conditions using vibroarthrographic signals	(Athavale and Krishnan 2020)	2019	Artículo
11	A UAV-assisted CH election framework for secure data collection in wireless sensor networks	(G. Wang et al. 2020)	2019	Artículo
12	Approximate-data-aggregation-in-sensor-equipped-IoT-networksTsinghua-Science-and-Technology	(J. Li et al. 2020)	2019	Evento
13	Assessment of interoperability in cloud manufacturing - Robotics and Computer Integrated Manufacturing	(Mourad et al. 2020)	2019	Artículo
14	Averaged dependence estimators for DoS attack detection in IoT networks	(Baig et al. 2020)	2019	Artículo
15	Demonstrability of Narrowband Internet of Things technology in advanced metering infrastructure	(Wan, Zhang, and Wang 2019)	2019	Artículo
16	Energy harvesting-based data uploading for Internet of Things	(G. Sun, Xing, and Qin 2019)	2019	Artículo
17	Industry 4.0 based process data analytics platform: A waste-to-energy plant case study	(Kabugo et al. 2020)	2019	Artículo

18	Intelligence and security in big 5G-oriented IoNT: An overview	(Al-Turjman 2020)	2019	Artículo
19	L 1 Subspace Tracking for Streaming Data	(Y. Liu et al. 2020)	2019	Artículo
20	Online heart monitoring systems on the internet of health things environments: A survey, a reference model and an outlook	(Santos et al. 2020)	2019	Artículo
21	PoRX A reputation incentive scheme for blockchain consensus of IIoT	(E. K. Wang et al. 2020)	2019	Artículo
22	Trust-based recommendation systems in Internet of Things: a systematic literature review	(Mohammadi et al. 2019)	2019	Evento
23	MOSDEN: An Internet of Things Middleware for Resource Constrained Mobile Devices	(Perera et al. 2014)	2014	Evento
24	A Highly Accurate Deep Learning Based Approach for Developing Wireless Sensor Network Middleware	(Alshinina and Elleithy 2018)	2018	Evento
25	SmartCityWare: A Service-Oriented Middleware for Cloud and Fog Enabled Smart City Services	(Mohamed et al. 2017)	2017	Artículo
26	Internet of things architecture for a smart passenger-car robotic first aid system	(Kurebwa and Mushiri 2019)	2019	Evento
27	A Middleware based on Service Oriented Architecture for Heterogeneity Issues within the Internet of Things	(Mesmoudi et al. 2018)	2018	Artículo
28	Understanding IoT Systems: A Life Cycle Approach	(Rahman, Ozcelebi, and Lukkien 2018)	2018	Evento
29	New Security Architecture for IoT Network	(Flauzac, Gonzalez, and Nolot 2015)	2015	Evento
30	Aspects of Quality in Internet of Things (IoT) Solutions A Systematic Mapping Study	(Ahmed et al. 2019)	2019	Artículo
31	Internet of Things Vision Applications and Challenges	(Mehta, Sahni, and Khanna 2018)	2018	Evento
32	Towards Security on Internet of Things Applications and Challenges in Technology	(Sadique, Rahmani, and Johannesson 2018)	2018	Evento

33	Management and Internet of Things	(Samaniego and Deters 2016)	2016	Evento
34	Networks and Devices Management	(Silva et al. 2019)	2019	Capítulo de libro
35	A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective	(Chen et al. 2014)	2014	Artículo
36	A Survey on Resource Management in IoT Operating Systems	(Musaddiq et al. 2018)	2018	Artículo
37	Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI)	(Aldaej 2019)	2017	Artículo
38	A roadmap for security challenges in the Internet of Things	(Riahi Sfar et al. 2018)	2017	Artículo
39	Analysis of identifiers on IoT platforms	(Aftab et al. 2019)	2019	Artículo
40	Middleware for internet of things: an evaluation in a small-scale IoT environment	(Palade et al. 2018)	2018	Artículo
41	Internet of Things Services for Small Towns	(Y. Sun et al. 2014)	2014	Evento
42	The Internet of Things for enterprises: An ecosystem,architecture, and IoT service business model	(Lee 2019)	2017	Capítulo de libro
43	On middleware for emerging health services	(Singh and Bacon 2014)	2014	Artículo
44	Fog Computing Over IoT A Secure Deployment	(Zahra et al. 2017)	2019	Artículo
45	Thing Relation Modeling in the Internet of Things	(A. Li, Ye, and Ning 2017)	2017	Artículo
46	Internet of Spatial Things: A New Reference Model With Insight Analysis	(Eldrandaly, Abdel-Basset, and Shawky 2019)	2019	Artículo
47	Performance evaluation of IoT middleware	(da Cruz et al. 2018)	2018	Capítulo de libro
48	An IoT Tree Health Indexing Method Using Heterogeneous Neural Network	(Wu et al. 2019)	2019	Artículo

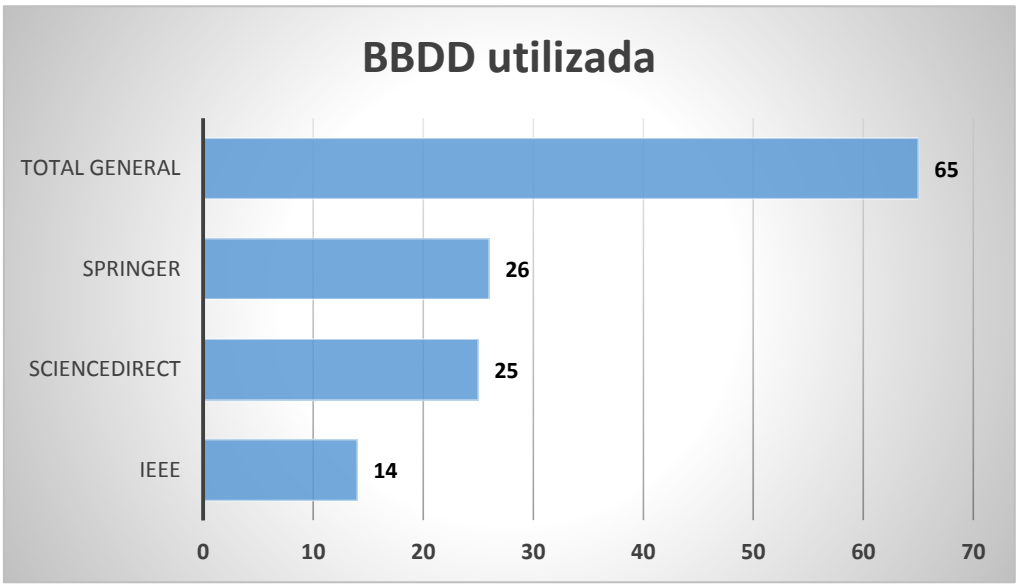
49	Motion Recommender for Preventing Injuries During Motion Gaming	(Paliyawan, Kusano, and Thawonmas 2019)	2018	Capítulo de libro
50	Controlled and Secure Access to Promote the Industrial Internet of Things	(Marquez et al. 2018)	2018	Artículo
51	Middleware Architecture for Health Sensors Interoperability	(Georgi, Corvol, and Le Bouquin Jeannes 2018)	2018	Capítulo de libro
52	Defending Against New-Flow Attack in SDN-Based Internet of Things	(Xu et al. 2017)	2016	Artículo
53	A Fog Based Middleware for Automated Compliance With OECD Privacy Principles in Internet of Healthcare Things	(Elmisery, Rho, and Botvich 2016)	2017	Capítulo de libro
54	Attitudes and Perceptions of IoT Security in Critical Societal Services	(Asplund and Nadjm-Tehrani 2016)	2016	Capítulo de libro
55	On the Performance Impact of Data Access Middleware for NoSQL Data Stores	(Rafique et al. 2018)	2018	Capítulo de libro
56	A resilient Internet of Things architecture for smart cities	(Abreu et al. 2017)	2017	Capítulo de libro
57	A review on smart home present state and challenges: linked to context-awareness internet of things (IoT)	(Almusaylim and Zaman 2019)	2019	Artículo
58	Adaptive Internet of Things and Web of Things convergence platform for Internet of reality services	(Yu et al. 2016)	2016	Artículo
59	Internet of things: from internet scale sensing to smart services	(Georgakopoulos and Jayaraman 2016)	2016	Artículo
60	Resource allocation mechanisms and approaches on the Internet of Things	(Ghanbari et al. 2019)	2019	Capítulo de libro
61	Mobile IMS Integration of the Internet of Things in Ecosystem	(Hsieh, Hsieh, and Chen 2014)	2015	Artículo

62	Intelligent assembly system for mechanical products and key technology based on internet of things	(M. Liu et al. 2017)	2014	Capítulo de libro
63	Middleware for Internet distribution in the context of cloud computing and the Internet of Things	(Blair, Schmidt, and Taconet 2016)	2016	Capítulo de libro
64	Research on the overall architecture of Internet of Things middleware for intelligent industrial parks	(Zhang et al. 2019)	2019	Artículo
65	Traceability and visual analytics for the Internet-of-Things (IoT) architecture	(Lomotey, Pry, and Chai 2018)	2017	Capítulo de libro

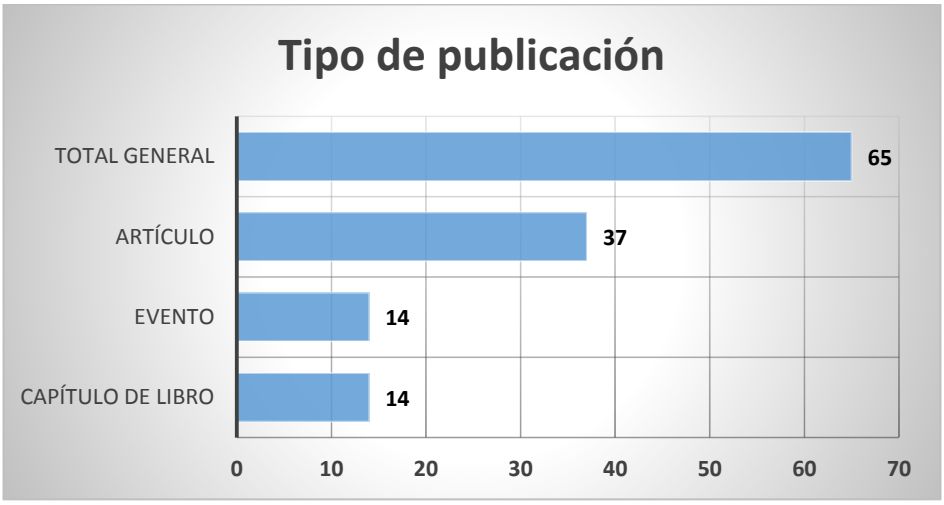
En la revisión se encontró que la distribución de los artículos se encuentra entre el siguiente rango de años:

Identificando al 2019 como el año que más se ha investigado, implementado e innovado con esta nueva tecnología.

La búsqueda de literatura se realizó a través de las siguientes Bases de datos:



Los artículos obtenidos fueron publicados en eventos, revistas y capítulos de libros.



Con respecto a las cuatro preguntas, se identificó lo siguiente:

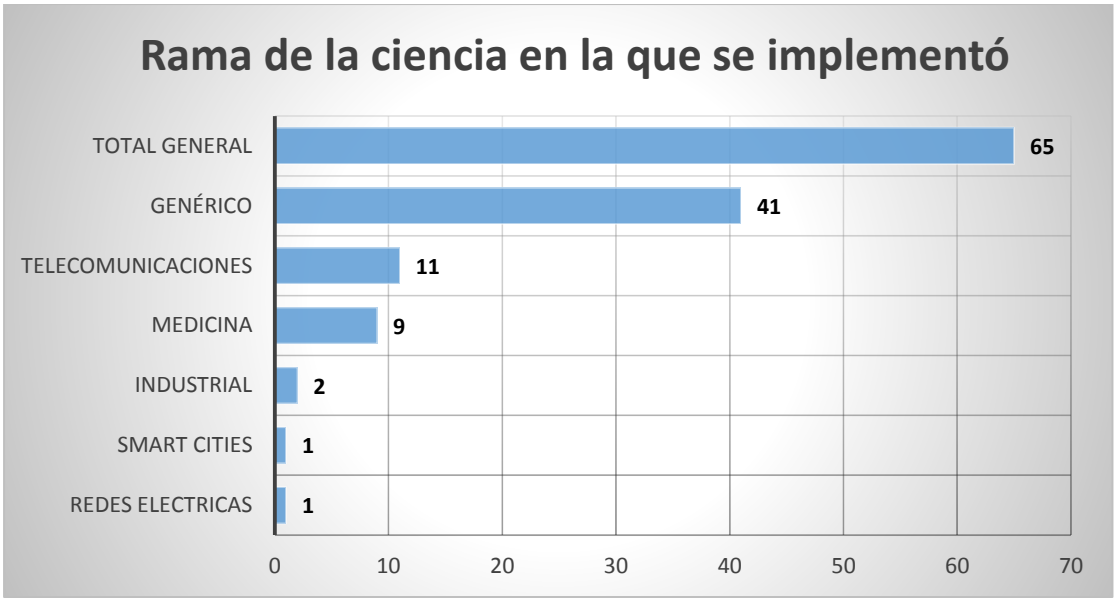
¿Se ha utilizado Middleware en esta implementación?

Se ha utilizado Middleware	No	Si	Total
	26	39	65

Se ha identificado que el número de artículos que utilizan, mencionan, implementan o proponen el uso del Middleware es de 39 mayor al número de los artículos que no lo utilizan, no obstante, esto no quiere decir que sea una tecnología ya desarrollada e implementada en su totalidad, un 80% fueron realizados en el 2018 – 2019 y solo están plasmados en el papel como propuesta, aún no tienen implementaciones o están iniciando esta etapa, por lo cual estos análisis son de suma importancia para continuar adquiriendo conocimiento el cual otorgue la efectividad necesaria al implementar el IoT. Adicionalmente permite tener un panorama más amplio de las falencias o puntos a mejorar que tiene dicha tecnología y como el Middleware puede dar un aporte importante a la solución de las mismas, lo anterior es el objetivo de este documento.

¿La implementación de IoT analizada fue utilizada en qué rama de la ciencia y/o la tecnología? (Movilidad y transporte, salud, telecomunicaciones, energía, monitoreo ambiental, entre otros)

La primera pregunta hace referencia a la rama de la ciencia en la que se ha implementado el Iot utilizando Middleware, siendo áreas genéricas multipropósitos las que mayor uso han tenido, posteriormente se encuentran las telecomunicaciones y la medicina.



¿Cómo influyen estas implementaciones de middleware para optimizar el IoT?

Revisando cada uno de los artículos que hacen alusión a la pregunta, se obtienen los siguientes hallazgos

#	Descripción
1	la IPV6 se implementa en nuevos dispositivos de redes de datos que permiten una conexión más optima entre los dispositivos de la red IoT, además este protocolo es aplicable en la mayoría de los métodos de conexión a la red.
2	Una arquitectura de middleware para dispositivos adaptativos, actuando como una capa de soporte entre el dispositivo basado en reglas subyacente y el mecanismo adaptativo. El middleware propuesto proporciona espontáneamente servicios de agregación y composición a ambos componentes, haciéndolos interoperables y funcionando como una sola unidad cohesiva. Una vez que el protocolo se establece correctamente, el middleware se vuelve transparente para el diseño adaptativo.
3	Se propone una arquitectura holística de IoT que consta de dispositivos heterogéneos, sistemas de Internet integrados (EIS), protocolos de comunicación estándar, y Paradigma SoA que utiliza el CoAP protocolo y servicios estándar, permitiendo el intercambio de datos del sensor con una nube basada en IoT y una nube privada, mientras difunde la interfaz web humano-máquina para la configuración, supervisión y visualización de datos de sensores estructurados.
4	La heterogeneidad puede ser vista desde los proveedores, lanzamientos y versiones, funcionalidad y complejidad, interfaces, compatibilidad y entre otros. Por lo tanto, la importancia del middleware no puede verse socavada ya que ayudan a integrar la heterogeneidad y facilitan la interoperabilidad. Además, la no

	estandarización de la arquitectura de IoT permite utilizar diferentes arquitecturas basadas en el dominio y la aplicación.
5	Dado que numerosas aplicaciones ya están utilizando algunas plataformas de IoT, la migración a un Esquema de identificación completamente nuevo podría ser difícil. Sin embargo, el objetivo de la interoperabilidad y el Inter funcionamiento se puede lograr proponiendo un mecanismo que actúa como middleware y proporciona una identificación unificada de los servicios de detección.
6	El middleware media la interacción entre las aplicaciones IoT y los dispositivos del mundo real, actuando como un software de adaptación de solicitudes para cada tipo de dispositivo. La idea básica del middleware es abstraer dispositivos en microservicios y, por lo tanto, proporcionar servicios más complejos a través de la composición de microservicios simples. En el caso de que los dispositivos IoT comprendan una red de sensores y actuadores, el consumidor de datos podría ser un software de middleware IoT que se conecta directamente al NFVI, sin la necesidad de administrar y controlar el acceso de los sensores a la red.
14	Con la llegada de la infraestructura 5G, las plataformas de middleware de IoT desempeñarán un papel crucial en la prestación de las abstracciones de dispositivos y los servicios de administración de datos necesarios. A medida que las redes de IoT comiencen a adoptar redes 5G, los desafíos de seguridad del middleware de IoT o de los capturadores de datos aumentarán drásticamente. Aunque las redes 5G proporcionarán un conocimiento rápido, confiable, de alto ancho de banda y de ubicación a ioTs, sigue habiendo muchas preocupaciones de seguridad sin abordar. Los autores destacan muchos posibles ataques contra las plataformas de middleware 5G IoT. Los ataques, como Man-in-The-Middle, modificación de mensajes, ataques de autenticación, ataques DoS, ataques de repetición, y el espionaje, será un desafío para el despliegue efectivo de la IoT en un 5G red.
20	IoT es un escenario en el que la mayoría de los dispositivos están restringidos por recursos, lo que significa que la inteligencia se delegará en una entidad más capaz. Esta entidad es un software identificado como middleware de IoT o plataforma de middleware de IoT
22	Se publicó una encuesta en la que los autores se referían a visiones abiertas en IoT, como el paradigma diferente, la naturaleza heterogénea de los objetos y las diversas arquitecturas. De un lado, analizaron la solución relacionada con la seguridad más aplicable (por ejemplo, integridad, confidencialidad, autenticación, control de acceso) en el entorno de IoT y por el otro lado emplearon la privacidad, y la confianza entre los usuarios y las cosas.
23	Se necesita una plataforma operativa común: middleware que es escalable y soporta un alto nivel de interoperabilidad. Esta plataforma permite a los datos del sensor de recolección, procesamiento y análisis. Las plataformas de middleware de IoT eficientes y ricas en características son factores clave para el paradigma de IoT. Actualmente estamos observando una tendencia emergente en las soluciones middleware que permiten IoT. Sin embargo, la mayoría de las soluciones están diseñadas y desarrolladas para su uso en los entornos de

	nube donde hay abundantes recursos disponibles. Creemos que las soluciones de middleware diseñadas específicamente para dispositivos de cálculo con recursos restringidos de baja potencia son fundamentales para lograr la visión de IoT. Creemos que una solución de middleware IoT ideal debe ser capaz de aprovechar y adaptarse a estos diferentes tipos de dispositivos con el fin de hacer la solución más eficiente y eficaz. El siguiente análisis breve ayuda a identificar esas debilidades, así como a identificar los requisitos de diseño ideales de un middleware de IoT que debe instalarse en dispositivos con recursos limitados. Aunque algunos de los componentes de hardware son de código abierto, los sistemas de software siguen siendo de código cerrado, lo que dificulta la ampliación e interoperación.
24	La pérdida de datos durante la transmisión hacia y desde el middleware sigue siendo propensa a ataques. Alshinina y Elleithy mostraron un estudio exhaustivo y sistemático de la investigación más reciente sobre el middleware de los WSN y compararon los diseños de sistemas eficientes existentes, abordaron los desafíos más significativos, hicieron varias contribuciones distinguidas, incluyendo seguridad, agregación de datos, intercambio de mensajes y calidad de servicio. Los autores concluyeron que el middleware tiene que ser escalable a recursos dinámicos y seguro al mismo tiempo. También se hipotetizó que la sincronización de nodos más recientes con los nodos existentes permitiría que el middleware funcionara de manera más eficiente mientras proporcionaba soporte a varios recursos. Recientemente, el middleware se ha integrado con WSN para abordar algunos de los desafíos antes mencionados. Alshinina y Elleithy revisaron y discutieron varios enfoques de middleware como SOMM, USEME, ESOA y MiSense. Es la primera vez que el algoritmo GANs se utiliza para resolver el problema de seguridad en el middleware de WSN. Además, en la contribución propuesta, el middleware de WSNs aplica un GAN que es capaz de ltear y detectar anomalías en los datos.
25	Este documento presenta un enfoque de middleware orientado a servicios para mitigar estos desafíos. Proponemos SmartCityWare, un SOM para integrar CoT y Fog Computing para apoyar el desarrollo y la ejecución de aplicaciones de ciudades inteligentes. Las tecnologías de middleware se han convertido en una parte necesaria de cualquier entorno distribuido. Middleware ofrece características y funcionalidades de habilitación esenciales para facilitar la integración de los componentes del entorno distribuido y las operaciones de todas las aplicaciones distribuidas y heterogéneas. Un enfoque nuevo y avanzado en tecnologías de middleware es el uso de middleware orientado a servicios (SOM). Se ha demostrado que este enfoque simplifica la implementación y las operaciones de muchas aplicaciones en diversos ámbitos industriales.

	SOM amplía las capacidades del middleware y proporciona una alta flexibilidad para agregar funciones nuevas y avanzadas a las aplicaciones de la ciudad inteligente.
27	Hay una necesidad de desarrollar un middleware como capa de software intermedia entre el lado del hardware y el de la aplicación. Con el fin de explotar eficientemente las capacidades de las tecnologías de comunicación actuales y proporcionar redes más flexibles, reconfigurables y eficientes, el modelo de middleware propuesto debe proporcionar compatibilidad de datos, gestión de ancho de banda, conectividad entre dispositivos heterogéneos y resolver problemas de seguridad. Esta arquitectura ayuda a centrarse en los problemas de presentación y aplicación, en lugar de en los problemas de los sistemas, por lo que se garantiza la interoperabilidad entre sistemas. Las herramientas y características de Java EE ayudan a crear aplicaciones que se estructuran en torno a módulos con diferentes propósitos.
29	Cada dominio de SDN tiene sus propias políticas de seguridad y estrategia de administración. Para resolver posibles problemas planteados por la heterogeneidad de las políticas de seguridad respectivas a los dominios SDN interconectados, utilizamos el concepto de cuadrícula de seguridad propuesto. La cuadrícula de seguridad es un middleware para la aplicación descentralizada de la seguridad de red.
30	La plataforma IoT es un motor de middleware en la nube computacional que administra el gran número de flujos de datos que provienen de diferentes sensores.
31	Capa de red: también se sabe que la capa de red es la capa de transmisión ". Esta capa garantiza la transferencia segura de la información recopilada de los sensores al sistema de procesamiento de información. Los medios de transmisión pueden ser cableados o inalámbricos y la tecnología puede ser 3G, UMTS, Wi-Fi, Bluetooth, infrarrojos, ZigBee, etc., según los sensores. Por lo tanto, la capa de red es responsable de transmitir la información de la capa del dispositivo a la capa de middleware.
33	La capa física representa los sensores que trabajan en el entorno. Las dos capas, abstracción de hardware y abstracción de vista, son middlewares de aplicaciones alojadas en el borde, cuyo objetivo es encapsular la complejidad del acceso y la configuración de los recursos físicos.
34	Actualmente, la plataforma se implementa junto con la plataforma de middleware in IoT de forma modular, es decir, puede funcionar conjuntamente o no con el middleware que solicita el cliente.
38	Se propuso una conciencia de contexto para el marco de IoT y se proporcionó un análisis en profundidad del ciclo de vida del contexto (técnicas, métodos, modelos, funcionalidades, sistemas, aplicaciones y soluciones de middleware) mediante el estudio de un conjunto de 50 proyectos durante la década entre 2001 y 2011.
40	Las tecnologías de middleware se han desarrollado para facilitar el desarrollo de aplicaciones mediante la integración de dispositivos heterogéneos de computación y comunicación, y admitiendo la interoperabilidad dentro de las diversas aplicaciones y servicios que se ejecutan en estos dispositivos. El IoT hace que las tareas de middleware sean aún más desafiantes, ya que los servicios ofrecidos por Things a menudo son dinámicos, móviles, menos confiables y dependen del dispositivo. Además de los componentes de la función, como el registro del servicio, el descubrimiento y la composición, un middleware de IoT también debe abordar requisitos no funcionales, que incluyen escalabilidad, oportunidad, confiabilidad, disponibilidad, seguridad, privacidad y facilidad de implementación. Además, un

	middleware IoT debe incluir características arquitectónicas para proporcionar abstracción de programación, interoperabilidad, adaptabilidad, conciencia de contexto, autonomía y distributividad. Todos los middlewares proporcionan un componente de descubrimiento semiautónomo y programamos las funciones para descubrir los servicios utilizando el componente proporcionado por cada middleware.
42	La arquitectura de la IoT empresarial consta de una capa de percepción, una capa de red, una capa de procesamiento, una capa de aplicación y una capa de gestión de servicios. Este documento presenta tres categorías de aplicaciones de IoT: IoT empresarial operativo, IoT empresarial analítico y IoT empresarial colaborativo.
43	Este documento explora el impacto de esta visión emergente de la atención médica y los requisitos que este modelo impone en la infraestructura de soporte. Comenzamos describiendo la evolución de la provisión de servicios de salud y los requisitos de los sistemas resultantes, antes de enfatizar la importancia de la política para permitir la gestión dinámica entre los componentes del sistema. Luego exploramos áreas de investigación de sistemas y consideramos su ajuste dentro de la visión más amplia de la atención médica. El middleware SBUS se presenta como prueba de concepto para ilustrar prácticamente los tipos de capacidades requeridas por la infraestructura de salud emergente. Luego se exploran los detalles de la aplicación de políticas, y concluimos con un resumen de los desafíos abiertos. La atención médica futura requiere un middleware genérico capaz de soportar tecnología actual y futura y los tipos de datos producidos. La atención médica futura requiere un middleware capaz de soportar una amplia variedad de patrones de comunicación. El middleware basado en eventos es el más apropiado.
47	Este problema de comunicación se puede resolver aplicando un estándar universal (que es difícil) o mediante un middleware. Un middleware es un software que proporciona interoperabilidad entre dispositivos y aplicaciones incompatibles. El middleware es una de las tecnologías que permite soluciones de IoT. Muchas organizaciones confían en soluciones de software integradas, incluso si tales soluciones son demasiado complejas para sus necesidades, debido al esfuerzo requerido para garantizar que las aplicaciones de diferentes proveedores puedan comunicarse con éxito. Las principales contribuciones de este documento se identifican de la siguiente manera: 1. La propuesta de métricas cualitativas y cuantitativas para evaluar objetivamente las soluciones de middleware IoT. 2. Un estudio de evaluación del desempeño (utilizando las métricas propuestas) de soluciones de middleware de código abierto, incluida una solución patentada desarrollada en Inatel para el escenario Inatel Smart Campus. El primer paso hacia la selección de una plataforma de middleware IoT es definir el escenario porque una parte considerable de las plataformas de middleware disponibles están construidas para escenarios específicos.
49	Hemos llevado a cabo un proyecto de desarrollo de middleware para promover juegos de movimiento saludables. Presentamos UKI, una aplicación de middleware que permite a los jugadores jugar cualquier

	juego existente utilizando movimientos corporales como entradas. Esta herramienta jugó un papel importante en varios estudios sobre promoción de la salud.
50	El middleware funciona como una capa de abstracción distribuida por software. Se encuentra entre la aplicación y las capas inferiores (sistema operativo, sistema operativo y capa de red).
51	En estos dos estudios, los desarrolladores implementaron cada protocolo por separado en una aplicación, lo que consume tiempo y dinero, mientras que es posible agregar todos estos protocolos en un middleware que se puede reutilizar y compartir con otros desarrolladores para fomentar la interoperabilidad. Además, como detallamos a continuación, la privacidad y la confiabilidad son muy importantes en la atención médica. A pesar de esto, pocos trabajos los tomaron en consideración. El middleware puede manejar datos en línea y en línea, cuando esta opción está disponible. De hecho, los usuarios pueden realizar mediciones sin tener sus sensores conectados a sus teléfonos inteligentes. Por ejemplo, algunos monitores de presión arterial pueden usarse sin teléfonos inteligentes, ya que la medida se muestra directamente en la pantalla del dispositivo. En este caso, las medidas se guardan en el dispositivo hasta que se sincroniza con el teléfono inteligente más adelante. El teléfono inteligente descarga estos datos del sensor para mantener un historial de las medidas del usuario o para el procesamiento. Por lo tanto, cualquier medida disponible guardada en el sensor se puede recuperar cuando el middleware está conectado a él.
52	En IoT basado en SDN, la arquitectura SDN sirve como un puente entre el escenario de comunicación IoT y el middleware. Los participantes de IoT pueden enviar paquetes directamente al conmutador habilitado para SDN en lugar de enviarlos a la puerta de enlace específica de IoT. Las reglas de control de acceso estático no son efectivas cuando los paquetes de ataque se disfrazan como varios flujos normales. Recientemente, el poderoso middleware de seguridad de IoT se considera una forma prometedora de manejar los flujos sospechosos. Sin embargo, debido a su ubicación física y la ausencia de una interfaz unificada, es difícil para el middleware de seguridad interceptar activamente los flujos de ataque en su interruptor de acceso.
53	Se conocen como tecnologías de mejora de la privacidad (PET). Un ejemplo de estos PET, que se mencionarán durante este documento, es un middleware de privacidad holística que ejecuta la formación topológica para la recopilación de datos junto con un proceso de ocultación en dos etapas que tiene como objetivo controlar la cantidad de información que los usuarios finales revelar en el contacto inicial, elimina la necesidad de liberar datos de salud personales en la forma sin procesar, y permite a los usuarios finales actuar de forma anónima.
55	El problema de la heterogeneidad entre los almacenes de datos NoSQL ha sido reconocido tanto por la industria como por la comunidad de investigación, lo que ha dado lugar a una serie de plataformas de middleware de acceso a datos para sistemas NoSQL. Estas plataformas de middleware de acceso a datos proporcionan una API uniforme para las soluciones NoSQL (muchas de ellas basadas o inspiradas en la API de persistencia de Java (JPA)) y este middleware proporciona la traducción de esta API uniforme en las API de cliente nativo.

56	La arquitectura propuesta tiene tres capas (infraestructura de IoT, middleware de IoT y servicios de IoT) que abordan funciones específicas para hacer posible el soporte del paradigma de la ciudad inteligente mediante IoT, cloud y cloudlets. Debido a la gran cantidad de tecnologías normalmente implementadas dentro de un escenario de IoT, se hace necesario tener una capa para ofrecer una integración perfecta de dispositivos y datos que construyan el IoT, el middleware de IoT. Administrador de heterogeneidad: dado que los dispositivos implementados en la infraestructura de IoT tienen una naturaleza heterogénea, es necesario tener un lenguaje estándar para alcanzar una comunicación agnóstica entre la infraestructura de IoT y las capas superiores. Heterogeneity Manager funciona como un intérprete entre los componentes de IoT ubicados en la nube y las islas IoT.
57	Existe la necesidad de un middleware sensible al contexto que se considere el requisito principal para desarrollar las aplicaciones sensibles al contexto para recopilar y analizar los cambios contextuales de manera eficiente. Context-Aware Middleware se define como un sistema de software que proporciona una capa abstracta entre las aplicaciones sensibles al contexto y los sistemas operativos. Las revisiones de la literatura sobre el middleware sensible al contexto mostraron que desarrollar e implementar un middleware sensible al contexto es un desafío debido a las características particulares de los dispositivos y contextos, como los recursos limitados de los dispositivos inteligentes y la naturaleza dinámica de los contextos.
58	El middleware COSMOS proporciona funciones generales requeridas para varios servicios y aplicaciones. En esta arquitectura de middleware, es muy adecuado colocar una plataforma de aplicación general entre las redes de cosas IoT heterogéneas, diversos servicios y aplicaciones.
59	El núcleo de la plataforma IoT propuesta se basa en el middleware abierto para Internet de las cosas (OpenIoT). Esta es una plataforma de integración de datos IoT basada en la nube distribuida que utiliza la ontología SSN.
60	Los dispositivos y los usuarios están conectados por una infraestructura de middleware, que se llama plataforma IoT. Apoyando la privacidad y seguridad de datos, compartiendo dispositivos heterogéneos y apoyando la Aplicación La interfaz de programación (API) son las características principales de la plataforma IoT.
61	Se presenta un marco para un banco de pruebas IoT sobre una red IMS para mejorar QoS y SLA en aplicaciones de ecosistemas. Teniendo en cuenta los parámetros únicos de QoS de IoT, que enfatizan la precisión y la exactitud de los datos, este marco proporciona un esquema basado en agentes para administrar los datos del ecosistema de acuerdo con los comportamientos de la capa de red.
62	IoT necesita tecnología de identificación, tecnología de detección, tecnología de comunicación y tecnología de middleware como tecnologías habilitadoras clave. La tecnología de identificación y detección está involucrada en la visión orientada a las cosas, la tecnología de comunicación se utiliza para la visión orientada a Internet y la tecnología de middleware es para la visión semántica. Lograr la integración de la gestión y el control basado en el middleware IoT se ha vuelto cada vez más

	significativo. Cada comando, propiedad de recurso y evento de producción se pueden combinar con una serie de direcciones de control físico que son supervisadas y moderadas por controladores inteligentes (por ejemplo, computadora de control industrial, PLC). El middleware IoT es una solución flexible y escalable para conectar, administrar, monitorear y controlar dispositivos heterogéneos y aplicaciones de software.
63	Dado su papel como integrador universal de elementos computacionales distribuidos, el middleware desempeña un papel clave en el apoyo al desarrollo de tales aplicaciones y servicios mejorados de IoT. Sin embargo, IoT presenta nuevos desafíos importantes para el middleware derivado de la gran cantidad de objetos conectados, el volumen y la riqueza de los datos producidos, los ricos patrones de comunicación requeridos, la heterogeneidad de los componentes de comunicación y los nuevos desafíos en términos de calidad de servicio, privacidad y seguridad. Esos desafíos deben ser abordados por investigadores y profesionales de la comunidad de middleware antes de que la sociedad pueda beneficiarse plenamente de este potencial.
64	Middleware no es una pieza específica de software, sino una serie de software que proporciona servicios básicos entre el sistema operativo y el sistema de aplicación. La intención original del middleware es proteger varios detalles técnicos complejos, simplificar problemas técnicos y reducir la complejidad de la programación. El middleware diseñado en este documento está entre el dispositivo sensor y el sistema de servicio de la capa superior. Adopta el diseño de la arquitectura SOA y tiene las características de granularidad gruesa y acoplamiento flojo, que satisface los requisitos de los dispositivos de acceso múltiple de Internet de las cosas y admite múltiples aplicaciones.
65	A medida que Internet de las cosas está creciendo rápidamente, se requiere un middleware para soportar y permitir que los consumidores de IoT y los desarrolladores de aplicaciones de IoT interactúen. Boman y col. propuso un middleware flexible que combina el uso de Global Sensor Network (GSN) (un middleware IoT de código abierto existente), Firebase (un servicio de almacenamiento en la nube) y un intérprete de datos IoT. Este sistema de software recientemente desarrollado da pasos hacia el middleware ubicuo para IoT. En este trabajo, consideraremos los dispositivos en lugar de los usuarios, ya que el primero tiene atributos únicos para la anotación. Tanto el middleware como la base de datos están alojados como servicios en la nube. Se propone un middleware alojado en la nube con el objetivo principal de facilitar las comunicaciones de máquina a infraestructura (M2I).

¿Cuáles fueron los resultados obtenidos que demuestran la efectividad del middleware para optimizar el IoT?

#	Descripción

1	Mayores tasas de transferencia entre dispositivos, incremento en la seguridad de la información que se transmite, una mayor cantidad de dispositivos finales e intermedios conectados a la red.
2	Una arquitectura de middleware para dispositivos adaptables, actuando como una capa de soporte entre el dispositivo basado en reglas subyacente y el mecanismo adaptativo, como un medio para abordar la heterogeneidad y la exposición de los componentes. Uno de los diseños de middleware presentado se puede mejorar aún más para cubrir un número más amplio de dominios y escenarios. Los resultados preliminares parecen prometedores, aunque hay desafíos con respecto a la interoperabilidad tolerante a errores.
20	Estas plataformas, tanto de código abierto, como propietarias se ocupan de abordar los problemas de heterogeneidad relacionados con la nube y el IoT mediante la implementación de dos middlewares, uno en el lado de la nube y el otro en el lado de las cosas, así como proporcionando una API para interacción de las aplicaciones encargadas de monitorear a los pacientes y sus constantes vitales.
27	Nuestra arquitectura de middleware es un servicio orientado basado en la API REST, que permite admitir varios objetos inteligentes utilizando diferentes interfaces de red (IP y NO basadas en IP) y sistemas operativos, así como unificar varios formatos de datos que se utilizan para proporcionar la información necesaria para el usuario final que trabaja en diferentes plataformas. La arquitectura de middleware orientada a servicios (SOM) es la mejor plataforma para desarrollar aplicaciones de IoT para abordar desafíos de hardware como QoS, seguridad y heterogeneidad.
43	El middleware proporciona una capa de abstracción que media entre las aplicaciones y las infraestructuras de red. A menudo descrito como pegamento de sistemas, el middleware es crucial para respaldar esta emergente atención médica porque el middleware opera en todos los sistemas, para ayudar a la comunicación y la gestión. Los desafíos de la atención médica generalizada significan que el middleware, además de su función tradicional de permitir la interoperabilidad, debe ser más activo en el control de los sistemas y en la interacción entre ellos, cuando y donde sea apropiado, para cumplir con los objetivos definidos por el usuario. Gran parte de la responsabilidad de gestionar estas preocupaciones recae en el middleware. Al mediar las comunicaciones entre los componentes del sistema, el middleware los "pega" entre sí. En la actualidad, la mayoría del middleware se enfoca en habilitar la comunicación a pedido de las aplicaciones. De hecho, el middleware resume varios detalles de comunicación, pero típicamente, las aplicaciones aún controlan cómo y cuándo se conectan e interactúan con sus pares, corredores o servicios. En esta sección, mostramos cómo el entorno de atención emergente extiende esta función tradicional de middleware para incluir la composición dinámica de los sistemas para admitir los requisitos en tiempo real. Nuestro trabajo en la infraestructura de middleware SBUS y los motores de políticas demuestran la

	viabilidad de este enfoque de sistemas abiertos. Esto va más allá de proporcionar "pegamento de nivel de sistema" para impulsar activamente nuevas posibilidades funcionales a través de preferencias de alto nivel especificadas por el usuario, lo que hace que la visión de la atención médica generalizada, preventiva y personalizada sea una posibilidad real.
6	Las aplicaciones, a su vez, utilizan los servicios proporcionados y administrados por el middleware para recopilar datos y actuar en dispositivos en diferentes contextos. Las aplicaciones virtuales se ejecutan en una infraestructura virtual, generalmente alojada en entornos de procesamiento de datos y computación en la nube. En este contexto, La computación en la nube es una tecnología habilitadora para Internet de las cosas, ya que permite el procesamiento oportuno de los datos capturados por los dispositivos IoT. Las aplicaciones de IoT se implementaron como una composición de microservicios proporcionados por el middleware, que interactúa con las aplicaciones y los dispositivos de bajo nivel. Sin embargo, en este punto de vista, la arquitectura IoT oculta las especificidades del servicio de red requeridas para cada tipo de aplicación en una sola infraestructura. Por lo tanto, las aplicaciones en tiempo real, como las aplicaciones industriales inteligentes, dependen del mismo servicio de transporte que las aplicaciones con requisitos de latencia menos estrictos, pero sensibles a la privacidad de los datos, como los dispositivos de detección de la casa.
3	Se ha propuesto un vínculo común entre el SoA y un middleware con un enfoque arquitectónico integrado, aprovechando las ventajas del SoA a través de la mejora de la funcionalidad del dispositivo, las comunicaciones y los servicios integrados. Una arquitectura de Middleware de IoT en capas basada en SoA donde los objetos se encuentran en la parte inferior y la abstracción de objetos, la administración de servicios (proporciona servicios como: detección dinámica, supervisión de estado y configuración de servicio de los objetos. Una infraestructura domótica basada en IoT orientada a SoA, se desarrolla en la literatura donde se ha implicado la lógica de consumo de energía automática basada en sensores y actuadores.
4	La seguridad es la principal amenaza en cualquier aplicación de red existen diferentes estudios exhaustivos de los problemas de seguridad en los diferentes niveles de los sistemas IoT y han dado una visión del estado actual del arte de las publicaciones que abordan las cuestiones de seguridad en dicha tecnología. Según los autores, la confidencialidad, la integridad y la disponibilidad son las preocupaciones principales de IoT esto se resume en la seguridad de los datos. Las tecnologías de comunicación que vinculan internet de las cosas deben ser capaces de proporcionar eficiencia de seguridad. Principales problemas de seguridad en las distintas capas operativas como, transporte, enrutamiento y aplicación. Otro problema principal debe analizar el efecto computacional de la Criptografía de la Curva Elíptica en los dispositivos de detección.
5	En este documento, hemos proporcionado un estudio inicial sobre los identificadores y la necesidad de un Esquema de identificación común para lograr la interoperabilidad entre varios estándares y plataformas de IoT.

	En cuanto al trabajo futuro, tenemos la intención de proporcionar una revisión sistemática en profundidad de las principales plataformas de IoT. A continuación, definiremos un mecanismo a través del cual los dispositivos de diferentes plataformas de IoT puedan descubrir e interactuar entre sí. El mecanismo unificado ayudará a lograr la interoperabilidad global entre aplicaciones y dispositivos de diferentes estándares y plataformas de la industria de La IoT.
14	Este artículo propone una metodología para esta nueva tecnología de conexión aplicada al IoT, pero aún no hay resultados ya que 5G como tal se encuentra en desarrollo, aún está en fase de pruebas y estabilización, por lo que no es posible incursionar en su uso para la IoT hasta que no esté funcional.
22	Presentamos los detalles de diseño e implementación de nuestra solución de middleware propuesta, Mobile Sensor Data Processing Engine (MOSDEN). MOSDEN está diseñado para apoyar la detección como un modelo de servicio de forma nativa. Además, MOSDEN es un
23	Presentamos los detalles de diseño e implementación de nuestra solución de middleware propuesta, Mobile Sensor Data Processing Engine (MOSDEN). MOSDEN está diseñado para apoyar la detección como un modelo de servicio de forma nativa. Además, MOSDEN es un verdadero middleware de programación cero donde los usuarios no necesitan escribir código de programa o cualquier otra especificación utilizando lenguajes declarativos. Nuestra solución también es compatible con el mecanismo de transmisión de datos push y pull, así como la comunicación de datos centralizada y descentralizada (por ejemplo, peer-to-peer). MOSDEN realiza el procesamiento de datos y el análisis antes de transmitirlos a través de una red. Más importante aún, nuestra plataforma de middleware propuesta se puede instalar en dispositivos que pertenecen a categorías de nivel inferior que tienen limitaciones de recursos similares a los teléfonos móviles o Raspberry Pi2. Cloud IoT middleware mantiene un registro de sensores que incluye sus disponibilidades y capacidades. El middleware de Cloud IoT recupera esta información a través de varias instancias MOSDEN. Una vez que el middleware Cloud IoT recibe una solicitud de un consumidor, busca los sensores necesarios y compone una consulta de solicitud. A continuación, registra la solicitud con la instancia MOSDEN conectada al sensor. Entonces, MOSDEN envía datos al middleware de Cloud IoT hasta que expire la solicitud. Lo que es más importante, MOSDEN realiza el procesamiento de datos antes de enviar los datos al servidor. Por ejemplo, en lugar de enviar datos cada 2 segundos, MOSDEN puede procesar localmente, almacenar los datos y enviar los datos a la nube una vez al minuto promediando los valores.
24	La investigación anterior ha demostrado que el uso del middleware como capa intermedia entre los WSN y el usuario final proporciona una solución a las limitaciones mencionadas anteriormente. El middleware proporciona una plataforma de puente entre las aplicaciones y los componentes de hardware de WSN. El middleware controla los nodos de datos del sensor mientras les proporciona almacenamiento temporal.

	The ability to synchronize newer nodes with the existing nodes allows the middleware to be more efficient while providing support to various resources. This allows minimum or no disturbance in the network's performance if changes occur to the network. La mayoría de los enfoques de middleware carecen del mecanismo de seguridad para proteger la red y los datos confidenciales de ataques malintencionados. Mientras que los sistemas de middleware se desarrollan principalmente para WSN, diferentes agentes lo utilizan para varias aplicaciones para detectar cualquier intrusión utilizando el modelo de agente. También se han introducido sistemas de middleware para aplicar algoritmos de aprendizaje automático (ML). Introducimos un sistema de seguridad inteligente para el middleware de WSN basado en GAL para mejorar el middleware tradicional en términos de mecanismo de seguridad, manejo de características heterogéneas de los nodos de sensores, y para filtrar y pasar sólo los datos reales.
29	Cada dominio de SDN tiene sus propias políticas de seguridad y estrategia de administración. Para resolver posibles problemas planteados por la heterogeneidad de las políticas de seguridad respectivas a los dominios SDN interconectados, utilizamos el concepto de cuadrícula de seguridad propuesto. La cuadrícula de seguridad es un middleware para la aplicación descentralizada de la seguridad de red.
25	Implica el desarrollo y la ejecución de aplicaciones distribuidas y oculta su complejidad. También proporciona servicios comunes para desafíos recurrentes en el entorno distribuido. Middleware también conecta cualquier conjunto de componentes en un entorno distribuido para proporcionar mejores funcionalidades. Estos componentes podrían ser dispositivos de hardware tales como sensores, actuadores, robots, UAVs, dispositivos de comunicación, microcontroladores, servidores en la nube; o componentes de software, incluidos módulos de control, aplicaciones de supervisión, servicios de análisis y módulos de software específicos de aplicaciones. En consecuencia, anticipamos una migración exitosa del modelo SOM para utilizar el concepto de IoT para admitir aplicaciones de ciudades inteligentes y proporcionar una plataforma de middleware genérica que aumentará la productividad y ampliará la gama de aplicaciones.
31	Capa de middleware: cada objeto inteligente se comunica con otros dispositivos solo si implementan el mismo tipo de servicio. Toma los datos de la capa de red y los almacena en la base de datos. Procesa información y decide la solución analizando los resultados. Capa de aplicación: esta capa es responsable de administrar la aplicación de forma global según el procesamiento de la información de los objetos en la capa de Middleware. Las diversas aplicaciones de IoT son salud inteligente, agricultura inteligente, hogar inteligente, ciudad inteligente, transporte inteligente, etc.

33	Este trabajo resumió la complejidad del acceso a los recursos de IoT y la configuración a una capa de computación de borde que se administra a través del protocolo CoAP. Nuestro recurso virtual funcionó de la manera esperada, respondiendo a todas las solicitudes sin importar el nivel de concurrencia que enfrentaron. La capa de recursos virtuales podría interactuar entre cada componente compuesto tan fácil como consumir un servicio RESTfull, en este caso un servicio RESTfull CoAP. La arquitectura propuesta constituye una solución económica ya que la evaluación de los datos se realiza en la red periférica de IoT y solo se transfiere información útil a la nube.
34	Esta característica podría usarse o no en la plataforma, debido a que el acceso de usuario de control se proporciona al middleware en IoT cuando está integrado. El prototipo realiza la comunicación entre componentes a través de protocolos de gestión. Por lo tanto, los sensores generan información como nuevas entradas en la base de datos, y la plataforma puede realizar consultas de datos a los datos insertados. Este documento presentó una descripción general de los protocolos y enfoques utilizados para dispositivos IoT y gestión de redes donde se identificaron sus motivaciones y desafíos técnicos. Se presentó un análisis comparativo de los enfoques estudiados para elegir las mejores tecnologías utilizadas para una nueva plataforma de gestión de red IoT.
30	Esta capa puede tener una subdivisión interna a la capa de soporte de aplicación que suele ser más general, incluido el middleware, máquina a máquina se puede organizar de diferentes maneras según diferentes servicios. Por lo general, incluye middleware, plataformas, como la informática en la nube y el soporte de servicios, etc. Dado que esperamos big data, el middleware aborda la escalabilidad y la elasticidad de los servicios. Lo más probable es que la capa de aplicación implique la integración de la lógica de negocios o del sistema de alto nivel. Se ocupa de la protección de la privacidad con huellas dactilares, marca de agua, etc.
38	Según su taxonomía, propusieron una serie de posibles direcciones de investigación basadas en problemas emergentes de IoT. En esta encuesta, los autores sugirieron que los problemas de seguridad y privacidad se aborden en el nivel de middleware y en varias capas del modelo (hardware del sensor, comunicación de datos del sensor, anotación de contexto y descubrimiento de contexto, modelado de contexto y capas de distribución de contexto) en orden para ganar la confianza de los usuarios de IoT. Esta iniciativa tiene como objetivo desarrollar un ecosistema de hogar inteligente y publicar requisitos y planes de prueba para puertas de enlace domésticas y redes domésticas inalámbricas / alámbricas. Mejora las aplicaciones y facilita las conexiones de middleware de puerta de enlace doméstica y dispositivos de comunicación. La HGI emitió requisitos técnicos para dispositivos y servicios en el hogar inteligente, incluidas puertas de enlace y redes.
42	La capa de procesamiento, también llamada capa de middleware, limpia, almacena, analiza y procesa los datos que se transportan desde la capa de red. La capa de procesamiento contiene plataformas como la gestión de bases de datos, análisis de datos y computación en la nube. Debido a la gran cantidad de datos generados por los dispositivos IoT, muchas aplicaciones de IoT requieren un almacenamiento masivo de datos, enormes velocidades de procesamiento para permitir la toma de decisiones en tiempo real y redes de banda ancha de alta velocidad para transmitir datos, audio o video. La computación en la nube se

	convirtió en una tecnología adecuada para manejar grandes flujos de datos y procesarlos para la gran cantidad de dispositivos IoT en tiempo real. Una infraestructura distribuida compleja de IoT requiere simplificar el desarrollo de nuevas aplicaciones y soluciones. La capa de procesamiento puede ocultar los detalles de las plataformas y es ideal para el desarrollo de aplicaciones IoT.
40	Registramos el tiempo para realizar el registro del servicio en cada middleware: 2 h para UBIWARE, 1 h para LinkSmart, 3 h para OpenIoT y 2 h para CHOReOS. En UBIWARE, el tiempo registrado incluye el desarrollo de los controladores para diferentes agentes y la lógica de negocios de la comunicación entre los agentes del escenario y el agente UDF. En LinkSmart, contamos el tiempo de implementación de la funcionalidad necesaria para usar la capacidad de registro proporcionada por el administrador de la red. En OpenIoT, el tiempo de implementación de los conectores requeridos se incluyó en la medición. Se implementaron envoltorios personalizados para conectar los servicios al middleware para cada servicio. CHOReOS tuvo el mejor rendimiento con una mediana de 1 milisegundo en 1000 ejecuciones, seguido de OpenIoT, UBIWARE y LinkSmart con medianas de 34, 68 y 240 milisegundos, respectivamente. CHOReOS funciona bien porque no utiliza almacenamiento persistente de descripciones de servicio. Estas descripciones se almacenan en la memoria y dejará de estar disponible después de reiniciar el middleware.
47	Existen muchas soluciones de middleware, tanto de código abierto como patentadas, ofrecidas por compañías de tecnología, todas muy similares entre sí con respecto a las características proporcionadas; y no se definen métricas de rendimiento, ni siquiera pautas para comparar objetivamente este tipo de software en la literatura. Con esto en mente, el documento propone métricas tanto cualitativas como cuantitativas. Luego, el rendimiento de las soluciones de middleware se evalúa utilizando las métricas propuestas. Es necesario eliminar espacios en blanco antes de enviar datos al middleware, y se debe evaluar la precisión de los datos: la mayoría de las comunicaciones REST se envían sin eliminar espacios en blanco, y cada espacio en blanco adicional se cuenta para la cantidad de bytes enviados. Las personas que implementan soluciones de IoT deben administrar cuidadosamente los datos enviados por sus dispositivos porque a medida que aumenta el número de usuarios simultáneos, los espacios en blanco adicionales comienzan a acumularse. El primer paso es recortar los espacios en blanco de antemano. Las personas que implementan soluciones de IoT deben administrar cuidadosamente los datos enviados por sus dispositivos porque a medida que aumenta el número de usuarios simultáneos, los espacios en blanco adicionales comienzan a acumularse. El primer paso es recortar los espacios en blanco de antemano. El segundo es planificar la precisión de los datos enviados de acuerdo con el escenario. Por ejemplo, si un dispositivo mide la temperatura, el usuario debe definir si le importa al escenario que la temperatura enviada al middleware sea 7.5 en lugar de 7.533323222.
49	UKI un middleware que permite a sus usuarios jugar cualquier juego existente mediante el uso de un conjunto de movimientos que pueden configurar libremente. Esta herramienta propuesta se puede utilizar para evaluar y optimizar el diseño de juegos de movimiento o una lista de movimientos utilizados en el juego.

	Recientemente, propusimos una idea de Asistente Inteligente (IA) en UKI. Los roles de IA incluyen proporcionar instrucciones a los jugadores sobre el entrenamiento previo al juego y alentarlos a usar sus cuerpos de manera saludable durante el juego. Al igual que con UKI, IA tiene como objetivo ser universal para cualquier juego.
50	El software desarrollado en la capa de middleware proporciona una interfaz de programación de aplicaciones (API). La API oculta la complejidad del problema de comunicación general. También oculta la programación de bajo nivel correspondiente al acceso directo por medio del software propietario. ULC (User Links Constructor) proporciona la API correspondiente a la capa de middleware. El navegador accede a esta API a través de un canal WebSocket, a través del cual el usuario envía los comandos codificados en notación de objetos JavaScript (JSON). En resumen, ULC es el enlace entre la computadora del usuario, su navegador, el software propietario y la nube donde se puede acceder al controlador.
51	Para fomentar la interoperabilidad en los sistemas de salud, proponemos un middleware, en forma de una biblioteca de software, capaz de comunicarse con un conjunto de sensores, utilizando protocolos estándar y patentados, con el objetivo de acceder a cualquier información. Este middleware está destinado a ser utilizado por desarrolladores de terceros, aplicaciones de servicios de salud o proveedores para recuperar los datos de los pacientes, lo que les permite garantizar la interoperabilidad con un número máximo de sensores de salud con un mínimo esfuerzo. Al utilizar dicha biblioteca, los desarrolladores no necesitan implementar cada protocolo de forma independiente y pueden centrarse en el análisis y procesamiento de datos. Ramírez-Ramírez et al. developed a hardware middleware device that handles data from a sensor and sends them to the cloud. The sensor is a prototype that measures body temperature and integrates a fall detector, and uses ISO/IEEE 11073 to communicate. Once retrieved by the middleware, these data are then transmitted to a remote server using HL7 protocol. Gracias a la pequeña cantidad de sensores implementados, el middleware recupera los datos solicitados rápidamente. Sin embargo, con el número cada vez mayor de dispositivos compatibles, el tiempo de búsqueda para encontrar el sensor apropiado podría volverse significativo. Por esta razón, implementamos la función de caché. Los sensores usados se almacenan en la memoria del middleware y se pueden reutilizar ahorrando tiempo de búsqueda.
52	Según los resultados del monitoreo, SSM primero redirige los flujos sospechosos al middleware de seguridad en el IoT, luego percibe los resultados de filtrado del middleware de seguridad. En base a eso, SSM asigna las reglas de control de acceso para interceptar los fl ujos de ataque en su interruptor de acceso en IoT basado en SDN. Proponemos un mecanismo de seguridad inteligente (SSM) para monitorear y mitigar el ataque de nuevo flujo utilizando las interfaces estándar hacia el sur y hacia el norte. SSM logra un monitoreo de bajo costo y hace que el controlador SDN sea consciente de los resultados de filtrado del middleware de seguridad en IoT basado en SDN. Redirigimos los flujos sospechosos desde el puerto de la víctima al middleware de seguridad, que puede

	filtrar los flujos de ataque. Luego, percibimos el comportamiento del middleware de seguridad analizando las tablas de flujo en sus conmutadores conectados directamente. Finalmente, el comportamiento percibido puede asignarse como las reglas de control de acceso dinámico a los interruptores de la víctima.
53	Este documento presenta middleware de privacidad holística para servicios de atención médica basados en IoHT que utilizan nodos de niebla (puertas de enlace personales) como puntos de aplicación de la privacidad. Estos nodos de niebla hospedarán el middleware de privacidad holística propuesto y los perfiles de estado del usuario. Los datos de salud del usuario pueden mantenerse privados de su lado o liberarse en forma oculta. Además, el middleware holístico propuesto que tiene en cuenta la formación topológica de dispositivos IoHT al recopilar los datos de estado de los usuarios para estos servicios. Este middleware holístico se puede utilizar para servicios de atención médica basados en la nube para facilitar el acceso a una gran cantidad de datos de salud de los usuarios de una manera que preserva la privacidad.
55	Aunque estas plataformas de middleware son relativamente nuevas y evolucionan a diario, de hecho, proporcionan una alternativa prometedora para las organizaciones que están interesadas en los beneficios de los almacenes de datos NoSQL. Hemos realizado un estudio en profundidad de la compensación entre la sobrecarga de rendimiento y el costo de la migración, inherente a la decisión de usar plataformas de middleware de acceso a datos. Presentamos dos estudios complementarios en los que comparamos tres plataformas de middleware de acceso a datos basadas en Java para sistemas NoSQL: Impetus Kundera, Playorm y Spring Data. Estas plataformas son inevitables para lograr portabilidad, interoperabilidad y fácil migración a través de los sistemas de almacenamiento NoSQL. Debido a la heterogeneidad y la creciente popularidad de los almacenes de datos NoSQL, creemos que dicha plataforma de middleware será cada vez más útil en el futuro cercano.
56	Para alcanzar la ubicuidad y una mayor flexibilidad de los componentes que dan forma a la arquitectura; el middleware IoT y las capas de servicios IoT residen en el entorno de la nube. Además, la arquitectura permite el despliegue y la virtualización de componentes cruciales en el borde de la nube o cloudlet (es decir, IoTGateways y servicios de IoT) logrando así una reducción de latencia que es importante particularmente para aplicaciones críticas y en tiempo real. Esta capa abarca funcionalidades comunes y mecanismos de abstracción que envuelven los detalles de la infraestructura de IoT para desarrolladores y usuarios, con el fin de lograr una interacción más fácil entre estos actores. Los proyectos de investigación como LinkSmart y OpenIoT proporcionaron contribuciones importantes a esta capa de integración; sin embargo, con respecto a los mecanismos de resiliencia necesarios en la infraestructura, todavía hay espacio para mejoras significativas. Con esto en mente, proponemos una capa de middleware de IoT centrada en la mejora de la capacidad de recuperación de IoT. A continuación, se presenta una discusión de los módulos de esta capa.

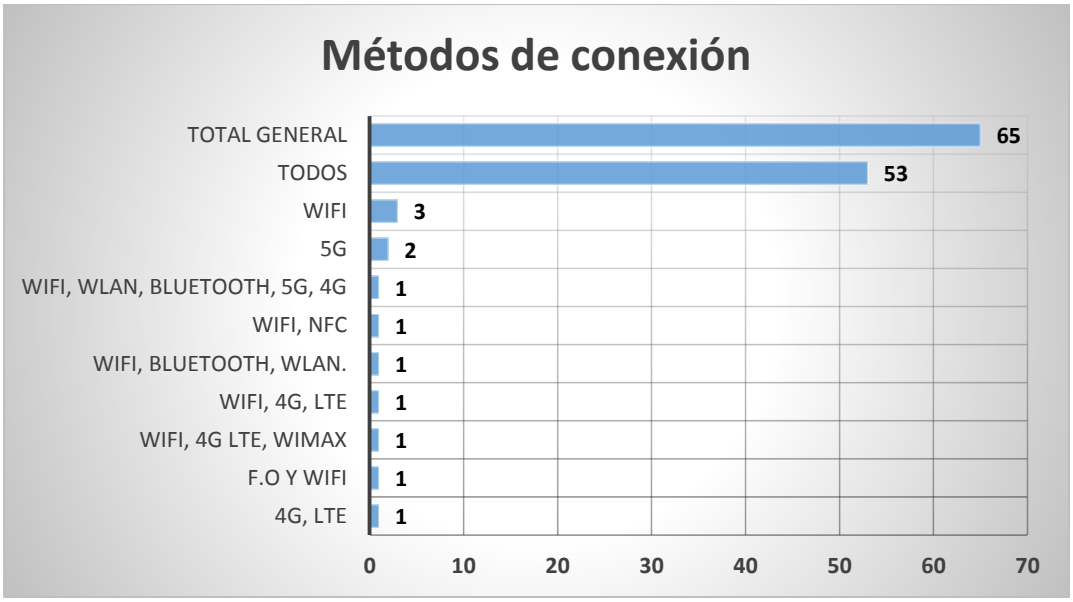
	La interacción entre los componentes del middleware IoT combinada con las tecnologías adecuadas permite cumplir con un proceso de comunicación eficiente entre los objetos inteligentes y los usuarios finales. En particular, la arquitectura propuesta se diseñó teniendo en cuenta el escenario del proyecto SusCity y los requisitos necesarios para su plataforma de comunicación.
57	El middleware sensible al contexto en el hogar inteligente permite que una puerta de enlace doméstica recopile datos y aprenda el comportamiento del usuario, que son cambios de contexto de los dispositivos inteligentes, y luego los basa en que puede realizar acciones y tomar decisiones. Se han realizado varios estudios y soluciones sugeridas para lograr middleware sensible al contexto en hogares inteligentes. Las soluciones ayudan a construir middleware consciente del contexto que tiene grandes beneficios para reducir el tiempo de desarrollo de aplicaciones contextuales y simplificar el comportamiento complejo de ellas. El middleware sensible al contexto puede ayudar a los desarrolladores a centrarse en el desarrollo de aplicaciones sin preocuparse por la gestión del contexto relacionado con las aplicaciones. La solución de Middleware consciente del contexto puede admitir estilo arquitectónico, gestión de servicios, adquisición / descubrimiento de contexto, razonamiento de contexto, abstracción de contexto, agregación de contexto, seguridad y privacidad, reutilización, difusión de contexto, evaluación de calidad de contexto, escalabilidad y tolerancia a fallas;
58	En este documento, propusimos una plataforma de convergencia adaptativa de IoT y WoT en servicios y aplicaciones de IoT que puede realizar una combinación de varias cosas y una operación eficiente en entornos de IoT y WoT. El propósito de este documento fue proponer la plataforma de convergencia adaptativa IoT y WoT que permite que las cosas implementen dinámicamente la web inteligente sin ningún control por parte de los usuarios. La plataforma de convergencia adaptativa IoT y WoT, propuesta en este documento, es un nuevo tipo de plataforma que proporciona interoperabilidad y compatibilidad global para ayudar a los usuarios a comunicarse fácilmente con todas las cosas mediante la conexión a través de las redes.
59	OpenIoT proporciona servicios de infraestructura para capturar datos de IoT desde cualquier dispositivo de IoT, anotando semánticamente dichos datos utilizando SSN, vinculando dinámicamente los datos de IoT utilizando datos vinculados y ofrece herramientas visuales para el descubrimiento y exploración de sensores / datos de IoT. Actualmente está disponible como un proyecto de código abierto en https://github.com/OpenIotOrg/openiot/.
60	El IoT incluye los sensores y actuadores físicos, que se refieren a la capa de percepción. Los datos producidos en esta capa se pasan a la capa de middleware por una capa de red. Los canales seguros para mover datos utilizan algunas tecnologías como RFID, Wireless Sensor Network (WSN), Wi-Fi, Interoperabilidad mundial para acceso de microondas (WiMAX) y Long Term Evolution (LTE). Además, la capa de middleware intenta combinar un servicio con su solicitante. La capa de aplicación proporciona los servicios solicitados para los clientes. Las actividades y servicios de los sistemas IoT se gestionan para generar un modelo comercial y diagramas de flujo, que se realizan en la capa empresarial.

61	La plataforma se implementa integrando el servicio de middleware EPCIS en el módulo HSS del IMS. Por lo tanto, la puerta de enlace de IoT puede descubrir cualquier objeto en cualquier evento, identificarlos y publicar su servicio en la capa de aplicación de IoT. Al usar este banco de pruebas para cada comportamiento en una red central IP, los datos de la capa de red IoT-IMS recopilados por el agente de red se pueden usar para ajustar los requisitos específicos de QoS e investigar soluciones de optimización de congestión en middleware para proporcionar referencias importantes para futuros IoT-IMS despliegue.
62	Capa de fusión de datos del sensor. En la capa de fusión de datos del sensor, los datos de detección del middleware pueden mapear todos los estados y el comportamiento de los recursos de ensamblaje. Por lo tanto, los datos se convierten en información, que se puede extraer e integrar. El middleware IoT puede integrar recursos heterogéneos y lograr la comunicación y transmisión de datos bidireccionales entre la capa de detección y la capa de toma de decisiones y aplicación. El middleware IoT también puede proporcionar interoperabilidad, lo que permite aprovechar la información de control de automatización en toda la organización.
63	En general, el middleware para la computación en la nube es más maduro que el middleware para IoT, pero quedan desafíos importantes. Uno de los desafíos clave es la heterogeneidad, que en realidad aumenta con el tiempo. Está claro que el middleware enfrenta desafíos importantes en las dos áreas principales de innovación: IoT y computación en la nube. Podría decirse, sin embargo, que el mayor desafío no es tratar con estos nuevos entornos, sino administrar el complejo sistema distribuido resultante. En lugar de buscar soluciones de middleware para IoT y (por definición) soluciones separadas para la computación en la nube, es necesario abordar el problema holístico y esto implica que la comunidad debe abordar los problemas del sistema como parte fundamental de los requisitos. Sin esto, el middleware se convertirá en parte del problema y no en parte de la solución a medida que surjan tecnologías dispares del middleware para cada uno de los diferentes dominios del problema.
64	El ciclo de desarrollo y el trabajo de mantenimiento y administración del sistema operativo se reducen. Basado en el papel del middleware en el sistema y la tecnología utilizada. Basado en el análisis de necesidad del middleware IoT en el campus inteligente opuesto, hemos implementado las capas funcionales de esta plataforma de middleware e introducido los métodos de implementación de módulos clave. La comunicación entre las diversas capas funcionales del middleware es impulsada por eventos, y el formato de datos es la clase de tipo de datos de objeto. Primero, se clasifican los datos recopilados por la capa de controlador de dispositivo y los datos de comando obtenidos por la capa de servicio de la aplicación; es decir, se llaman diferentes eventos de acuerdo con diferentes códigos de comando de los datos y se transmiten a la capa de programación de servicios, y la capa de programación de servicios

	transmite además los mensajes. El formato de datos pasado entre el middleware y la aplicación superior y la base de datos es un archivo xml. Los mensajes del middleware se pueden proporcionar directamente a la aplicación en forma de xml o se pueden almacenar en la base de datos a través de la interfaz de la base de datos.
65	Este es un entorno de múltiples capas que comprende dispositivos IoT (objetos), middleware y servicios de aplicaciones alojados en la nube. Los datos de IoT se pueden transmitir desde múltiples fuentes en función de los intereses y actividades de los usuarios. Para garantizar la trazabilidad en la red IoT, se considera un middleware liviano que facilitará la transmisión de los datos generados a una base de datos de back-end. La transmisión de datos es crucial en este trabajo porque el concepto de trazabilidad y detección de propagación de datos defectuosos requiere un análisis en tiempo real en ciertos escenarios. El middleware está basado en eventos y sigue la arquitectura centrada en datos. El diseño es un servicio típico de distribución de datos (DDS) que describe un modelo de publicación-suscripción centrado en datos (DCPS). El middleware difunde datos en función de las suscripciones de temas. En línea con los objetivos de la investigación, se considera que el enfoque propuesto adoptado para el diseño de middleware ofrece las siguientes ventajas: manipulación fácil de construcciones de datos, verificación del tiempo de compilación y preasignación de recursos. Estas ventajas pueden ayudar aún más a la propagación más rápida de los datos de transmisión en la fuente de análisis visual.

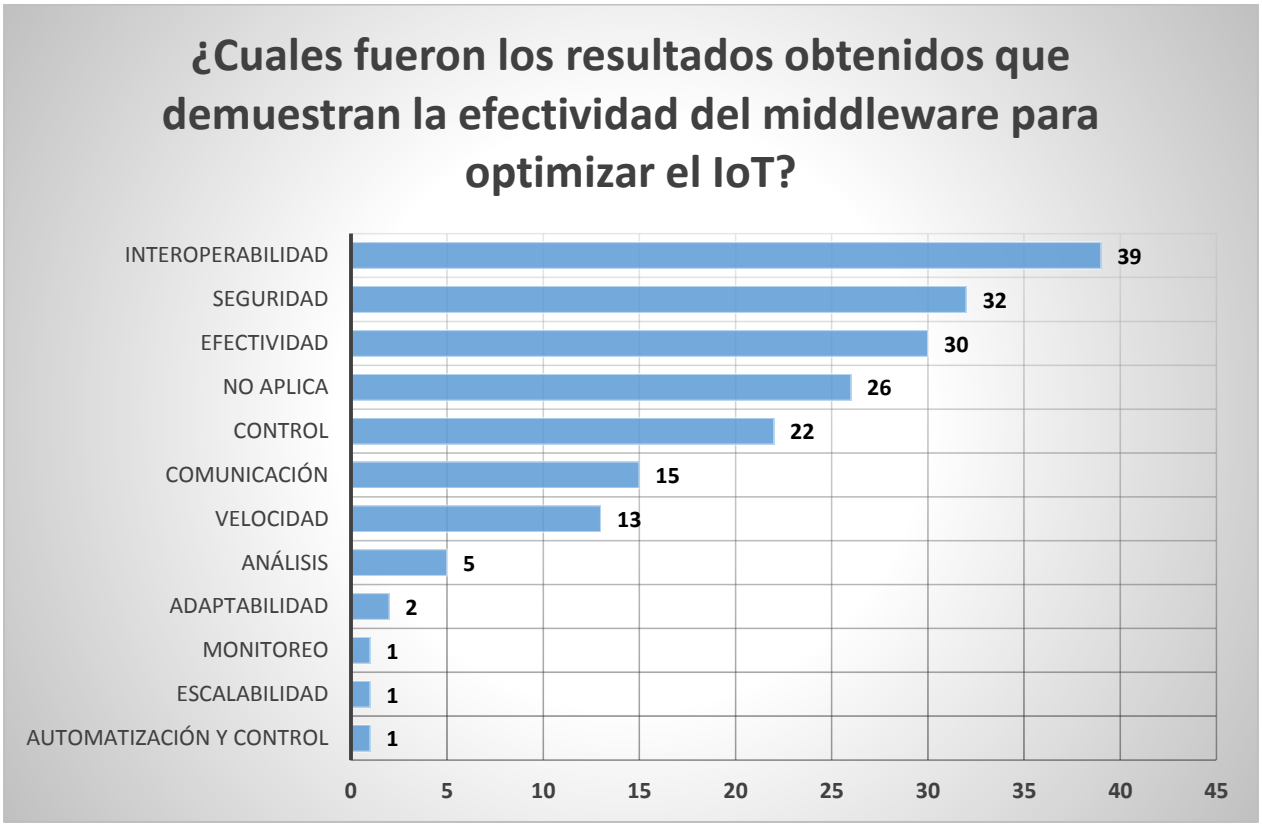
¿Qué tipo de conexiones utilizan dichas implementaciones? (F.O, NFC, 4G, 5G, Wifi, Bluetooth, LoRa, Bluetooth Ble, etc)

En general se observa que las implementaciones han sido para múltiples tipos de conexión, cobijando casi siempre a la mayoría de estas.


Métodos de conexión
TOTAL GENERAL
TODOS
WIFI
5G
WIFI, WLAN, BLUETOOTH, 5G, 4G
WIFI, NFC
WIFI, BLUETOOTH, WLAN.
WIFI, 4G, LTE
WIFI, 4G LTE, WIMAX
F.O Y WIFI
4G, LTE
65
53
3
2
1
1
1
1
1
1
1
0
10
20
30
40
50
60
70

7. RESULTADOS Y DISCUSIÓN

La revisión de los artículos tuvo un enfoque preciso en identificar el los resultados y la influencia de utilizar Middleware en las implementaciones de IoT y como resultado se identificaron unos factores cruciales que demuestran las falencias existentes y la necesidad de mejorar la tecnología de a tal punto de que dichas falencias no sean una preocupación para los usuarios del IoT:



Como la gráfica lo muestra la Interoperabilidad es el punto crítico en las implementaciones del IoT es la Interoperabilidad ya que el conjunto de objetos que interactúan con el IoT (Dispositivos, Lenguajes, Fabricantes y estándares) crean un ambiente heterogéneo no apto para su uso, y el Middleware quiere homogenizar dicho ambiente mejorando así los resultados entregados por IoT. La segunda causal de desconfianza es la Seguridad, y va muy ligado al punto anterior, ya que

un ambiente heterogéneo provoca una vulnerabilidad bastante considerable de la información que transita por esté medio.

Los avances alcanzados en materia de automatización y ambientes inteligentes han llegado a niveles importantes, cada vez son más las aportaciones en este sentido a través de los conceptos de IoT: ciudades inteligentes, automatización de casas, e-health, manejo inteligente de uso de agua, por mencionar algunos. Con los beneficios que han generado estos nuevos paradigmas, se ha presentado también la complejidad en su desarrollo; es por ello que se han buscado alternativas que faciliten los procesos de generación e implementación de aplicaciones innovadoras. Entonces, el contar con modelos que conceptualicen el dominio de un problema específico, y que permitan identificar, clasificar, y abstraer los elementos que lo conforman, representa la posibilidad de alcanzar una implementación automática eficiente.

8. IMPACTO ESPERADO

Con este trabajo se conoce de forma detallada el estado actual del uso del Middleware en el IOT y las áreas en donde más se han aplicado lo que favorecerá la realización de trabajos futuros haciendo la implementación directa del Middleware en el IoT.

9. CONCLUSIONES

El nuevo paradigma denominado Internet de las Cosas o Internet of Things (IOT) se considera ya una de las tecnologías habilitadoras de lo que se conoce como entornos inteligentes. El despliegue de dispositivos interconectados se está llevando a ámbitos como las ciudades, edificios, industria, agricultura, etc., para la mejora del confort y el bienestar, la productividad, la eficiencia energética o la seguridad entre otras. Estos entornos constituyen un verdadero ecosistema de dispositivos y servicios distribuidos y heterogéneos que deberán proveerse de mecanismos específicos para dar soporte a la cooperación de los mismos para la consecución de unos objetivos generales y comunes. Propone un middleware de comunicaciones con el que poder soportar la integración de dispositivos heterogéneos y la generación de respuestas inteligentes ante la detección de necesidades, en base a la reconfiguración dinámica y la composición automática de servicios.

En los últimos años, el Internet de las Cosas (IoT) ha ganado suficiente impulso y se está convirtiendo en una de las tecnologías de más rápido crecimiento en el espacio empresarial. IoT aumentará masivamente la cantidad de datos utilizados para el análisis por parte de las organizaciones.

El middleware para IoT actúa como un enlace que une los dominios mixtos de aplicaciones que se comunican a través de interfaces heterogéneas.

El middleware implica la necesidad de integración, transmisión y seguridad. Será necesario analizar los datos de los dispositivos y luego se deben tomar las medidas correctas con respecto a esos datos. Estas acciones podrían generar alertas o invocar procesos correctivos antes de que los problemas de rutina se desvanezcan en el desastre.

Se necesita middleware para la integración antes de que se puedan analizar los datos. Debe haber una herramienta que realice todas las acciones en lugar de tener diferentes herramientas de diversos proveedores.

El middleware es necesario para facilitar el desarrollo de diversos aplicativos y servicios en IoT.

Las propuestas discutidas son diversas e involucran varios middlewares enfoque de diseño y soporte de diferentes requisitos.

Las soluciones de middleware existentes no han explorado algunos requisitos tales como; descubrimiento dinámico de recursos, escalabilidad, fiabilidad, seguridad, privacidad y conciencia del contexto.

Alcance significativo para el trabajo futuro.

REFERENCIAS

Abreu, David Perez, Karima Velasquez, Marilia Curado, and Edmundo Monteiro. 2017. "A Resilient Internet of Things Architecture for Smart Cities." *Annales des Telecommunications/Annals of Telecommunications* 72(1–2): 19–30. http://dx.doi.org/10.1007/s12243-016-0530-y.

Aftab, Haris et al. 2019. "Analysis of Identifiers on IoT Platforms." *Digital Communications and Networks* (January).

Ahmed, Bestoun S., Miroslav Bures, Karel Frajtak, and Tomas Cerny. 2019. "Aspects of Quality in Internet of Things (IoT) Solutions: A Systematic Mapping Study." *IEEE Access* 7: 13758–80.

Al-Turjman, Fadi. 2020. "Intelligence and Security in Big 5G-Oriented IoNT: An Overview." *Future Generation Computer Systems* 102: 357–68. https://doi.org/10.1016/j.future.2019.08.009.

Aldaej, Abdulaziz. 2019. "Enhancing Cyber Security in Modern Internet of Things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI)." *IEEE Access* PP(c): 1–1.

Almusaylim, Zahrah A., and Noor Zaman. 2019. "A Review on Smart Home Present State and Challenges: Linked to Context-Awareness Internet of Things (IoT)." *Wireless Networks* 25(6): 3193–3204. https://doi.org/10.1007/s11276-018-1712-5.

Alshinina, Remah A., and Khaled M. Elleithy. 2018. "A Highly Accurate Deep Learning Based Approach for Developing Wireless Sensor Network Middleware." *IEEE Access* 6: 29885–98.

Andrés, Moisés Barrio. 2018. *Internet De Las Cosas*. https://www.editorialreus.es/static/pdf/primeraspaginas_9788429020380_internetdelascosas.pdf (April 25, 2019).

Asplund, Mikael, and Simin Nadjm-Tehrani. 2016. "Attitudes and Perceptions of IoT Security in Critical Societal Services." *IEEE Access* 4: 2130–38.

Athavale, Yashodhan, and Sridhar Krishnan. 2020. "A Telehealth System Framework for Assessing Knee-Joint Conditions Using Vibroarthrographic Signals." *Biomedical Signal Processing and Control* 55: 101580. https://doi.org/10.1016/j.bspc.2019.101580.

Baig, Zubair A. et al. 2020. "Averaged Dependence Estimators for DoS Attack Detection in IoT Networks." *Future Generation Computer Systems* 102: 198–209. https://doi.org/10.1016/j.future.2019.08.007.

Blair, Gordon, Douglas Schmidt, and Chantal Taconet. 2016. "Middleware for Internet Distribution

in the Context of Cloud Computing and the Internet of Things: Editorial Introduction." *Annales des Telecommunications/Annals of Telecommunications* 71(3–4): 87–92.

Cereda, Paulo Roberto Massa, and João José Neto. 2017. "A Middleware Architecture for Adaptive Devices." *Procedia Computer Science* 109: 1158–63. http://dx.doi.org/10.1016/j.procs.2017.05.388.

Chen, Shanzhi et al. 2014. "A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective." *IEEE Internet of Things Journal* 1(4): 349–59.

CHENG, ROGER. 2018. "¿Qué Es La Red 5G? Esto Es Lo Que Debes Saber." *17-09-2018*. https://www.cnet.com/es/como-se-hace/que-es-el-5g-esto-es-lo-que-debes-saber/ (May 26, 2019).

da Cruz, Mauro A.A. et al. 2018. "Performance Evaluation of IoT Middleware." *Journal of Network and Computer Applications* 109(December 2017): 53–65. https://doi.org/10.1016/j.jnca.2018.02.013.

Eldrandaly, Khalid A., Mohamed Abdel-Basset, and Laila A. Shawky. 2019. "Internet of Spatial Things: A New Reference Model with Insight Analysis." *IEEE Access* 7: 19653–69.

Elmisery, Ahmed M., Seungmin Rho, and Dmitri Botvich. 2016. "A Fog Based Middleware for Automated Compliance with OECD Privacy Principles in Internet of Healthcare Things." *IEEE Access* 4(Idc): 8418–41.

Feldner, Benjamin, and Paula Herber. 2018. "A Qualitative Evaluation of IPv6 for the Industrial Internet of Things." *Procedia Computer Science* 134: 377–84. https://doi.org/10.1016/j.procs.2018.07.195.

Flauzac, Olivier, Carlos Gonzalez, and Florent Nolot. 2015. "New Security Architecture for IoT Network." *Procedia Computer Science* 52(1): 1028–33. http://dx.doi.org/10.1016/j.procs.2015.05.099.

Georgakopoulos, Dimitrios, and Prem Prakash Jayaraman. 2016. "Internet of Things: From Internet Scale Sensing to Smart Services." *Computing* 98(10): 1041–58.

Georgi, Nawras, Aline Corvol, and Regine Le Bouquin Jeannes. 2018. "Middleware Architecture for Health Sensors Interoperability." *IEEE Access* 6: 26283–91.

Ghanbari, Zahra, Nima Jafari Navimipour, Mehdi Hosseinzadeh, and Aso Darwesh. 2019. "Resource Allocation Mechanisms and Approaches on the Internet of Things." *Cluster Computing* 22(4): 1253–82. https://doi.org/10.1007/s10586-019-02910-8.

Global Tag Srl. 2016. “Tecnología BLE (Smart Bluetooth Low Energy) - Global Tag Srl.” https://www.global-tag.com/es/tecnologia-ble/ (May 26, 2019).

Gomes, Porfírio et al. 2019. “A Semantic-Based Discovery Service for the Internet of Things.” *Journal of Internet Services and Applications* 10(1): 0–13.

Hsieh, Han Chuan, Wen Hsu Hsieh, and Jiann Liang Chen. 2014. “Mobile IMS Integration of the Internet of Things in Ecosystem.” *Wireless Personal Communications* 80(2): 819–36.

Kabugo, James Clovis, Sirkka Liisa Jämsä-Jounela, Robert Schiemann, and Christian Binder. 2020. “Industry 4.0 Based Process Data Analytics Platform: A Waste-to-Energy Plant Case Study.” *International Journal of Electrical Power and Energy Systems* 115(August 2019): 105508. https://doi.org/10.1016/j.ijepes.2019.105508.

Kurebwa, Joseph G., and Tawanda Mushiri. 2019. “Internet of Things Architecture for a Smart Passenger-Car Robotic First Aid System.” *Procedia Manufacturing* 35: 27–34. https://doi.org/10.1016/j.promfg.2019.05.006.

Lee, In. 2019. “The Internet of Things for Enterprises: An Ecosystem, Architecture, and IoT Service Business Model.” *Internet of Things* 7: 100078.

Li, Ali, Xiaozhen Ye, and Huansheng Ning. 2017. “Thing Relation Modeling in the Internet of Things.” *IEEE Access* 5: 17117–25.

Li, Ji et al. 2020. “Approximate Data Aggregation in Sensor Equipped IoT Networks.” *Tsinghua Science and Technology* 25(1): 44–55.

Liu, Mingzhou et al. 2017. “Intelligent Assembly System for Mechanical Products and Key Technology Based on Internet of Things.” *Journal of Intelligent Manufacturing* 28(2): 271–99. http://dx.doi.org/10.1007/s10845-014-0976-6.

Liu, Wei et al. 2020. “A Method of NC Machine Tools Intelligent Monitoring System in Smart Factories.” *Robotics and Computer-Integrated Manufacturing* 61(April 2018): 101842. https://doi.org/10.1016/j.rcim.2019.101842.

Liu, Ying et al. 2020. “L1-Subspace Tracking for Streaming Data.” *Pattern Recognition* 97: 1–13.

Lomotey, Richard K., Joseph C. Pry, and Chenshean Chai. 2018. “Traceability and Visual Analytics for the Internet-of-Things (IoT) Architecture.” *World Wide Web* 21(1): 7–32.

Madakam, Somayya, R Ramaswamy, and Siddharth Tripathi. 2015. “Jcc_2015052516013923.” *Journal of Computer and Communications* (May): 164–73.

Marquez, Marco A. et al. 2018. “Controlled and Secure Access to Promote the Industrial Internet of Things.” *IEEE Access* 6: 48289–99.

Mattos, Diogo Menezes Ferrazani, Pedro Braconnot Velloso, and Otto Carlos Muniz Bandeira Duarte. 2019. “An Agile and Effective Network Function Virtualization Infrastructure for the Internet of Things.” *Journal of Internet Services and Applications* 10(1).

Mehta, Rishika, Jyoti Sahni, and Kavita Khanna. 2018. “Internet of Things: Vision, Applications and Challenges.” *Procedia Computer Science* 132: 1263–69. https://doi.org/10.1016/j.procs.2018.05.042.

Mesmoudi, Yasser et al. 2018. “A Middleware Based on Service Oriented Architecture for Heterogeneity Issues within the Internet of Things (MSOAH-IoT).” *Journal of King Saud University - Computer and Information Sciences* (xxxx). https://doi.org/10.1016/j.jksuci.2018.11.011.

Mohamed, Nader et al. 2017. “SmartCityWare: A Service-Oriented Middleware for Cloud and Fog Enabled Smart City Services.” *IEEE Access* 5(Cc): 17576–88.

Mohammadi, Venus, Amir Masoud Rahmani, Aso Mohammed Darwesh, and Amir Sahafi. 2019. “Trust-Based Recommendation Systems in Internet of Things: A Systematic Literature Review.” *Human-centric Computing and Information Sciences* 9(1). https://doi.org/10.1186/s13673-019-0183-8.

Mourad, Mohamed H., Aydin Nassehi, Dirk Schaefer, and Stephen T. Newman. 2020. “Assessment of Interoperability in Cloud Manufacturing.” *Robotics and Computer-Integrated Manufacturing* 61(June 2018): 101832. https://doi.org/10.1016/j.rcim.2019.101832.

Musaddiq, Arslan et al. 2018. “A Survey on Resource Management in IoT Operating Systems.” *IEEE Access* 6: 8459–82.

Naciones Unidas. 2012. “Interoperabilidad.” http://tfig.itcilo.org/SP/contents/interoperability.htm (May 26, 2019).

Palade, Andrei et al. 2018. “Middleware for Internet of Things: An Evaluation in a Small-Scale IoT Environment.” *Journal of Reliable Intelligent Environments* 4(1): 3–23. https://doi.org/10.1007/s40860-018-0055-4.

Paliyawan, Pujana, Takahiro Kusano, and Ruck Thawonmas. 2019. “Motion Recommender for Preventing Injuries during Motion Gaming.” *IEEE Access* 7: 7977–88.

Perera, Charith et al. 2014. “MOSDEN: An Internet of Things Middleware for Resource

Constrained Mobile Devices." *Proceedings of the Annual Hawaii International Conference on System Sciences*: 1053–62.

Pickering, Paul. 2017. "Descripción General de La Plataforma LoRa | DigiKey." *2017-06-29*. https://www.digikey.com/es/articles/techzone/2017/jun/develop-lora-for-low-rate-long-range-iot-applications (May 26, 2019).

Rafique, Ansar, Dimitri Van Landuyt, Bert Lagaisse, and Wouter Joosen. 2018. "On the Performance Impact of Data Access Middleware for NoSQL Data Stores A Study of the Trade-Off between Performance and Migration Cost." *IEEE Transactions on Cloud Computing* 6(3): 843–56.

Rahman, Leila Fatmasari, Tanir Ozcelebi, and Johan Lukkien. 2018. "Understanding IoT Systems: A Life Cycle Approach." *Procedia Computer Science* 130: 1057–62. https://doi.org/10.1016/j.procs.2018.04.148.

Ray, P. P. 2018. "A Survey on Internet of Things Architectures." *Journal of King Saud University - Computer and Information Sciences* 30(3): 291–319. https://doi.org/10.1016/j.jksuci.2016.10.003.

Riahi Sfar, Arbia, Enrico Natalizio, Yacine Challal, and Zied Chtourou. 2018. "A Roadmap for Security Challenges in the Internet of Things." *Digital Communications and Networks* 4(2): 118–37. https://doi.org/10.1016/j.dcan.2017.04.003.

Rouse, Margaret. 2014. "¿Qué Es Privacidad de Datos (Privacidad de Información)? - Definición En WhatIs.Com." *Junio 2014*. https://searchdatacenter.techtarget.com/es/definicion/Privacidad-de-datos-privacidad-de-informacion (May 26, 2019).

Sadique, Kazi Masum, Rahim Rahmani, and Paul Johannesson. 2018. "Towards Security on Internet of Things: Applications and Challenges in Technology." *Procedia Computer Science* 141: 199–206. https://doi.org/10.1016/j.procs.2018.10.168.

Samaniego, Mayra, and Ralph Deters. 2016. "Management and Internet of Things." *Procedia Computer Science* 94(MobiSPC): 137–43. http://dx.doi.org/10.1016/j.procs.2016.08.022.

Santos, Marcus A.G. et al. 2020. "Online Heart Monitoring Systems on the Internet of Health Things Environments: A Survey, a Reference Model and an Outlook." *Information Fusion* 53(December 2018): 222–39. https://doi.org/10.1016/j.inffus.2019.06.004.

SGSI-ISO. 2015. "ISO 27001: ¿Qué Significa La Seguridad de La Información?" *21-05-2015*.

https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/ (May 26, 2019).

Siboni, Shachar et al. 2019. “Security Testbed for Internet-of-Things Devices.” *IEEE Transactions on Reliability* 68(1): 23–44.

Silva, Jonathan De C. et al. 2019. “M4DN.IoT-A Networks and Devices Management Platform for Internet of Things.” *IEEE Access* 7: 53305–13.

Singh, Jatinder, and Jean M. Bacon. 2014. “On Middleware for Emerging Health Services.” *Journal of Internet Services and Applications* 5(1): 1–19.

Sosa, Victor. 2014. “MIDDLEWARE: Arquitectura Para Aplicaciones Distribuidas.” : 1–21. http://www.tamps.cinvestav.mx/~vjsosa/clases/sd/Middleware_Recorrido.pdf.

Sun, Gaofei, Xiaoshuang Xing, and Xiangping Qin. 2019. “Energy Harvesting-Based Data Uploading for Internet of Things.” *Eurasip Journal on Wireless Communications and Networking* 2019(1).

Sun, Yunchuan, Ye Xia, Houbing Song, and Rongfang Bie. 2014. “Internet of Things Services for Small Towns.” *Proceedings - 2014 International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI 2014*: 92–95.

Wan, Liang, Zhijian Zhang, and Jian Wang. 2019. “Demonstrability of Narrowband Internet of Things Technology in Advanced Metering Infrastructure.” *Eurasip Journal on Wireless Communications and Networking* 2019(1).

Wang, Eric Ke et al. 2020. “PoRX: A Reputation Incentive Scheme for Blockchain Consensus of IIoT.” *Future Generation Computer Systems* 102: 140–51. https://doi.org/10.1016/j.future.2019.08.005.

Wang, G., B. Lee, J. Ahn, and G. Cho. 2020. “A UAV-Assisted CH Election Framework for Secure Data Collection in Wireless Sensor Networks.” *Future Generation Computer Systems* 102: 152–62. https://doi.org/10.1016/j.future.2019.07.076.

Wu, Chung Kit et al. 2019. “An IoT Tree Health Indexing Method Using Heterogeneous Neural Network.” *IEEE Access* 7: 66176–84.

Xu, Tong et al. 2017. “Defending Against New-Flow Attack in SDN-Based Internet of Things.” *IEEE Access* 5: 3431–43.

Yu, Jaehak, Hyo Chan Bang, Hosung Lee, and Yang Sun Lee. 2016. “Adaptive Internet of Things

and Web of Things Convergence Platform for Internet of Reality Services." *Journal of Supercomputing* 72(1): 84–102.

Zahra, Samman et al. 2017. "Fog Computing over IoT: A Secure Deployment and Formal Verification." *IEEE Access* 5: 27132–44.

Zhang, Li, Huiqun Yuan, Sheng Hung Chang, and Anthony Lam. 2019. "Research on the Overall Architecture of Internet of Things Middleware for Intelligent Industrial Parks." *International Journal of Advanced Manufacturing Technology*.