



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Estudio del estado del arte de la computación perimetral y el Internet de las Cosas aplicados a sistemas y tecnologías de la información para la Defensa

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: David Álvarez Sánchez

DIRECTOR: Rubén Nocelo López

CURSO ACADÉMICO: 2023-2024

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Estudio del estado del arte de la computación perimetral y el Internet de las Cosas aplicados a sistemas y tecnologías de la información para la Defensa

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de Telecomunicación

UniversidadeVigo

RESUMEN

Este Trabajo de Fin de Máster se centra en la integración del Internet de las Cosas (Internet of Things, IoT) con la Computación Perimetral (Edge Computing), un tema de creciente importancia en la era digital. La estructura del trabajo incluye una introducción y objetivos, un análisis del estado del arte, un estudio de la integración de IoT con Edge Computing, casos de aplicación, y finalmente, conclusiones y líneas futuras.

En la introducción, se establece el contexto y la motivación del estudio, resaltando la relevancia y el impacto del IoT y la Computación Perimetral en el mundo tecnológico actual. Se definen los objetivos del trabajo y se presenta la estructura general del mismo.

El análisis del estado del arte se divide en dos secciones principales: una dedicada al IoT, incluyendo su historia, los tipos de sensores utilizados y los principales desafíos que enfrenta; y otra enfocada en la Computación Perimetral, comparándola con el paradigma tradicional de Computación en la Nube y discutiendo aspectos como la ubicación del procesamiento de datos, la latencia, y una comparativa de casos de uso.

La integración de IoT con Edge Computing se analiza desde perspectivas legales y arquitectónicas. Se examinan las regulaciones actuales y normas internacionales, y se detallan las arquitecturas de tres, cuatro y cinco capas, enfatizando los elementos clave en la arquitectura IoT-Edge. También se discuten protocolos de comunicación y tecnologías esenciales.

Los casos de aplicación presentados incluyen el sector de la salud, las ciudades inteligentes (transporte, red eléctrica, agricultura y acuicultura) y el uso militar, destacando el IoT en el campo de batalla y el uso de drones en redes Edge. El trabajo concluye con un resumen de los hallazgos y perspectivas de futuras investigaciones, señalando posibles direcciones para el estudio de la integración de IoT con la Computación Perimetral.

PALABRAS CLAVE

Internet de las Cosas, Computación perimetral, Latencia, Seguridad Multimedia, Vehículos Aéreos no Tripulados.

AGRADECIMIENTOS

A mi padre, por animarnos siempre a dar lo mejor de nosotros. Gracias por inculcarnos los valores del esfuerzo, el sacrificio y la constancia. Nada de lo que hayamos conseguido habría sido posible sin el tesón que le has puesto a nuestra educación. Siempre llevaré conmigo esas cuatro palabras que nos enseñaste y que han marcado mi etapa formativa: “El continuo aburrimiento diario”.

A mi madre, por su apoyo incondicional y amor inquebrantable.

A mis hermanos, porque vosotros me enseñasteis a celebrar y llevar con orgullo los éxitos de un hermano como si fueran propios.

Gracias a mi familia. Vuestro cariño y amor ha sido el pilar fundamental que me ha permitido crecer y prosperar.

Y, por último, gracias a Andrea. Gracias por tu comprensión y ánimos a pesar de todo el tiempo que los estudios me quitan. Gracias por ser mi refuerzo positivo en este viaje que no ha hecho más que comenzar.

Gracias a todos.

Os quiero.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	4
1 Introducción y objetivos	5
1.1 Contexto y motivación	5
1.2 Objetivos	6
1.3 Estructura de la memoria	6
2 Estado del arte	8
2.1 Estado del arte del Internet de las Cosas.....	8
2.1.1 Historia	8
2.1.2 Sensores	11
2.1.3 Principales desafíos	12
2.2 Estado del arte de la Computación Perimetral	14
2.2.1 Introducción	14
2.2.2 Comparativa con la Computación en la Nube	15
2.2.2.1 Ubicación del procesamiento de datos	16
2.2.2.2 Latencia y ancho de banda.....	16
2.2.2.3 Escalabilidad.....	17
2.2.2.4 Costes, mantenimiento y eficiencia energética	17
2.2.2.5 Seguridad y privacidad de los datos	18
2.2.2.6 Casos de uso.....	18
2.2.3 Principales desafíos	19
3 Integración del IoT con Edge Computing	22
3.1 Marco legal y regulatorio.....	22
3.1.1 Regulaciones actuales.....	23
3.1.2 Normas y Estándares internacionales	24
3.2 Arquitectura	26
3.2.1 Arquitectura de tres capas.....	26
3.2.2 Arquitectura de cuatro capas	28
3.2.3 Arquitectura de cinco capas.....	29
3.2.4 Análisis de los elementos clave en la arquitectura IoT-Edge	31
3.3 Protocolos de comunicación y tecnologías esenciales	32
3.3.1 Tecnologías de comunicación.....	33

3.3.2 Protocolos de comunicación	38
4 Casos de aplicación	42
4.1 Ámbito de la salud	42
4.2 Ciudades inteligentes	46
4.2.1 Transporte inteligente	47
4.2.2 Red eléctrica inteligente	48
4.2.3 Agricultura y acuicultura	49
4.3 Ámbito militar.....	51
4.3.1 El Internet de las Cosas en el campo de batalla.....	51
4.3.2 La computación perimetral en Defensa	53
5 Conclusiones y líneas futuras	58
5.1 Conclusiones	58
5.2 Líneas futuras	59
6 Bibliografía.....	60
7 Listado de acrónimos.....	65

ÍNDICE DE FIGURAS

Figura 2-1 El nacimiento del Internet de las Cosas según IBSG Cisco [9].....	9
Figura 2-2 Evolución del número de dispositivos IoT conectados en miles de millones [10].....	10
Figura 2-3 Distribución de dispositivos IoT por regiones [11]	10
Figura 2-4 Diferentes tipos de sensores en IoT [13]	12
Figura 2-5 Comparativa visual Cloud computing vs Edge computing [20].....	16
Figura 3-1 Protección integral desde sensores hasta usuarios [27]	23
Figura 3-2 Arquitectura básica de tres capas [38]	27
Figura 3-3 Arquitectura básica de cuatro capas [40].....	28
Figura 3-4 Arquitectura básica de cinco capas [40].....	29
Figura 3-5 Arquitecturas IoT-Edge. (a) 3 capas. (b) 4 capas. (c) 5 capas.....	30
Figura 3-6 Comparativa entre Sigfox, LoRa y NB-IoT [44].....	33
Figura 3-7 Resumen tecnologías inalámbricas según alcance [46].....	37
Figura 3-8 Visión de alto nivel de los modelos de interacción en MQTT y CoAP [48].....	39
Figura 4-1 Modelo de trabajo en H-IoT [49]	43
Figura 4-2 Telecirugía [Tomada de Intramed.net]	45
Figura 4-3 Wearable para monitorizar electrocardiograma, temperatura y capacidad pulmonar [Tomada de convertronic.net]	46
Figura 4-4 Parking inteligente para ciudades inteligentes [Tomada de clevercity.com]	48
Figura 4-5 Smart Grid usando el modelo de computación en el borde [55]	49
Figura 4-6 Sensores de humedad en viñedos [Tomada de plantae.garden]	50
Figura 4-7 IoT en la agricultura [Tomada de javatpoint.com/iot-in-agriculture]	50
Figura 4-8 IoBT [59]	52
Figura 4-9 Aplicación de un sistema C3I en una operación militar y una operación de rescate [61]	53
Figura 4-10 Estructura de una red de Edge Computing basada en drones [64]	54
Figura 4-11 Mejora en la latencia respecto otras técnicas [64]	55

ÍNDICE DE TABLAS

Tabla 3-1 Comparativa entre las distintas arquitecturas IoT-Edge	31
Tabla 3-2 Comparativa entre Bluetooth clásico y Bluetooth Low Energy [45].....	35
Tabla 3-3 Resumen principales características protocolos de comunicación	41
Tabla 4-1 Latencia del sistema según aumenta el número de drones [64]	56
Tabla 4-2 Principales ventajas del Edge Computing aplicadas al ámbito militar	57

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Contexto y motivación

En la era actual, caracterizada por un crecimiento exponencial en la generación de datos y la necesidad de procesamiento en tiempo real, el Internet de las Cosas (Internet of Things, IoT) y la computación perimetral (Edge Computing) emergen como pilares fundamentales en la transformación digital de múltiples sectores. Este trabajo de fin de Máster se centra en explorar la convergencia de estas dos tecnologías, proporcionando una comprensión profunda de su estado actual, desafíos y potencial de aplicación en diferentes contextos, especialmente en el de la Defensa.

El IoT ha emergido como un paradigma disruptivo, transformando objetos cotidianos en entes inteligentes capaces de comunicarse entre sí, recoger y transmitir datos y tomar decisiones. Esta red de dispositivos interconectados promete una eficiencia sin precedentes y una nueva forma de interactuar con el mundo físico. Sin embargo, su potencial depende en gran medida de la capacidad para procesar y analizar los datos generados de manera eficiente, lo cual plantea desafíos en términos de ancho de banda, latencia y seguridad.

Es aquí donde la computación perimetral se convierte en un complemento fundamental. Al trasladar el procesamiento de datos y servicios desde el núcleo de la red a la periferia de ésta, es decir, cerca de donde se generan los datos, conseguimos por un lado aliviar la carga sobre las infraestructuras de red centralizadas, y por otro reducir la latencia y mejorar la eficiencia del ancho de banda. Estas características son de vital importancia en aplicaciones de Defensa, donde decisiones rápidas y seguras pueden suponer la vida o la muerte.

En nuestro sector de aplicación, el IoT ofrece una gran variedad de posibilidades, desde una logística mejorada hasta la vigilancia avanzada o sistemas de armas autónomos. La integración de dispositivos IoT en sistemas de Defensa está revolucionando la manera en la que se llevan a cabo las operaciones militares, aumentando la percepción del entorno táctico, mejorando la toma de decisiones y potenciando la eficacia operativa.

Estos avances también traen consigo desafíos significativos. La seguridad de los datos, la gestión del espectro electromagnético y la integración de sistemas heterogéneos son solo algunos de los obstáculos que deben superarse para aprovechar plenamente el potencial de esta tecnología.

Este trabajo propone examinar cómo la integración del IoT y el Edge Computing puede revolucionar las operaciones de Defensa. A través de un análisis del estado del arte, estudios de caso y exploración de arquitecturas tecnológicas, se busca no solo comprender el panorama actual de estas

tecnologías sino también identificar tendencias emergentes, desafíos pendientes y oportunidades para futuras investigaciones y aplicaciones prácticas.

La motivación principal de este trabajo radica en la necesidad de entender a fondo cómo la convergencia del IoT y la computación perimetral puede ser aprovechada para fortalecer y modernizar las capacidades en el ámbito de la Defensa, un sector donde la innovación tecnológica juega un papel crucial en la seguridad nacional.

1.2 Objetivos

El presente TFM tiene como fin estudiar la sinergia entre el IoT y el Edge Computing, con un enfoque particular en su aplicación en el sector de la Defensa. Los objetivos se detallan a continuación:

- Analizar el estado actual del IoT y la computación perimetral: Profundizar en avances recientes, tendencias y desafíos principales. Explorar el impacto de estas tecnologías en diversos sectores y realizar comparativas, como entre Edge Computing y Cloud Computing, destacando sus ventajas e inconvenientes.
- Estudiar la integración del IoT y la computación perimetral: Comprender los conceptos fundamentales a través de un desarrollo teórico seguido de un análisis de la integración de ambas tecnologías.
- Estudio de casos prácticos: Investigar casos específicos de aplicación del IoT y la computación perimetral en distintos sectores como el de la salud y las ciudades inteligentes, con especial mención al ámbito militar.
- Identificación de desafíos: Reconocer áreas en las que estas tecnologías pueden ser mejoradas, especialmente en lo que respecta a la seguridad y la gestión eficiente de datos.
- Desarrollo de recomendaciones y líneas futuras: El objetivo de este punto será, en base al estudio previo, ofrecer recomendaciones para futuras implementaciones y desarrollos tecnológicos en el IoT y la computación perimetral en la Defensa.

1.3 Estructura de la memoria

La memoria de este trabajo se estructura en seis secciones principales para proporcionar una comprensión integral del tema:

1. Introducción y objetivos: Esta sección establece el marco del estudio, presentando el tema, la motivación detrás de la investigación, los objetivos específicos del trabajo y el enfoque metodológico adoptado.
2. Estado del Arte: Aquí se realiza un análisis detallado del panorama actual del IoT y la computación perimetral, abordando los avances recientes, tendencias y desafíos.

3. Integración del IoT con el Edge Computing: Esta parte se centra en los fundamentos del IoT y la computación perimetral. Además, sienta las bases teóricas de ambas tecnologías para analizar la manera en que éstas se integran y potencian mutuamente.
4. Aplicaciones y casos de uso: Se examina el uso práctico del IoT y la computación perimetral en distintos sectores, haciendo especial énfasis en el de la Defensa.
5. Conclusiones: En este apartado se sintetizan los hallazgos principales del estudio, se presentan recomendaciones basadas en la investigación y se identifican líneas futuras de desarrollo en el campo.
6. Bibliografía: Finalmente, se incluye una compilación de todas las fuentes y referencias utilizadas a lo largo del trabajo, ofreciendo un respaldo académico y metodológico a la investigación.

2 ESTADO DEL ARTE

2.1 Estado del arte del Internet de las Cosas

2.1.1 Historia

Aunque el término “Internet de las Cosas” (Internet of Things, IoT) es ampliamente utilizado, no existe una definición única y exclusiva. En [1] se define el concepto como una red abierta y completa de objetos inteligentes que tienen la capacidad de autoorganizarse, compartir información, datos y recursos, y reaccionar y actuar frente a situaciones y cambios en el entorno.

La historia y evolución del IoT es un viaje fascinante a través de la innovación y la tecnología, marcando la transición desde simples conceptos hasta sistemas complejos que hoy influyen en numerosos aspectos de la vida cotidiana y la industria.

El término Internet de las Cosas es usado por primera vez en 1999 por Kevin Ashton en una presentación en Procter & Gamble (P&G) [2]. Ashton lo utilizó para describir un sistema donde el mundo físico se conecta a través de Internet mediante sensores omnipresentes, aunque el concepto de dispositivos conectados comienza a tomar forma mucho antes.

En 1982, en la Universidad Carnegie Mellon en Pittsburgh, Pensilvania, un grupo de estudiantes de ciencias informáticas añadieron un interfaz de red a una máquina expendedora. Los estudiantes estaban cansados de subir hasta la tercera planta, donde se encontraba la máquina de refrescos, para encontrársela vacía o con bebidas calientes. Al conectarla a la red, podían comprobar si tenía Coca Colas frías, evitando así viajes inútiles. Este ingenioso “invento” marcó un hito histórico: probablemente fue la primera vez que un objeto cotidiano se integraba a la red de internet [3].

En 1989, Dan Lynch, presidente del show *Interop Internet Networking* desafió a John Romkey a conectar una tostadora a Internet. Lynch le prometió que, si lo conseguía, la tostadora ocuparía un lugar privilegiado en la zona de exposiciones. Romkey, junto a Simon Hackett consiguieron conectar la tostadora a internet a través de TCP/IP, sobre la cual se podía actuar para controlar el encendido y apagado, regulando así como de tostado salía el pan [4].

En 1999, Neil A. Gershenfeld publica su libro “Cuando las Cosas empiezan a pensar”, en el que ofrece una visión del futuro de la tecnología y como ésta podría integrarse en nuestra vida cotidiana. El libro, pionero en presentar ideas sobre IoT y la computación ubicua, explora cómo los objetos podrían empezar a “pensar”. Gershenfeld argumentaba que, en lugar de tener ordenadores personales, la tecnología estaría integrada en objetos que usamos día a día, como ropa, joyas, muebles, incluso en materiales de construcción, lo que permitiría una interacción más natural y fluida entre humanos y máquinas [5].

Con el cambio de milenio llegó la primera nevera inteligente, comercializada por LG y el término IoT se empieza a mencionar en publicaciones de referencia como *The Guardian*, *Scientific American* y el *Boston Globe* [6].

Inventado por Rafi Haladjian y Olivier Mével, en 2005 nace Nabaztag [7], un conejo artificial conectado a través de WiFi capaz de leer correos electrónicos, noticias, o previsiones meteorológicas entre otros.

En el año 2008 surge la *IPSO Alliance* (Internet Protocol for Smart Objects Alliance), cuyo objetivo principal era promover el uso del protocolo IP como estándar para conectar objetos inteligentes. Esta unión de empresas del sector tecnológico jugó un papel clave en el avance y la adopción del Internet de las Cosas, destacando la importancia de contar con un enfoque estandarizado para la comunicación en un mundo cada vez más interconectado. Su trabajo ayudó a sentar las bases para que dispositivos de distintos fabricantes y tecnologías puedan funcionar conjuntamente de manera más armoniosa y eficiente [8].

De acuerdo con el Grupo de Soluciones Empresariales para Internet (IBSG) de Cisco, el Internet de las Cosas cobra vida en el momento en el que hay más objetos que personas conectadas a internet, suceso que se estima ocurrió en algún momento entre 2008 y 2009 [9].

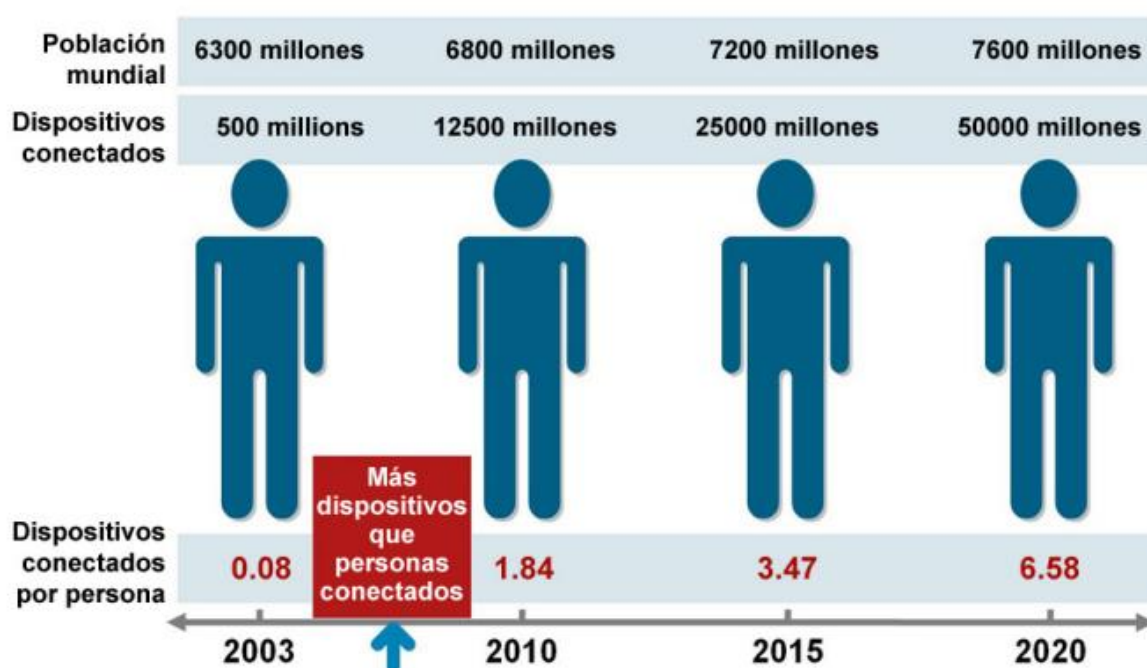


Figura 2-1 El nacimiento del Internet de las Cosas según IBSG Cisco [9]

Esta tendencia de crecimiento exponencial de dispositivos IoT conectados se ha mantenido y, según las proyecciones actuales, se espera que se acelere aún más en la próxima década. Los avances tecnológicos, como la mayor capacidad de procesamiento, la posibilidad de fabricar dispositivos cada vez más pequeños y la mejora en la conectividad, han facilitado esta expansión.

Se espera que la cantidad de dispositivos relacionados con el Internet de las Cosas experimente un notable incremento, duplicándose de 15.1 mil millones en 2020 a más de 29 mil millones hacia el año 2030 [10].

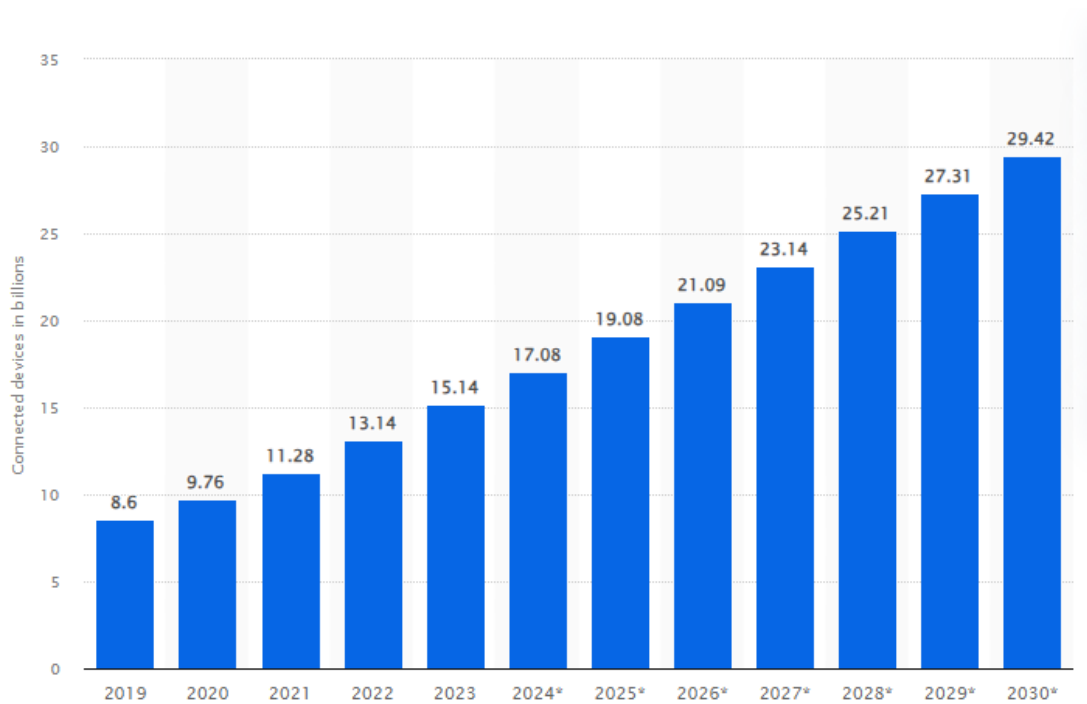


Figura 2-2 Evolución del número de dispositivos IoT conectados en miles de millones [10]

China liderará esta expansión con aproximadamente 8 mil millones de dispositivos en uso. Estos dispositivos, que ya se encuentran en una amplia gama de industrias y mercados, representaron alrededor del 60% del total de dispositivos IoT en 2020, tendencia que se prevé continúe en la próxima década.

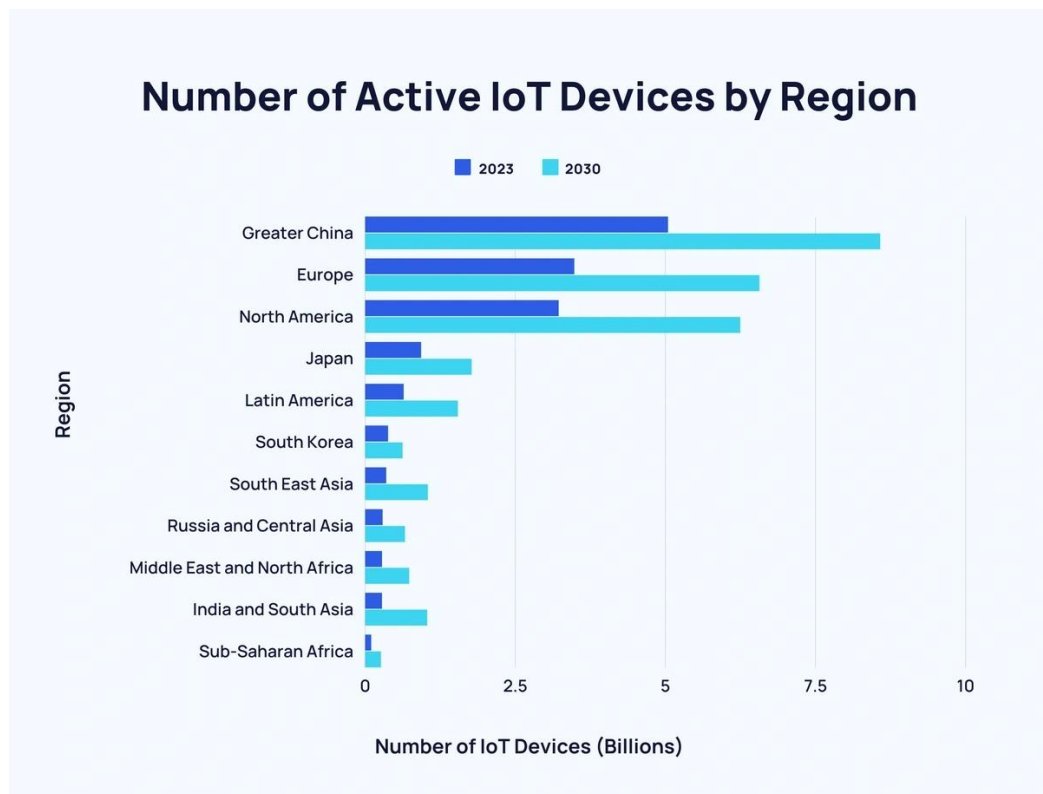


Figura 2-3 Distribución de dispositivos IoT por regiones [11]

En la figura 2-3 tenemos la distribución por regiones de dispositivos IoT, donde se puede observar que, China lidera con la mayor cantidad de dispositivos, seguida por Europa y Norteamérica [11]. Todas las regiones muestran una previsión de crecimiento significativo en el número de dispositivos IoT hacia 2030. Se observa que las regiones con menor cantidad de dispositivos son India, Sudáfrica, y la África Subsahariana.

Este crecimiento refleja cómo el IoT se ha convertido en un elemento integral de nuestra sociedad, transformando la manera en que vivimos, trabajamos y nos conectamos. A medida que avanzamos hacia 2030, la integración profunda del Internet de las Cosas en nuestras vidas cotidianas se volverá aún más evidente, marcando un hito significativo en la historia de la tecnología y su influencia en la sociedad.

2.1.2 Sensores

Los sensores son elementos esenciales que recogen información del entorno físico. Estos dispositivos detectan cambios en su alrededor, como temperatura, luz o movimiento, entre otros, y convierten estas variables en señales digitales. Esta capacidad de recolección y conversión de datos es lo que los hace indispensables en el IoT.

Los sensores se integran en diversos dispositivos y sistemas del Internet de las Cosas, recopilando datos necesarios para el funcionamiento de esta tecnología. Estos datos se envían a plataformas de procesamiento y análisis, lo que facilita la toma de decisiones automatizadas y mejora la interacción entre los usuarios y los dispositivos conectados.

La importancia de los sensores en el IoT reside principalmente en su capacidad para proveer información precisa y actualizada. Esta información es crucial para el rendimiento y la eficacia de las aplicaciones de IoT. Además, los avances en la tecnología de sensores, como la reducción de su tamaño y el aumento de su eficiencia energética, han sido claves para expandir el alcance del IoT a diferentes campos como la salud, la agricultura y la gestión de ciudades inteligentes.

Existen multitud de tipos de sensores, que abarcan desde los más básicos hasta los más avanzados. Los criterios para clasificarlos pueden variar si nos centramos en sus características técnicas, el método utilizado para convertir las señales, el material con el que están fabricados, el tipo de fenómeno físico que son capaces de percibir, las características específicas que miden y el área o sector donde son usados.

Una posible clasificación sería la siguiente [12]:

- **Sensores de temperatura:** estos detectan y miden cambios en la temperatura. Ejemplos comunes son los termopares y los termistores.
- **Sensores de presión:** miden la presión de gases o líquidos. Incluyen sensores piezoeléctricos y sensores de presión de membrana.
- **Sensores de flujo:** utilizados para medir la velocidad de flujo de un líquido o gas. Ejemplos son los medidores de flujo de turbina y los medidores de flujo volumétrico.
- **Sensores de nivel:** estos sensores determinan el nivel de un líquido o sólido en un contenedor, como los sensores de flotador o los sensores capacitivos de nivel.
- **Sensores de imágenes:** cámaras digitales, máquinas de imagen médica y dispositivos de visión nocturna usan este tipo de sensores. Éstos capturan información de imagen al recoger y transformar las variaciones en la atenuación de las ondas en señales.
- **Sensores de ruido:** detectan y miden niveles de sonido. Los micrófonos son un ejemplo común.

- **Sensores del nivel de polución ambiental:** diseñados para detectar contaminantes en el aire, como los sensores de gases y partículas.
- **Sensores de proximidad:** detectan la presencia o ausencia de un objeto cercano sin contacto físico. Ejemplos incluyen sensores ultrasónicos y sensores capacitivos.
- **Sensores infrarrojos:** utilizados para detectar y medir radiación infrarroja, a menudo utilizados en sistemas de control remoto y sensores de movimiento.
- **Sensores de humedad:** miden la humedad del aire o de otros gases. Los higrómetros y los sensores de humedad capacitivos son ejemplos típicos.
- **Sensores de velocidad:** estos sensores se utilizan para medir la velocidad de un objeto, como los sensores Doppler y los anemómetros en aplicaciones de velocidad del viento.

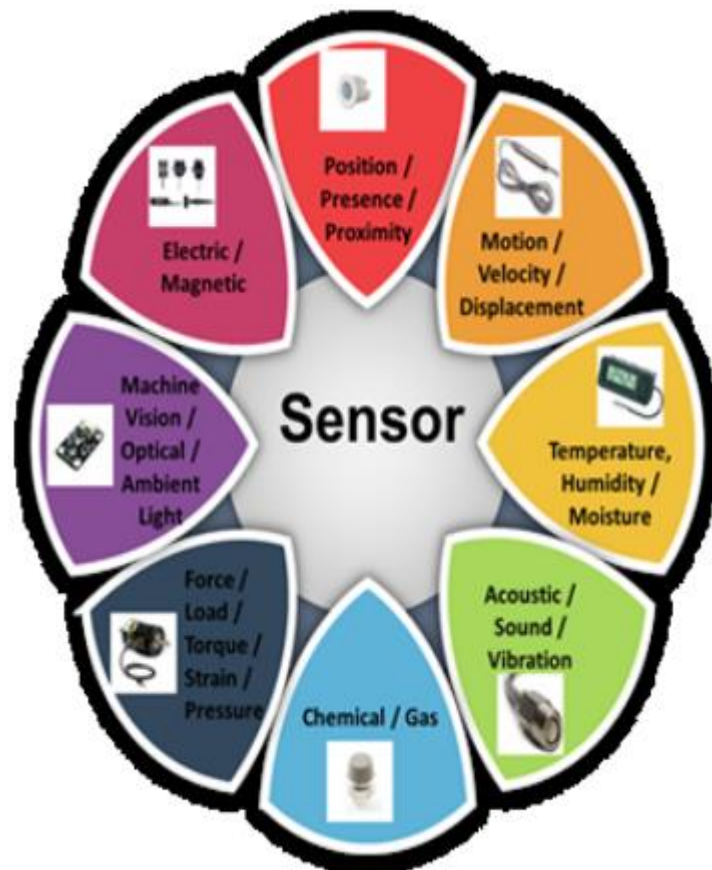


Figura 2-4 Diferentes tipos de sensores en IoT [13]

Estos dispositivos son fundamentales para la recopilación de datos que impulsan el IoT. Su variedad, precisión y capacidad de adaptación a diferentes aplicaciones permiten que esta tecnología se integre de manera efectiva en números aspectos de la vida cotidiana y sectores industriales.

2.1.3 Principales desafíos

El Internet de las Cosas está transformando desde la vida cotidiana hasta industrias enteras con su capacidad para conectar y automatizar innumerables dispositivos y sistemas. Sin embargo, este avance trae consigo desafíos significativos que son cruciales para el desarrollo sostenible y seguro de esta tecnología. Estos desafíos abarcan desde la seguridad de los datos y la privacidad hasta la escalabilidad y la interoperabilidad de los sistemas, cada uno representando una faceta importante que necesita ser abordada para aprovechar plenamente el potencial del IoT.

Los desafíos actuales se resumen a continuación [14]:

- **Seguridad y privacidad:** Éste es uno de los desafíos más apremiantes en el ámbito del IoT. A medida que el número de dispositivos que se conecta a internet crece, recopilando y transmitiendo datos sensibles, surge la necesidad de proteger estos dispositivos y la información que manejan contra amenazas cibernéticas. La variedad de dispositivos y la amplitud de su aplicación en distintos entornos complican aún más la tarea de implementar medidas de seguridad estandarizadas. Además, la privacidad de los usuarios se ve desafiada por la recopilación masiva de datos personales, lo que plantea importantes preguntas sobre el uso y la gestión de esta información. Por lo tanto, abordar la seguridad y la privacidad en el IoT no es solo una cuestión técnica, sino también una de gobernanza y ética, requiriendo un enfoque holístico que incluya tecnología, regulaciones y conciencia del usuario.
- **Interoperabilidad y estándares:** Debido a la diversidad de dispositivos y protocolos existentes, la interoperabilidad supone un desafío crítico. La integración de una amplia gama de terminales, desde sensores simples hasta sistemas complejos, se ve obstaculizada por el uso de diferentes tecnologías y protocolos de comunicación, lo que resulta en problemas de compatibilidad. Esto se complica aún más por la falta de estándares universales, lo que dificulta la integración y el análisis de datos a gran escala. La solución a este desafío radica en el desarrollo y adopción de estándares universales que permitan la comunicación fluida entre dispositivos, faciliten la gestión de datos y mejoren la funcionalidad y eficiencia de los sistemas IoT. Sin embargo, lograr un consenso entre fabricantes, desarrolladores y organismos reguladores sigue siendo un obstáculo importante, ya que cada parte tiene sus propias prioridades y requisitos.
- **Legislación y regulación:** La incorporación de dispositivos IoT en diversos aspectos de la vida cotidiana y la industria plantea cuestiones críticas sobre la privacidad de los datos y la seguridad cibernética. Estos dispositivos recopilan, transmiten y almacenan grandes volúmenes de datos, algunos de los cuales pueden ser sensibles o personales. Por lo tanto, es esencial desarrollar marcos legales robustos que no solo protejan la privacidad del usuario y aseguren la integridad de los datos, sino que también establezcan normas claras para el manejo y uso responsable de esta información. Además, con la variedad de dispositivos y la globalización del IoT, se hace imprescindible armonizar las regulaciones a nivel mundial para asegurar la compatibilidad y seguridad en las redes de IoT.
- **Escalabilidad:** Desafío fundamental que abarca la capacidad de los sistemas y redes para adaptarse y manejar eficientemente un creciente número de dispositivos conectados. Como vimos en la figura 2-2, se espera que miles de millones de dispositivos estén interconectados, generando enormes volúmenes de datos. Este aumento masivo plantea serias preocupaciones sobre la capacidad de las infraestructuras actuales para soportar tal carga, tanto en términos de procesamiento de datos como de ancho de banda de la red. Igualmente, a medida que aumenta el número de dispositivos, también lo hace la complejidad en la gestión y mantenimiento de estos sistemas. Es esencial implementar soluciones que puedan escalar dinámicamente para acomodar este crecimiento, manteniendo al mismo tiempo altos estándares de rendimiento, seguridad y confiabilidad. La adopción de tecnologías como la computación perimetral, así como el desarrollo de nuevos protocolos de comunicación y arquitecturas de red más eficientes, son pasos clave

para abordar el desafío de escalabilidad en el IoT como veremos a lo largo de esta memoria.

- **Gestión y análisis de datos masivos:** Este desafío se centra en la interacción entre dispositivos como sensores y actuadores y los datos que producen. La convergencia del IoT con el Big Data es clave en este contexto, requiriendo no solo métodos eficientes para almacenar y procesar datos, sino también técnicas avanzadas para su interpretación. Esto implica emplear análisis de datos y aprendizaje automático, manteniendo la seguridad y privacidad, y abordando la variedad y velocidad de los datos generados en tiempo real por una red de dispositivos conectados en continua expansión.
- **Consumo energético y sostenibilidad:** Cada dispositivo, desde sensores hasta sistemas más complejos, requiere energía para funcionar, lo que lleva a un aumento significativo en el consumo global de energía. Este aumento plantea preocupaciones sobre la huella de carbono y la sostenibilidad a largo plazo del IoT. Para abordar este desafío, es esencial desarrollar dispositivos IoT más eficientes energéticamente y explorar fuentes de energía renovables y sostenibles. También es vital implementar algoritmos y tecnologías que reduzcan el consumo energético, como lo es la computación perimetral, que procesa datos localmente y disminuye la cantidad de datos que deben enviarse a través de la red, reduciendo así el consumo de energía. Además, la optimización del ciclo de vida de los dispositivos IoT, incluyendo el reciclaje y la gestión de residuos, es fundamental para minimizar el impacto ambiental. En conjunto, estos esfuerzos contribuyen a un ecosistema de IoT más sostenible y ambientalmente responsable.

2.2 Estado del arte de la Computación Perimetral

2.2.1 Introducción

La computación perimetral o Edge Computing representa un cambio paradigmático en el procesamiento y análisis de datos, donde estas tareas se realizan cerca del lugar donde se generan los datos, en lugar de en un centro de datos centralizado o en la nube (Cloud Computing). Esta aproximación implica llevar la capacidad computacional y de almacenamiento directamente al "borde" de la red, es decir, más cerca de dispositivos IoT, sensores y usuarios finales. Esta tecnología es esencial en el contexto del Internet de las Cosas, ya que permite una respuesta más rápida y reduce la latencia al procesar datos en el lugar donde se generan.

La importancia del Edge Computing en el IoT es multifacética. Al procesar datos en el borde, se mejora significativamente la eficiencia en el uso del ancho de banda, se reduce la congestión en la red y se minimiza la dependencia de conexiones a la nube constantes y de alta velocidad. Esto es particularmente crucial en aplicaciones donde la toma de decisiones en tiempo real es fundamental, como en el monitoreo de la salud, la gestión de infraestructuras críticas y la automatización industrial. Además, la computación perimetral puede mejorar la seguridad y la privacidad de los datos al limitar la transmisión de información sensible a través de la red y permitir un control más localizado sobre estos datos.

El concepto de Edge Computing se originó a finales de los años 90 [15], inicialmente con la introducción de las redes de entrega de contenido (Content Delivery Networks, CDN) por Akamai, destinadas a acelerar el rendimiento web [16]. Estas CDNs utilizaban nodos en el borde de la red, cerca de los usuarios, para precargar y almacenar en caché contenido web, e incluso personalizarlo,

como añadir publicidad relevante para la ubicación. Este enfoque era especialmente valioso para el contenido de video, donde el ahorro de ancho de banda debido al almacenamiento en caché era sustancial. El Edge Computing generalizó y extendió el concepto de CDN al aprovechar la infraestructura de computación en la nube, permitiendo que los cloudlets (centros de datos en nube a pequeña escala, mejorados en movilidad y ubicados en el borde de la red) cercanos a los usuarios no solo almacenaran contenido web, sino que también ejecutaran código arbitrario, típicamente encapsulado en una máquina virtual o contenedor.

En 1997, Brian Noble demostró el potencial del Edge Computing para la informática móvil, mostrando cómo el reconocimiento de voz podría implementarse en dispositivos móviles con recursos limitados trasladando la computación a un servidor cercano [17]. Más tarde, con la irrupción de la computación en la nube a mediados de los 2000, esta se convirtió en la infraestructura más utilizada para aprovechar desde un dispositivo móvil, como se ve en servicios como Siri de Apple y el reconocimiento de voz de Google.

Sin embargo, la dependencia de un centro de datos en la nube no es aconsejable para aplicaciones que requieren un control estricto del retardo de extremo a extremo. El concepto de Edge Computing aboga por una arquitectura de dos niveles: la infraestructura de nube existente y una segunda capa de elementos dispersos llamados cloudlets.

En 2012, Flavio Bonomi introdujo el término "Fog Computing" para referirse a esta infraestructura de nube dispersa, enfocándose en la escalabilidad de la infraestructura de IoT en lugar del rendimiento interactivo de las aplicaciones móviles [18].

2.2.2 Comparativa con la Computación en la Nube

Antes de adentrarnos en hacer una comparativa con el Edge Computing, es esencial comprender qué es la Computación en la Nube. El Cloud Computing es un modelo de computación que permite el acceso a recursos de computación (como servidores, almacenamiento, bases de datos, redes, software) a través de Internet, conocido como 'la nube'. Este modelo se caracteriza por su capacidad para ofrecer una gran potencia de procesamiento y almacenamiento de datos, escalabilidad y flexibilidad, sin que el usuario final necesite poseer la infraestructura física. En el Cloud Computing, los datos se procesan y almacenan en centros de datos remotos, gestionados por proveedores de servicios, lo que facilita el acceso a recursos computacionales desde cualquier lugar y en cualquier momento.

El Cloud Computing es ideal para aplicaciones que requieren un procesamiento intensivo de datos, análisis complejos y almacenamiento a gran escala. Este modelo también proporciona beneficios significativos en términos de eficiencia de costes, ya que los usuarios pueden pagar únicamente por los recursos que utilizan. Además, ofrece diversos tipos de servicios como Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como Servicio (IaaS), cada uno proporcionando diferentes niveles de control, flexibilidad y gestión. En SaaS, los usuarios acceden a aplicaciones de software a través de la nube; en PaaS, los desarrolladores utilizan herramientas y plataformas hospedadas para crear aplicaciones; y en IaaS, los usuarios tienen acceso a recursos de computación fundamentales como servidores y almacenamiento. La gestión y el mantenimiento de toda esta infraestructura corren a cargo de los proveedores del servicio [19].

A partir de esta base, podemos comenzar a explorar cómo el Edge Computing se diferencia y complementa al Cloud Computing, especialmente en el contexto del Internet de las Cosas, donde la ubicación del procesamiento de datos y la latencia son aspectos críticos. Mientras la computación en la nube centraliza los recursos, la computación perimetral o en el borde, los distribuye, acercando el

procesamiento de datos a donde se generan, lo que resulta en una reducción de la latencia y una respuesta más rápida a las necesidades de procesamiento en tiempo real.

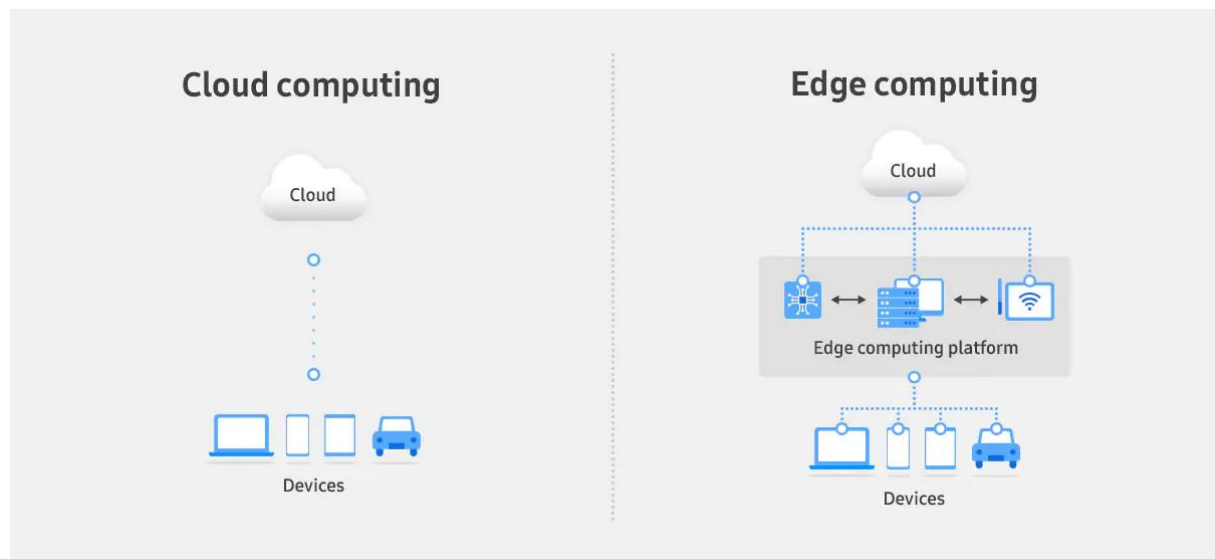


Figura 2-5 Comparativa visual Cloud computing vs Edge computing [20]

2.2.2.1 Ubicación del procesamiento de datos

Una de las distinciones fundamentales entre el Cloud Computing y el Edge Computing es dónde se realiza el procesamiento de los datos, determinando sus aplicaciones, eficiencias y limitaciones.

En el Cloud Computing, éste se lleva a cabo en centros de datos remotos, a menudo ubicados a grandes distancias de los usuarios finales y dispositivos. Esta centralización ofrece una poderosa capacidad de cómputo y almacenamiento masivo, permitiendo manejar grandes volúmenes de datos y complejas operaciones de análisis. Sin embargo, puede resultar en latencias más altas debido a la distancia física que los datos deben recorrer entre el dispositivo y el centro de datos. Esta característica del Cloud Computing lo hace ideal para aplicaciones no sensibles al tiempo, como el almacenamiento a largo plazo, el análisis de Big Data y las operaciones que no requieren una respuesta inmediata.

Por otro lado, el Edge Computing coloca recursos de análisis y almacenamiento más cerca de donde se originan los datos, es decir, en el "borde" de la red. Esto puede significar integrar capacidad de procesamiento en dispositivos IoT, en estaciones base de telecomunicaciones o en servidores localizados en un sitio específico, como fábricas u hospitales. Al realizar el procesamiento de datos cerca de la fuente, el Edge Computing reduce significativamente la latencia, facilitando respuestas en tiempo real.

2.2.2.2 Latencia y ancho de banda

La computación en la nube tiene una fuerte dependencia de centros de datos remotos para el procesamiento de datos, lo que conlleva desafíos relacionados con el ancho de banda. El envío de grandes volúmenes de datos a través de largas distancias puede resultar en un uso intensivo éste, lo que, a su vez, puede provocar congestiones en la red. Esta situación es particularmente notable cuando muchos dispositivos transmiten datos simultáneamente, una circunstancia común en aplicaciones IoT. A pesar de las mejoras en la infraestructura de red, los picos de tráfico pesado pueden llevar a un

rendimiento reducido, lo cual es un factor a considerar especialmente en aplicaciones que dependen de la rápida transmisión y procesamiento de datos.

La computación perimetral sin embargo aborda estas preocupaciones de una manera más eficiente. Al procesar los datos localmente, cerca de donde se generan, reduce drásticamente la necesidad de transmitir grandes cantidades de información a través de la red hasta la nube. Esta proximidad no solo alivia la carga sobre el ancho de banda, sino que también minimiza los cuellos de botella potenciales, mejorando significativamente la eficiencia en el uso de los recursos de red. Además, la reducción en la distancia de transmisión de datos conlleva una disminución notable en la latencia. Esta ventaja es crucial para aplicaciones que requieren una toma de decisiones rápidas, como por ejemplo en situaciones de operaciones militares.

2.2.2.3 Escalabilidad

Aunque el Edge Computing ofrece ventajas significativas en términos de latencia y procesamiento local de datos, en el aspecto de escalabilidad, el modelo de Cloud Computing frecuentemente lleva la delantera. La computación en la nube permite una expansión de recursos casi ilimitada y dinámica, facilitando un rápido escalado para satisfacer la demanda sin la necesidad de invertir en infraestructura física adicional. Esta flexibilidad lo hace ideal para aplicaciones que experimentan fluctuaciones en el uso o que necesitan escalar rápidamente.

En contraste, aunque el Edge Computing puede ser escalable en cierto sentido, su enfoque en el procesamiento localizado implica que el escalado a menudo requiere la implementación de hardware adicional en el sitio. Esto puede aumentar la complejidad y los costos asociados con la expansión, así como las necesidades de mantenimiento. Cada nodo de Edge debe ser mantenido y gestionado, lo que puede representar un desafío logístico en entornos con numerosos dispositivos distribuidos.

2.2.2.4 Costes, mantenimiento y eficiencia energética

En términos de costes, el Cloud Computing destaca por su modelo de pago por uso, lo que permite a las organizaciones pagar solo por los recursos que consumen. Esta flexibilidad resulta en una reducción significativa de los costes iniciales, ya que elimina la necesidad de inversiones significativas en hardware y otras infraestructuras de Tecnologías de la Información (TI). Además, al delegar la gestión de la infraestructura a los proveedores de servicios en la nube, las empresas pueden reducir sus gastos operativos y de capital.

Por otro lado, el Edge Computing puede implicar un coste inicial más alto debido a la necesidad de instalar y configurar hardware en el sitio. Aunque este enfoque puede conducir a ahorros a largo plazo en términos de ancho de banda y eficiencia operativa, el gasto en mantenimiento puede ser más elevado. Cada dispositivo Edge debe ser mantenido, actualizado y, en algunos casos, reparado, lo que puede resultar en costes más altos en comparación con un modelo de nube centralizado.

En cuanto al mantenimiento, el Cloud Computing ofrece una ventaja fundamental. Al centralizar los recursos, el mantenimiento y la actualización de sistemas se simplifican, ya que se manejan de forma remota por el proveedor de servicios. Esto contrasta con el Edge Computing, donde el sostenimiento de múltiples dispositivos distribuidos puede ser más complejo y laborioso.

Respecto a eficiencia energética, la computación en el borde destaca por su menor consumo de energía. Al procesar datos localmente, se reduce la cantidad de datos que deben enviarse a través de la red, lo que resulta en un mayor ahorro de energía. Sin embargo, esta eficiencia debe equilibrarse con el consumo energético de los dispositivos Edge individuales. En comparación, los centros de datos utilizados en el Cloud Computing suelen ser altamente eficientes desde el punto de vista energético, aunque el costo energético total puede ser más elevado debido a la gran escala de operaciones.

2.2.2.5 Seguridad y privacidad de los datos

La seguridad y privacidad de los datos son aspectos fundamentales tanto en Cloud Computing como en Edge Computing, cada uno con sus propios desafíos y enfoques para garantizar la protección de la información.

En el Cloud Computing, los datos se almacenan y procesan en centros de datos remotos, lo que plantea desafíos únicos en términos de seguridad y privacidad. La centralización de grandes cantidades de datos en un solo lugar puede hacer que estos centros de datos sean objetivos atractivos para ataques cibernéticos. Por lo tanto, los proveedores de servicios en la nube invierten cuantiosamente en medidas de seguridad avanzadas, como encriptación de datos, sistemas de autenticación robustos y protección contra ataques cibernéticos. Además, la privacidad de los datos es una preocupación clave, ya que las leyes y regulaciones, como el GDPR en Europa, imponen estrictas normas sobre el manejo de datos personales, obligando a los proveedores de la nube a adoptar políticas de privacidad rigurosas.

El Edge Computing en cambio distribuye el procesamiento y el almacenamiento de datos a través de numerosos dispositivos en el borde de la red, lo que puede complicar la gestión de la seguridad y la privacidad. Si bien la dispersión de los datos puede reducir el riesgo de ataques masivos, cada dispositivo Edge se convierte en un potencial punto vulnerable. Esto requiere un enfoque de seguridad que sea tanto robusto como distribuido, con medidas como la encriptación de datos en el dispositivo, seguridad de red mejorada y actualizaciones regulares de software para proteger contra vulnerabilidades emergentes. Además, la computación perimetral a menudo procesa datos sensibles y personales en tiempo real, lo que aumenta la importancia de cumplir con las normativas de privacidad y garantizar que la recopilación y el uso de datos se realicen de manera ética y legal.

2.2.2.6 Casos de uso

El Cloud Computing y el Edge Computing ofrecen soluciones distintas y complementarias, cada una adecuada para diferentes tipos de aplicaciones y escenarios. Generalmente, el Cloud Computing es más adecuado para situaciones que requieren un gran poder de procesamiento y almacenamiento, donde la latencia no es un factor crítico. Por su parte, el Edge Computing es preferible en escenarios donde la respuesta rápida y el procesamiento local de datos son esenciales [21].

Situaciones ideales para la Computación en la Nube:

- El Cloud Computing brilla en escenarios donde se manejan grandes volúmenes de datos que requieren un procesamiento intensivo, como en el análisis de Big Data. Aquí, su capacidad para almacenar y analizar enormes conjuntos de datos es sobresaliente.
- En aplicaciones que necesitan una amplia gama de recursos computacionales, como SaaS, plataformas de desarrollo e infraestructuras, el Cloud Computing ofrece la flexibilidad y escalabilidad necesarias.
- Para la recuperación de desastres y el respaldo de datos, su capacidad y robustez lo hacen una opción segura y confiable.

Situaciones ideales para la Computación en el borde:

- En el ámbito del IoT, especialmente en la automatización industrial, el Edge Computing es crucial. Su capacidad para procesar datos en tiempo real facilita la toma de decisiones instantánea, esencial en la fabricación y monitorización automatizada.
- Para aplicaciones sensibles al tiempo, como los vehículos autónomos y los sistemas de gestión de ciudades inteligentes, el Edge Computing proporciona la baja latencia necesaria para respuestas rápidas y eficientes.
- En el sector de la salud, especialmente en el monitoreo en tiempo real de pacientes, el Edge Computing mejora significativamente la calidad de la atención al paciente, proporcionando datos críticos de manera instantánea.
- En el ámbito de la Defensa, donde la velocidad de respuesta y la seguridad de los datos son críticas, el Edge Computing permite el procesamiento de datos en tiempo real para aplicaciones como el monitoreo táctico, la vigilancia mediante drones y la comunicación segura en el campo de batalla.

2.2.3 Principales desafíos

Tras explorar la evolución histórica del Edge Computing y su comparativa con el Cloud Computing, es esencial abordar los desafíos que enfrenta esta tecnología emergente. Aunque el Edge Computing ofrece numerosas ventajas, como la reducción de la latencia y una mejor gestión del ancho de banda, existen varios obstáculos que aún deben superarse para su implementación efectiva y su integración en el ecosistema tecnológico actual.

Los principales desafíos a los que se enfrenta la computación perimetral son los siguientes [22]:

- **Confianza del usuario:** Ganar la confianza del usuario en sistemas de Edge Computing es un desafío crítico que juega un papel vital en la adopción y eficacia de esta tecnología emergente. Esta confianza es esencial debido a su naturaleza distribuida, que implica el procesamiento y almacenamiento de datos en dispositivos ubicados físicamente cerca del usuario final, a menudo en entornos menos seguros que los centros de datos tradicionales. La principal preocupación para los usuarios radica en la seguridad de sus datos. Dado que el Edge Computing maneja información potencialmente sensible directamente en el borde de la red, los riesgos de brechas de seguridad y accesos no autorizados son significativos. Por lo tanto, es crucial implementar medidas de seguridad robustas, como encriptación avanzada y autenticaciones fuertes, para proteger los datos y generar confianza en los usuarios. Además de la seguridad, la fiabilidad y la consistencia en el rendimiento de los sistemas de Edge Computing son fundamentales para mantener la confianza del usuario. Esto requiere no solo hardware y redes estables, sino también sistemas capaces de adaptarse y recuperarse rápidamente de fallos. La transparencia en el manejo de los datos y en las operaciones de los sistemas también es vital. Los usuarios deben ser conscientes de

cómo se utilizan sus datos y tener la seguridad de que se cumplen las leyes y regulaciones de privacidad aplicables.

- **Costes:** Aunque esta tecnología ofrece beneficios significativos en términos de latencia y procesamiento de datos, el coste puede suponer una barrera para la adopción del Edge Computing por parte de las organizaciones. Éstas deben tener en cuenta la inversión inicial de implantar la infraestructura de borde, así como los costes de funcionamiento, como el consumo de energía y el mantenimiento.
 - Hardware inicial: La computación perimetral requiere la instalación de hardware adicional en el borde de la red. Estos dispositivos pueden incluir servidores Edge, dispositivos de almacenamiento y otros equipos de red, lo que representa un gasto significativo.
 - Mantenimiento: Una vez desplegados, los dispositivos Edge necesitan mantenimiento regular, que puede incluir actualizaciones de software, reparaciones y reemplazo de hardware. Estos costes pueden aumentar con el tiempo, especialmente en redes extensas y distribuidas.
 - Gestión de red: Asegurar y gestionar una red de dispositivos Edge también conlleva costes. Esto incluye la protección contra ciberataques, la gestión de la seguridad de los datos y el monitoreo continuo de la red.
 - Integración: Integrar tecnología de Edge Computing con sistemas existentes, como infraestructuras de IoT o plataformas en la nube, puede requerir inversiones adicionales en desarrollo de software y adaptaciones de sistemas.
- **Eficiencia energética:** En el Edge Computing, la energía necesaria para operar una amplia gama de dispositivos en el borde de la red puede acumularse significativamente, sobre todo en aplicaciones a gran escala con numerosos dispositivos funcionando simultáneamente. Esta situación se complica aún más en entornos remotos o de difícil acceso, donde la eficiencia energética es vital para la longevidad y la fiabilidad de los dispositivos, muchos de los cuales dependen de baterías o fuentes de energía limitadas. El consumo total de energía en tales escenarios, sumado a la necesidad de mantener operaciones continuas y eficientes, pone de relieve la importancia de gestionar eficazmente el consumo energético. En respuesta a este desafío, se están desarrollando varias soluciones orientadas a mejorar la eficiencia energética en la computación perimetral. Estas incluyen la optimización del hardware, con el diseño de dispositivos que ofrezcan un mejor rendimiento, y la implementación de sistemas de gestión de energía avanzados capaces de ajustar el consumo de energía en función de las necesidades de procesamiento. Además, se están explorando tecnologías de enfriamiento más eficientes para dispositivos Edge, particularmente en entornos con condiciones extremas [23] [24]. La optimización del software también juega un papel crucial, mediante el uso de algoritmos que procesan los datos de manera más eficiente, reduciendo así la carga de trabajo y el consumo energético de los dispositivos. Finalmente, la integración de fuentes de energía renovable, como paneles solares o turbinas eólicas, está ganando terreno como una solución sostenible y a largo plazo para alimentar infraestructuras de Edge Computing. Estas medidas no solo

abordan los desafíos actuales de eficiencia energética, sino que también contribuyen a la sostenibilidad y viabilidad a largo plazo de esta tecnología.

- **Seguridad:** Un aspecto crítico de este desafío es la vulnerabilidad inherente de los dispositivos Edge a una variedad de ataques cibernéticos. A diferencia de los potentes servidores de nube, los dispositivos Edge suelen tener una menor capacidad de cómputo y, por lo tanto, sistemas de defensa más frágiles. Esto los hace susceptibles a ataques que podrían no ser efectivos contra servidores más robustos. Además, muchos dispositivos de IoT que forman parte del ecosistema de la computación en el borde carecen de interfaces de usuario convencionales, lo que dificulta para los usuarios detectar si un dispositivo ha sido comprometido. La heterogeneidad en los sistemas operativos y protocolos de comunicación de estos dispositivos también añade complejidad a la tarea de diseñar mecanismos de protección unificados y eficaces [25]. Un ejemplo notable de los peligros que enfrenta el Edge Computing es el virus Mirai [26], que en 2016 infectó más de 65,000 dispositivos IoT explotando vulnerabilidades de autenticación débil, y posteriormente utilizó estos dispositivos para lanzar ataques de denegación de servicio distribuido (DDoS) contra servidores Edge, causando daños sustanciales.

3 INTEGRACIÓN DEL IoT CON EDGE COMPUTING

La integración del Internet de las Cosas con la Computación Perimetral representa un avance significativo en el mundo de la tecnología, marcando una evolución en la forma en que recopilamos, procesamos y utilizamos datos en un amplio espectro de aplicaciones. Esta convergencia entre IoT y Edge Computing no es solo una mejora en términos de eficiencia y velocidad, sino un cambio fundamental en la arquitectura de los sistemas de TI, con un potencial transformador para innumerables sectores.

En esta integración, el IoT actúa como la fuente de una inmensa cantidad de datos generados por una multitud de dispositivos y sensores interconectados, desplegados desde entornos domésticos hasta en complejos industriales. Por otro lado, el Edge Computing lleva la capacidad de procesamiento y análisis de datos más cerca de estos dispositivos IoT, reduciendo así la latencia y mejorando la respuesta en tiempo real. Este acercamiento del procesamiento de datos al origen donde se generan es lo que distingue a la integración IoT-Edge de las arquitecturas de TI tradicionales, donde los datos se envían a servidores remotos o a la nube para su procesamiento.

La relevancia de esta integración va más allá de la mera eficiencia operativa. Al procesar los datos localmente, en el borde, se pueden tomar decisiones más rápidas y contextuales, lo que es crucial en aplicaciones donde el tiempo de respuesta es crítico, como en la gestión de emergencias y respuestas a desastres, en sistemas de transporte inteligentes o en el ámbito de la seguridad pública y vigilancia. Además, esta aproximación contribuye a una mayor seguridad y privacidad de los datos, ya que reduce la necesidad de transmitir información sensible a través de la red.

A la hora de la integración de IoT con Edge Computing se requiere de un marco legal para garantizar su implementación sostenible y segura que presentamos a continuación.

3.1 Marco legal y regulatorio

En el núcleo de la importancia del marco legal en IoT está la protección de datos personales. Con una cantidad enorme de información recopilada por dispositivos en línea, es crucial garantizar que estos datos sean manejados con respeto a la privacidad y el consentimiento de los usuarios. Las regulaciones como el GDPR (Reglamento General de Protección de Datos) en Europa son ejemplos de cómo los marcos legales buscan equilibrar la innovación tecnológica con los derechos individuales, estableciendo límites y obligaciones en la recopilación y uso de datos personales.

De igual manera, la seguridad cibernética es una preocupación primordial en el IoT. A medida que más dispositivos se integran en nuestra vida diaria, las vulnerabilidades a ataques cibernéticos y fallos técnicos aumentan. Es en este punto donde el marco legal juega un papel esencial en definir y exigir estándares de seguridad robustos, obligando a los fabricantes a considerar la seguridad desde el diseño inicial de los productos. Esto no solo protege la información personal, sino que también salvaguarda infraestructuras críticas que dependen cada vez más de la tecnología IoT.

El marco legal también clarifica la responsabilidad y el cumplimiento en el ecosistema IoT. Determina quién es responsable en caso de fallos de seguridad o mal uso de datos, proporcionando un camino claro para la resolución de disputas y la compensación. Además, fomenta un entorno de confianza, esencial para la adopción y el éxito a largo plazo de las tecnologías IoT.

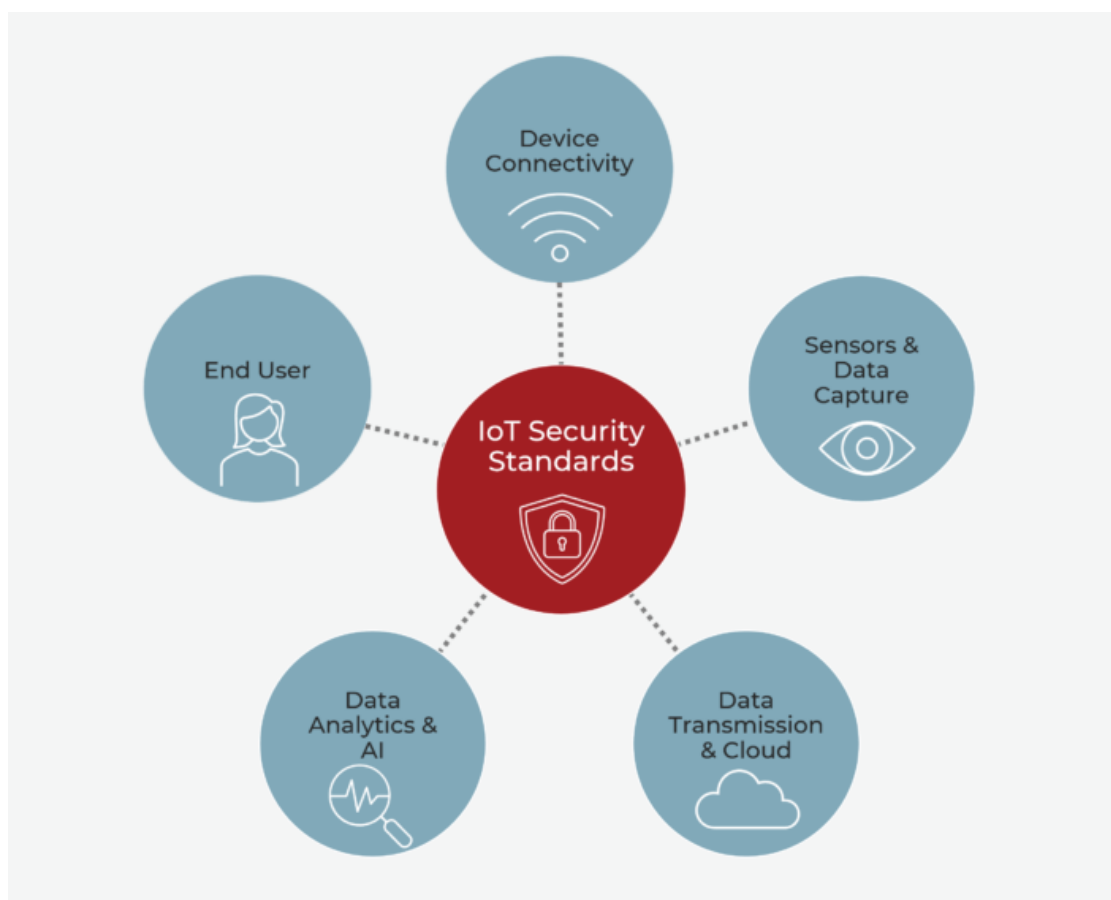


Figura 3-1 Protección integral desde sensores hasta usuarios [27]

3.1.1 Regulaciones actuales

En el ámbito IoT, las regulaciones varían significativamente entre diferentes regiones, reflejando distintos enfoques y prioridades. A continuación, se detallan algunos casos:

- **Reglamento General de Protección de Datos (GDPR)** en Europa [28]: Esta regulación ha establecido un nuevo estándar en la protección de datos personales. Es particularmente

relevante para IoT, ya que impone estrictas reglas sobre la recopilación, almacenamiento y procesamiento de datos personales. El GDPR exige que las empresas obtengan consentimiento explícito para recopilar datos personales y les otorga a los individuos un mayor control sobre su información, incluyendo el derecho a ser olvidados.

- **Leyes de Privacidad en Estados Unidos:** La regulación del IoT está más fragmentada en los EE. UU., con leyes específicas en algunos estados, como la **Ley de Privacidad del Consumidor de California (CCPA)** [29]. A nivel federal, la Comisión Federal de Comercio (FTC) ha sido un actor clave en la protección de la privacidad y la seguridad en el IoT, ofreciendo directrices y tomando medidas contra prácticas desleales o engañosas [30].
- En países asiáticos como China el enfoque regulatorio del IoT también difiere. China está avanzando rápidamente en el desarrollo del IoT con fuerte apoyo gubernamental, pero también enfrenta desafíos en cuanto a normas y regulaciones, particularmente en relación con la seguridad de los datos y la privacidad. En concreto, la **Ley de Protección de la Información Personal (PIPL)** de China [31], en vigor desde noviembre de 2021, es una legislación integral destinada a regular la recopilación, uso, procesamiento y transferencia de datos personales. Inspirada en el Reglamento General de Protección de Datos (GDPR) de la UE, la PIPL exige consentimiento explícito para el manejo de datos personales, impone restricciones en la transferencia de datos fuera de China, y proporciona a los individuos amplios derechos sobre sus datos personales. Con estrictas sanciones por incumplimiento, la PIPL representa un paso significativo en la protección de la privacidad y los datos personales en China.

3.1.2 Normas y Estándares internacionales

Las normas y estándares internacionales facilitan la cohesión y compatibilidad en el amplio espectro de tecnologías y aplicaciones del IoT. Establecen criterios uniformes que ayudan a los fabricantes y desarrolladores a asegurar que sus productos y soluciones sean seguros, fiables y capaces de integrarse con otros sistemas y dispositivos a nivel mundial.

Las organizaciones más importantes en la formulación de normas y estándares son las siguientes:

- **ISO** (Organización Internacional de Normalización) y **IEC** (Comisión Electrotécnica Internacional): Trabajan conjuntamente en la creación de estándares internacionales para el IoT, abarcando áreas como seguridad de datos, interoperabilidad y calidad de servicio.
- **IEEE** (Instituto de Ingenieros Eléctricos y Electrónicos): Esencial en el desarrollo de estándares para la tecnología de comunicaciones y redes, fundamentales para la infraestructura del IoT.
- **ITU** (Unión Internacional de Telecomunicaciones): Centra sus esfuerzos en estándares de telecomunicaciones y radiocomunicación, cruciales para la conectividad en el IoT.

Algunos de los estándares más relevantes y de aplicación en el ámbito del Internet de las Cosas son los siguientes:

- **ISO/IEC 30141:2018:** norma internacional que proporciona un marco de referencia arquitectónico para el Internet de las Cosas. Esta norma establece principios y modelos generales para guiar el diseño, implementación y gestión de sistemas IoT. Su objetivo principal es asegurar la interoperabilidad, seguridad, fiabilidad y eficiencia en la implementación de soluciones IoT. Esta ISO/IEC aborda aspectos como la definición de términos clave, la identificación de funciones críticas y la especificación de arquitecturas típicas, facilitando un enfoque coherente y sistematizado para el desarrollo de tecnologías IoT en diversos sectores [32].
- **ISO/IEC 27400:2022:** Esta norma establece directrices sobre la gestión de riesgos de ciberseguridad y privacidad en soluciones de IoT. Su objetivo es ayudar a las organizaciones a implementar medidas efectivas para proteger la confidencialidad, integridad y disponibilidad de los datos del mundo IoT, al tiempo que garantizan que estas soluciones respeten la privacidad. Aplicable a todas las organizaciones involucradas en el desarrollo, despliegue, operación o uso de dispositivos y aplicaciones de IoT, esta norma cubre todo el ciclo de vida del IoT, enfatizando principios como el enfoque basado en riesgos, la privacidad por diseño y por defecto, la minimización de datos, y la transparencia y responsabilidad. Proporciona un conjunto de controles, incluyendo el control de acceso, cifrado de datos, gestión de vulnerabilidades y respuesta a incidentes, para abordar estos riesgos. Al seguir estas directrices, las organizaciones pueden reducir significativamente los riesgos de ciberseguridad y privacidad, mejorar el cumplimiento con normativas y estándares internacionales, y fortalecer la confianza de clientes, socios y partes interesadas [33].
- **IEEE 802.11:** Este estándar conocido comúnmente como Wi-Fi, es esencial en el ecosistema del Internet de las Cosas por ofrecer una conectividad inalámbrica de alta velocidad y fácil integración con la infraestructura de red existente. Aunque originalmente no fue diseñado para el IoT, se ha convertido en una opción predominante para dispositivos que demandan una alta tasa de transferencia de datos y conexiones estables, tales como dispositivos de entretenimiento en el hogar, sistemas de seguridad, y electrodomésticos inteligentes. Wi-Fi permite a estos dispositivos formar parte de la red IoT sin necesidad de hardware especializado, aprovechando las redes Wi-Fi ya presentes en entornos domésticos y empresariales. Con la evolución del estándar, como se ve en Wi-Fi 6 [34], se están abordando desafíos críticos para el IoT, incluyendo la eficiencia energética y la capacidad de soportar una mayor densidad de dispositivos, lo que optimiza aún más su aplicación en este ámbito.
- **IEEE 802.15.4:** El estándar IEEE 802.15.4 se ha consolidado como una solución clave dentro del mundo IoT por su eficiencia en el consumo energético y su capacidad para operar redes inalámbricas de área personal (WPAN) a distancias cortas. A diferencia de su contraparte más conocida, el IEEE 802.11 o Wi-Fi, que es preferido para aplicaciones que demandan un mayor ancho de banda y alcance, el 802.15.4 brilla en escenarios donde se requiere una larga duración de la batería y transmisiones de baja tasa de datos. Este estándar es particularmente adecuado para sensores y dispositivos de automatización del hogar que se benefician de redes malladas robustas y confiables. Al facilitar la conectividad

en redes densas con numerosos nodos, el IEEE 802.15.4 es fundamental para sistemas de monitoreo y control que operan con limitaciones de energía y que no necesitan la intensidad de datos que Wi-Fi puede proporcionar, ofreciendo así una alternativa optimizada para dispositivos IoT que se integran en el entorno conectado de manera más sutil y eficiente [35].

- **IEEE 802.15.6:** A diferencia de los anteriores, éste es un protocolo de comunicaciones inalámbricas diseñado específicamente para la atención médica y aplicaciones biomédicas dentro del Internet de las Cosas, enfocado en redes de área corporal (Body Area Networks, BAN). Este estándar destaca por su enfoque en la seguridad y el bajo consumo energético, siendo crucial para dispositivos que se colocan sobre o dentro del cuerpo humano y que requieren una transmisión de datos segura y eficiente. En contraste con el IEEE 802.11 que proporciona conectividad inalámbrica de alta velocidad y mayor alcance, y del IEEE 802.15.4 que favorece redes de área personal de bajo consumo energético para dispositivos como sensores domésticos, el 802.15.6 está diseñado para trabajar en proximidad inmediata al cuerpo humano, lo cual implica una consideración especial de la influencia del tejido humano en la señal y la necesidad de minimizar la exposición a la radiación. Este protocolo es esencial para aplicaciones críticas donde la fiabilidad y la precisión de la transmisión de datos son vitales, como en el seguimiento de signos vitales y la administración de medicamentos, asegurando una integración segura y efectiva de la tecnología médica en el entorno conectado de la salud [36].

3.2 Arquitectura

Cuando nos adentramos en el estudio de cómo el Internet de las Cosas y la Computación Perimetral se combinan, es esencial entender los distintos tipos de arquitectura que hacen posible esta unión. Estas estructuras van desde las más sencillas de tres capas hasta otras más complejas de cinco capas. Son el marco que define cómo se conectan los dispositivos, cómo se manejan los datos y cómo se procesa la información. Al aprender sobre estos modelos, no solo vamos a conocer los detalles técnicos, sino también cómo influyen en el rendimiento y la funcionalidad de los sistemas IoT-Edge. Este entendimiento es clave, ya que nos ayuda a diseñar sistemas que sean eficientes y seguros, y que puedan ajustarse a los nuevos desarrollos tecnológicos.

3.2.1 Arquitectura de tres capas

El modelo de tres capas es una de las estructuras arquitectónicas más fundamentales en la integración IoT-Edge Computing. Esta arquitectura simplificada pero eficiente se compone de tres niveles distintos que facilitan la recopilación, procesamiento y análisis de datos [37].

- **Capa de percepción:** Esta es la capa más baja y se compone de sensores y dispositivos IoT que actúan como puntos de recopilación de datos. En esta capa, diversos sensores recogen datos del entorno, como temperatura, movimiento, presión, etc. Estos dispositivos pueden ser desde simples sensores hasta componentes más complejos como cámaras inteligentes o wearables. La función principal de esta capa es detectar, recoger y transmitir datos brutos a

la capa superior. En el contexto del Edge Computing, estos datos a menudo se envían directamente a un dispositivo de borde cercano para su procesamiento inicial.

- **Capa de red:** Esta capa actúa como un puente entre la capa de percepción y la capa de aplicación. Su función principal es facilitar la transmisión segura y eficiente de los datos recogidos. Incluye varias tecnologías de comunicación y protocolos, como WiFi, Bluetooth, Zigbee o LTE, que permiten la transferencia de datos desde los dispositivos de la capa de percepción a los nodos de procesamiento de edge o, en algunos casos, a la nube. Además de la transmisión de datos, esta capa también juega un papel crucial en la seguridad, garantizando que los datos transmitidos estén protegidos contra accesos no autorizados o alteraciones.
- **Capa de aplicación:** Esta es la capa superior y se encarga del procesamiento y análisis de los datos recibidos. En un entorno de Edge Computing, esto implica procesar los datos en nodos de bordes cercanos a los dispositivos IoT. La capa de procesamiento utiliza los datos para realizar diversas funciones, como análisis en tiempo real, toma de decisiones basada en datos, y ejecución de acciones de control a través de los dispositivos IoT. Esta capa puede incluir servidores de borde, plataformas de análisis de datos y aplicaciones de usuario final, todas trabajando juntas para extraer valor de los datos recogidos y generar respuestas rápidas y eficaces.

Este modelo de tres capas es valorado por su simplicidad y eficiencia, permitiendo una clara separación de funciones y facilitando la gestión y el mantenimiento del sistema integrado IoT-Edge. Es especialmente adecuado para aplicaciones donde la rapidez en el procesamiento y la respuesta a los datos es esencial, y donde la gestión eficiente de los recursos es una prioridad.

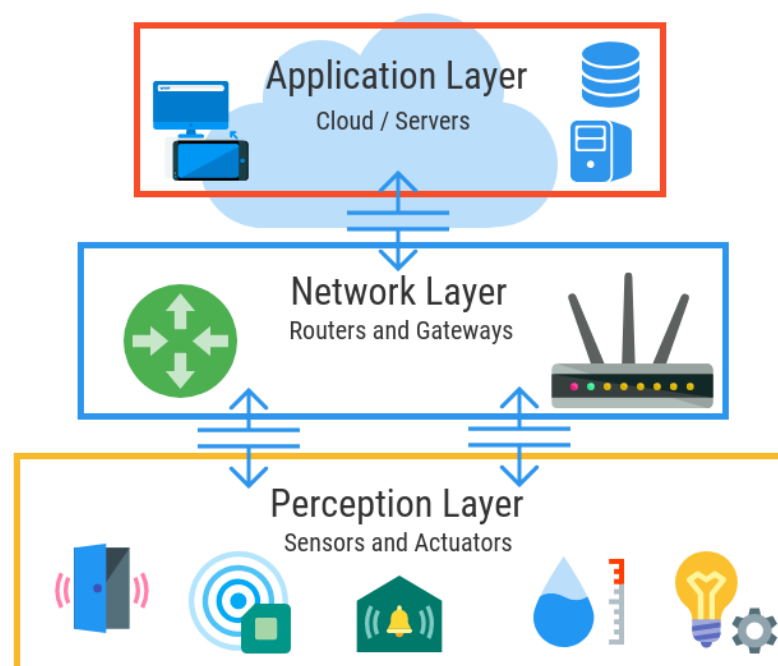


Figura 3-2 Arquitectura básica de tres capas [38]

3.2.2 Arquitectura de cuatro capas

El diseño de cuatro capas en la combinación de IoT con Edge Computing añade una capa extra de servicios situada entre las capas de red y de aplicación. Esta incorporación se realiza en consonancia con los conceptos de la arquitectura orientada a servicios (Service-oriented Architecture, SOA).

En esencia, la arquitectura orientada a servicios se fundamenta en un enfoque de componentes, concebido para enlazar diversas unidades funcionales de aplicaciones mediante el uso de interfaces y protocolos específicos. La finalidad de SOA es coordinar eficazmente los servicios y posibilitar la reutilización tanto de componentes de software como de hardware, facilitando su integración dentro de la arquitectura IoT. Esta integración enriquece la estructura tradicional de tres capas al añadir un nivel adicional entre la capa de red y la de aplicación, conocido como la **capa de servicio**. Dicha capa ofrece apoyo a la capa de aplicación y representa una evolución hacia una arquitectura IoT de cuatro capas basada en SOA.

En esta arquitectura ampliada, nos encontramos con la capa de percepción, seguida por la capa de red, la novedosa capa de servicio y, finalmente, la capa de aplicación. La capa de servicio recién integrada va más allá de las arquitecturas anteriores, incorporando funcionalidades de SOA como el descubrimiento de servicios, que facilita la identificación de requerimientos de servicios; la composición de servicios, que permite la interacción con objetos conectados y la integración eficiente de servicios; la gestión de servicios, encargada de administrar y definir mecanismos de confianza para comprender las solicitudes de servicios; y las interfaces de servicio, diseñadas para soportar la interacción entre todos los servicios ofrecidos [39].

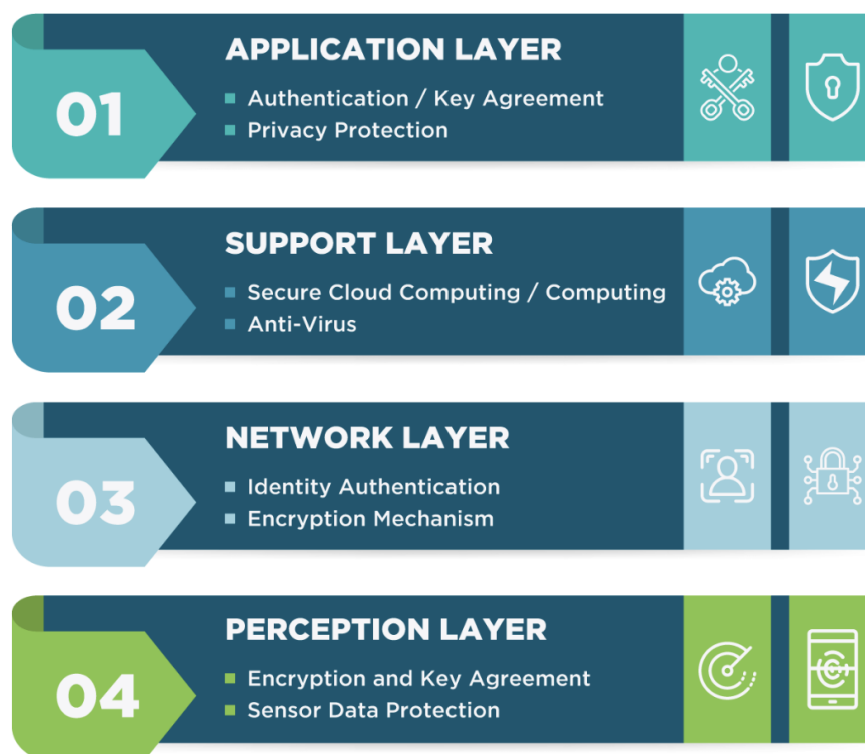


Figura 3-3 Arquitectura básica de cuatro capas [40]

3.2.3 Arquitectura de cinco capas

La arquitectura de cinco capas introduce una dimensión empresarial esencial a través de su quinta y nueva capa, la **capa de negocio**. Esta capa amplía el alcance del modelo tradicional, añadiendo una perspectiva estratégica y operativa clave en el análisis y la gestión de las operaciones de IoT. En esta capa, se realiza un registro y análisis exhaustivo de todas las actividades, aplicando análisis de datos a gran escala que se adhieren rigurosamente a las políticas de cumplimiento y retención de registros. Esta función no solo asegura la eficiencia de las operaciones, sino que también garantiza que estén alineadas con los marcos regulatorios pertinentes.

En la capa de negocio se despliegan modelos avanzados de aprendizaje automático, lo que representa un salto cualitativo para la planificación y desarrollo empresarial. Esta implementación de tecnologías de inteligencia artificial es fundamental para impulsar la innovación y mejorar continuamente las operaciones de IoT. Además, esta capa se encarga de la gestión integral de metadatos y datos de referencia, así como de la administración de las reglas empresariales. Esto se traduce en una supervisión y control eficientes sobre los aspectos operativos de las capas inferiores, asegurando que el sistema funcione de manera coherente y efectiva.

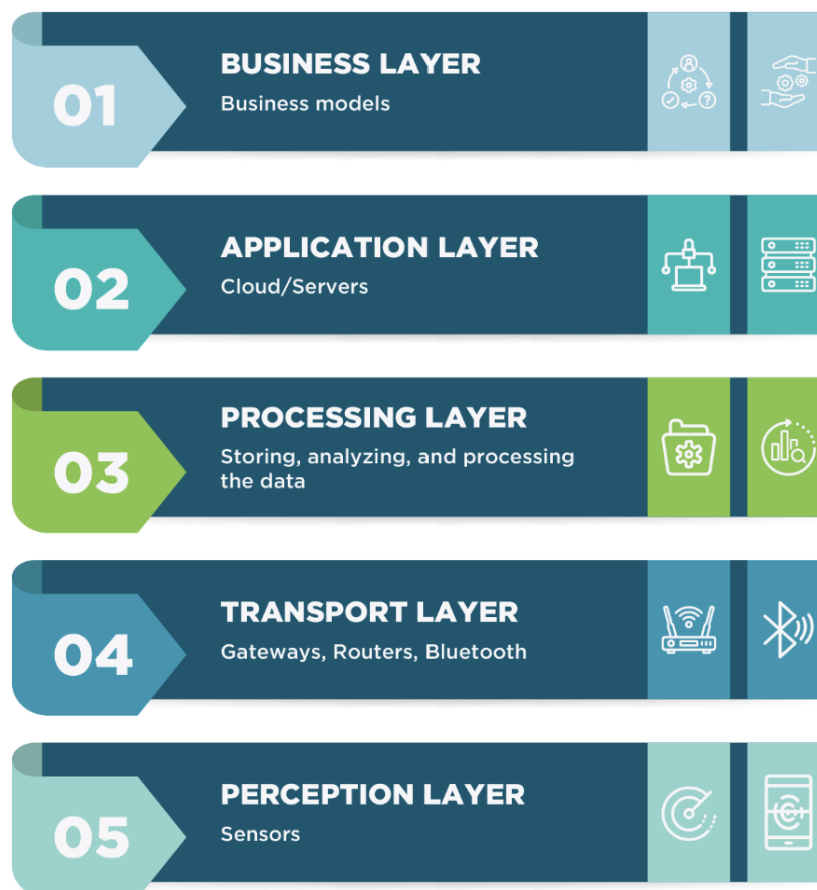


Figura 3-4 Arquitectura básica de cinco capas [40]

La administración del sistema IoT en su totalidad, que abarca desde las aplicaciones hasta los modelos de negocio y la información confidencial de los usuarios, recae también en esta capa. Esto implica un enfoque holístico que cubre todos los elementos del ecosistema de IoT, garantizando así una gestión y un funcionamiento eficientes a nivel global.

La interacción con la arquitectura orientada a servicios en esta capa facilita la creación de sistemas que soportan la generación de soluciones empresariales independientes de las restricciones tecnológicas, lo que es vital para la adaptabilidad y sostenibilidad de los negocios en el ámbito de IoT [41].

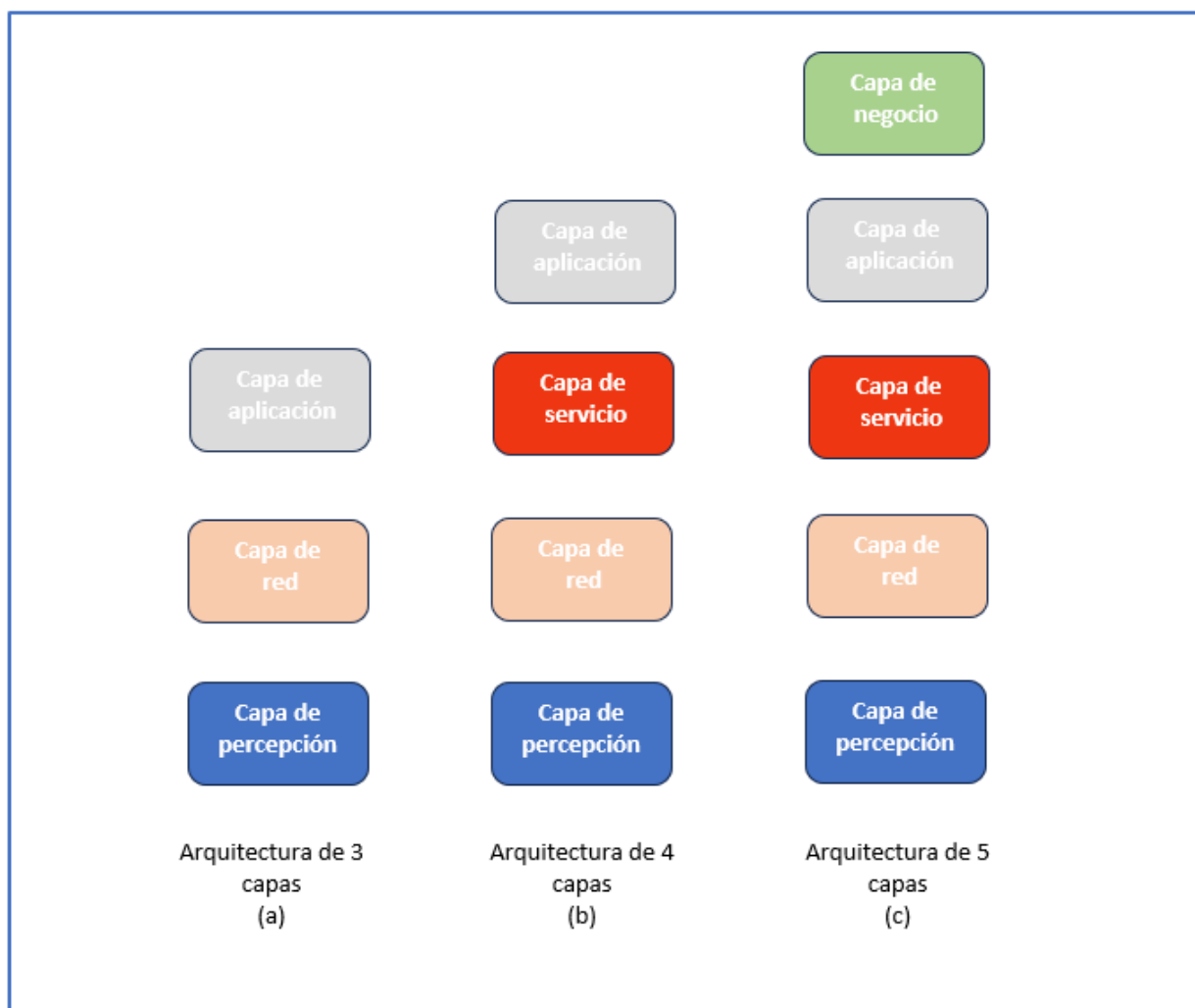


Figura 3-5 Arquitecturas IoT-Edge. (a) 3 capas. (b) 4 capas. (c) 5 capas.

En la tabla 3-1 se muestra una comparativa resumen de las características principales de cada modelo y las ventajas e inconvenientes de cada uno.

Modelo de Capas	Características Únicas	Ventajas	Inconvenientes
Arquitectura de tres capas	Recopilación, transmisión y procesamiento básico de datos. Estructura sencilla y directa.	Menor complejidad, fácil de implementar. Ideal para sistemas pequeños y menos complejos.	Limitado en términos de gestión avanzada de servicios. Menos flexible para sistemas complejos.
Arquitectura de cuatro capas	Incluye una capa de servicios entre la red y la aplicación. Gestión y coordinación de servicios.	Mejor manejo de servicios y datos. Más flexible y escalable.	Mayor complejidad en la implementación. Requiere más recursos para la gestión.
Arquitectura de cinco capas	Añade una capa de negocio para análisis y operaciones empresariales. Enfoque en análisis de datos a gran escala y decisiones de negocio.	Permite un análisis de negocio profundo. Ideal para sistemas grandes y complejos.	La más compleja en términos de implementación y gestión. Puede ser excesiva para proyectos pequeños o simples.

Tabla 3-1 Comparativa entre las distintas arquitecturas IoT-Edge

3.2.4 Análisis de los elementos clave en la arquitectura IoT-Edge

Aunque previamente hemos explorado los diferentes modelos de arquitectura de tres, cuatro y cinco capas, en este apartado vamos a profundizar en los elementos específicos que componen cada una de estas capas. Este análisis detallado es crucial para entender no solo cómo funciona cada capa individualmente, sino también para comprender cómo interactúan entre sí para formar un sistema integrado y cohesivo. Al desglosar los componentes de cada capa, desde los sensores en la capa de percepción hasta las herramientas de análisis de negocios en la capa empresarial, tendremos una visión holística de la infraestructura y las operaciones en los sistemas IoT-Edge.

La **capa de percepción** es la interfaz tangible con el mundo físico en los sistemas IoT-Edge. Compuesta por dispositivos como sensores y actuadores, esta capa es fundamental para recoger información del entorno, que varía desde datos de temperatura hasta imágenes capturadas por cámaras. Los elementos de esta capa, que incluyen una variedad de sensores (temperatura, humedad, movimiento, etc. como vimos en el apartado 2.1.2), son responsables de detectar cambios en el entorno y convertirlos en datos digitales que pueden ser procesados. Esta capa es el punto de partida crítico para cualquier interacción entre el mundo físico y los sistemas digitales, proporcionando los datos brutos necesarios para todas las operaciones subsiguientes.

En la **capa de red** el foco se traslada a la conectividad y la transmisión de datos. Aquí, tecnologías como Wi-Fi, LTE y Bluetooth, junto con routers, switches y gateways, juegan un papel crucial en la transferencia segura y eficiente de los datos recogidos por los sensores a las capas superiores. Esta capa no solo se encarga de la comunicación de datos, sino que también implementa medidas de seguridad para proteger la información transmitida de accesos no autorizados y otras amenazas cibernéticas, asegurando así una transmisión de datos fiable y segura desde y hacia los dispositivos de borde y la nube.

La **capa de servicios**, una adición específica en los modelos de cuatro y cinco capas, introduce una dimensión abstracta centrada en la gestión y el procesamiento intermedio de datos. Compuesta por plataformas de middleware y software de gestión, esta capa realiza la normalización y preprocesamiento de los datos, la orquestación de servicios y la implementación de políticas de seguridad. Actúa como un puente entre la recogida de datos y su análisis final, mejorando la eficiencia y la efectividad del sistema al permitir una gestión más detallada y adaptativa de los datos y servicios.

En la **capa de aplicación** encontramos la concreción de los datos en funciones y servicios útiles. A través de aplicaciones y plataformas de software, esta capa procesa y analiza los datos para propósitos específicos como monitoreo de salud, automatización de hogares o sistemas de gestión de ciudades inteligentes. Los elementos de esta capa traducen los datos procesados en acciones prácticas y resultados perceptibles, facilitando la interacción directa entre los usuarios y el sistema IoT-Edge.

La **capa de negocio**, exclusiva del modelo de cinco capas, aborda el análisis y la toma de decisiones a nivel empresarial. Utilizando herramientas de análisis de datos a gran escala y sistemas de gestión empresarial, esta capa se concentra en evaluar el impacto de las operaciones de IoT en el negocio, ayudando en la planificación estratégica y la toma de decisiones. Los elementos de esta capa incluyen plataformas de modelado de negocios y herramientas de inteligencia de negocio, que permiten a las empresas maximizar el valor de sus operaciones de IoT y Edge Computing.

3.3 Protocolos de comunicación y tecnologías esenciales

La eficacia de la comunicación y el procesamiento de datos depende en gran medida de dos pilares fundamentales: los protocolos de comunicación y las tecnologías de conectividad. Estos elementos son vitales para establecer un flujo de información coherente y confiable entre una amplia gama de dispositivos y plataformas. Su rol es esencial para enlazar los numerosos componentes del Internet de las Cosas con la capacidad de procesamiento en la computación perimetral, creando así un ecosistema donde la recopilación, transmisión y análisis de datos se realizan de manera óptima.

Las tecnologías de comunicación, incluyendo diversas plataformas como LPWAN, Zigbee, Wi-Fi, y Bluetooth, proporcionan la infraestructura física y de red necesaria para el despliegue de soluciones IoT. Son el medio a través del cual se transmiten los datos, conectando dispositivos de captura de datos con sistemas de procesamiento avanzados. Estas tecnologías no solo aseguran que los datos se transmitan de manera eficiente y segura a través de distintas distancias y configuraciones, sino que también se adaptan a las necesidades específicas de los diferentes escenarios de IoT, desde aplicaciones de bajo consumo hasta soluciones que requieren un ancho de banda alto y una baja latencia.

Por otro lado, los protocolos de comunicación como MQTT y CoAP, definen el conjunto de reglas y procedimientos para el intercambio de datos. Estos protocolos son esenciales para asegurar que los dispositivos puedan comunicarse entre sí de manera confiable, interpretando y respondiendo a los

datos de manera adecuada. Permiten la interoperabilidad entre dispositivos y sistemas heterogéneos, y son fundamentales para garantizar la integridad y la seguridad de los datos transmitidos.

La combinación efectiva de estas tecnologías y protocolos es lo que permite a la integración IoT-Edge Computing funcionar con la máxima eficiencia posible. Proporcionan la base para una comunicación robusta y segura, esencial para el procesamiento en tiempo real, la toma de decisiones automatizada y la respuesta ágil a las condiciones cambiantes del entorno.

3.3.1 Tecnologías de comunicación

Cada tecnología posee características únicas que la hacen idónea para ciertos tipos de aplicaciones dentro del IoT, y su elección es determinante en el diseño y eficacia de cualquier solución basada en IoT-Edge. A continuación, detallaremos las tecnologías más relevantes en este campo [42]:

- **LPWAN** (Low-Power Wide Area Network): Tecnología clave en el ecosistema de IoT, especialmente por su capacidad para proporcionar comunicaciones de largo alcance con un consumo energético muy bajo. Esta característica es fundamental para aplicaciones IoT que no tienen acceso frecuente a fuentes de energía, como por ejemplo sensores agrícolas remotos. Su largo alcance, que puede cubrir decenas de kilómetros, junto con su eficiencia energética, hace de LPWAN una opción ideal para una amplia gama de aplicaciones, desde la monitorización ambiental hasta el control de infraestructuras urbanas.

Dentro de LPWAN, existen varias variantes como LoRaWAN, Sigfox y NB-IoT [43], cada una con sus propias particularidades y casos de uso específicos. Por ejemplo, LoRaWAN es conocido por su capacidad de comunicación de largo alcance y se utiliza ampliamente en la gestión de recursos en ciudades inteligentes y la agricultura de precisión. Por otro lado, NB-IoT, aprovechando bandas de frecuencia con licencia, ofrece mayor seguridad, siendo adecuado para aplicaciones como medidores inteligentes y monitoreo de infraestructuras. La elección entre estas variantes depende de los requisitos específicos de cada aplicación IoT, como la necesidad de cobertura extensa, baja latencia o seguridad reforzada.

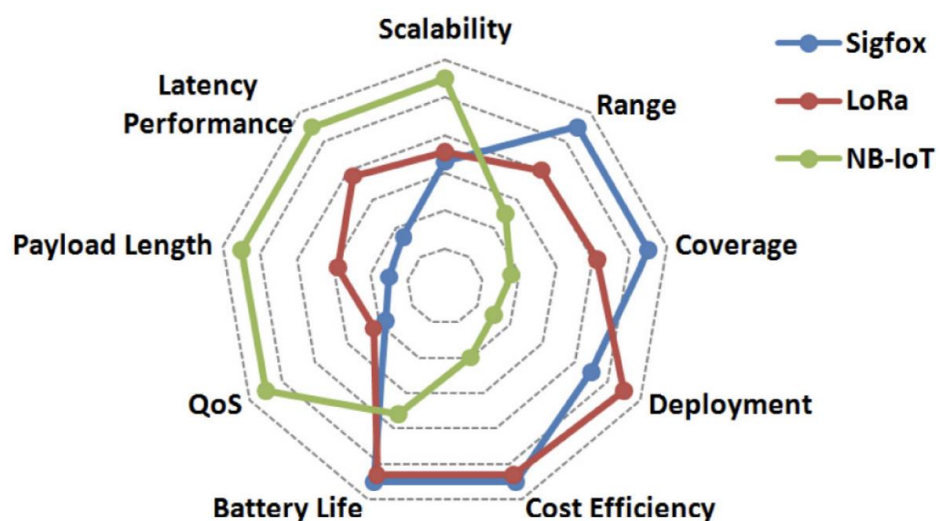


Figura 3-6 Comparativa entre Sigfox, LoRa y NB-IoT [44]

En la figura 3-4 tenemos una comparativa visual entre LoRaWAN, Sigfox y NB-IoT, destacando sus fortalezas y debilidades en diversos aspectos críticos para IoT. LoRa sobresale en términos de alcance y capacidad de la batería, lo que lo hace ideal para aplicaciones que requieren una amplia cobertura y dispositivos con una larga vida útil. Sigfox, con su modelo de bajo coste y eficiencia en el consumo energético, se posiciona favorablemente para despliegues que necesitan una amplia cobertura con un enfoque en la eficiencia de costes. Por su parte, NB-IoT muestra un rendimiento superior en calidad de servicio (Quality of Service, QoS) y capacidad de carga de datos (payload length), destacando en escenarios donde se necesita una conexión segura y la transmisión de mayores cantidades de datos, a pesar de su alcance más limitado y costes potencialmente más altos.

- **6LoWPAN** (IPv6 over Low-Power Wireless Personal Area Networks): Esta tecnología, ampliamente utilizada en los protocolos de comunicación IoT por estar basado en IP, permite a los dispositivos conectarse directamente con otras redes IP sin la necesidad de entidades intermediarias, como gateways de traducción o proxies, facilitando así una integración más fluida y directa. La fortaleza de 6LoWPAN reside en su capacidad para soportar un enorme número de direcciones IP (hasta 2^{128}), asegurando una amplia escalabilidad para la incorporación de dispositivos IoT. Además, esta tecnología destaca por su bajo costo y eficiencia en términos de consumo de energía y uso de ancho de banda, lo que la hace ideal para aplicaciones donde estos factores son críticos.

La versatilidad de 6LoWPAN también se refleja en su capacidad para soportar diferentes topologías de red, como malla y estrella, lo que amplía su aplicabilidad en diversos escenarios IoT, desde la automatización del hogar hasta el sector de la salud. El factor distintivo de 6LoWPAN es su capa de adaptación, ubicada entre la capa MAC y la capa de red (IPv6). Esta capa es fundamental para facilitar la interoperabilidad entre el estándar IEEE 802.15.4 y IPv6, manejando la compresión y fragmentación de los paquetes IPv6 para su eficiente transmisión a través de redes de baja potencia y bajo ancho de banda.

- **Zigbee:** Basado en el estándar IEEE 802.15.4, Zigbee es una tecnología destacada en el mundo del IoT por su capacidad para crear redes de malla autoorganizadas (los dispositivos pueden unirse y abandonar la red sin afectar a su funcionamiento) y eficientes en energía. Sus principales características incluyen un bajo consumo de energía, lo que lo hace ideal para dispositivos alimentados por baterías, y la capacidad de soportar un gran número de nodos, lo que lo hace escalable para redes más grandes. Zigbee también ofrece una comunicación segura mediante el uso de cifrado AES-128, garantizando la protección de los datos transmitidos.

Entre los casos de uso más habituales de Zigbee se encuentran la automatización del hogar y edificios inteligentes, donde se utiliza para controlar dispositivos como luces, termostatos y sistemas de seguridad. En el ámbito industrial, Zigbee es útil para conectar una variedad de sensores destinados a monitorear condiciones como la temperatura y la humedad. En el sector de la salud, se emplea para conectar dispositivos médicos y sensores de monitoreo de pacientes, facilitando la atención médica remota. Las ventajas de Zigbee,

como su eficiencia energética, la seguridad de los datos y la flexibilidad de red, lo hacen una opción atractiva para una amplia gama de aplicaciones IoT.

- **Bluetooth Low Energy:** Esta versión más eficiente del clásico Bluetooth es fundamental en el ámbito IoT por su bajo consumo de energía y su capacidad de comunicación efectiva a corta distancia. BLE se ha diseñado específicamente para aplicaciones donde la eficiencia energética es primordial, lo que le permite operar en dispositivos alimentados por batería durante largos periodos sin necesidad de recarga. Otra característica clave de BLE es su capacidad para manejar múltiples conexiones simultáneamente, lo que facilita la interconexión de varios dispositivos IoT.

Los casos de uso más comunes se encuentran en la industria de dispositivos wearables, como relojes inteligentes y bandas de fitness, donde su eficiencia energética es esencial para el seguimiento continuo de la salud y la actividad física. En la automatización del hogar, BLE se utiliza para conectar una variedad de dispositivos domésticos inteligentes, como cerraduras, luces y termostatos, ofreciendo una solución de baja potencia para el control y la monitorización del hogar. En el ámbito comercial y de la salud, BLE es útil para la localización en interiores y el seguimiento de activos, permitiendo una gestión precisa y eficiente de recursos y personal. La eficiencia energética, la capacidad de conexión con múltiples dispositivos y la facilidad de integración con smartphones y otros dispositivos hacen de BLE una tecnología clave en el Internet de las Cosas.

Parámetro	Bluetooth clásico	Bluetooth Low Energy
Bit rate	Hasta 3 Mbps	Hasta 1 Mbps
Latencia	<100 ms	< 3ms
Consumo de energía	Mayor	Menor, optimizado para transmisiones esporádicas y dispositivos de baja energía
Tamaño de implementación	~100 kB (ROM), ~30 kB (RAM)	~40 kB (ROM), ~2.5 kB (RAM)
Seguridad	Emparejamiento, generación de clave de enlace, algoritmos E0	Modos de seguridad, emparejamiento, generación de clave, AES-128 encriptación
Roles de dispositivo	Maestro y esclavo	Maestro y esclavo

Tabla 3-2 Comparativa entre Bluetooth clásico y Bluetooth Low Energy [45]

La tabla 3-2 muestra una comparativa a modo de resumen de las principales características de la versión clásica de bluetooth y la versión Low Energy o Smart.

- **RFID** (Radio Frequency Identification): La tecnología RFID es un sistema de identificación automática que utiliza ondas de radio para transferir datos desde una etiqueta electrónica, llamada tag RFID, hacia un lector RFID con el propósito de identificar y rastrear objetos. Estas etiquetas pueden ser pasivas, activas o semi-pasivas, y su elección depende del alcance y la aplicación específica. Las etiquetas pasivas no tienen fuente de energía propia y obtienen energía del campo generado por el lector; las activas tienen su propia fuente de energía que permite una mayor distancia de lectura; y las semi-pasivas combinan características de ambas.

En el ámbito del Internet de las Cosas, la tecnología RFID desempeña un rol fundamental por su capacidad de proporcionar una identificación única y automatizada de objetos, lo cual es esencial para la conectividad y la inteligencia de los sistemas IoT. Su aplicación abarca desde la gestión de inventarios y logística hasta la integración en dispositivos personales para la salud y el bienestar, ofreciendo una interacción sin fisuras entre el mundo físico y los sistemas digitales. La importancia esta tecnología reside en su eficiencia para automatizar procesos, reducir errores humanos, mejorar la trazabilidad de los productos y permitir decisiones basadas en datos en tiempo real.

- **NFC** (Near Field Communication): La tecnología NFC se caracteriza por su capacidad para facilitar la comunicación inalámbrica de corto alcance entre dispositivos. Operando a una frecuencia de 13.56 MHz, permite el intercambio de datos entre dispositivos que se encuentran a pocos centímetros de distancia, lo cual garantiza una alta seguridad en la transmisión de la información. Una de sus características distintivas es la simplicidad de su operación: un dispositivo NFC puede actuar tanto como lector como emisor, lo que posibilita una amplia gama de interacciones, desde el simple emparejamiento de dispositivos hasta transacciones más complejas.

NFC desempeña un papel crucial en la creación de experiencias de usuario más intuitivas y seguras. Esta tecnología se utiliza ampliamente para aplicaciones como pagos móviles, donde la facilidad de uso y la seguridad son primordiales. En cuanto a su relevancia en el mundo IoT, NFC facilita la configuración rápida y segura de dispositivos inteligentes, permitiendo que se conecten y comuniquen entre sí con un simple toque. Además, su uso en etiquetas inteligentes permite a los usuarios interactuar con objetos cotidianos conectados a Internet, proporcionando acceso instantáneo a información adicional, control de dispositivos y personalización de experiencias. Esta interacción segura y sin esfuerzo es esencial para la expansión y aceptación del IoT en la vida cotidiana, haciendo que la tecnología sea más accesible y amigable para el usuario final.

- **Z-Wave**: Esta tecnología de comunicación inalámbrica ha sido diseñada específicamente para la automatización del hogar y aplicaciones IoT. Funciona en una banda de frecuencia de baja potencia (alrededor de 900 MHz), lo que le permite tener un alcance efectivo y evitar interferencias con otros dispositivos domésticos como Wi-Fi y Bluetooth. Una de sus

características más destacadas es la creación de una red de malla, donde cada dispositivo conectado actúa como un repetidor, aumentando la fiabilidad y el alcance de la red.

Z-Wave se ha establecido como un estándar referente en la automatización del hogar debido a su robustez, bajo consumo de energía y alta interoperabilidad. Los dispositivos Z-Wave pueden comunicarse entre sí independientemente del fabricante, lo que facilita la creación de un entorno doméstico inteligente y adaptable. Esta tecnología se utiliza ampliamente en dispositivos como termostatos inteligentes, sistemas de seguridad, cerraduras de puertas, detectores de movimiento y luces, permitiendo a los usuarios controlar y automatizar su entorno de vida de manera eficiente.

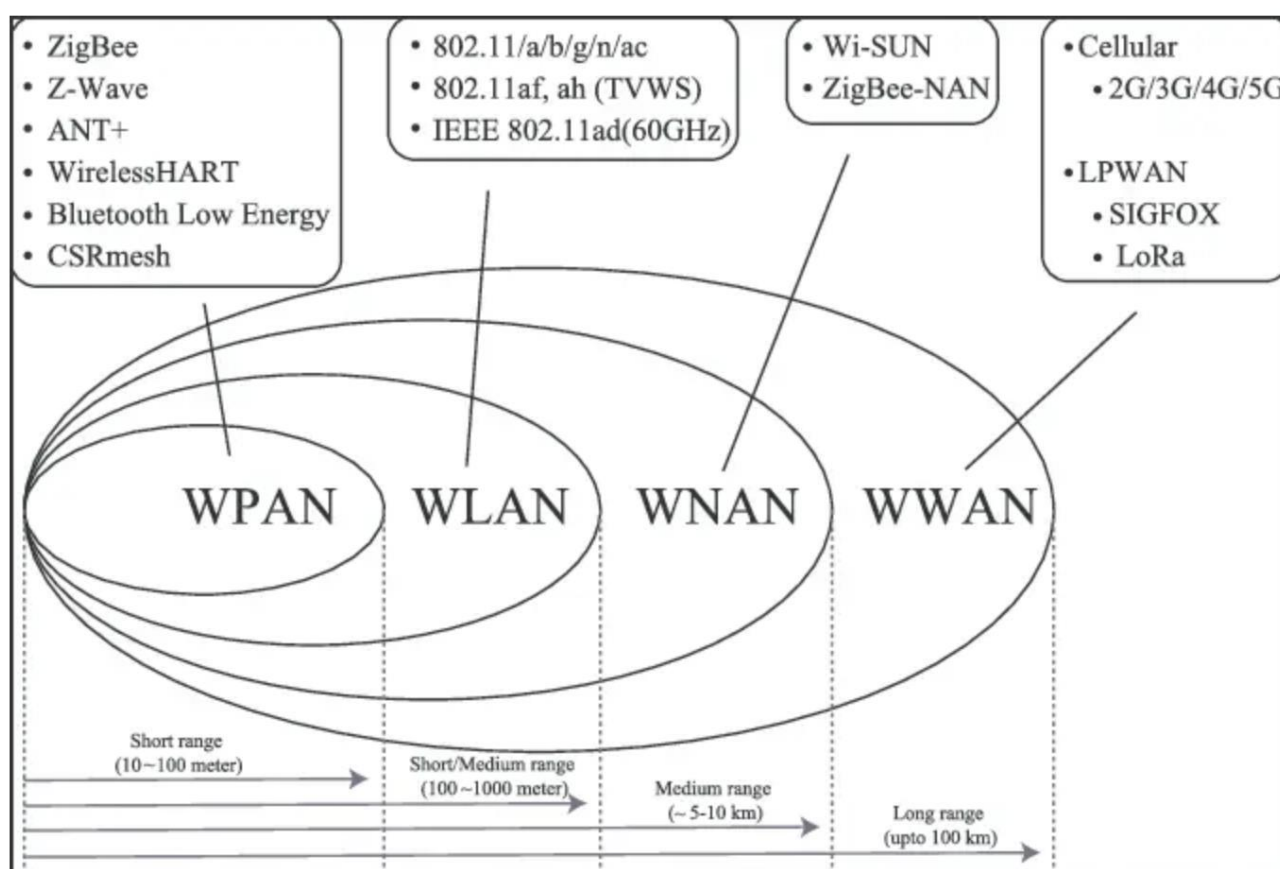


Figura 3-7 Resumen tecnologías inalámbricas según alcance [46]

La figura 3-5 muestra un diagrama que clasifica diferentes tecnologías de redes inalámbricas según su alcance, desde redes de área personal (WPAN) hasta Redes Inalámbricas de Área Amplia (Wireless Wide Area Network, WWAN). Tecnologías como ZigBee, Z-Wave, y Bluetooth Low Energy se encuentran en la categoría WPAN, con un alcance corto de 10 a 100 metros, ideales para conectividad cercana. Las Redes Inalámbricas de Área Local (Wireless Local Area Network, WLAN) como las variantes de Wi-Fi (802.11 a/b/g/n/ac) y las Redes Inalámbricas de Área de Vecindario (Wireless Neighbourhood Area Network, WNAN) ofrecen alcances medios de 100 a 1000 metros y hasta aproximadamente 10 km respectivamente, adecuados para conectividad en hogares y comunidades. Por último, las WWAN incluyen tecnologías de telefonía móvil (4G/5G) y LPWAN (Sigfox, LoRa), que proporcionan una cobertura extensa, llegando hasta 100 km, para aplicaciones que requieren un alcance amplio y conexiones a larga distancia.

3.3.2 Protocolos de comunicación

Los protocolos de comunicación representan el conjunto de reglas y estándares que gobiernan la transferencia de datos entre los dispositivos IoT, actuando como una columna vertebral para la interoperabilidad y la integración efectiva de estas tecnologías. En este apartado vamos a explorar estos protocolos, destacando el papel que juegan en la facilitación de una comunicación robusta y segura dentro de este ecosistema tecnológico.

Estos protocolos deben abordar una serie de desafíos únicos impuestos por las características inherentes a estos entornos. Estos incluyen la heterogeneidad de los dispositivos y plataformas, las limitaciones de recursos en términos de energía y capacidad de procesamiento, y la necesidad de soportar conexiones seguras y confiables a través de una amplia gama de contextos operativos. Por lo tanto, estos protocolos no solo deben ser altamente eficientes y flexibles, sino también capaces de garantizar la seguridad y la privacidad de los datos transmitidos en un panorama en constante evolución de amenazas cibernéticas.

En este capítulo, nos centraremos en los protocolos de la capa de aplicación, examinando cómo estos protocolos de alto nivel, como MQTT, CoAP, HTTP y AMQP, facilitan la comunicación y el procesamiento de datos en el Internet de las Cosas [47].

- **MQTT** (Message Queuing Telemetry Transport): este protocolo destaca por su eficiencia y simplicidad en la comunicación entre dispositivos. Funciona a través de un modelo de publicación/suscripción, donde un elemento central llamado "broker" desempeña un rol crucial. El broker actúa como intermediario, recibiendo mensajes de los dispositivos (publicadores) y enviándolos a los suscriptores apropiados. Esta estructura es óptima para entornos con recursos limitados y conectividad variable, siendo ideal para aplicaciones como la monitorización de infraestructuras, automatización del hogar y telemetría industrial.

La eficiencia de MQTT en el uso del ancho de banda y su confiable entrega de mensajes son dos de sus puntos fuertes. El protocolo permite una comunicación selectiva, reduciendo el tráfico innecesario y adaptándose a redes con limitación en ancho de banda. Ofrece varios niveles de calidad de servicio, lo que permite equilibrar la garantía de entrega de mensajes con el uso eficiente de recursos. Sin embargo, su enfoque en la ligereza implica desafíos en términos de seguridad. Al carecer de características de seguridad integradas, depende de la implementación de medidas adicionales, como TLS/SSL, para asegurar la protección de los datos.

- **CoAP** (Constrained Application Protocol): Especialmente diseñado para entornos con recursos limitados, este protocolo, ligero y eficiente, se adapta perfectamente a las necesidades de los dispositivos IoT que operan con restricciones de energía y ancho de banda, como sensores y actuadores en entornos remotos o distribuidos. CoAP, al igual que MQTT, utiliza un modelo de comunicación basado en la solicitud/respuesta, pero está especialmente optimizado para redes M2M (Machine to Machine) y se alinea bien con los estándares web existentes, como HTTP.

Uno de los grandes atractivos de CoAP es su capacidad para interactuar de manera sencilla con la web, facilitando la integración de dispositivos IoT con aplicaciones y servicios basados en la nube. Esto lo hace ideal para aplicaciones que requieren una interacción constante con servidores web o para situaciones en las que los dispositivos IoT deben ser accesibles y manejables a través de interfaces web estándar. Además, CoAP es conocido por su uso eficiente del ancho de banda y su bajo consumo energético, lo que lo hace perfectamente adecuado para redes de sensores inalámbricos y aplicaciones de IoT que operan en entornos con conectividad limitada o intermitente.

Sin embargo, CoAP también enfrenta desafíos, especialmente en lo que respecta a la seguridad y la escalabilidad. Aunque soporta medidas de seguridad como DTLS (Datagram Transport Layer Security) para la encriptación y la autenticación de mensajes, la implementación de estas características de seguridad puede ser compleja en dispositivos con recursos muy limitados. Además, mientras que CoAP se maneja bien en redes de pequeña y mediana escala, puede encontrarse con limitaciones en entornos IoT de gran escala debido a su naturaleza principalmente basada en UDP, que es menos robusta frente a la pérdida de paquetes en comparación con TCP.

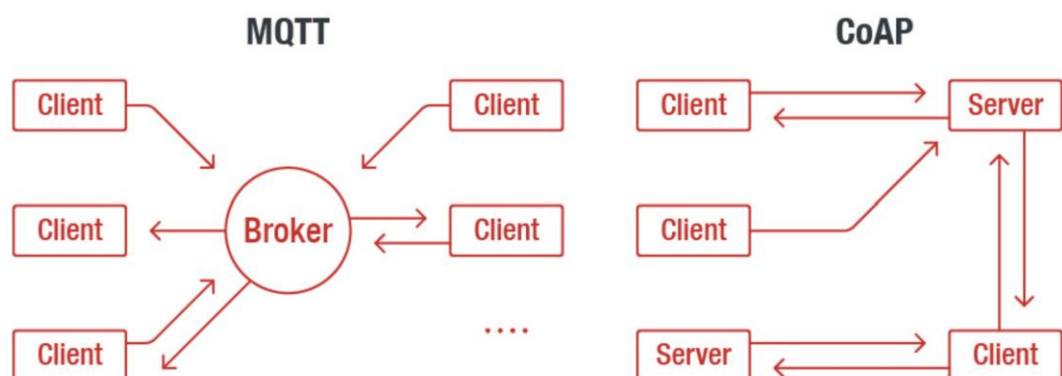


Figura 3-8 Visión de alto nivel de los modelos de interacción en MQTT y CoAP [48]

La figura 3-6 muestra dos diagramas que representan la arquitectura de comunicación de los protocolos MQTT y CoAP en el contexto del IoT. En la parte de MQTT, se ilustra un conjunto de clientes intercambiando información a través de un broker central, donde los clientes pueden ser tanto publicadores como suscriptores de mensajes. Por otro lado, en la sección de CoAP, se representa un modelo más descentralizado en el que múltiples clientes interactúan directamente con un servidor en un patrón de solicitud y respuesta, lo que refleja una aproximación más tradicional, similar a la del protocolo HTTP.

- **AMQP** (Advanced Message Queuing Protocol): Este protocolo avanzado de mensajería orientado a colas, sobresale por su naturaleza de código abierto y su conformidad con

estándares internacionales, lo que garantiza fiabilidad, interoperabilidad y un alto grado de seguridad. Es ideal para entidades y aplicaciones que dependen de entregas de mensajes rápidas y con confirmación, apoyándose en el uso de TCP para el transporte de datos y en TLS/SSL y SASL (Simple Authentication and Security Layer) para una comunicación segura. Su diseño robusto, que incluye características como calidad de servicio (QoS) y un modelo de publicación/suscripción, permite la transmisión segura y eficaz de datos críticos.

No obstante, a pesar de sus ventajas, AMQP viene con desafíos que pueden limitar su uso en algunos contextos de IoT. No es tan simple como HTTP u otros protocolos de bajo nivel, lo que puede complicar su implementación y mantenimiento. Además, requiere un ancho de banda superior, lo que puede ser un obstáculo en entornos con recursos de red limitados o para dispositivos IoT que operan con restricciones de energía y capacidad de procesamiento. Por tanto, la decisión de utilizar AMQP en proyectos de IoT debe equilibrar su funcionalidad y seguridad frente a la simplicidad y las limitaciones de la infraestructura.

- **HTTP (Hypertext Transfer Protocol):** HTTP es el protocolo de comunicación fundamental de la web y, aunque no se diseñó específicamente para el Internet de las Cosas, su compatibilidad con los sistemas existentes lo hacen una opción viable para ciertas aplicaciones IoT. Su importancia está en su capacidad para facilitar la integración con servicios web y plataformas en la nube, permitiendo que los dispositivos IoT se comuniquen y actúen como clientes web. Es especialmente útil para aplicaciones que requieren una interacción regular con APIs (Application Programming Interface) web o para dispositivos que actualizan su estado o recuperan información utilizando los mecanismos estándar de la web.

Sin embargo, a pesar de su universalidad, HTTP puede no ser la mejor opción para todos los escenarios de IoT. En comparación con protocolos específicos como MQTT y CoAP, HTTP puede ser más demandante en términos de ancho de banda debido a su modelo de comunicación de solicitud y respuesta que no está optimizado para las restricciones de dispositivos y redes IoT. A diferencia de AMQP, que ofrece garantías de entrega y una serie de funcionalidades avanzadas para la mensajería, HTTP carece de estas características y, por lo tanto, puede no ser adecuado para aplicaciones IoT que requieren una alta confiabilidad y un manejo de mensajes complejo. En última instancia, mientras HTTP se beneficia de su estandarización y facilidad de uso, las aplicaciones IoT que buscan eficiencia energética, bajo uso de ancho de banda y comunicaciones persistentes pueden necesitar considerar otros protocolos más especializados.

A continuación, se presenta una tabla resumen con las principales características de cada protocolo de comunicación:

Característica	MQTT	CoAP	AMQP	HTTP
Modelo de comunicación	Cliente/broker	Cliente/servidor o Cliente/broker	Cliente/broker o Cliente/servidor	Cliente/ servidor
Eficiencia en ancho de banda	Alta	Alta para dispositivos limitados	Baja comparada con MQTT/CoAP	Baja (no optimizada para IoT)
Seguridad	TLS/SSL para cifrado	DTLS	TLS/SSL y SASL para cifrado y autenticación	TLS/SSL para cifrado
Fiabilidad/QoS	Alta con tres niveles de QoS	Mediana, con confirmación de mensajes	Muy alta con confirmación de mensajes y transacciones	Limitada
Interoperabilidad	Alta con brokers MQTT	Alta con gateways y traducción a HTTP	Alta, diseñada para interoperabilidad entre sistemas	Universal en la web
Protocolo de transporte	TCP	UDP	TCP	TCP

Tabla 3-3 Resumen principales características protocolos de comunicación

4 CASOS DE APLICACIÓN

Este capítulo se centra en cómo IoT y Edge Computing están siendo implementados en tres áreas vitales: salud, ciudades inteligentes y el sector militar. Iniciaremos con el sector salud, donde estas tecnologías están haciendo avanzar la atención al paciente y optimizando la gestión de datos médicos. Destacaremos casos específicos que ilustran la influencia positiva de IoT y Edge Computing en la mejora de la eficiencia y la efectividad del cuidado de la salud.

En el ámbito de las ciudades inteligentes, examinaremos cómo están revolucionando aspectos clave como el transporte y el aparcamiento inteligente, la red eléctrica inteligente, y las prácticas de agricultura y acuicultura. Esta sección analiza la forma en que estas tecnologías están contribuyendo a hacer nuestras ciudades más eficientes y sostenibles.

Finalmente, abordaremos su aplicación en el sector militar, con especial atención al Internet de las Cosas del Campo de Batalla (Internet of Battlefield Things, IoBT) y la computación perimetral en la Defensa. Aquí discutiremos el impacto de estas tecnologías en las operaciones militares, incluyendo el uso avanzado de drones y su integración en sistemas de defensa.

A través de este capítulo, se pretende proporcionar una perspectiva clara de las aplicaciones prácticas del IoT y Edge Computing en estos sectores, subrayando su relevancia y el potencial que ofrecen.

4.1 Ámbito de la salud

En el sector sanitario, la incorporación del Internet de las Cosas junto con la Computación Perimetral está revolucionando la manera en que se manejan y procesan los datos de salud. Estas tecnologías emergentes están redefiniendo los sistemas sanitarios conectados (Healthcare Internet of Things, H-IoT), llevando la capacidad de procesamiento más cerca de la fuente de datos, lo que resulta en un análisis más rápido y eficiente, crucial para la atención médica en tiempo real.

Los sistemas H-IoT generan una cantidad masiva de datos a través de diversos nodos sensoriales, desde dispositivos portátiles de monitoreo de pacientes hasta sensores integrados en equipos médicos avanzados. La gestión eficiente de estos datos es fundamental para el funcionamiento óptimo de los sistemas de salud. Aquí es donde el Edge Computing descentraliza los recursos computacionales y extiende los servidores de la nube mediante nodos de borde. Esta descentralización permite un procesamiento más cercano a la fuente de datos, mejorando la velocidad y la eficiencia en el manejo de la información de salud.

La integración de la computación en el borde en los sistemas H-IoT no solo mejora el rendimiento de la red al reducir la utilización del ancho de banda y la congestión, sino que también optimiza los requerimientos energéticos, logra integridad de datos y mejora la seguridad de la red y la calidad del servicio. Estas mejoras son fundamentales en aplicaciones de salud donde la rapidez y la precisión en el procesamiento de datos son esenciales para decisiones clínicas críticas y para mejorar los resultados de salud de los pacientes.

En [49] se propone un enfoque estructurado a través de un modelo de cuatro capas para las soluciones de salud basadas en IoT, similar al estudiado en el apartado 3.2.2 de este TFM. Este modelo se revela como un marco fundamental para entender cómo la tecnología IoT puede ser desplegada de manera efectiva en el sector sanitario.

En la primera capa se encuentran los dispositivos IoT como sensores de signos vitales que recopilan información vital para entender las condiciones actuales del paciente. En la segunda capa es donde se usa la tecnología de comunicación inalámbrica para asegurar que los datos lleguen a donde se necesitan sin demoras significativas. En la tercera capa los datos en bruto se convierten en información útil mediante uso de algoritmos avanzados y técnicas de aprendizaje automático que pueden detectar patrones, identificar tendencias y alertar a los médicos sobre posibles problemas antes de que se conviertan en emergencias. En la última capa los datos procesados y analizados se utilizan para proporcionar servicios directos a los usuarios, ya sean pacientes, médicos o cuidadores. Esta capa abarca desde sistemas de diagnóstico remoto y monitoreo de comportamiento hasta la detección de emergencias y la autogestión de condiciones de salud. Es en esta capa donde el verdadero potencial del H-IoT se hace tangible, transformando la manera en que se presta la atención sanitaria y mejorando significativamente la calidad de vida de los pacientes.

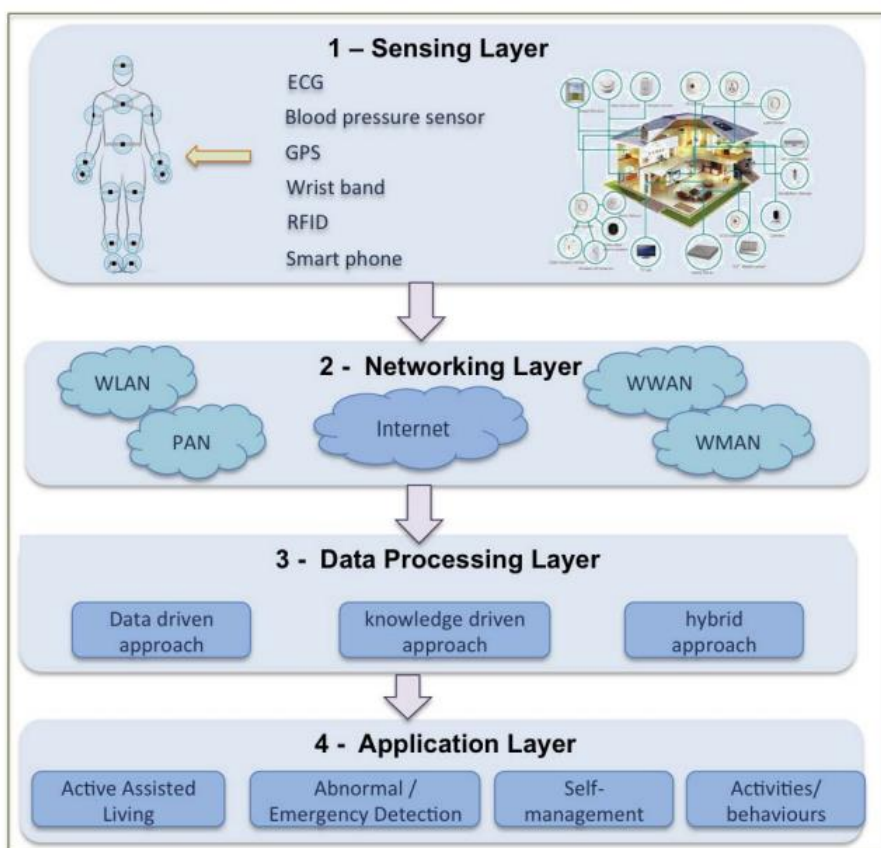


Figura 4-1 Modelo de trabajo en H-IoT [49]

La variedad de aplicaciones del IoT en el sector de la salud es extensa [50], desde la vida cotidiana asistida por el entorno (Ambient Assisted Living, AAL) que mejora la calidad de vida de los ancianos mediante dispositivos portátiles que monitorean datos vitales, hasta los hospitales inteligentes y las salas de operaciones inteligentes, donde el H-IoT mejora la eficiencia y la seguridad de los procedimientos médicos.

La tecnología vestible, también conocida como dispositivos wearables, ofrece nuevas oportunidades para el monitoreo y la gestión de la salud personal. Estos dispositivos, que incluyen relojes inteligentes, pulseras de actividad, monitores de ritmo cardíaco y parches de salud, se utilizan para recopilar datos de salud en tiempo real, como la frecuencia cardíaca, la actividad física, los patrones de sueño y los niveles de oxígeno en sangre. Esta información es crucial para el seguimiento continuo de pacientes con enfermedades crónicas, la prevención de enfermedades y la promoción de estilos de vida saludables. Además, la integración de estos dispositivos con sistemas de salud digitales permite a los profesionales médicos acceder a datos valiosos para diagnósticos más precisos y tratamientos personalizados, mejorando significativamente la eficacia de la atención médica.

En [51] se analiza un caso de estudio específico en el que la Computación Perimetral se aplica para minimizar la latencia en el sector de la salud. La solución propuesta se centra en la Computación en la Niebla (Fog Computing), que ofrece un enfoque distribuido similar al Edge Computing, para operar de manera más eficiente que las soluciones basadas únicamente en la Nube. El corazón de esta solución es un modelo innovador que utiliza el algoritmo de aprendizaje automático de bosque aleatorio para la segregación inteligente de datos multimedia (Intelligent Multimedia Data Segregation, IMDS). Este modelo no solo clasifica con precisión los datos de salud en diferentes categorías de riesgo, sino que también reduce significativamente la latencia en la transmisión de datos, mejorando así la calidad del servicio en el cuidado de la salud.

Los resultados del estudio son notables, mostrando una reducción de la latencia de aproximadamente el 95% en comparación con modelos anteriores. Esto representa un avance importante en la capacidad de transferir datos de sensores de salud a usuarios finales en tiempo real, abordando así uno de los problemas más críticos en la atención médica moderna: la necesidad de acceso rápido y fiable a datos relevantes.

Este enfoque de computación cerca de la fuente que origina y colecta los datos, con su énfasis en la minimización de la latencia y la mejora de la calidad del servicio, es particularmente relevante para aplicaciones en el sector de la salud donde el IoT y el Edge Computing son fundamentales. La capacidad de procesar y responder rápidamente a datos críticos puede ser vital en situaciones que requieren decisiones rápidas y precisas basadas en datos en tiempo real. Algunas de estas situaciones son las siguientes:

- **Telecirugía:** En procedimientos donde los cirujanos operan a distancia utilizando sistemas robóticos, una latencia mínima es crítica para garantizar que los movimientos del cirujano se traduzcan instantáneamente en acciones del robot quirúrgico. Cerca del paciente se realiza el control de los dispositivos robóticos y el procesamiento de datos sensoriales, asegurando respuestas rápidas y precisas en el movimiento de los instrumentos quirúrgicos. Esta proximidad reduce la latencia en las acciones del robot, un factor crítico para la seguridad del procedimiento quirúrgico. Además, se procesan localmente los datos sensoriales, como imágenes y retroalimentación táctil, para disminuir la carga de transmisión y mejorar la calidad de la respuesta en tiempo real.

Por otro lado, en la ubicación del cirujano, la consola de control procesa los comandos del cirujano y los convierte en señales para el equipo quirúrgico. Aquí también se realiza la visualización y el procesamiento de la retroalimentación que se transmite desde el sitio del paciente. La latencia es un factor crítico en esta interacción, por lo que se utilizan redes de alta velocidad para minimizar el retraso en la comunicación. Los sistemas de telecirugía suelen incorporar medidas de redundancia y seguridad en ambos extremos, asegurando que cualquier fallo de comunicación no resulte en acciones peligrosas, garantizando una operación segura y fiable.



Figura 4-2 Telecirugía [Tomada de Intramed.net]

- **Monitoreo de pacientes en tiempo real:** En unidades de cuidados intensivos y en el seguimiento de pacientes con condiciones crónicas, es vital tener datos actualizados constantemente. La baja latencia asegura que cualquier cambio crítico en los signos vitales del paciente se detecte y se responda de inmediato.
- **Sistemas de alerta médica de emergencia:** Para pacientes que utilizan dispositivos de alerta médica, especialmente aquellos con enfermedades cardíacas o riesgo de accidente cerebrovascular, una respuesta rápida puede ser la diferencia entre la vida y la muerte. Una baja latencia en la transmisión de datos asegura que las señales de alerta lleguen rápidamente a los centros de monitoreo y a los profesionales de la salud.
- **Dispositivos wearables:** Como hemos comentado anteriormente en las distintas aplicaciones del IoT en este sector, en dispositivos médicos portátiles que monitorizan continuamente la salud del usuario, una rápida transmisión de datos es esencial para un seguimiento eficaz y para alertar tanto a los usuarios como a los sanitarios sobre cualquier anomalía detectada.



Figura 4-3 Wearable para monitorizar electrocardiograma, temperatura y capacidad pulmonar [Tomada de convertronic.net]

Estos dispositivos, como la pulsera de actividad de la figura 4-3, están cada vez más equipados con sensores capaces de recopilar datos vitales como la frecuencia cardíaca, el oxígeno en sangre, la temperatura corporal y otras métricas de salud.

Los wearables juegan un papel importante al proporcionar datos continuos y en tiempo real, lo que permite a los usuarios y profesionales médicos monitorizar y gestionar condiciones de salud crónicas, así como mejorar la prevención y la detección temprana de posibles afecciones. La capacidad de estos dispositivos para recopilar datos a lo largo del tiempo ofrece una visión más completa de la salud del individuo, facilitando un enfoque personalizado y proactivo en la atención médica.

4.2 Ciudades inteligentes

En los últimos años, el concepto de ciudad inteligente ha cobrado una relevancia creciente, marcando un cambio en cómo pensamos y gestionamos los entornos urbanos. Esta transformación es el resultado de la convergencia de las dos tecnologías de estudio de este TFM: el Internet de las Cosas y la Computación Perimetral.

El IoT, con su red interconectada de dispositivos y sensores, permite una recopilación de datos sin precedentes en el ambiente urbano. Esta información, que va desde patrones de tráfico hasta el uso de recursos, ofrece una visión detallada y en tiempo real de la ciudad. Sin embargo, el verdadero potencial de esta cantidad de datos solo puede desbloquearse a través de la computación perimetral. Al procesar los datos cerca de donde se generan, el Edge Computing reduce la latencia, ahorra ancho de banda y mejora la capacidad de respuesta, características esenciales para la toma de decisiones rápida y eficiente en un entorno urbano.

Al integrar IoT y Edge Computing, las ciudades inteligentes pueden no solo gestionar sus recursos de manera más eficaz, sino también mejorar significativamente la calidad de vida de sus habitantes. Desde semáforos que se adaptan en tiempo real para aliviar la congestión del tráfico hasta sistemas de alerta temprana que mejoran la seguridad pública, las aplicaciones son tan variadas como prometedoras.

A continuación, vamos a explorar cómo estas tecnologías están redefiniendo la infraestructura y los servicios urbanos, sentando las bases para ciudades más eficientes, sostenibles y habitables. Para ello, se explorarán distintos componentes urbanos, evaluando cómo el IoT y la computación en el borde los están transformando.

4.2.1 Transporte inteligente

El transporte inteligente es una pieza clave en el diseño y funcionamiento de las ciudades inteligentes, aprovechando las tecnologías del IoT y la computación perimetral para revolucionar la forma en que se gestionan y monitorean los sistemas de transporte urbano. La integración de sensores y dispositivos conectados en vehículos y a lo largo de la infraestructura vial permite recopilar datos en tiempo real sobre las condiciones del tráfico, el estado de los vehículos y el uso de las vías, lo que a su vez facilita una gestión del tráfico más eficiente y segura.

En un escenario de ciudad inteligente, los vehículos equipados con aplicaciones de IoT recogen datos del entorno y los transmiten a servidores de computación de borde. Estos servidores, ubicados estratégicamente cerca de los puntos de recogida de datos, permiten un procesamiento y análisis más rápido y eficiente. Esto facilita un procesamiento y análisis más eficiente de los datos, lo que es clave para mantener una conectividad continua y una gestión efectiva de los recursos en la red de transporte [52].

Esta integración tecnológica no solo mejora la movilidad y la seguridad en las ciudades, sino que también tiene el potencial de reducir significativamente los costes asociados con la infraestructura de transporte. Al optimizar el flujo de tráfico y mejorar la eficiencia del transporte público, las ciudades pueden reducir la congestión, disminuir las emisiones contaminantes y mejorar la calidad del aire, contribuyendo así a un entorno urbano más sostenible y agradable para vivir.

En el distrito de Nippes en Colonia, el sistema de estacionamiento inteligente de Cleverciti ofrece una solución avanzada dentro del marco del transporte en ciudades inteligentes. Utiliza pantallas LED en intersecciones viales para mostrar en tiempo real el número y ubicación de espacios de estacionamiento disponibles. Esto elimina la necesidad de buscar espacios a ciegas, reduciendo tanto el tráfico como la contaminación por emisiones.

El sistema se compone de 89 sensores Cleverciti y 27 pantallas LED Circ™, integrados en postes de luz existentes. Estos sensores, basados en inteligencia artificial y computación perimetral, detectan la disponibilidad de espacios de estacionamiento y transmiten esta información a las pantallas y una aplicación móvil [53].

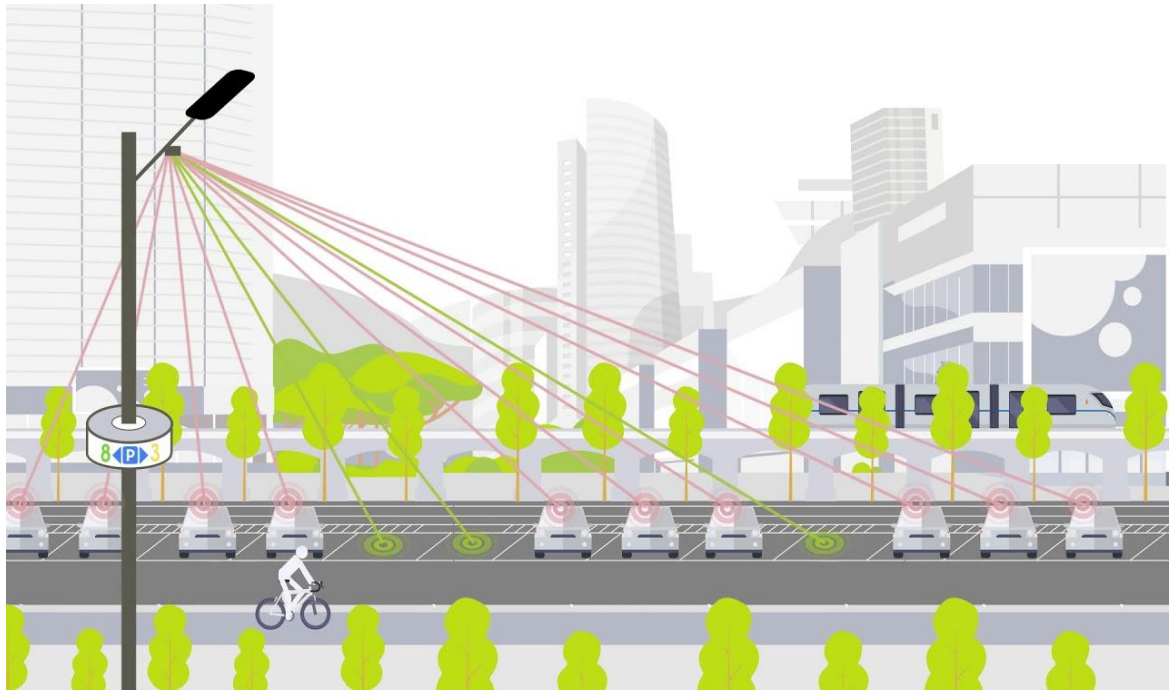


Figura 4-4 Parking inteligente para ciudades inteligentes [Tomada de clevercity.com]

El sistema de transporte inteligente en el metro de Nueva York, desarrollado por Transit Wireless en colaboración con la Autoridad de Transporte Metropolitano (Metropolitan Transportation Authority, MTA), es un ejemplo destacado de cómo el Internet de las Cosas y la Computación Perimetral están transformando el transporte público. Iniciado en 2011, este proyecto tenía como objetivo principal mantener a los viajeros del metro conectados e informados durante sus trayectos. La infraestructura implementada es enorme, la cual incluye una red de fibra óptica de 160 millas, cinco centros de datos, y más de 5,000 puntos de acceso Wi-Fi, junto con un sistema de 7000 antenas distribuidas. Esta red juega un papel importante en la conexión de millones de dispositivos diariamente, garantizando una operación fluida y continua.

Estos puntos de acceso Wi-Fi no solo proporcionan conectividad, sino que también actúan como sensores para recopilar datos en tiempo real sobre la densidad de pasajeros en las estaciones. Esta información es vital para analizar y gestionar la afluencia de personas, mejorando así la experiencia de los viajeros. La red también está lista para aprovechar los avances en inteligencia artificial y aprendizaje automático, abriendo posibilidades para un mantenimiento preventivo más efectivo y una mejora en la satisfacción del usuario [54].

4.2.2 Red eléctrica inteligente

La red eléctrica inteligente o Smart Grid es una evolución de la infraestructura tradicional de suministro de energía. Utiliza la tecnología digital para mejorar la eficiencia, fiabilidad y sostenibilidad del sistema eléctrico. En una Smart Grid, los componentes de la red, como las subestaciones, líneas de transmisión y distribución, y hasta los medidores en hogares y negocios, están interconectados y pueden comunicarse entre sí. Esto permite un control más preciso y en tiempo real de la distribución de la energía, una mejor detección y respuesta ante fallos, y una gestión más eficaz de la demanda y el suministro de energía.

En [55] se analiza la integración de la computación en la niebla en las redes eléctricas inteligentes. Esto permite un control y monitoreo casi en tiempo real del uso y producción de energía por parte de proveedores de servicios y clientes, lo que a su vez facilita un equilibrio eficaz de la carga y una

transmisión de energía fiable. Sin embargo, la gestión de los datos generados por los medidores inteligentes en las Smart Grids presenta desafíos en términos de privacidad, seguridad, flexibilidad y escalabilidad, especialmente cuando estos datos se almacenan en centros de datos basados en la Nube.

La computación en el borde emerge como una solución efectiva para estos desafíos, trasladando las tareas de procesamiento y almacenamiento de datos desde la nube hasta el perímetro de la red. Esto permite mantener localmente los datos privados, garantizando un acceso más rápido y seguro por parte de los clientes. El modelo propuesto en [55] integra esta computación distribuida en las Smart Grids, aprovechando su naturaleza descentralizada para separar la recopilación de datos públicos y privados. Este enfoque no solo reduce la latencia y mejora la seguridad, sino que también aumenta la confiabilidad de las redes eléctricas inteligentes.

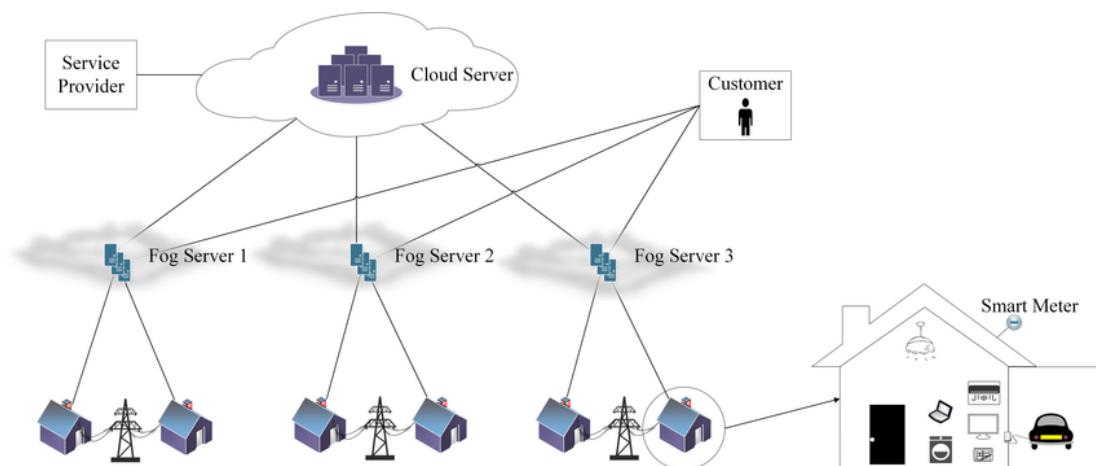


Figura 4-5 Smart Grid usando el modelo de computación en el borde [55]

4.2.3 Agricultura y acuicultura

La integración del Internet de las Cosas en la agricultura está revolucionando el sector, llevándolo hacia un futuro más eficiente, sostenible y productivo. La agricultura de precisión implica el uso de una gama de tecnologías y dispositivos IoT que permiten a los agricultores tomar decisiones precisas basadas en datos en tiempo real.

En la agricultura de precisión, los sensores desempeñan un papel crucial. Sensores de humedad del suelo ayudan a determinar los niveles óptimos de riego, evitando el desperdicio de agua y asegurando que las plantas reciban la cantidad adecuada para su crecimiento. Sensores de temperatura y humedad ambiental proporcionan información valiosa sobre las condiciones climáticas, lo que permite a los agricultores ajustar sus prácticas de cultivo, como vemos en la figura 4-6, donde vemos una aplicación práctica de un sensor de humedad en un viñedo. Sensores de nutrientes del suelo son esenciales para analizar la composición del suelo y determinar la necesidad de fertilizantes, lo que mejora la salud del cultivo y reduce el uso excesivo de químicos. Además, la utilización de imágenes satelitales y drones ofrece una perspectiva detallada y amplia de los campos, ayudando a identificar problemas como plagas o enfermedades y a tomar acciones correctivas de manera oportuna [56].



Figura 4-6 Sensores de humedad en viñedos [Tomada de plantae.garden]

En el ámbito de la acuicultura, el IoT está proporcionando herramientas similares para mejorar la eficiencia y sostenibilidad de las operaciones. El monitoreo de la calidad del agua es fundamental en la acuicultura, y se logra mediante el uso de diversos dispositivos y sensores IoT. Sensores de pH son vitales para mantener el equilibrio ácido-base adecuado en el agua, crucial para la salud de los peces. Sensores de temperatura aseguran que el agua se mantenga dentro de un rango óptimo para diferentes especies. Sensores de oxígeno disuelto monitorean los niveles de oxígeno, esenciales para la vida acuática. Además, los sensores de amoníaco y nitratos detectan niveles potencialmente dañinos de desechos en el agua, previniendo condiciones perjudiciales para los peces [57].

Tanto en la agricultura como en la acuicultura, la aplicación del IoT no solo mejora la eficiencia y la productividad, sino que también juega un papel fundamental en la sostenibilidad ambiental. Al proporcionar datos en tiempo real y un control más preciso sobre los recursos naturales, el IoT está ayudando a estos sectores a adaptarse a los desafíos del cambio climático y a satisfacer la creciente demanda de alimentos de manera más responsable y sostenible. Estos avances tecnológicos no solo benefician a los productores en términos de rendimiento y rentabilidad, sino que también contribuyen a un futuro más verde y saludable para el planeta.

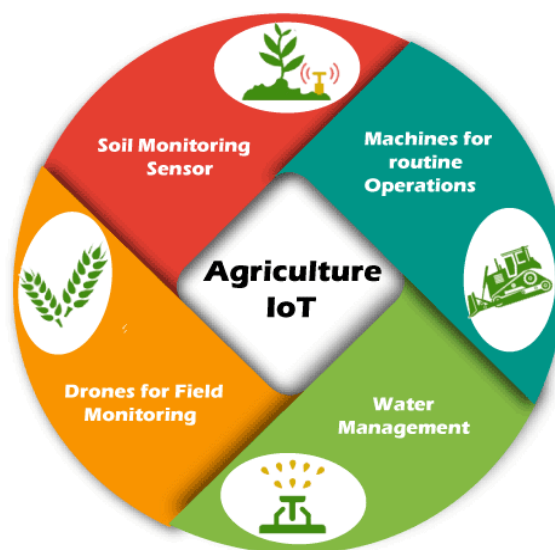


Figura 4-7 IoT en la agricultura [Tomada de javatpoint.com/iot-in-agriculture]

4.3 Ámbito militar

Tras haber explorado el impacto de estas tecnologías en el sector de la salud y las ciudades inteligentes, donde su aplicación ha resultado en avances significativos en términos de eficiencia y calidad de vida, nos enfrentamos ahora a un campo donde los desafíos son aún más complejos y las implicaciones, mucho más profundas. El sector de la Defensa, con su necesidad intrínseca de seguridad, rapidez y precisión, nos presenta un escenario donde el IoT y la computación en el borde no solo optimizan procesos, sino que se vuelven cruciales para el éxito de las misiones. En este apartado vamos a analizar cómo estas tecnologías están transformando el ámbito militar, marcando un nuevo horizonte en las estrategias de Defensa.

4.3.1 *El Internet de las Cosas en el campo de batalla*

El concepto del Internet de las Cosas se ha expandido más allá de sus aplicaciones civiles, adentrándose en el terreno del combate y la estrategia militar. En este contexto, el IoT se transforma en lo que conocemos como "Internet of Battlefield Things" (IoBT), un entramado de dispositivos interconectados que proporcionan datos críticos en tiempo real.

Adentrándonos en las aplicaciones específicas del IoT en el sector militar, uno de los usos más destacados es la recolección de conciencia del campo de batalla, donde drones y cámaras conectadas tienen un rol fundamental a la hora de mapear terrenos y posiciones enemigas, transmitiendo datos vitales al centro de mando.

Respecto al estado de salud de los soldados en el campo de batalla, se pueden adherir a los uniformes una serie de sensores que permitan no solo rastrear su estado físico en tiempo real, sino también enviar alertas sobre cambios en sus condiciones médicas. Esta capacidad de monitoreo centralizado es fundamental, ya que permite una respuesta rápida en situaciones adversas, desde la evacuación de un soldado herido hasta la administración inmediata de tratamientos médicos específicos.

La ventaja de esta tecnología es doble: por un lado, garantiza la seguridad y el bienestar de los soldados en primera línea, y por otro, permite a los equipos médicos estar preparados con el equipo y los tratamientos necesarios antes incluso de que el soldado regrese del campo. Esta anticipación en la respuesta médica significa que no se pierde tiempo vital, lo que puede marcar la diferencia en el resultado de las emergencias médicas en el campo de batalla.

Uno de los principales beneficios del IoT en la logística y el transporte militar es que permite la monitorización en tiempo real de los vehículos. Esto significa que los mandos pueden conocer en todo momento la ubicación y el estado de sus vehículos, lo que puede ser de gran utilidad en situaciones de emergencia. Por ejemplo, si un vehículo militar se avería en medio del campo de batalla, el personal a cargo puede enviar rápidamente una unidad de rescate.

Otra ventaja del IoT es que permite un enfoque proactivo en el mantenimiento. Los sensores instalados en los vehículos pueden recopilar datos sobre su rendimiento, lo que permite a los técnicos identificar posibles problemas antes de que se produzcan. Esto puede ayudar a reducir los tiempos de inactividad y mejorar la disponibilidad de los vehículos.

En el manejo de inventarios, gracias al uso de dispositivos como sensores RFID y otros sistemas de seguimiento, tenemos una visión precisa y actualizada de los recursos disponibles, desde municiones hasta equipos médicos esenciales. Esta precisión en el seguimiento garantiza que los suministros necesarios estén siempre disponibles y puedan ser desplegados con rapidez. La capacidad

de monitorear el estado y la ubicación de cada artículo no solo mejora la eficiencia en la distribución, sino que también minimiza el riesgo de escasez o excedentes [58].



Figura 4-8 IoBT [59]

La fusión del IoBT con los sistemas de Mando, Control, Comunicaciones e Inteligencia (Command, Control, Communications and Intelligence, C3I) marca un hito en las operaciones militares. Esta integración no es solo una suma de tecnologías; representa una evolución hacia un enfoque multidominio, donde la recopilación de información en tiempo real y su procesamiento inmediato son claves para una toma de decisiones ágil y certera. En este escenario, el IoBT actúa como el nervio sensorial del campo de batalla, alimentando a los sistemas C3I con datos fundamentales para una respuesta estratégica efectiva.

Esta convergencia tiene un impacto transformador en la estrategia militar. Por un lado, amplía significativamente la conciencia situacional de los mandos, proporcionándoles una visión panorámica y detallada de las dinámicas del campo de batalla. Este conocimiento profundo y actualizado permite a los líderes militares diseñar las estrategias correspondientes de una manera más precisa, optimizando la eficiencia de las operaciones.

Por otro lado, la integración del IoBT con los sistemas C3I refuerza la capacidad de las fuerzas armadas para realizar operaciones tácticas más efectivas. La agilidad en la toma de decisiones, potenciada por la accesibilidad a información en tiempo real, posibilita una respuesta rápida y adaptativa a las condiciones cambiantes del campo de batalla. Este nivel de respuesta no solo mejora la eficacia de las acciones militares, sino que también contribuye a la seguridad y protección de las tropas en primera línea [60].

La figura 4-9 muestra dos aplicaciones distintas de los sistemas C3I que resaltan la interconexión entre múltiples sistemas y dispositivos para una operación coordinada y eficiente. En el escenario militar, carros de combate, helicópteros y soldados están interconectados, proporcionando una conciencia situacional integral y facilitando una respuesta táctica conjunta en tiempo real. Esta red compleja es un ejemplo práctico de cómo el IoBT se integra con los sistemas C3I para mejorar la toma de decisiones y la eficacia operativa en un entorno de combate.

Por otro lado, el escenario de rescate ilustra la adaptabilidad de los sistemas C3I más allá del ámbito militar, mostrando su aplicación en operaciones de salvamento civiles. Aquí, la coordinación entre ambulancias y lanchas de rescate, guiadas por un centro de mando a través de comunicaciones por satélite permite una gestión eficiente y una rápida respuesta a emergencias. Este uso transversal de la tecnología C3I evidencia su valor en una variedad de situaciones críticas, tanto en defensa como en servicios civiles.

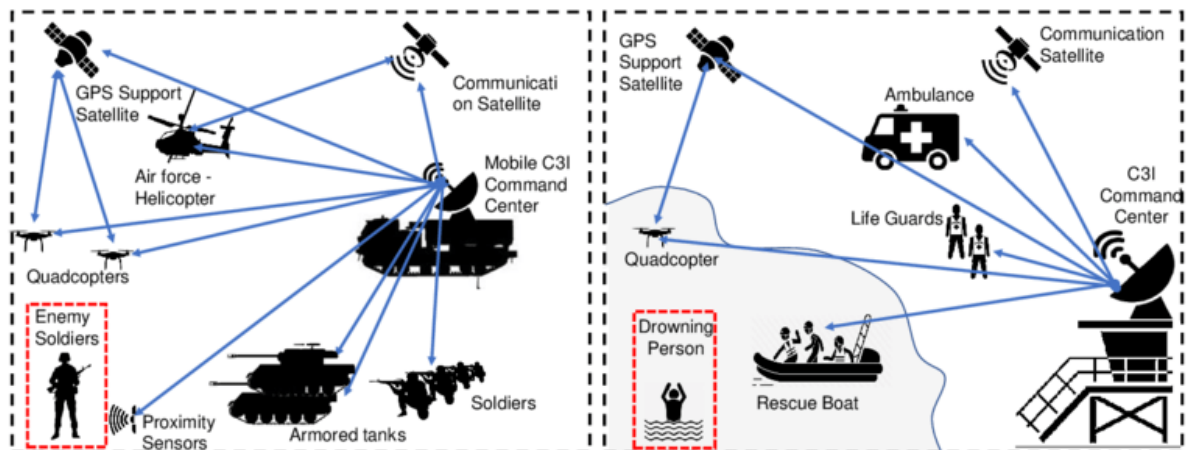


Figura 4-9 Aplicación de un sistema C3I en una operación militar y una operación de rescate [61]

4.3.2 La computación perimetral en Defensa

Las operaciones militares presentan desafíos como la necesidad de una conectividad segura y fiable en entornos de alto riesgo y en ubicaciones globales dispersas. Las misiones pueden ocurrir en ambientes con conectividad poco confiable, y cualquier retraso en la comunicación puede ser perjudicial. El Edge Computing resuelve estos problemas al procesar datos en el lugar donde se recopilan, eliminando así la dependencia de conexiones centrales que pueden ser vulnerables o lentas. Esto permite una toma de decisiones más rápida y segura directamente en el campo de acción.

La computación en el borde transforma la infraestructura de Defensa al permitir que las operaciones críticas se realicen más cerca de donde se generan los datos, lo que es fundamental en entornos de combate donde la rapidez y la fiabilidad son esenciales. Al procesar datos directamente en dispositivos locales, como en vehículos o equipos portados por soldados, se reduce la necesidad de enviar información a través de redes potencialmente comprometidas, lo que agiliza la toma de decisiones tácticas y mejora la autonomía operativa. Esta capacidad mejora la eficiencia y la seguridad de las misiones al proporcionar inteligencia y control en tiempo real en el lugar exacto donde se necesita.

Los drones tienen la capacidad de revolucionar la estrategia militar en el campo de batalla. Equipados como servidores de borde aéreos o relés, ofrecen movilidad, flexibilidad y eficiencia de costes, convirtiéndolos en soluciones óptimas para el entorno de la Defensa. Los UAVs (Unmanned Aerial Vehicles) permiten a los dispositivos IoT descargar sus tareas computacionales, ya sea procesándolas localmente o enviándolas a servidores de borde o nube cercanos. Esta capacidad de procesamiento distribuido es fundamental para operaciones que requieren una toma de decisiones rápida y precisa, como el seguimiento de objetivos en tiempo real o la evaluación de situaciones complejas.

La implementación de UAVs en sistemas de Edge Computing mejora significativamente la colaboración y sincronización entre unidades terrestres y aéreas. Actuando como nodos intermedios, no solo recopilan, sino que también procesan y distribuyen inteligencia de manera eficiente y segura. Esta tecnología es crucial en operaciones que abarcan amplias áreas geográficas o en entornos de difícil acceso, donde las comunicaciones tradicionales podrían estar comprometidas. Así, los drones habilitados para Edge Computing mantienen una ventaja táctica para las fuerzas armadas, maximizando la recopilación de datos y minimizando la latencia, lo que les permite operar con una conciencia situacional superior y, por tanto, en ventaja estratégica [62] [63].

Para equipar un dron como servidor de borde o relé en Edge Computing, se requiere instalar hardware de computación avanzado para el procesamiento intensivo de datos, sensores y cámaras de alta calidad para la recopilación de datos, tecnologías de comunicación robustas como 5G para una transmisión eficaz, software especializado para manejar el procesamiento y la toma de decisiones en tiempo real, y sistemas de seguridad y cifrado para proteger los datos y comunicaciones. Estos componentes convierten al dron en un nodo autónomo capaz de procesar y retransmitir datos.

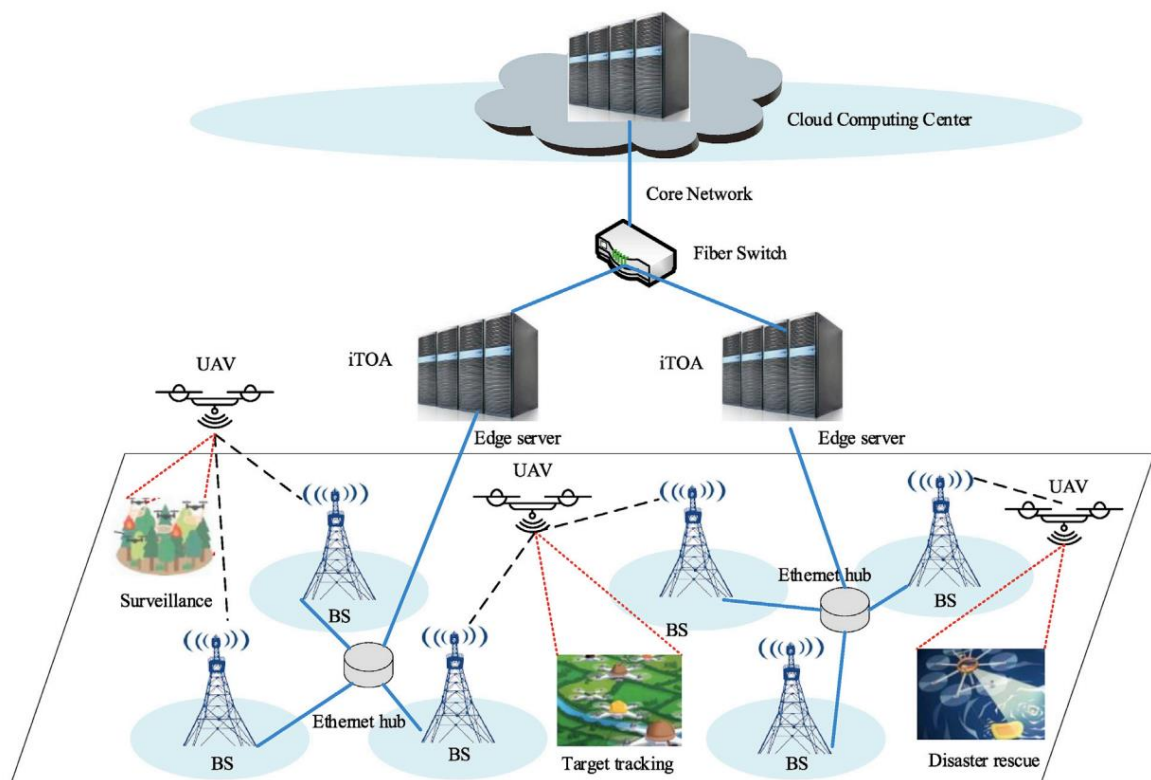


Figura 4-10 Estructura de una red de Edge Computing basada en drones [64]

En la red ilustrada en la figura 4-10, los UAVs operan como nodos de borde móviles y relés que procesan y transmiten datos, y simultáneamente como usuarios finales que llevan a cabo operaciones específicas como la vigilancia y el rescate. Esta configuración demuestra la capacidad de los UAVs para integrarse en una red de Edge Computing, desempeñando múltiples funciones críticas dentro de la misma infraestructura y mejorando así la eficiencia y efectividad de las operaciones militares.

El algoritmo inteligente de descarga de tareas (Intelligent Task Offloading Algorithm, iTOA) está diseñado específicamente para entornos de Edge Computing con UAVs, y se centra en la optimización de la latencia y la asignación de tareas [64]. Este algoritmo utiliza un enfoque de aprendizaje profundo y búsqueda de árbol para prever las condiciones futuras de la red y tomar decisiones inteligentes sobre la descarga de tareas. La latencia se consigue reducir mediante dos estrategias principales:

- Predicción de la calidad del canal de comunicación: Utilizando redes LSTM (Long Short Term Memory), el algoritmo puede anticipar la calidad futura del canal de comunicación, lo que permite a los UAVs transmitir datos a los servidores de borde en el momento óptimo. Esta predicción habilita un procesamiento más rápido de las tareas, ya que se evita esta descarga en momentos de alta latencia o baja calidad de conexión.
- Asignación eficiente de tareas: A través de la Búsqueda de Árbol de Monte Carlo (Monte Carlo Tree Search, MCTS) y una Red Neuronal Profunda Dividida (splitting Deep Neuronal Network, sDNN), iTOA evalúa múltiples políticas de descarga de tareas y selecciona la que ofrece la mejor recompensa en términos de latencia. La asignación de éstas se realiza, por tanto, de manera que se maximiza la eficiencia de los recursos disponibles, asegurando que cada tarea se envíe al servidor de borde más adecuado en el momento más oportuno.

La combinación de estas dos técnicas permite al algoritmo iTOA adaptarse a cambios en tiempo real en la demanda de la carga de trabajo y las condiciones de la red, lo que resulta en decisiones de descarga que son tanto proactivas como reactivas a las circunstancias cambiantes. Este enfoque dinámico y flexible garantiza que los UAVs no solo procesen y transmitan datos con la menor latencia posible, sino que también manejen sus cargas de trabajo de manera energéticamente eficiente, lo cual es fundamental para operaciones prolongadas y críticas. En la figura 4-11 se muestra una gráfica comparativa del algoritmo iTOA con otros algoritmos para reducir la latencia, en función de la banda de trabajo.

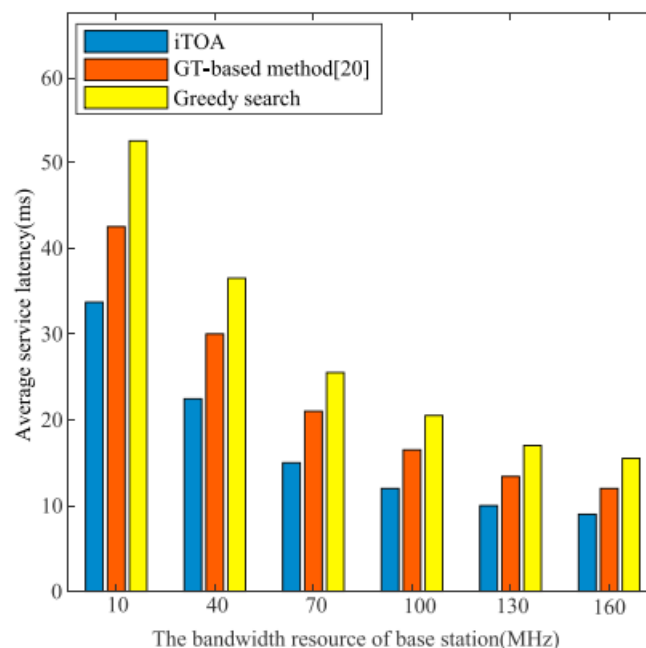


Figura 4-11 Mejora en la latencia respecto otras técnicas [64]

Numero de drones	Latencia (ms)
10	10
20	11
30	12
40	13
50	15
60	20

Tabla 4-1 Latencia del sistema según aumenta el número de drones [64]

Con los datos del estudio realizado en [64] se ha elaborado la tabla 4-1 donde se refleja la latencia media del sistema en función del número de drones. Es de esperar que a medida que aumenta el número de drones, lo hace también el tiempo de procesamiento de las tareas, y, por ende, la latencia del sistema.

El concepto subyacente de la computación perimetral, esto es, realizar el procesado de datos cerca de la fuente de donde se generan, en lugar de transmitirlos a un centro de datos centralizado para su análisis, al ser aplicado en plataformas militares como el F-35, ha revolucionado la forma en que se llevan a cabo las operaciones aéreas. Los F-35, equipados con sensores y conectados mediante el enlace de datos avanzado multifunción (Multifunction Advanced Data Link, MADL), analizan su entorno y comparten esta información entre ellos, creando así un panorama operacional unificado. Esta red de datos permite una colaboración y una comprensión del entorno de batalla en tiempo real que supera la capacidad de cualquier avión por sí solo, mejorando la toma de decisiones y la eficacia de las misiones.

La expansión de la tecnología MADL más allá de los F-35, para comunicarse con otras plataformas como aviones antiguos, buques de guerra y tanques, ilustra el potencial de la computación de borde en el ámbito militar. Un ejemplo notable es cómo un buque naval, utilizando datos de un F-35 vinculado, pudo interceptar y destruir un misil enemigo antes de que entrara en su rango de detección, demostrando así la capacidad de las fuerzas armadas para responder con rapidez y precisión a las amenazas gracias a la red de información en tiempo real [65].

Siguiendo con el F-35, en una entrevista con el director ejecutivo (Chief Executive Officer, CEO) de Lockheed Martin, Jim Taiclet aseguró que la futura versión de la aeronave que se espera para mediados del año 2024 hará computación en el borde. Destaca que el TR-2 del F-35 posee las características esenciales para un nodo de computación de borde eficaz: capacidad de almacenamiento de datos adecuada, habilidad de procesamiento de datos y un servidor robusto, así como una conexión de múltiples caminos con la nube. Taiclet subraya la necesidad de asegurarse de que estas capacidades funcionen eficientemente, lo que es crucial para el éxito del F-35 en la computación de borde [66].

Ventaja	Descripción
	Procesamiento de Datos en Tiempo Real
Procesamiento de datos en tiempo real	Permite tomar decisiones rápidas y basadas en información actualizada, crucial en operaciones militares.
Funcionamiento con conectividad limitada	Facilita operaciones en zonas remotas u hostiles donde la conexión de red es restringida.
Seguridad y privacidad de los datos	Reduce el riesgo de interceptación o manipulación de datos al procesarlos localmente.
Reducción de la latencia	Minimiza el tiempo de respuesta al procesar datos cerca de su origen, esencial en situaciones de combate.
Ahorro en ancho de banda	Envía solo información relevante o procesada a la red central, optimizando el uso del ancho de banda.
Resiliencia y autonomía	Los sistemas pueden seguir operando aun si se pierde la conexión con el centro de datos central.
Integración con tecnologías avanzadas	Facilita la combinación con IA, drones y otros sistemas avanzados, mejorando las capacidades militares.

Tabla 4-2 Principales ventajas del Edge Computing aplicadas al ámbito militar

En la tabla 4-2 se destacan las principales ventajas de la computación perimetral en el ámbito militar. Se subraya la importancia del procesamiento de datos en tiempo real para la toma de decisiones rápida y efectiva, así como la capacidad de operar en entornos con conectividad limitada, lo cual es fundamental en zonas remotas o hostiles. También se enfatiza la seguridad y privacidad de los datos, cruciales en misiones militares, y la reducción de la latencia, que mejora la velocidad de respuesta en situaciones críticas. Además, se resalta el ahorro de ancho de banda y la resiliencia y autonomía de los sistemas, permitiendo que continúen funcionando incluso en caso de desconexión del centro de datos principal. Por último, se menciona la integración con tecnologías avanzadas como la inteligencia artificial y los drones, ampliando las capacidades operativas militares. Estos aspectos consolidan al Edge Computing como una herramienta indispensable para el progreso en el sector de la Defensa.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

En este TFM se ha realizado un análisis profundo a través de las complejidades y el potencial del Internet de las Cosas y la Computación Perimetral, destacando especialmente su relevancia en el sector de la Defensa. A lo largo de este estudio, hemos visto la evolución del IoT desde sus orígenes hasta su estado actual, donde se manifiesta como un paradigma disruptivo, transformando la interacción entre el mundo digital y el físico. Sin embargo, este avance no está exento de desafíos, como la seguridad de los datos, la privacidad, la escalabilidad y la interoperabilidad, que son cruciales para su desarrollo sostenible y seguro.

En el corazón de este análisis, la integración del IoT con la Computación Perimetral ha surgido como una solución estratégica para superar limitaciones inherentes a cada tecnología por separado. Esta sinergia es particularmente potente en contextos donde la rapidez y la eficiencia en el procesamiento de datos son críticos. Hemos observado cómo las regulaciones actuales y los estándares internacionales forman el esqueleto legal y ético que sustenta esta integración, garantizando que su implementación sea segura y responsable. Además, el estudio de las arquitecturas de múltiples capas en estos sistemas ha revelado cómo se pueden estructurar de manera eficiente para optimizar el rendimiento y la seguridad, especialmente en aplicaciones sensibles como las militares.

La exploración de casos prácticos en sectores como la salud, las ciudades inteligentes y, más intensamente, en la Defensa, muestra solo una pequeña parte del amplio espectro de aplicaciones del Internet de las Cosas y la computación en el borde. En el ámbito militar, en particular, la fusión de estas tecnologías está marcando el comienzo de una era revolucionaria. La mejora en la percepción del entorno táctico y el fortalecimiento de las capacidades operativas son solo algunos de los beneficios de esta integración. La capacidad de tomar decisiones fiables y rápidas en el campo de batalla, apoyadas por datos procesados en tiempo real y cerca de donde se generan, subraya el valor incalculable de esta sinergia tecnológica.

En conclusión, este trabajo ha revelado que, aunque el IoT y la Computación Perimetral presentan desafíos individuales, su combinación abre un nuevo abanico de posibilidades, ofreciendo soluciones innovadoras a problemas complejos en varios sectores. La integración de estas tecnologías no solo aborda eficazmente sus limitaciones individuales, sino que también potencia sus fortalezas, lo que es especialmente crucial en el sector de la Defensa, donde la eficiencia, la seguridad y la rapidez son de vital importancia. Este estudio no solo proporciona una comprensión profunda de estas tecnologías en el presente, sino que también sienta las bases para su evolución y aplicación futura, abriendo caminos para investigaciones adicionales y desarrollos tecnológicos avanzados.

5.2 Líneas futuras

Este estudio ha descubierto aspectos cruciales de estas tecnologías, pero también ha revelado áreas clave donde la investigación y el desarrollo pueden expandirse y profundizarse. Las siguientes líneas futuras representan direcciones prometedoras para la continuación de este estudio:

- **Exploración de medidas de seguridad:** Una investigación más profunda sobre las medidas de seguridad actuales y emergentes en el ámbito del IoT y la Computación Perimetral es esencial. Esto incluiría el análisis de tecnologías de encriptación, autenticación y defensa contra ciberataques, con un enfoque en cómo estas medidas pueden ser optimizadas y adaptadas a nuestro caso de uso.
- **Integración con tecnologías emergentes:** La combinación de estas tecnologías con otras como la inteligencia artificial y el aprendizaje automático ofrece una línea interesante para la innovación. Investigar cómo éstas pueden complementarse para crear sistemas más eficientes y autónomos podría abrir nuevas fronteras en múltiples sectores.
- **Sostenibilidad y eficiencia energética:** Con la creciente implementación de dispositivos IoT, es vital investigar formas de mejorar su sostenibilidad y eficiencia energética. Esto podría incluir el desarrollo de dispositivos de bajo consumo, así como la integración de fuentes de energía renovables y sostenibles.
- **Aplicaciones en nuevos sectores:** Ampliar el enfoque a sectores no explorados en este trabajo. Por ejemplo, en el sector educativo, estas tecnologías podrían revolucionar la forma en que se gestionan y monitorean las instituciones educativas, desde el mantenimiento de la infraestructura hasta la personalización de la experiencia de aprendizaje. Otro sector interesante es el de la energía, donde estas tecnologías podrían optimizar la distribución y el consumo de energía, contribuyendo a la creación de ciudades más sostenibles y eficientes.
- **Avances en comunicación y conectividad:** La evolución de la tecnología de comunicaciones, como las redes 5G y futuras, es crucial para el desarrollo del IoT y el Edge Computing. Investigar cómo estas tecnologías pueden mejorar la comunicación y la interconectividad entre dispositivos podría llevar a un mayor rendimiento y capacidad de respuesta.
- **Impacto y desarrollo social:** Esta línea de investigación se centraría en explorar cómo estas dos tecnologías pueden ser impulsores para el progreso social y la reducción de desigualdades. Podría evaluarse el potencial de estas tecnologías para mejorar el acceso a servicios esenciales como educación y salud en comunidades marginadas, analizar su rol en el desarrollo económico de regiones en crecimiento, y estudiar su impacto en la cohesión social y la integración comunitaria. Este enfoque permitiría no solo entender el alcance tecnológico del IoT y el Edge Computing, sino también su capacidad para generar cambios sociales significativos y duraderos.

6 BIBLIOGRAFÍA

- [1] Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, 3(05), 164.
- [2] Ashton, K. (2009). That ‘internet of things’ thing. *RFID journal*, 22(7), 97-114.
- [3] The "Only" Coke Machine on the Internet. cs.cmu.edu/~coke/history_long.txt
- [4] Romkey, J. (2016). Toast of the IoT: the 1990 interop internet toaster. *IEEE Consumer Electronics Magazine*, 6(1), 116-119.
- [5] Gershenfeld, N. A. (1999). *When things start to think*. Macmillan.
- [6] "Internet of Things History". postscapes.com/iot-history/
- [7] "Nabaztag" nabaztag.com
- [8] Vasseur, J. P., Bertrand, C. P., Aboussouan, B., Gnoske, E., Pister, K., Culler, D., ... & Huotari, A. (2010). A survey of several low power link layers for IP smart objects. *White Paper, IPSO Alliance*.
- [9] Evans, D. (2011). The internet of things. *How the Next Evolution of the Internet is Changing Everything, Whitepaper, Cisco Internet Business Solutions Group (IBSG)*, 1, 1-12.
- [10] Statista & Transforma Insights. statista.com/statistics/1183457/iot-connected-devices-worldwide/
- [11] Transforma Insights. transformainsights.com/research/forecast/highlights
- [12] Rayes, A., & Salam, S. (2022). The things in iot: Sensors and actuators. In *Internet of Things From Hype to Reality: The Road to Digitization* (pp. 63-82). Cham: Springer International Publishing.
- [13] Sehrawat, D., & Gill, N. S. (2019, April). Smart sensors: Analysis of different types of IoT sensors. In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 523-528). IEEE.
- [14] Irmak, E., & Bozdal, M. (2018). Internet of Things (IoT): The most up-to-date challenges, architectures, emerging trends and potential opportunities. *International Journal of Computer Applications*, 179(40), 20-27.
- [15] Satyanarayanan, M. (2017). The emergence of edge computing. *Computer*, 50(1), 30-39.
- [16] Dilley, J., Maggs, B., Parikh, J., Prokop, H., Sitaraman, R., & Weihl, B. (2002). Globally

distributed content delivery. *IEEE Internet Computing*, 6(5), 50-58.

- [17] Noble, B. D., Satyanarayanan, M., Narayanan, D., Tilton, J. E., Flinn, J., & Walker, K. R. (1997). Agile application-aware adaptation for mobility. *ACM SIGOPS Operating Systems Review*, 31(5), 276-287.
- [18] Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13-16).
- [19] Surbiryala, J., & Rong, C. (2019, August). Cloud computing: History and overview. In *2019 IEEE Cloud Summit* (pp. 1-7). IEEE.
- [20] impulso06.com/edge-computing-la-mayor-revolucion-desde-la-nube/
- [21] Cao, K., Liu, Y., Meng, G., & Sun, Q. (2020). An overview on edge computing research. *IEEE access*, 8, 85714-85728.
- [22] Khan, W. Z., Ahmed, E., Hakak, S., Yaqoob, I., & Ahmed, A. (2019). Edge computing: A survey. *Future Generation Computer Systems*, 97, 219-235.
- [23] Li, J., Zhou, G., Tian, T., & Li, X. (2021). A new cooling strategy for edge computing servers using compact looped heat pipe. *Applied Thermal Engineering*, 187, 116599.
- [24] Pei, Q., Chen, S., Zhang, Q., Zhu, X., Liu, F., Jia, Z., ... & Yuan, Y. (2022, February). CoolEdge: hotspot-relievable warm water cooling for energy-efficient edge datacenters. In *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems* (pp. 814-829).
- [25] Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., & Lv, W. (2019). Edge computing security: State of the art and challenges. *Proceedings of the IEEE*, 107(8), 1608-1631.
- [26] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zhou, Y. (2017). Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)* (pp. 1093-1110).
- [27] cardinalpeak.com/blog/leveraging-iot-security-standards-to-help-ensure-embedded-security
- [28] General Data Protection Regulation (GDPR). gdpr-info.eu/
- [29] California Consumer Privacy Act (CCPA). oag.ca.gov/privacy/ccpa
- [30] ftc.gov/business-guidance/blog/2023/06/hey-alexa-what-are-you-doing-my-data
- [31] http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm
- [32] isotools.us/2018/11/21/norma-iso-iec-30141-internet-cosas-iot/
- [33] news.itsmf.es/iso-iec-274002022-para-la-ciberseguridad-y-privacidad-del-iot/
- [34] Oughton, E. J., Lehr, W., Katsaros, K., Selinis, I., Bubley, D., & Kusuma, J. (2021). Revisiting wireless internet connectivity: 5G vs Wi-Fi 6. *Telecommunications Policy*, 45(5), 102127.
- [35] Ahmed, N., Rahman, H., & Hussain, M. I. (2016). A comparison of 802.11 ah and 802.15. 4 for IoT. *Ict Express*, 2(3), 100-102.
- [36] Kwak, K. S., Ullah, S., & Ullah, N. (2010, November). An overview of IEEE 802.15. 6 standard. In *2010 3rd international symposium on applied sciences in biomedical and communication technologies (ISABEL 2010)* (pp. 1-6). IEEE.

- [37] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE internet of things journal*, 4(5), 1125-1142.
- [38] netburner.com/learn/architectural-frameworks-in-the-iot-civilization/
- [39] Lombardi, M., Pascale, F., & Santaniello, D. (2021). Internet of things: A general overview between architectures, protocols and applications. *Information*, 12(2), 87.
- [40] jelvix.com/blog/iot-architecture-layers
- [41] Omoniwa, B., Hussain, R., Javed, M. A., Bouk, S. H., & Malik, S. A. (2018). Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues. *IEEE Internet of Things Journal*, 6(3), 4118-4149.
- [42] Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017, May). Internet of Things (IoT) communication protocols. In *2017 8th International conference on information technology (ICIT)* (pp. 685-690). IEEE.
- [43] Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2018, March). Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT. In *2018 IEEE international conference on pervasive computing and communications workshops (percom workshops)* (pp. 197-202). IEEE.
- [44] Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT express*, 5(1), 1-7.
- [45] Gomez, C., Oller, J., & Paradells, J. (2012). Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *sensors*, 12(9), 11734-11753.
- [46] mokolara.com/es/lora-and-wireless-technologies/
- [47] Naik, G. P., & Bapat, A. U. (2020). A brief comparative analysis on application layer protocols of internet of things: MQTT, CoAP, AMQP and HTTP. *Int. J. Comput. Sci. Mob. Comput*, 9(9), 135-141.
- [48] trendmicro.com/vinfo/es/security/news/internet-of-things/mqtt-and-coap-security-and-privacy-issues-in-iot-and-iiot-communication-protocols
- [49] Wan, J., Gu, X., Chen, L., & Wang, J. (2017, October). Internet of things for ambient assisted living: challenges and future opportunities. In *2017 International conference on cyber-enabled distributed computing and knowledge discovery (CyberC)* (pp. 354-357). IEEE.
- [50] Krishnamoorthy, S., Dua, A., & Gupta, S. (2023). Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. *Journal of Ambient Intelligence and Humanized Computing*, 14(1), 361-407.
- [51] Kishor, A., Chakraborty, C., & Jeberson, W. (2021). A novel fog computing approach for minimization of latency in healthcare using machine learning.
- [52] Zantalis, F., Koulouras, G., Karabetsos, S., & Kandris, D. (2019). A review of machine learning and IoT in smart transportation. *Future Internet*, 11(4), 94.
- [53] cleverciti.com/en/resources/blog/cleverciti-launches-state-of-the-art-smart-parking-guidance-system-in-cologne
- [54] govtech.com/transportation/making-new-york-a-smart-city-through-connected-public-transport.html

- [55] Okay, F. Y., & Ozdemir, S. (2016, May). A fog computing based smart grid model. In *2016 international symposium on networks, computers and communications (ISNCC)* (pp. 1-6). IEEE.
- [56] Khanna, A., & Kaur, S. (2019). Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture. *Computers and electronics in agriculture*, 157, 218-231.
- [57] Tamim, A. T., Begum, H., Shachcho, S. A., Khan, M. M., Yeboah-Akowuah, B., Masud, M., & Al-Amri, J. F. (2022). Development of IoT based fish monitoring system for aquaculture. *Intelligent Automation & Soft Computing*, 32(1), 55-71.
- [58] analyticssteps.com/blogs/7-applications-iot-defence-and-military
- [59] Kott, A., Swami, A., & West, B. J. (2016). The internet of battle things. *Computer*, 49(12), 70-75.
- [60] Russell, S., & Abdelzaher, T. (2018, October). The internet of battlefield things: the next generation of command, control, communications and intelligence (C3I) decision-making. In *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)* (pp. 737-742). IEEE.
- [61] Ahmad, H., Dharmadasa, I., Ullah, F., & Babar, M. A. (2023). A review on c3i systems' security: Vulnerabilities, attacks, and countermeasures. *ACM Computing Surveys*, 55(9), 1-38.
- [62] Xia, X., Fattah, S. M. M., & Babar, M. A. (2023). A survey on UAV-enabled edge computing: Resource management perspective. *ACM Computing Surveys*, 56(3), 1-36.
- [63] Wu, W., Zhou, F., Wang, B., Wu, Q., Dong, C., & Hu, R. Q. (2022). Unmanned aerial vehicle swarm-enabled edge computing: Potentials, promising technologies, and challenges. *IEEE Wireless Communications*, 29(4), 78-85.
- [64] Chen, J., Chen, S., Luo, S., Wang, Q., Cao, B., & Li, X. (2020). An intelligent task offloading algorithm (iTOA) for UAV edge computing network. *Digital Communications and Networks*, 6(4), 433-443.
- [65] boozallen.com/s/insight/blog/how-the-us-military-is-using-edge-computing.html
- [66] airandspaceforces.com/lockheed-ceo-f-35-tech-refresh-3/

7 LISTADO DE ACRÓNIMOS

Acronym	Definition
AAL	Ambient Assisted Living
AES	Advanced Encryption Standard
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
BAN	Body Area Network
C3I	Command, Control, Communications and Intelligence
CCPA	California Consumer Privacy Act
CDN	Content Delivery Network
CEO	Chief Executive Officer
CoAP	Constrained Application Protocol
DDoS	Distributed Denial of Service
DTLS	Datagram Transport Layer Security
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
H-IoT	Healthcare Internet of Things
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IBSG	Internet Business Solution Group
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMDS	Intelligent Multimedia Data Segregation
IoBT	Internet of Battlefield Things

IoT	Internet of Things
IP	Internet Protocol
IPSO	Internet Protocol for Smart Objects
ISO	International Organization for Standardization
iTOA	Intelligent Task Offloading Algorithm
ITU	International Telecommunication Union
LED	Light Emitting Diode
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power Wide Area Network
LSTM	Long Short Term Memory
M2M	Machine to Machine
MADL	Multifunction Advanced Data Link
MCTS	Monte Carlo Tree Search
MQTT	Message Queuing Telemetry Transport
MTA	Metropolitan Transportation Authority
NB-IoT	Narrowband Internet of Things
NFC	Near Field Communication
PaaS	Platform as a Service
PIPL	Personal Information Protection Law
QoS	Quality of Service
RAM	Random Access Memory
RFID	Radio Frequency Identification
ROM	Read Only Memory
SaaS	Software as a Service
SASL	Simple Authentication and Security Layer

sDNN	Splitting Deep Neuronal Network
SOA	Service-oriented Architecture
TCP	Transmission Control Protocol
TI	Tecnologías de la Información
TFM	Trabajo de Fin de Máster
UAV	Unmanned Aerial Vehicles
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network
WNAN	Wireless Neighbourhood Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network