ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELECTRÍCA Y ELECTRÓNICA

ARQUITECTURAS Y MODELOS DE REFERENCIA PARA SISTEMAS IOT

ESTADO DEL ARTE DE LAS ARQUITECTURAS PARA SISTEMAS IOT

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

DUSTIN FELIPE BUITRÓN RUIZ

dustin.buitron@epn.edu.ec

SORAYA LUCÍA SINCHE MAITA, PHD

soraya.sinche@epn.edu.ec

DMQ, febrero 2022

CERTIFICACIONES

Yo, DUSTIN FELIPE BUITRÓN RUIZ declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

Dustin Felipe Buitrón Ruiz

Certifico que el presente trabajo de integración curricular fue desarrollado por DUSTIN FELIPE BUITRÓN RUIZ, bajo mi supervisión.

Soraya Lucía Sinche Maita, PhD
DIRECTORA

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

DUSTIN FELIPE BUITRÓN RUIZ

SORAYA LUCÍA SINCHE MAITA, PHD

DEDICATORIA

Dedico este trabajo a mis padres, ellos han sido las personas que desde instancias cortas de la vida me han enseñado el significado del esfuerzo, han sido mi fuente de inspiración para lograr cada meta que me he propuesto. Son los pilares de mi vida, quienes han estado para brindarme su cariño y apoyo tanto en los momentos felices como en las penurias. Sin ellos nada de esto sería posible, los amo.

AGRADECIMIENTO

A mis padres: María Ruiz y Felipe Buitrón

Por su apoyo, confianza, motivación y los valores que me supieron inculcar desde pequeño.

A mis hermanos: Juan y María Buitrón

Por su motivación y apoyo incondicional brindados durante todos estos años.

A los amigos formados en la universidad

Por su amistad y conocimiento brindado durante esta etapa.

A Soraya L. Sinche Maita, PhD.

Por el apoyo, esfuerzo y tiempo dedicado en la dirección de este trabajo.

A Ing. Pablo Hidalgo

Por el apoyo y tutoría brindada durante esta etapa.

A la Escuela Politécnica Nacional

y a cada docente por los conocimientos impartidos, los cuales son la base tanto de mi formación académica como personal.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Los sistemas IoT han tomado gran importancia, llegando a ser desplegados en varias áreas de aplicación y permitiendo a los usuarios la posibilidad de controlar las acciones del sistema desde un dispositivo inteligente de manera remota e instantánea. Sin embargo, estos sistemas poseen arquitecturas IoT distintas, pues no se cuenta con una arquitectura estandarizada común que haya sido aceptada por los desarrolladores, esto provoca que la interoperabilidad de sistemas IoT sea compleja o en el peor de los casos, imposible.

En el presente trabajo se realiza una revisión y análisis de las diferentes arquitecturas y modelos de referencia para sistemas IoT desarrolladas en los últimos 5 años, comparando sus áreas de aplicación y su estructura por capas, así como sus funcionalidades. De modo que se contribuye a mejorar la perspectiva del estado actual de arquitecturas y modelos de referencia para sistemas IoT y conocer cuáles son los principales problemas (y sus respectivas soluciones) al momento de trabajar con dispositivos heterogéneos.

El trabajo cuenta con un total de 3 capítulos. En el primer capítulo se presentan los conceptos de un sistema IoT, sus componentes, áreas de aplicación y beneficios. En el segundo capítulo se analizan arquitecturas y modelos de referencia IoT, comparando sus capas y las funcionalidades de éstas. En el tercer capítulo se establece el nivel de madurez de cada arquitectura y modelo de referencia para sistemas IoT que ha sido revisado, y se definen los principales problemas al trabajar con dispositivos heterogéneos.

PALABRAS CLAVE: Arquitecturas IoT, Sistemas IoT, Modelo de Referencia IoT.

ABSTRACT

Actually, IoT systems have taken on great importance by becoming deployed in diverse areas and allowing users to control the system's actions remotely and instantly from smart devices. Nevertheless, these systems have different IoT architectures, since there is no common standardized architecture that has been accepted by developers, thus causing the interoperability of the IoT system to be complex or, in the worst cases impossible.

This work reviews and analyzes the different architectures and models developed in the last 5 years, that are used as a reference for IoT systems, by comparing their application areas and their layered structure and their functionalities. This contributes to improving the current perspective of the reference architectures and models for IoT systems and identifying the main problems and their respective solutions when working with heterogeneous devices.

This study has a total of 3 chapters. The first chapter presents the concepts of an IoT system, its components, application areas, and benefits. In the second chapter architectures and IoT reference models are analyzed, comparing their layers and functionalities. The third chapter establishes the maturity level of each reference architecture and model for IoT systems that have been reviewed and defines the main problems when working with heterogeneous devices.

KEYWORDS: IoT Architectures, IoT Systems, IoT Reference Model.

1 INTRODUCCIÓN

En la actualidad, los sistemas IoT (*Internet of Things*) se encuentran trabajando en diferentes campos, formando parte de la vida diaria de las personas, debido a esto surgen varios desafíos relacionados con la estandarización, el manejo de dispositivos heterogéneos, escalabilidad y seguridad.

Si se aborda lo relacionado a la estandarización, se dispone de varias arquitecturas y modelos de referencias, algunos propietarios otros de tipo abierto, dando cabida a problemas debido a la falta de un estándar común y la poca madurez de las arquitecturas propuestas.

Al no disponer de un único estándar al momento de implementar un sistema IoT se pueden presentar fallos al interoperar los diferentes dispositivos y muchas de las veces se tenga que estar atado a soluciones propietarias. Por este motivo es importante disponer de un estudio del estado del arte de las arquitecturas en sistemas IoT y mostrar como éstas evolucionan y se adaptan a un mundo cambiante, en el que la seguridad se vuelve un factor crítico en varias aplicaciones IoT que van acoplándose a todo tipo de industrias existentes.

El presente Trabajo de Integración Curricular, presenta el estado del arte de las arquitecturas propuestas para sistemas IoT en los últimos 5 años. Para lo cual se ha recopilado información de diversas publicaciones en las que se observan propuestas de arquitectura o modelos de referencia para sistemas IoT, lo que evidencia la gran cantidad de arquitecturas propuestas, pues cada autor en función de suplir una necesidad desarrolla su propia idea y la aplica en un área determinada de los sistemas IoT.

Al observar la diversidad existente en cuanto a arquitecturas y modelos de referencia para sistemas IoT, resulta importante abstraer las funcionalidades de las capas propuestas en cada una éstas, de modo que, sea posible contrastar estas funcionalidades para observar las similitudes presentes entre las arquitecturas y modelos de referencia para sistemas IoT. Otro aspecto relevante por analizar es la evolución de las arquitecturas y modelos de referencia a lo largo de los últimos 5 años.

De igual manera, es importante definir el nivel de madurez que posee cada arquitectura y si ésta se encuentra estandarizada o no, con el fin de determinar cuáles son las mejores opciones al momento de implementar un sistema IoT. Contribuyendo así con una perspectiva más clara del estado actual de las arquitecturas y modelos de referencia para sistemas IoT y cuáles son las tendencias en este campo.

1.1 OBJETIVO GENERAL

Analizar el Estado del Arte de las Arquitecturas para Sistemas IoT.

1.2 OBJETIVOS ESPECÍFICOS

1. Presentar los Conceptos de los Sistemas IoT y sus áreas de aplicación.
2. Analizar las arquitecturas y modelos de referencia para Sistemas IoT, considerando la cantidad de capas que define cada una y sus funcionalidades.
3. Contrastar las arquitecturas y modelos de referencia con diferentes áreas de aplicación.
4. Analizar el nivel de madurez de las Arquitecturas de Sistemas IoT, así como sus limitaciones.

1.3 ALCANCE

El presente Trabajo de Integración Curricular tiene como objetivo presentar el estado del arte de las arquitecturas y modelos de referencia definidos para sistemas IoT, para lo cual se empezará por desarrollar una fase teórica en donde se estudiarán las características de sistemas IoT, poniendo énfasis en las aplicaciones de estos, como lo son, el cuidado de la salud, ciudades inteligentes, medio ambiente, industrial, educación, entre otros. La información de los modelos de referencia y las arquitecturas será recopilada de fuentes publicadas en los últimos 5 años.

De la información recopilada se extraerá aquella que se considere más relevante, de manera que se revise cada modelo de referencia o arquitectura. Esto permitirá desarrollar una fase de análisis metodológico. Entre los puntos a analizar se tiene la cantidad de capas que define cada una y las funcionalidades establecidas para dichas capas. Se esquematizará mediante una línea del tiempo las arquitecturas y modelos de referencia relevantes para el estado del arte.

Se desarrollará un análisis comparativo en donde se encontrarán las coincidencias entre las arquitecturas y modelos de referencia de diferentes áreas de aplicación de sistemas IoT, permitiendo así conocer qué arquitecturas o modelos de referencia son más afines a cierto tipo de aplicaciones IoT.

Finalmente, se entrará en una fase de análisis de resultados, donde se podrá tener una visión global de las arquitecturas en sistemas IoT, de modo que se definirá el detalle de madurez de cada una de ellas y se analizarán las limitaciones que están presentes en la interoperabilidad de dispositivos heterogéneos.

1.4 MARCO TEÓRICO

1.4.1 DEFINICIÓN DE UN SISTEMA IOT

El término "*Internet of Things*" (IoT) fue empleado por primera vez en 1999 por Kevin Ashton, refiriéndose a IoT como la conexión de objetos mediante tecnología de identificación por radiofrecuencia (RFID) [1]. Sin embargo, en la actualidad, el objetivo y la visión que persigue IoT es el de convertir dispositivos tradicionales (relojes, televisores, cámaras de seguridad, entre otros) en dispositivos inteligentes que interactúen a través del Internet, por lo que, de manera general IoT puede verse como una red de objetos físicos interconectados mediante diversas tecnologías [2].

Existen tres principales visiones o perspectivas de IoT, que son: orientada al "Internet", orientada a las "Cosas" y orientada a la "Semántica". Según la perspectiva orientada al "Internet", IoT puede ser considerado como una infraestructura global permitiendo la interconexión entre objetos físicos y virtuales. La perspectiva orientada a las "Cosas" incluye únicamente aspectos físicos, es decir, se considera a las cosas como "entidades reales" o "entidades virtuales" las cuales pueden escuchar, procesar, sensar, compartir información y coordinar decisiones para cumplir con un propósito en específico. Finalmente, la perspectiva orientada a la "Semántica" hace referencia a la capacidad de extraer conocimiento de diferentes dispositivos para proporcionar un servicio [3].

De acuerdo con las perspectivas tomadas en cuenta, se pueden encontrar diferentes definiciones del Internet De las Cosas. IBM (*International Business Machines Corporation*) define a IoT como la red que conecta personas y cosas, las cuales recopilan y comparten información del entorno que las rodea [4]. Por otra parte, Gartner en [5] define a IoT como la red de objetos físicos que usan diferentes tecnologías para poder comunicarse con su entorno y con sus estados internos. Por último, el Diccionario de Oxford define a IoT como la interconexión de dispositivos (objetos cotidianos) a través de Internet, permitiendo así compartir datos [6]. Como se puede observar la definición de IoT es variada, por este motivo es importante considerar todas las perspectivas de IoT para tener un concepto más claro sobre el tema.

1.4.2 ESTRUCTURA DE UN SISTEMA IOT

Para tener una mejor percepción del significado de IoT es importante conocer los elementos que conforman un sistema IoT. Según [7] un sistema IoT se encuentra formado por 4 bloques fundamentales, los cuales pueden ser observados en la Figura 1.1.

A continuación, se detallará cada uno de los elementos que conforman un sistema IoT.

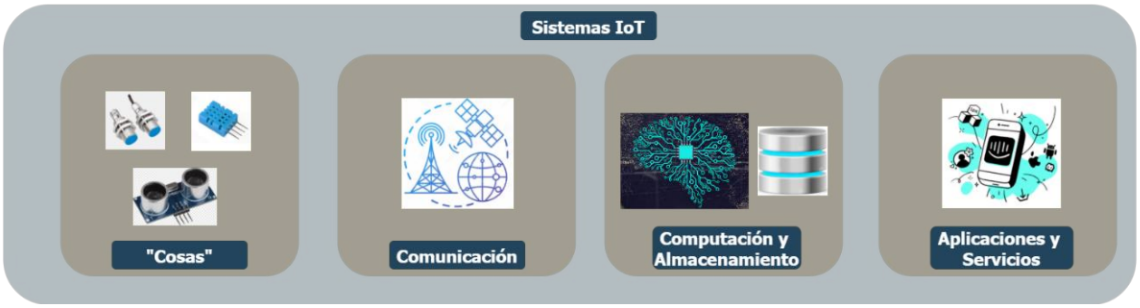


Figura 1.1. Diagrama de bloques de un sistema IoT basado en [7]

- **"Cosas":** es un dispositivo inteligente con la capacidad de recopilar datos mediante uno o varios sensores. Una "Cosa" puede ser un hardware embebido, un dispositivo o un sensor inteligente. Un sistema IoT puede estar conformado por una gran cantidad de dispositivos, por lo que se incluyen métodos de identificación como EPC (*Electronic Product Codes*) y uCode (*ubiquitous Code*). Las "Cosas" pueden estar interconectadas con tecnologías IP o no-IP.
- **Comunicación:** hace referencia a la infraestructura de red que permita el envío y recepción de datos a través de redes cableadas o inalámbricas. Entre las tecnologías de comunicación más usadas se tienen: Bluetooth, BLE (*Bluetooth Low Energy*), RFID, UWB (*Ultra-Wide Band*), NFC (*Near Field Communication*), WiFi, IEEE 802.15.4, Z-Wave, LTE (*Long Term Evolution*), LTE-Advanced, entre otras.
- **Computación y Almacenamiento:** donde se procesan y almacenan datos para obtener información relevante para una determinada aplicación IoT. En estos sistemas la Inteligencia Artificial (IA) y el Aprendizaje Automático (ML-*Machine Learning*) tienen un rol importante, primero en el procesamiento de los datos y segundo en el análisis de la información obtenida.

  Con el avance tecnológico y la migración de la computación física a la nube, las plataformas en la nube han pasado a formar una parte importante del elemento de la computación de los sistemas IoT, donde los datos pueden ser procesados en tiempo real, para proveer a las aplicaciones y servicios del conocimiento extraído.
- **Aplicaciones y Servicios:** los sistemas IoT tienen la finalidad de ofrecer servicios gracias a los cuales los usuarios pueden interactuar con determinadas aplicaciones. Las áreas de aplicación se pueden clasificar en dominios como: el cuidado de la salud, cuidado de la salud, medio ambiente, industria, comercio, entre otros [8].

1.4.3 IMPACTO DE LOS SISTEMAS IOT

Los sistemas IoT impactan en las actividades realizadas por las personas, por ejemplo, el propietario de una empresa puede mejorar la toma de decisiones en base a conocimiento

generado por el procesamiento de datos en un sistema IoT, de manera que pueda gestionar correctamente sus recursos mejorando así la productividad. En un contexto cotidiano, una persona puede hacer uso de un reloj inteligente para llevar un registro de la actividad física realizada de manera periódica [9]. De esta manera, se puede observar cómo los sistemas IoT influyen en las actividades realizadas por las personas día a día.

La cantidad de dispositivos conectados a Internet ha crecido de manera exponencial, hasta llegar a tal punto en que supera a la población mundial. En el año 2015 existían alrededor de 15 billones de dispositivos conectados al Internet, para el año 2020 se observó un gran cambio al tener alrededor de 31 billones de dispositivos conectados, para el año 2025, se proyecta tener 75 billones de dispositivos conectados al Internet [9] (Figura 1.2).

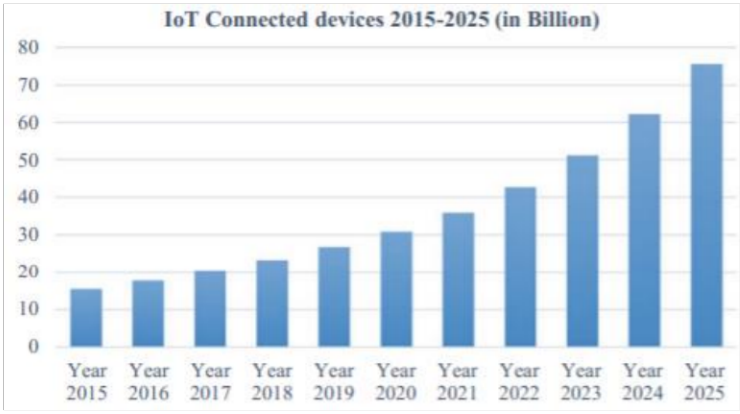


Figura 1.2. Dispositivos IoT conectados al Internet entre 2015 y 2025 [9]

La calidad de vida no es el único factor relacionado con el desarrollo de sistemas IoT, según McKinsey's global Economic [10], para el año 2025 el impacto económico del Internet de las Cosas se encontrará entre 2.7 y 6.2 billones de dólares. Llegando a tener un gran impacto en el desarrollo de dispositivos para el cuidado de la salud, con un 41% del total de dispositivos IoT desarrollados para dicho año [11].

1.4.4 ÁREAS DE APLICACIÓN

De acuerdo con lo planteado en [8] y [12] las áreas o dominios de aplicación de los sistemas IoT son variadas y se despliegan en diversos tipos de mercado, en el presente trabajo de integración curricular se ha generado un taxonomía compuesta por: Cuidado de la Salud, Transporte, Hogar Inteligente, Ciudad Inteligente, Agricultura y Cuidado Ambiental, Comercio e Industria, la cual puede observarse en la Figura 1.3.

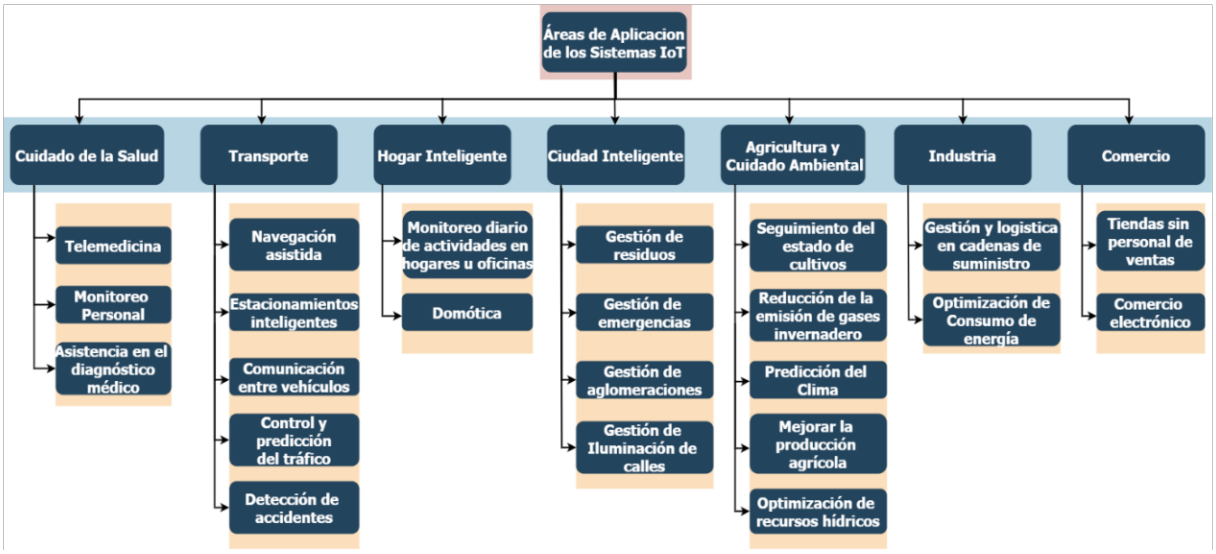


Figura 1.3. Taxonomía de áreas de aplicación de sistemas IoT basado en [8] y [12]

1.4.4.1 Cuidado de la Salud

Las aplicaciones de los sistemas IoT en el Cuidado de la Salud pueden realizar tareas simples como monitorear signos vitales de una persona (presión arterial, ritmo cardíaco, nivel de oxigenación en la sangre, etc.) o incluso en un futuro poder monitorear enfermedades crónicas, de manera que los datos recopilados sirvan como apoyo para el diagnóstico médico realizado por un especialista [12].

Una visión al futuro en el campo de la medicina puede ser muy prometedora siempre que el desarrollo en esta área evolucione y permita que la atención médica de manera remota (Telemedicina) sea accesible para una gran cantidad de personas. De tal modo que especialistas de la salud puedan dar un seguimiento continuo a personas con enfermedades crónicas como diabetes, obesidad, arritmia cardíaca, insuficiencia cardíaca, entre otras, posibilitando la opción de brindar un atención rápida y oportuna [13] y [14].

1.4.4.2 Transporte

La incorporación de los sistemas IoT ha dotado a los sistemas de transporte de la capacidad de “recolectar” y “procesar” datos, llevando así a desarrollar sistemas de transporte inteligentes. Uno de los temas a destacar en el área del Transporte inteligente es la Navegación, mediante la recolección de datos generados por sensores IoT embebidos en sistemas de transporte o dispositivos IoT colocados en lugares estratégicos de las zonas viales; estos sistemas pueden llegar estimar el tráfico y la congestión vehicular de una zona, establecer rutas que optimicen el tiempo de viaje del usuario y por ende reducir las emisiones de gases tóxicos de los automóviles, de este modo se puede

evidenciar que el desarrollo de una sistema de transporte inteligente también puede beneficiar en la salud del ser humano [12] y [15].

En esta área de aplicación también se han propuesto sistemas IoT que incorporen sensores inteligentes en luces de carretera, estos son capaces de detectar las condiciones o presencia de tráfico y operar en presencia de automóviles o peatones, apoyando así a reducir el consumo de energía excesivo en las carreteras [15].

1.4.4.3 Hogar Inteligente

Las casas inteligentes se encuentran provistas con una cantidad significativa de dispositivos inteligentes y sensores como teléfonos celulares, laptops, cámaras de seguridad, luces, electrodomésticos y persianas. Los sistemas IoT en esta área permiten a las personas controlar los dispositivos de casa en forma remota ya sea desde un celular o una aplicación web. Por ejemplo, el teléfono celular puede ser usado como centro de control, mediante el cual es posible administrar los dispositivos del hogar, ya sea para apagar luces, revisar cámaras de seguridad o inclusive programar actividades de electrodomésticos como el ciclo de lavado de una lavadora [16].

De manera general un sistema IoT orientado al área de Hogar Inteligente debe cumplir con 4 funciones básicas [17]:

- **Recolección de datos:** se puede considerar la función primordial en un sistema IoT de este tipo, ya que en una casa inteligente se podrían recolectar datos de su entorno a través de sensores y dispositivos inteligentes, y mediante el procesamiento ejecutado por sistema se puede notificar al usuario final.
- **Alerta:** un sistema debe ser capaz de emitir una alerta de acuerdo con umbrales especificados, en base al tipo de parámetro medido. Por ejemplo, un detector de humo puede medir la cantidad de humo en el ambiente y emitir una alerta de posible incendio. La alerta debe contener información del parámetro medido y puede ser enviada por email, notificación de una aplicación o inclusive una red social.
- **Control:** permite al usuario controlar los dispositivos inteligentes del hogar, pueden ser controles desde encender o apagar una luz hasta automatizar una actividad como encender el aire acondicionado cuando la temperatura supera un umbral.
- **Procesamiento de datos:** función que hace uso de la Inteligencia Artificial del sistema IoT, la cual permite generar conocimiento que sea útil tanto para el usuario final de la aplicación como para el desarrollador de ésta.

1.4.4.4 Ciudad Inteligente

En el presente trabajo se ha tomado al transporte como un área de aplicación adicional ya que puede funcionar independientemente del desarrollo de otras áreas que se consideran en las Ciudades Inteligentes.

Los sistemas IoT desarrollados para Ciudades Inteligentes buscan optimizar servicios públicos como la gestión de aparcamiento, iluminación de calles, gestión de residuos y emergencias. Todos estos servicios implican la generación de grandes volúmenes de datos, por lo que la tecnología *Big Data* es esencial en el desarrollo de este tipo de aplicaciones. Una de las aplicaciones más importantes en esta área es la gestión de residuos, ésta implica el monitoreo del espacio libre en un contenedor de basura, clasificación de basura, así como el seguimiento y registro de la cantidad de basura generada en un intervalo de tiempo dentro de la ciudad. Por la parte de emergencias existen sistemas IoT capaces de captar la movilidad humana mediante cámaras o sensores ubicados en toda la ciudad, que buscan predecir zonas de aglomeración [12]. Esta última aplicación tras la pandemia generada por el COVID-19, puede permitir la identificación de zonas de aglomeración para evitar el contagio masivo de la enfermedad.

1.4.4.5 Agricultura y Cuidado Ambiental

Primero se tratará el tema sobre el Cuidado Ambiental, en la actualidad el cambio climático y la contaminación representan problemas críticos a nivel global, ante esto surge la necesidad de desarrollar sistemas IoT que permitan realizar un monitoreo de parámetros ambientales en espacios abiertos tales como la humedad, temperatura, calidad de aire, intensidad de lluvia, entre otros, mediante los cuales sea posible determinar niveles atípicos, con el fin de llegar a proponer acciones que ayuden en el Cuidado Ambiental [18].

Sin embargo, este monitoreo también resulta importante realizarlo en interiores, tal puede ser el caso de hogares situados cerca de carreteras o sitios de agricultura intensiva, lugares en donde la generación de gases invernadero es alta, y llevar un monitoreo de estos gases permitirá alertar a las personas sobre una posible afectación en su salud [19]. En la Figura 1.4 se podrá observar un esquema básico de sistema IoT, el cual mediante el uso de sensores inteligentes permite realizar la recolección de datos relacionados con la temperatura y humedad del ambiente para almacenarlos en un servidor centralizado y poder visualizar esta información desde un teléfono celular.

Por otra parte, la agricultura representa una importante fuente de ingresos en varios países. Gracias a los sistemas IoT, los agricultores pueden administrar sus granjas de forma

remota. Se han desarrollado e implementado varias aplicaciones IoT en el sector agrícola en países como Tailandia, China, Taiwan, entre otros. Por ejemplo, en China fue diseñado un sistema IoT para controlar las plantaciones en un invernadero, como resultado se obtuvo una reducción del 80% en el uso de plaguicidas; además de verse reducido el costo laboral en un 60%. Sin embargo, existen ciertos problemas en este campo de aplicación, como lo son el consumo de energía, el hardware (los dispositivos inteligentes deben ser diseñados para condiciones extremas, como altos niveles de temperatura o humedad), la comunicación (Internet es un servicio que en ciertas zonas rurales no es de buena calidad), confiabilidad y escalabilidad [20].

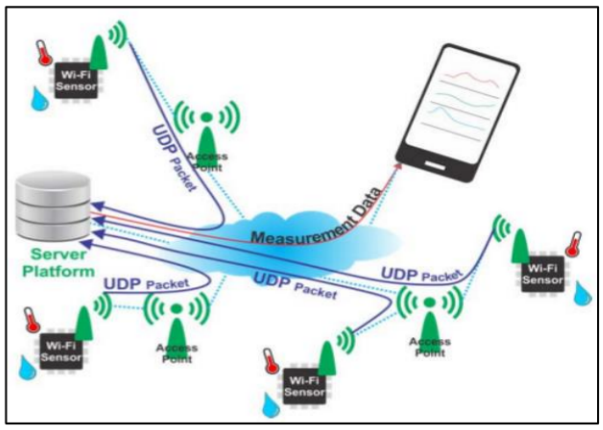


Figura 1.4. Sistema de monitoreo ambiental [19]

1.4.4.6 Comercio

En la actualidad, en países como Estados Unidos o China, se ha visto un crecimiento de negocios de ventas minoristas, con la novedad de que no poseen personal de ventas. Según lo planteado por Xu en [21], se espera que para el año 2022, los negocios de ventas sin personal tengan alrededor de 245 millones de consumidores en China. El concepto de negocios de ventas sin personal consiste en incorporar sensores inteligentes en estanterías y alrededor del lugar, y permitir la detección de los productos que sean tomados por los clientes, información que será procesada para finalmente generar la factura correspondiente y realizar el respectivo cobro. Un ejemplo de este esquema es el de la línea Go de la cadena Amazon, en donde la presencia de personal de ventas es nula [21].

1.4.4.7 Industria

Esta área de aplicación de los sistemas IoT se la puede relacionar con el concepto de industria 4.0, la cual tiene como objetivo integrar sensores inteligentes en sus sistemas industriales, de modo que los procesos de fabricación sean automáticos y flexibles. Los sensores recolectan grandes cantidades de datos, los cuales tras ser procesados dan

soporte a la creación de procesos de fabricación mejorados, optimización de recursos y generación de modelos de negocio innovadores. En este punto, se puede mencionar el término de “Fábrica inteligente”, la cual se encuentra formada por CPPS (Unidades de Producción Inteligentes) vinculadas en la cadena de producción generalmente mediante una comunicación máquina a máquina (M2M) [22].

Otro punto importante en la industria 4.0 es el de las cadenas de suministro, que abarcan tanto el proceso de elaboración del producto como el de comercialización. Éstas deben ser eficientes y precisas en tiempos de entrega, con el fin de generar valor agregado en el proceso de distribución a clientes finales. Sin embargo, la logística es compleja pues requiere un nivel de coordinación alto entre proveedores y canales de comercialización, el cual es posible gracias al desarrollo de sistemas IoT en este campo [23].

1.4.5 BENEFICIOS DE LOS SISTEMAS IOT

Como se ha podido apreciar en la sección 1.4.4, los sistemas IoT pueden ser desarrollados en múltiples áreas permitiendo a modo general mejorar la calidad de vida de las personas. Sin embargo, este no es el único beneficio que presentan este tipo de sistemas, a continuación, se listarán algunos beneficios de los sistemas IoT [24]:

- **Generación de Información:** los sensores y dispositivos inteligentes en los sistemas IoT recolectan grandes volúmenes de datos, que son procesados para obtener información valiosa para las aplicaciones. El acceso a esta información permite a las personas mejorar la toma de decisiones.
- **Eficiencia:** gracias a la información generada por los algoritmos de *Machine Learning*, el sistema IoT puede optimizar procesos y trabajar eficientemente con la información que se retroalimenta, reduciendo errores en tareas monótonas.
- **Control Automatizado:** los sistemas IoT permiten administrar una gran cantidad de dispositivos, con el desarrollo de algoritmos de inteligencia artificial, donde la intervención del humano puede ser requerida únicamente en casos de emergencia, y dejar que una inteligencia artificial controle las tareas a ser llevadas por el sistema IoT, notificando al usuario cualquier irregularidad en el proceso.
- **Monitoreo:** al tener los dispositivos inteligentes interconectados, es posible monitorear cada uno de estos de manera remota desde un dispositivo como puede ser un celular o incluso desde un sitio web.

1.4.6 DESAFÍOS DE LOS SISTEMAS IOT

Los sistemas IoT, manejan una gran cantidad de información, ésta puede ser vista como una “moneda”, especialmente los datos personales, ya que se puede realizar la construcción de perfiles comerciales y realizar publicidad dirigida llegando a violentar la privacidad de un usuario. Por este motivo, los hackers han centrado su atención en los dispositivos IoT, ya que se podrían considerar como objetivos fáciles a ser vulnerados. Todos estos aspectos provocan grandes desafíos en los sistemas IoT, los cuales se detallan a continuación [25] y [26]:

- **Estandarización:** representa uno de los principales desafíos en el desarrollo de sistemas IoT, debido a problemas de compatibilidad que se presentan el momento de incluir dispositivos heterogéneos. Organismos de normalización como la IEEE (*Institute of Electrical and Electronics Engineers*) e ITU (*International Telecommunications Union*) se encuentran desarrollando un marco estándar para solucionar este problema y permitir que la interoperabilidad de diferentes tecnologías IoT sea posible.
- **Escalabilidad:** hace referencia a la capacidad de agregar nuevos dispositivos en un sistema IoT ya implementado. Sin embargo, las tecnologías usadas para integrar estos nuevos dispositivos no siempre son compatibles con el sistema IoT, por lo que asegurar la interoperabilidad entre el dispositivo y el sistema IoT resulta complicado, limitando a los sistemas a no poder incluir nuevos dispositivos y dejándolos obsoletos con el paso de los años.
- **Seguridad:** los sistemas IoT implican el manejo de dispositivos cotidianos los cuales suelen tener capacidades limitadas, éstos recopilan diferentes tipos de datos, entre los cuales se encuentran los datos personales. El no implementar de manera correcta medidas de seguridad en los sistemas IoT puede terminar en afectar a la privacidad del usuario final, por ende, es importante garantizar la confiabilidad, disponibilidad e integridad de los datos recolectados por los dispositivos IoT.

2 METODOLOGÍA

El desarrollo del presente componente utiliza como base la metodología Kanban, con el fin de implementar una estructura organizacional que maximice el rendimiento del flujo de trabajo del Componente de Integración Curricular [27]. Las tareas a realizar fueron tomadas del Plan de Trabajo, teniendo así un total de 12 tareas para ser desarrolladas en este componente. Cabe mencionar que se trata de un componente individual por lo que el tablero Kanban es aplicado en uso personal para realizar controles de cumplimiento de las tareas semanales.

Se adoptó un enfoque cualitativo con el fin de recolectar información sobre arquitecturas o modelos de referencia para sistemas IoT, desarrollando así un trabajo exploratorio, que ofrece una visión global de las arquitecturas en sistemas IoT. Para iniciar con el desarrollo del presente trabajo se creó el tablero Kanban simplificado en donde constan las 12 tareas a ser realizadas. En el ANEXO I se presenta el tablero Kanban con todas las tareas, las que ya han sido finalizadas se encuentran colocadas en la columna denominada “Finalizadas”, las tareas que se encuentran en proceso de desarrollo (para este caso, el tablero Kanban corresponde a la Semana 4 del trabajo) en la columna “En proceso” y las tareas restantes en la columna “Pendientes”. Con cada avance del presente trabajo, se realiza una actualización en el tablero, para reflejar las tareas que ya han sido cumplidas, las que se encuentran en proceso de realizarse y las que aún están pendientes.

Con el flujo de actividades establecido se empieza por recolectar información pertinente para el cumplimiento de cada tarea, bajo el enfoque cualitativo a ser usado se emplea un análisis documental como técnica de recopilación de información. La información a recolectar es tomada de diferentes motores de búsqueda fiables como IEEE Xplore, MPDI, ACM, Google Scholar y de las diferentes páginas web de proyectos u organismos que desarrollen marcos de trabajo, recomendaciones o estándares para sistemas IoT.

Para cumplir con el primer objetivo específico planteado, se recopiló información de diferentes publicaciones ingresando en los motores de búsqueda mencionados, palabras clave como: “*Systems*”, “IoT” y “*Area*” obteniendo así información relacionada con los conceptos de sistemas IoT y sus áreas de aplicación.

El núcleo de este trabajo es la recopilación y análisis de la información, por este motivo, el cumplimiento del segundo objetivo específico planteado es esencial para el desarrollo del presente componente, para esto se continuó con el trabajo exploratorio, ingresando palabras clave como: “*Architecture*”, “*Reference Model*” e “IoT”. Para limitar la información, se empezó por seleccionar únicamente aquella información que se encuentre publicada

dentro de los últimos 5 años. Este es el primer filtro de la búsqueda aplicado. Como segundo filtro se eliminó aquella información que no tenga relación con sistemas IoT. Finalmente, se seleccionó aquellas arquitecturas o modelos de referencia que posean información sustancial y relevante para realizar el análisis sobre las capas y funcionalidades definidas en cada modelo de referencia o arquitectura para sistemas IoT.

Con el cumplimiento del objetivo antes mencionado, la realización de los dos últimos objetivos específicos planteados se encuentra estrechamente relacionada, ya que la información de cada arquitectura y modelo de referencia para sistemas IoT se encuentra depurada. Para cumplir el tercer objetivo, se realizó un análisis en cada uno de los artículos de arquitecturas o modelos, con el fin de encontrar una relación con un área de aplicación (Figura 1.3), para así poder crear un organizador gráfico en donde se asocien las diferentes áreas de aplicación con cada uno de los modelos de referencia o arquitecturas para sistemas IoT que les correspondan.

Para el cumplimiento del último objetivo planteado, se realiza una extensión del trabajo exploratorio, pues analizar el nivel de madurez de cada arquitectura o modelo de referencia para sistemas IoT implica revisar publicaciones en las que se hagan referencia a la arquitectura o modelo, de modo que, se dé una continuación al trabajo y conlleve a la implementación de sistemas IoT que apliquen dicha arquitectura o modelo. Para lograr esto, se utilizaron motores de búsqueda como Google Scholar e IEEE Xplore, en donde se colocó el nombre de los diferentes artículos analizados en la sección 2.1, para poder observar las publicaciones en donde estos hayan sido referenciados. De modo que, se tenga el sustento necesario para colocar un nivel de madurez a cada arquitectura o modelo de referencia para sistemas IoT analizados en el presente Trabajo de Integración Curricular.

2.1 ANÁLISIS METODOLÓGICO

De la información recopilada, se han clasificado a las arquitecturas para sistemas IoT en base al número de capas propuestas (3, 4, 5 y 6 capas o superior) y a la tecnología que implementan (basadas en servicios, basadas en la nube e integración con Blockchain). Con respecto a los modelos de referencia se los ha colocado en una categoría diferente juntándolos con proyectos para el desarrollo de sistemas IoT. A continuación, se presenta el detalle de cada arquitectura y modelo de referencia para sistemas IoT.

2.1.1 ARQUITECTURAS DE 3 CAPAS

2.1.1.1 Arquitectura de 3 Capas (Survey)

La arquitectura de 3 capas fue propuesta en los inicios de la investigación de sistemas IoT, por lo que es considerada como una de las arquitecturas básicas, las capas se encuentran ilustradas en la Figura 2.1.(a) y son [28]:

- **Percepción:** formada por un conjunto de objetos, estos sirven como un intermediario entre el ambiente y el mundo digital. El objetivo principal de esta capa es la de capturar datos del entorno mediante sensores.
- **Transporte:** responsable de permitir la comunicación entre Internet y los dispositivos IoT, puede ser vista como la infraestructura que da soporte a las aplicaciones y servicios.
- **Aplicación:** representa una abstracción de los servicios IoT, estos son solicitados por un usuario mediante un API (*Application Programming Interface*), para que esta capa procese la información y pueda responder a la solicitud recibida.

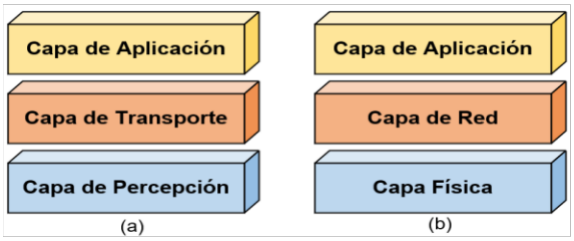


Figura 2.1. Arquitecturas de 3 capas: (a) revisada en [28] y (b) en [29]

En [29] se puede observar que sus autores plantean de manera similar esta arquitectura básica, renombrando sus capas a Capa Física, Capa de Red y Capa de Aplicación, tal como se observa en la Figura 2.1.(b).

2.1.1.2 Arquitectura de Sincronización de Reloj de un Sistema de Acceso IoT

En [30] se plantea un sistema de acceso que permite que dispositivos con recursos limitados pueden ser considerados para formar parte de un sistema IoT. Esta arquitectura asegura escalabilidad gracias a su sistema de acceso, y permite solucionar el problema de sincronización de reloj de manera precisa en varios dispositivos heterogéneos. La Figura 2.2 muestra las 3 capas de esta arquitectura, y son:

- **Adquisición:** encargada de iniciar y sincronizar el reloj de referencia del sistema, este puede ser RTC (*Real Time Clock*), GPS (*Global Position System*), NTP (*Network Time Protocol*).
- **Mantenimiento:** se encarga de mantener el reloj del *kernel* de cada sistema operativo para otorgar un reloj de referencia a la capa de distribución.

- **Distribución:** se encarga de sincronizar el reloj de todo el sistema IoT, tomando como referencia el reloj del *kernel*. La sincronización se lleva a cabo mediante NTP o directamente por interfaz de comunicación RS232 con los dispositivos IoT que se acoplan al sistema de acceso.

Figura 2.2. Arquitectura para la sincronización de reloj basada en [30]

2.1.1.3 Arquitectura Biométrica Descentralizada de 3 Capas

En [31] se propone una arquitectura descentralizada formada por 3 capas como se puede observar en la Figura 2.3. La cual asegura escalabilidad y administración completa del sistema. Puede verse como una versión mejorada de la arquitectura tradicional de 3 capas. Esta propuesta se encuentra orientada a la detección de rostros, con el propósito de controlar la cantidad de personas que salen de sus hogares durante las cuarentenas provocadas por el COVID-19. Las capas son:

- **Dispositivo:** encargada de recolectar los datos provistos por las cámaras de seguridad y dispositivos de detección.
- **Borde:** capa principal de la arquitectura, encargada del procesamiento, almacenamiento y transmisión de los datos a ser manejados por la capa de Aplicación. La infraestructura de esta capa ha sido colocada en la nube para obtener un procesamiento constante (mediante redes convolucionales) y rápido de los datos (capturas de rostros).
- **Aplicación:** Reside el servicio y aplicación de detección e identificación facial.

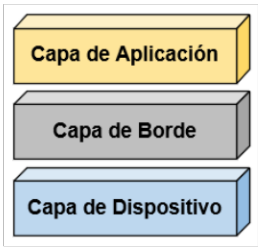


Figura 2.3. Arquitectura biométrica descentralizada basada en [31]

2.1.1.4 Arquitectura IoT Bajo un Esquema Pregunta – Respuesta

De acuerdo con lo planteado en [32] se puede observar cómo la arquitectura de 3 capas es orientada para aplicaciones de ciudad inteligente, al emplear módulos con sensores embebidos que tengan la capacidad de intercambiar preguntas con diferentes usuarios que se encuentren cerca de estos módulos, creando así un sistema de aprendizaje ubicuo y accesible a una gran cantidad de personas. Por ejemplo, una persona que se encuentre cerca de uno de estos módulos puede recibir en su celular una pregunta sobre la fauna de las Islas Galápagos, puede responder y recibir una retroalimentación, de igual manera puede colocar una pregunta para que ésta sea recibida por otra persona que se encuentre cerca. Esta arquitectura se presenta en la Figura 2.4 y define sus capas de la siguiente manera:

- **Aplicaciones de Front-end:** contienen la aplicación, en donde personas puedan recibir y postear preguntas.
- **Módulo de Aprendizaje:** es el elemento principal de la arquitectura, está compuesto de 3 partes: 1) Detección: contiene sensores analógicos y digitales; 2) Procesamiento: responsable de procesar y almacenar datos; 3) Mensaje: recibe mensajes de diversos nodos.
- **Comunicaciones:** permite la comunicación entre un dispositivo final (celular) y un módulo de aprendizaje, o directamente entre estos módulos, con el objetivo de intercambiar datos.

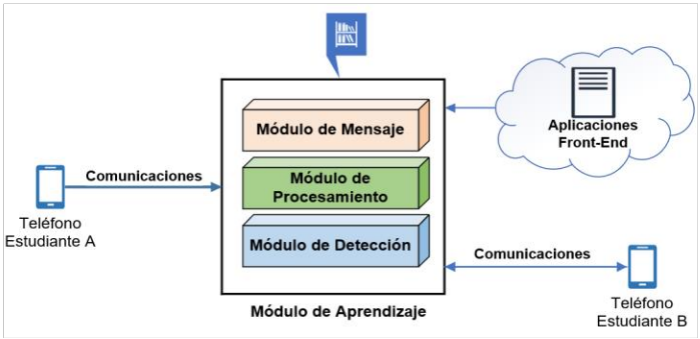


Figura 2.4. Arquitectura IoT-Esquema Pregunta Respuesta basada en [32]

2.1.2 ARQUITECTURAS DE 4 CAPAS

2.1.2.1 Arquitectura NFV IoT para un Ambiente Médico

La presente arquitectura emplea funciones NFV (*Network Functions Virtualization*) en una arquitectura tradicional para sistemas IoT, gracias a dichas funciones la arquitectura asegura ser escalable, flexible y rápida. Para probar la arquitectura se desarrolló un sistema médico para un ambiente OPIC (*OPerating room Innovation Center*). Como se

puede observar en la Figura 2.5 se ha propuesto un esquema compuesto de 4 módulos importantes que son [33]:

- **Sensores y Actuadores:** dispositivos encargados de sensar y recolectar datos.
- **Gateway IoT:** provee compatibilidad entre los protocolos de capa 2 y el protocolo IP manejado en la red del sistema.
- **Red IP:** encargada de intercambiar información entre el Centro de Datos y el Gateway IoT.
- **Centro de Datos:** encargado de soportar las aplicaciones IoT. Propuesto bajo un enfoque por capas; éstas son: 1) Capa HW: plataforma de hardware escalable, emplea componentes comerciales listos para usar (COTS); 2) Capa de visualización: posee las máquinas virtuales de cada aplicación; 3) Capa de administración: administra el ciclo de vida de las aplicaciones.

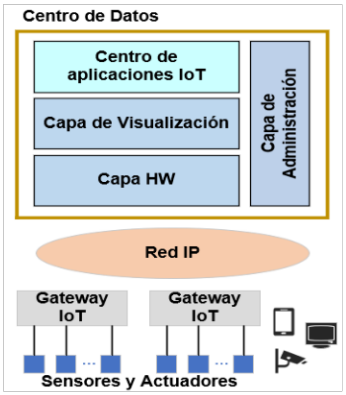


Figura 2.5. Arquitectura NFV IoT basada en [33]

2.1.2.2 Arquitectura IoT Basada en la Teoría Fractal

En [34] se propone una arquitectura basada en la teoría fractal. Esta arquitectura considera a GIoT (*Global IoT*) y LIoT (*Local IoT*), mencionando que GIoT (Sistema IoT más grande del mundo) se encuentra formada recurrentemente por LIoT (Sistema IoT de aplicación específica), como se muestra en la Figura 2.6. Este concepto es concebido bajo la teoría Fractal, en donde un componente (GIoT) se encuentra formado por múltiples componentes de la misma estructura (LIoT), generando así una estructura global y robusta. La arquitectura forma una red GIoT robusta y estable ante ataques distribuidos. GIoT presenta una fácil escalabilidad al estar integrada de LIoT (aplicaciones en áreas específicas). Cada LIoT se fundamenta en la arquitectura de cuatro capas, las cuales son:

- **Capa de Percepción:** concerniente al hardware del sistema (actuadores, sensores y controladores), esta capa es la responsable de recopilar datos relevantes.

- **Capa de Red:** se encuentra formada por tecnologías de comunicaciones (como Internet y WiFi). Se encarga de la transmisión de los datos recolectados por la capa de percepción.
- **Capa de Soporte:** constituida por un middleware, se encarga de la depuración masiva de datos heterogéneos, del análisis de múltiples protocolos y de la abstracción de los datos sin procesar.
- **Capa de Aplicación:** en esta capa se realiza el análisis de *Big Data* y la Inteligencia Artificial, para obtener conocimiento de los datos, de modo que se logre implementar la lógica empresarial y satisfacer los requisitos del usuario.

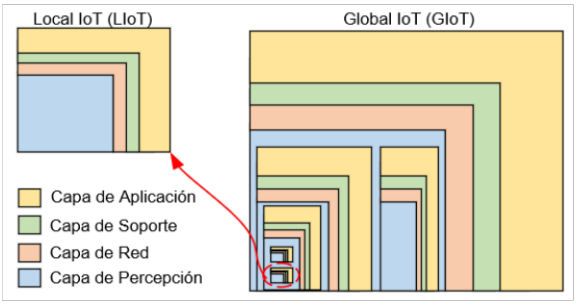


Figura 2.6. Arquitectura IoT en base a la Teoría Fractal, basada en [34]

2.1.2.3 Arquitectura IoT para Integrar Políticas de Seguridad Dinámicas

Para soportar servicios IoT seguros, esta arquitectura aplica diversos aspectos como, servicios ligeros, gestión por capas, administración y control de políticas de seguridad detalladas, y ajuste dinámico de políticas de seguridad. La arquitectura emplea conceptos de SDN (*Software Defined Networking*). Debido a la gran apertura de programación y control de flujo de las SDN, es posible gestionar y controlar rápidamente la seguridad en la arquitectura. Sus capas están representadas en la Figura 2.7.(a), y son [35]:

- **Dispositivo:** formada por dispositivos heterogéneos que se encargan de recolectar datos en diferentes formatos. Los dispositivos pueden tener diferentes capacidades como almacenamiento, *networking*, batería y tipo.
- **Red:** compuesta por Gateways SDN y routers, los cuales reenvían datos indicados por el controlador SDN o bajo instrucciones de políticas de seguridad locales.
- **Computación:** formada por controladores SDN, encargados de controlar el intercambio de datos bajo las peticiones o requerimientos de los servicios, políticas de seguridad o aplicaciones IoT. Estos controladores SDN también gestionan las políticas de seguridad.

- **Servicio:** en esta capa los programadores de los controladores SDN pueden operar servicios y aplicaciones IoT, incluyendo requisitos de seguridad para cada uno de estos, resultando en una implementación rápida y ágil.

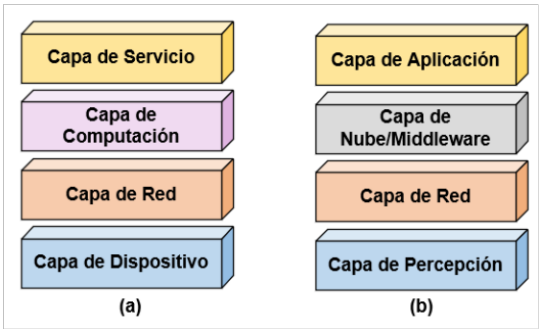


Figura 2.7. Arquitecturas de 4 capas: (a) Integración de Políticas de Seguridad [35] y (b) WBAN-IoT [36]

2.1.2.4 Arquitectura WBAN para Sistemas IoT

Esta arquitectura emplea la tecnología WBAN (*Wireless Body Area Network*), la cual es una tecnología que permite interconectar diferentes sensores colocados en el cuerpo o humano o cerca de este. Estos sensores miden parámetros biológicos como: temperatura, ritmo cardiaco, presión de la sangre, movimiento acelerado, entre otros. Esta propuesta de 4 capas, puede visualizarse en la Figura 2.7.(b) y sus capas son [36]:

- **Percepción:** compuesta de sensores, actuadores y controladores, los cuales se encargan de recolectar datos.
- **Red:** define los diferentes protocolos de comunicación a ser usados en el sistema.
- **Nube/Middleware:** provee una infraestructura distribuida para el procesamiento y análisis de los datos.
- **Aplicación:** encargada de presentar la información procesada para cumplir con los servicios presentados por la aplicación.

En [36] se puede evidenciar cómo la arquitectura de 4 capas, es orientada a redes WBAN y aplicada a un sistema IoT relacionado con el cuidado de la salud.

2.1.2.5 Arquitectura IoT para el Monitoreo de Fermentación del Vino

En [37] se propone una arquitectura de 4 capas aplicada al monitoreo del proceso de fermentación del vino, prácticamente se puede considerar como una aplicación directa de dicha arquitectura; ya que, si bien sus componentes se denominan con nombres puntuales referentes a la jerga industrial, las funcionalidades de cada capa son las comunes de una arquitectura tradicional. Los componentes propuestos son: 1) Sistema de Barril Inteligente:

incluye sensores y actuadores encargados de monitorizar las condiciones del vino (temperatura, proporción de alcohol, pH, presión); 2) Colector de datos: microcomputador encargado de recolectar todos los datos medidos por los sensores; 3) Infraestructura de Red Inalámbrica: realiza el envío de información entre el colector y la estación central; y 4) Estación Central: contiene la lógica y procesamiento de la aplicación, mediante regresión lineal se busca estimar las condiciones del vino.

2.1.3 ARQUITECTURAS DE 5 CAPAS

2.1.3.1 Arquitectura de 5 Capas (*Survey*)

Debido a que la arquitectura de 3 capas presentada en la sección 2.1.1.1 no posee las suficientes funcionalidades para la implementación de un sistema IoT moderno, se ha planteado una arquitectura de 5 capas visualizada en la Figura 2.8.(b). Como se expone en [29], esta arquitectura consta de las siguientes capas:

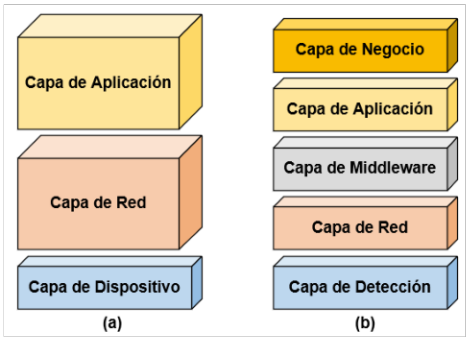


Figura 2.8. Comparación entre arquitecturas de 3 y 5 capas, basada en [29]

- **Detección:** consiste en dispositivos IoT como sensores, tags RFID, dispositivos NFC, entre otros. Esta capa es responsable de la conexión de estos dispositivos, recolección de información y el intercambio de ésta con la capa superior.
- **Red:** se encarga de la transmisión de la información.
- **Middleware:** debido a la gran cantidad de dispositivos heterogéneos usados en los sistemas IoT, estos dispositivos poseen diferentes formatos de datos y tipos de consulta de datos, por ende, esta capa permite manejar problemas de compatibilidad. Además, es responsable del almacenamiento y procesamiento de datos, y de la administración de servicios.
- **Aplicación:** representa una abstracción de los servicios IoT, estos son solicitados por un usuario mediante un API (*Application Programming Interfaces*), para que esta capa procese la información y pueda responder a la solicitud recibida.

- **Negocio:** permite realizar análisis de datos, gráficos, modelos de negocio que ayuden a los desarrolladores o *stakeholders* de los sistemas IoT en la toma de decisiones.

2.1.4 ARQUITECTURAS DE 6 CAPAS O SUPERIOR

2.1.4.1 Arquitectura IoT Middleware

Debido a las limitaciones presentes en los dispositivos finales, la inteligencia es colocada en una entidad intermedia denominada Middleware. En [38] se propone una arquitectura de Middleware que puede acoplarse a sistemas IoT, asegurando escalabilidad e interoperabilidad. Tal como se muestra en la Figura 2.9, esta entidad se encuentra compuesta de 6 módulos, que son:

- **Módulo de Interoperabilidad:** permite integrar diversos dispositivos heterogéneos mediante un API, el cual es capaz de soportar diversos protocolos como CoAP (*Constrained Application Protocol*) y MQTT (*MQ Telemetry Transport*).
- **Módulo de Analítica y Persistencia:** proporciona un procesamiento básico (valores máximos/mínimos, promedios) de los datos recolectados, al igual que un almacenamiento limitado.
- **Módulo de Contexto:** el contexto de un sistema IoT puede entenderse como la capacidad de proveer información relevante acorde a la tarea demandada por un usuario. Existen tres tipos de contexto: 1) Personalizado, el usuario es capaz de programar al sistema para cumplir con una tarea; 2) Pasivo, el sistema sugiere acciones de acuerdo con los datos recolectados; y 3) Activo, el sistema ejecuta de manera automática acciones de acuerdo con los datos recolectados.
- **Módulo de Recursos y Eventos:** administra y optimiza las interacciones entre dispositivos IoT.
- **Interfaz Gráfica de Usuario (GUI):** visto como un dominio transversal, permite al middleware ser amigable al usuario proporcionando una interfaz nativa.
- **Módulo de Seguridad:** es un dominio transversal aplicado en todos los módulos del middleware. La seguridad del modelo está prevista bajo 4 requisitos: 1) la autenticación se realiza por dispositivo; 2) que las credenciales usadas por los dispositivos para la consulta de datos al middleware sean diferentes; 3) que los dispositivos accedan a los datos con sus propias credenciales; y 4) el middleware debe conocer la dirección MAC e IP de los dispositivos.

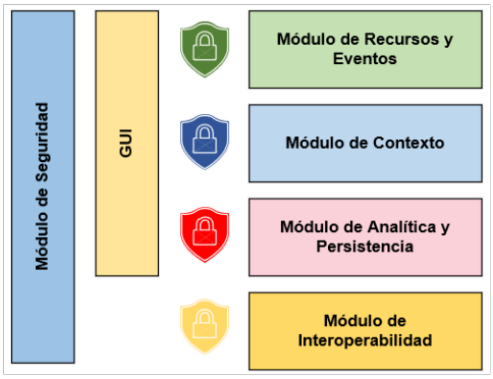


Figura 2.9. Arquitectura de 6 capas IoT basada en [38]

2.1.4.2 Aura Minora: Arquitectura IoT basada en el Usuario

Arquitectura eficiente y segura, que cubre las necesidades de una ciudad inteligente en crecimiento. La arquitectura posee 3 puntos de vista: arquitectónico, funcional e informativo. Su diseño fue realizado con una perspectiva "*bottom up*", esto quiere decir que primero se diseñaron las capas inferiores (donde se encuentran los sensores o "Cosas"). La capa de Gateway implementa un firewall, el cual otorga privacidad y seguridad en la red del usuario final. En la Figura 2.10 se pueden observar las 6 capas definidas en esta arquitectura [39].

- **Detección:** encargada de la recolección de datos provenientes de dispositivos heterogéneos.
- **Gateway:** formada por switches, routers, hubs y otros dispositivos encargados de recopilar los datos de la salida de la capa anterior.
- **Nube:** representa un enlace entre la red local del usuario y los servicios IoT ubicados en la nube (Por ejemplo, una plataforma IP).
- **Servicio:** permite utilizar los datos recolectados mediante aplicaciones integradas en las casas de los usuarios. Es decir, se tienen Unidades de Servicio (SU) orientadas a la seguridad del hogar, gestión del agua, monitoreo de jardines, y cada SU posee una base de datos y un sistema ERP (*Enterprise Resource Planning*) para administrar sus funcionalidades.
- **Administración:** permite el acceso a un repositorio central formado por todas las bases de datos de cada SU, este acceso puede ser requerido por un proveedor de servicios, auditores del gobierno o terceros agentes aprobados.
- **Plataforma:** permite que los usuarios finales puedan acceder a la red IoT desde cualquier lugar, ya sea mediante aplicaciones, servicios web, entre otros. Se presentan datos depurados, convertidos en conocimiento, para que el usuario comprenda el propósito de cada aplicación o servicio.

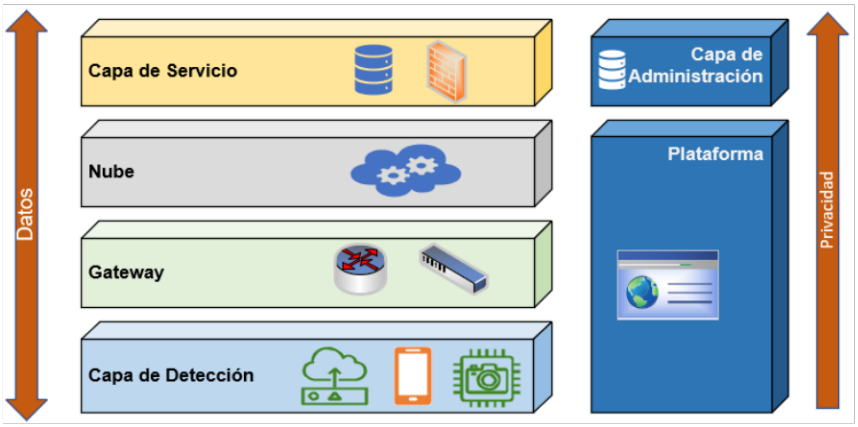


Figura 2.10. Arquitectura IoT Aura Minora, basada en [39]

2.1.4.3 Arquitectura de 7 Capas

En [40] se propone una arquitectura de 7 capas que considera las dificultades existentes en los dispositivos encargados de la recolección de datos al estar expuestos a un entorno dinámico. Estas capas se presentan en la Figura 2.11 y son:

- **Capa de Aplicación:** recolecta información sobre las tareas a ser realizadas en base a los requisitos del cliente.
- **Capa de Soporte y Gestión de Aplicación (SGA):** otorga un control gerencial completo y seguridad en todo el sistema IoT.
- **Capa de Servicios:** proporciona ayuda en la ejecución de las actividades requeridas por el cliente.
- **Capa de Comunicación:** actúa como un puente de información, encargado de comunicar la capa donde se recolectan datos con la capa de servicios para la transmisión de datos.
- **Capa de Red:** permite la transmisión y procesamiento de la información por medio del Internet.
- **Capa de Hardware:** encargada de integrar todos los componentes de hardware necesarios para la implementación de un sistema IoT.
- **Capa de Entorno:** permite realizar la detección de objetos, personas o diferentes parámetros del entorno en el cual se encuentran colocados los dispositivos IoT.

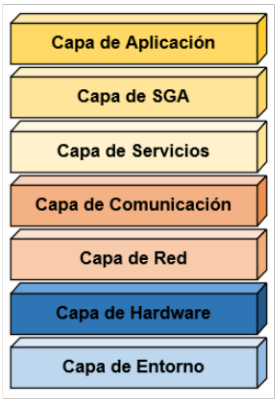


Figura 2.11. Arquitectura de 7 capas, basada en [40]

2.1.4.4 Arquitectura 5G-IoT

En [41] se propone una arquitectura que emplea tecnologías de nueva generación específicamente 5G. La arquitectura se caracteriza por ser escalable, modular, eficiente, simple, sostenible y brindar robustez ante ataques de ciber seguridad. Permite la accesibilidad de servicios de alta demanda. Su diseño admite que las capas intercambien datos de manera bidireccional. De igual manera Rahimi en [41], lista una serie de posibles ataques que pueden ser realizados en cada capa, destacando la capa de Almacenamiento de Datos, al no poseer posibles ataques y asegurar confidencialidad, privacidad e integridad de los datos que manipula. Las capas planteadas en esta arquitectura se muestran en la Figura 2.12, y son:

- **Capa de Dispositivos Físicos:** compuesta de las “Cosas” como sensores, actuadores y controladores, los cuales se encargan de recopilar datos del entorno.
- **Capa de Comunicación:** formada por 2 subcapas que son: 1) Dispositivo a Dispositivo (D2D): la tecnología 5G mejora la comunicación D2D; y 2) Conectividad: permite conectar a los dispositivos con centros de comunicación, en donde se analizan y envían datos mediante Internet a una unidad de almacenamiento.
- **Capa de Computación de Borde:** se encarga del procesamiento en borde de los datos, esta actividad es realizada por nodos distribuidos a lo largo del sistema.
- **Capa de Almacenamiento de Datos:** encargada de recibir la información procesada en el borde por diferentes dispositivos físicos, debido a esto maneja un gran volumen de datos.
- **Capa de Administración de Servicios (AS):** compuesta por 3 subcapas, que son: 1) Administración de red: permite la comunicación entre los dispositivos y los centros de datos, se emplean tecnologías como WSDN (*Wireless Software Defined Network*); 2) Computación en la nube: se encarga de volver a procesar la

información generada por la capa de computación de borde; y 3) Análisis de Datos: toma los datos de la anterior subcapa y aplica algoritmos de aprendizaje automático para generar conocimiento, el cual es la base para la toma de decisiones.

- **Capa de Aplicación:** concerniente a las aplicaciones IoT.
- **Capa de Colaboración y Procesos:** permite que personas externas al sistema IoT colaboren en los Servicios IoT.
- **Capa de Seguridad:** se puede considerar como un dominio vertical, encargada de proveer seguridad a todas las demás capas de la arquitectura.

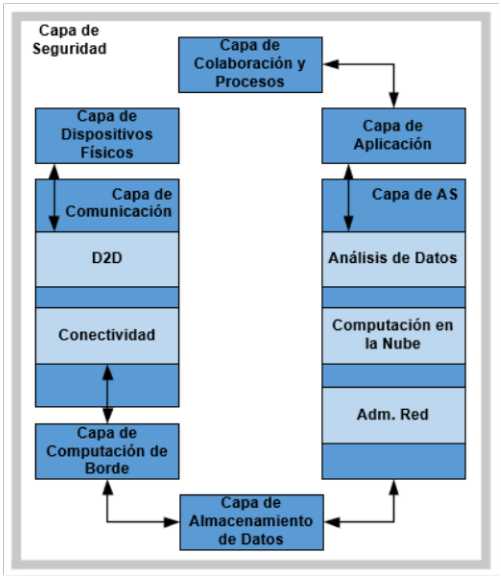


Figura 2.12. Arquitectura 5G-IoT

2.1.5 ARQUITECTURAS BASADAS EN SERVICIOS/MICROSERVICIOS

2.1.5.1 MSA: Arquitectura IoT basada en Microservicios

La MSA (*MicroService-based Architecture*) esquematizada en la Figura 2.13, es considerada una de las mejores opciones para arquitecturas en sistemas IoT. Provee Calidad de Servicio (QoS) mediante técnicas de autoadaptación proactivas (uso de *Machine Learning*) y reactivas (uso de microservicios). La calidad de servicio se proporciona en tres niveles: 1) a nivel de dispositivos; 2) a nivel de servicio; y 3) a nivel de aplicación. Sus tres capas son [42]:

- **Borde:** formada por un grupo de dispositivos IoT (sensores y actuadores), estos dispositivos envían los datos medidos e información de QoS (*Quality of Service*) como el consumo de memoria, nivel de batería, entre otros, a la capa Fog.

- **Fog:** encargada de realizar cálculos ligeros sobre los datos medidos. Además, realiza reconfiguraciones en los dispositivos IoT (basadas en la información de QoS). Se encuentra formada por múltiples nodos de computación, que a su vez están compuestos por: 1) Componente de computación, para depurar los datos medidos (cálculos preliminares); y 2) Componente de adaptación, el cual mediante técnicas de procesamiento de datos y *Machine Learning* permite predecir un nivel de QoS esperado (en base a la información de QoS de los dispositivos finales).
- **Nube:** Encargada de realizar cálculos pesados. Está formada de 4 subcapas: 1) Microservicios, que conceden las funcionalidades al sistema IoT; 2) Administración: encargada del descubrimiento de microservicios, otorgar información sobre su estado y ejecutar un plan de adaptación (en base a la información de QoS) en caso de ser necesario; 3) Adaptación, subcapa dedicada únicamente recopilar datos de QoS para generar modelos de aprendizaje y predecir el mejor plan de adaptación en un sistema; y 4) Aplicación, ejecuta planes de adaptación a nivel de aplicación.

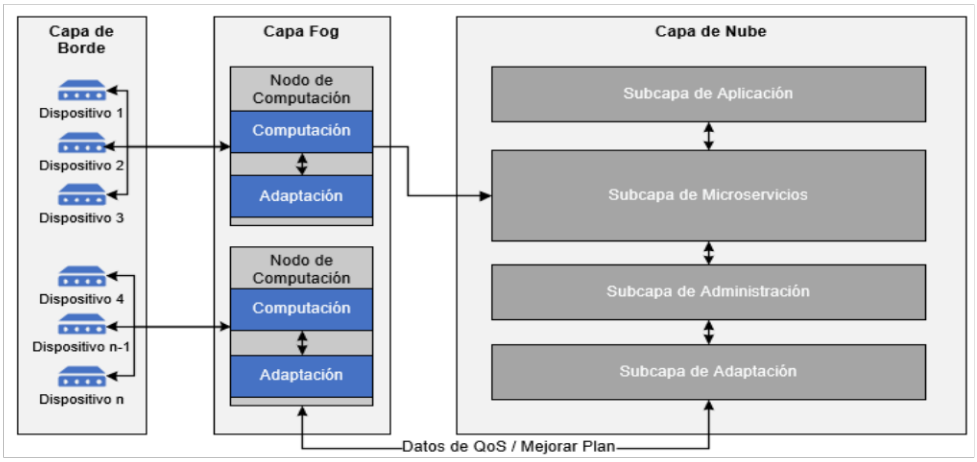


Figura 2.13. Arquitectura MSA, basada en [42]

2.1.5.2 SOA IoT Middleware

El Middleware es una capa de Software que se encuentra entre la capa Física/Percepción y la capa Aplicación. En [43] se presenta una arquitectura de Middleware para sistemas IoT; además, incorpora un enfoque de Arquitectura Basada en Servicios (SOA), que permite convertir sistemas complejos en aplicaciones compuestas de componentes simples y bien definidos. Las capas para esta arquitectura se muestran en la Figura 2.14 y son:

- **Objetos:** relacionada con tecnologías para el monitoreo y recolección de datos.
- **Abstracción de Objetos:** permite que mediante un procedimiento estándar y lenguaje común sea permitida la incorporación de dispositivos heterogéneos.

- **Administración de Servicios:** ofrece funcionalidades que permitan que cada objeto se encuentre habilitado y disponible para ser administrado en el sistema.
- **Composición de Servicios:** provee funcionalidades para el desarrollo de servicios únicos que ofrecen los objetos de una red para elaborar aplicaciones específicas.
- **Aplicación:** capa superficial de la arquitectura, sin embargo, no es considerada como parte del Middleware.

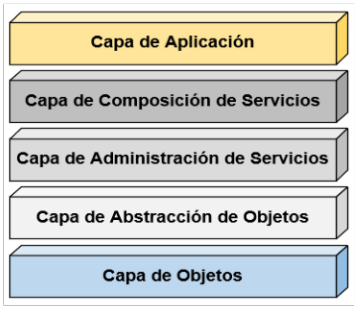


Figura 2.14. Arquitectura SOA IoT Middleware, basada en [43]

2.1.6 ARQUITECTURAS BASADAS EN LA NUBE

2.1.6.1 Arquitectura CloudWoT

Considerada una solución para aplicaciones IoT en tiempo real, ya que gracias a la Computación de borde es posible disminuir la carga computacional en el Centro de Datos, reduciendo la latencia de la transferencia de datos sobre la nube, por lo que hace uso de la computación en la nube. Sus 4 capas se muestran en la Figura 2.15 y son [44]:

- **Campo:** compuesta de sensores que recopilan información de su entorno y actuadores que pueden ser controlados bajo ciertas condiciones.
- **Comunicación:** distribuye los datos recolectados a diferentes locaciones del sistema. La comunicación entre dispositivos IoT puede ser inalámbrica o cableada, las tecnologías más usadas son IPv6 (*Internet Protocol Version 6*), BLE (*Bluetooth Low Energy*), LoWPAN (*Low Power Wireless Personal Area Networks*) y NFC (*Near Field Communication*).
- **Procesamiento de Datos:** posee un middleware encargado de generar formatos de datos comunes para asegurar su interoperabilidad en las etapas de procesamiento, almacenamiento y gestión de datos. Además, incluye un módulo de computación de borde para incrementar la capacidad computacional del sistema.
- **Computación en la Nube:** concerniente a la parte de las aplicaciones IoT, la nube aloja los recursos necesarios para que una aplicación funcione correctamente, ya que otorga un poder computacional alto.

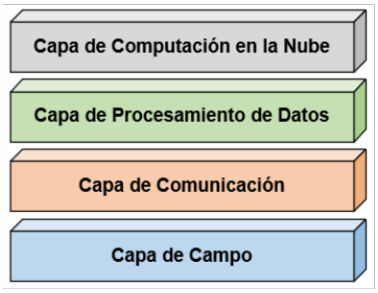


Figura 2.15. Arquitectura CloudWoT, basada en [44]

2.1.6.2 IoT-HC: Arquitectura Híbrida basada en la Nube

Es una arquitectura que busca combinar dos paradigmas distintos pero complementarios, IoT con la Nube. Presenta una solución para gestionar la nube privada con la nube pública y una infraestructura IoT. Busca solventar problemas de heterogeneidad en sistemas IoT. Sus capas se muestran en la Figura 2.16 y son [45]:

- **Capa IoT:** compuesta de sensores y actuadores encargados de la recolección de datos y de la modificación del ambiente físico.
- **Capa de Borde:** ejecuta tareas en tiempo real que no requieran recursos computacionales altos. Integra y filtra los datos, así como los enruta de manera dinámica a la nube pública o privada.
- **Capa de Nube:** realiza tareas que no requieran ser en tiempo real, pero que consuman gran cantidad de recursos computacionales y de almacenamiento. Tiene dos subcapas: 1) Nube Privada, es una infraestructura privada; y 2) Nube Pública, infraestructura ofrecida por terceros (*Amazon Web Services*, Google Cloud).

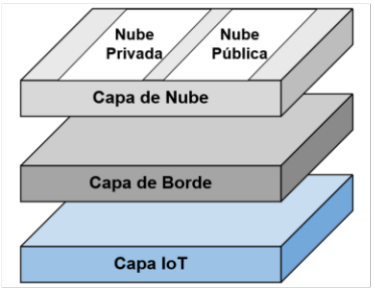


Figura 2.16. Arquitectura IoT-HC, basada en [45]

2.1.6.3 Arquitectura basada en la Computación Transparente

Arquitectura basada en la computación transparente, cuyo objetivo principal es el de desplegar aplicaciones IoT en dispositivos ligeros. Busca proveer a los sistemas IoT de procesamiento de datos en tiempo real. Entre los principales beneficios que otorga aplicar

el paradigma de la computación transparente en sistemas IoT se tiene la reducción del tiempo de respuesta, administración de recursos centralizada y escalabilidad funcional mejorada. Las capas de la arquitectura se pueden observar en la Figura 2.17 y son [46]:

- **Capa de Usuario Final:** compuesta de dispositivos IoT mediante los cuales los usuarios pueden acceder a los servicios proporcionados por una aplicación IoT, pueden verse como un cliente de los servicios IoT.
- **Capa de Servidor de Borde:** responsable de distribuir funciones de computación, control y almacenamiento a los dispositivos finales; por ejemplo, enrutadores de alto rendimiento, estaciones base para dispositivos de comunicación, unidades de carretera en redes vehiculares, entre otros. Los dispositivos de esta capa se denominan servidores de borde.
- **Capa de Red Central:** encargada de vincular los servidores de borde con la nube mediante Internet.
- **Capa de Nube:** realiza el procesamiento y almacenamiento de datos complejos. Además, puede proporcionar una colección de servicios o aplicaciones para la capa de servidor.
- **Capa de Administración e Interfaz:** provee herramientas de gestión para la administración del sistema IoT completo y varias interfaces, para que desarrolladores puedan elaborar y publicar nuevos servicios o aplicaciones IoT.

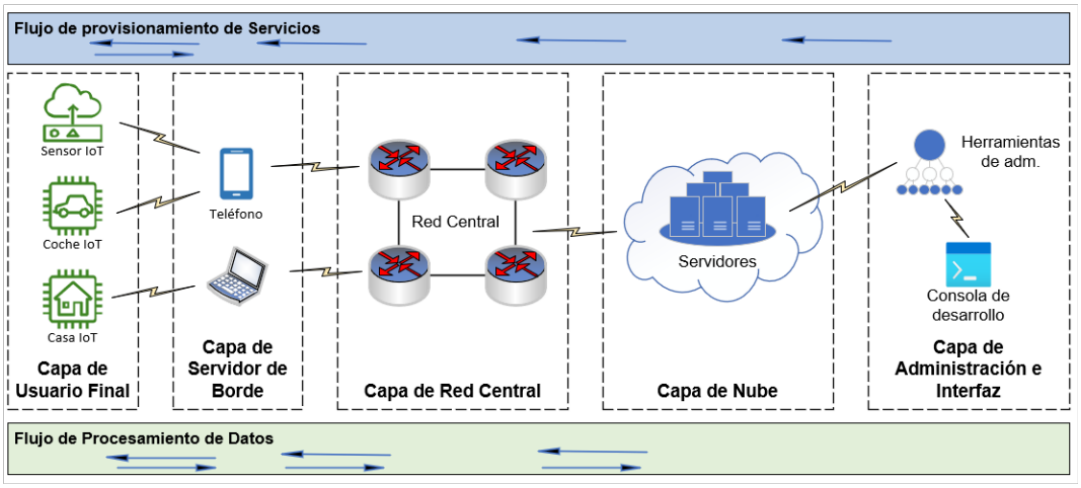


Figura 2.17. Arquitectura IoT con computación transparente, basada en [46]

2.1.7 ARQUITECTURAS QUE INTEGRAN BLOCKCHAIN

2.1.7.1 Arquitectura IoT-Blockchain

En los últimos años se ha podido ver un aumento en el desarrollo de sistemas IoT que implementen la tecnología Blockchain con el propósito de incrementar su seguridad. Es así como en [29] se propone una arquitectura IoT-Blockchain que combina características de sistemas IoT y sistemas Blockchain. Esta arquitectura se encuentra compuesta por 5 capas mostradas en la Figura 2.18, que son:

- **Física:** formada por dispositivos IoT que se encargan de la recolección de datos.
- **Red:** responsable de la interconexión, direccionamiento y enrutamiento entre dispositivos IoT. Se suele emplear redes P2P (*Peer-to-Peer*).
- **Blockchain:** provee funciones de Blockchain como el consenso (todos los datos posean un registro común), almacenamiento y transmisión de la información.
- **Middleware:** responsable de la administración Blockchain, integración de servicios Blockchain y proveer un servicio de seguridad extra a la arquitectura.
- **Aplicación:** permite interacción entre APIs IoT e interfaces finales de usuario.

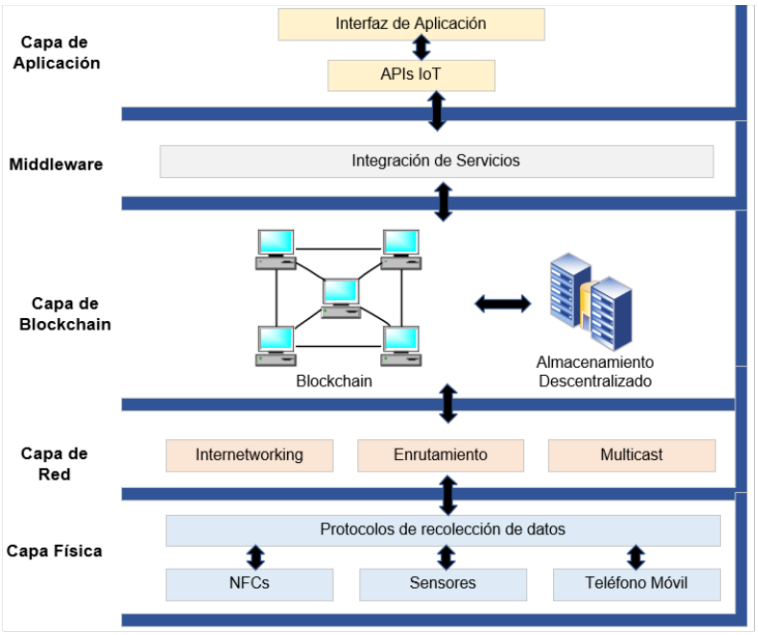


Figura 2.18. Arquitectura IoT de 5 capas con Blockchain, basada en [29]

En aplicaciones que usan esta arquitectura, los dispositivos IoT generan datos y la tecnología Blockchain sirve como una base de datos segura y distribuida, que protege la integridad de los datos. Luego que un bloque de datos se envía, es confirmado y se añade a Blockchain al igual que sus transacciones. Un usuario al usar la aplicación puede tener la certeza de que la respuesta a su petición tiene información consistente y verificada.

2.1.7.2 Estándar para la Gestión de Datos de Sistemas IoT con Blockchain

Esta propuesto por el comité de estándares de Blockchain de la Sociedad del consumo de la tecnología de IEEE, aprobado el 3 de diciembre del 2020, define un marco de referencia

para guiar el desarrollo de la gestión de datos de sistemas IoT basados en Blockchain. Es decir, se plantean los bloques fundamentales para habilitar Blockchain durante el ciclo de vida de los datos (adquisición, procesamiento, almacenamiento, análisis, uso y eliminación) [47]. El estándar tiene 4 capas y un dominio transversal, como se observa en la Figura 2.19, y se detalla a continuación.

- **Capa de Aplicación:** residen las aplicaciones de los sistemas IoT.
- **Capa de Servicio:** permite realizar funciones como el análisis de datos, intercambio de datos y da soporte a la capa de aplicación.
- **Capa de Función:** gestiona datos del sistema IoT. En un inicio permite ingresar datos en el sistema de manera segura, procesamiento de datos, almacenamiento de datos y contiene APIs (Interfaz de programación de aplicaciones).
- **Capa de Transporte Seguro:** identifica que los datos han sido generados por dispositivos IoT verificados, asegura la transmisión de datos en una red *peer-to-peer*. La tecnología Blockchain es importante en esta capa, porque permite la identificación descentralizada, cifrado de credenciales de dispositivos IoT, entre otras funciones. Contiene nodos Blockchain que funcionan con una infraestructura propia o pueden correr en la nube gracias a Blockchain como servicio (BaaS).
- **Panel de Control y Administración (PCA):** dominio transversal que engloba a todas las capas. Coordina las operaciones entre capas, monitoriza el rendimiento del sistema (y mejorarlo). Contiene múltiples interfaces para cada capa, las cuales se encargan de recibir o entregar políticas y reglas de seguridad.

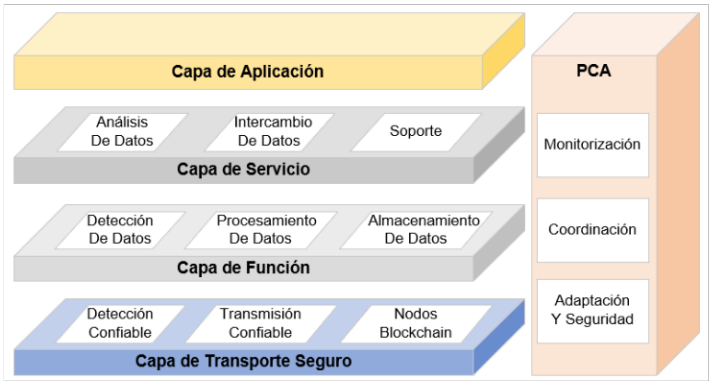


Figura 2.19. Estándar para la gestión de datos en sistemas IoT con Blockchain, basada en [47]

2.1.7.3 Arquitectura Blockchain para la Reconfiguración Masiva de Dispositivos IoT

En [48] se propone una arquitectura basada en Blockchain que permite la reconfiguración masiva de dispositivos IoT. Se presenta como una solución para la administración de millones de dispositivos, asegurando una fácil escalabilidad en sistemas IoT. Tal como se muestra en la Figura 2.20 la arquitectura consta de 3 componentes que son:

- **Administradores:** permite gestionar aquellas personas autorizadas a realizar configuraciones en dispositivos IoT.
- **Dispositivos IoT:** encargados de la recopilación de datos, para una fácil administración son divididos en grupos.
- **Red Blockchain:** otorga una interacción segura entre un administrador y un dispositivo IoT. Permite la comunicación con los dispositivos IoT mediante un mecanismo de publicación/suscripción (REST API). Además, hace uso de políticas de control de acceso, para la autenticación y monitorización de actualizaciones de configuración de los dispositivos IoT, y contratos inteligentes que permiten la actualización de las configuraciones en la red Blockchain.

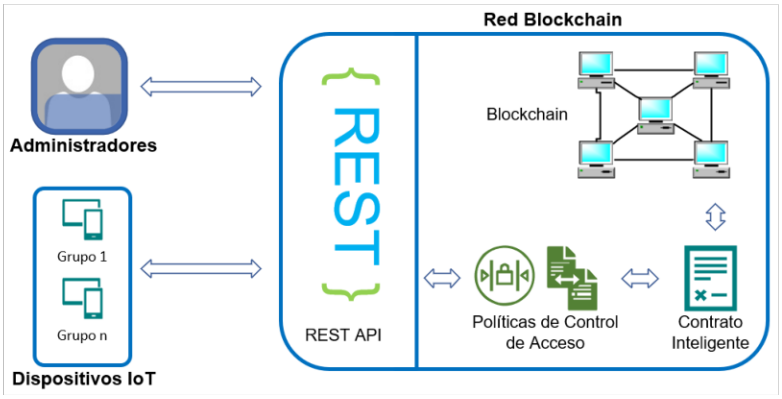


Figura 2.20. Arquitectura Blockchain para la reconfiguración masiva de dispositivos IoT, basada en [48]

2.1.8 MODELOS DE REFERENCIA Y PROYECTOS DE DESARROLLO DE SISTEMAS IOT

2.1.8.1 Arquitectura de Referencia del Modelo de Fusión de Información

Se basa en el modelo de 6 dominios IoT esquematizado en la Figura 2.21. Su objetivo principal es fusionar la información médica obtenida para asistir en la toma de decisiones. Este modelo de fusión de información se encuentra centrado en dispositivos capaces de medir parámetros del cuerpo humano (presión, ritmo cardiaco, entre otros). Para soportar el procedimiento de fusión de la información se plantean 5 niveles de fusión. Los componentes de la arquitectura se exponen a continuación [49].

- **Dominio de Usuario:** provee una interfaz de interacción humano-computador.

- **Dominio de Control de Detección:** formado por las fuentes de detección de información. Se completa el control de la fusión de nivel 0.
- **Dominio de Provisión de Servicios:** formado por servicios básicos como soporte de base de datos y la fusión de éstas, el cual es un requisito para la fusión de los niveles 1, 2 y 3.
- **Dominio de Control de Administración y Operación (CAO):** administra, monitorea y optimiza los dispositivos de detección. Permite configurar y optimizar información como parámetros operativos y algoritmos de fusión (niveles 0-3).
- **Dominio de Intercambio de Recursos:** otorga acceso a datos externos en la base de datos.
- **Dominio Objetivo:** busca proporcionar objetos de fusión de la información (objetos de percepción humana).

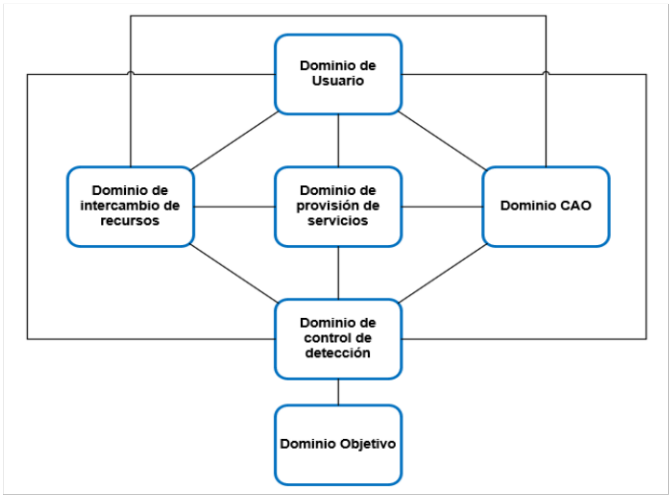


Figura 2.21. Modelo de Referencia IoT de 6 dominios, basada en [49]

Tanto los dominios de la arquitectura como los niveles de fusión son abstractos. Como se menciona en [49], el combinar el modelo de referencia de 6 dominios con una aplicación médica resulta complejo, pero otorga efectividad, confiabilidad y extensibilidad al modelo.

2.1.8.2 Proyecto FIWARE

FIWARE [50] es un proyecto de una comunidad independiente, de la Unión Europea. Desarrolla una plataforma completa para aplicaciones y servicios de nueva generación; es decir, la visión general es construir una Plataforma Central para el Internet del Futuro.

FIWARE es una plataforma abierta basada en componentes denominados *Generic Enablers* (GE), que se encuentran disponibles en APIs, que permiten el desarrollo de aplicaciones inteligentes. Los GE ofrecen un conjunto de funciones de propósito general; además, son reusables y compatibles en varias áreas de aplicación.

Se definen roles como: 1) *GE Provider:* implementa un GE con sus especificaciones; 2) *Instance Provider:* organización que implementa y opera una instancia FIWARE; y 3) *Application Provider:* organización que desarrolla aplicaciones FIWARE (FIApp).

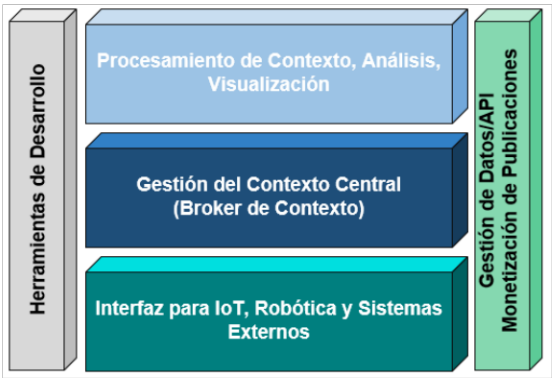


Figura 2.22. Componentes de la Plataforma FIWARE de acuerdo con [51]

La Figura 2.22, muestra los componentes de la Plataforma FIWARE, donde el Broker de Contexto es considerado el bloque principal de esta plataforma, alrededor del cual se construyen varios componentes. Otro punto importante de la Plataforma son sus interfaces, que se denominan *Next Generation Services Interfaces* (NGSI) y se definen como un conjunto de interfaces estandarizadas para conocer los recursos de red y las capacidades del dispositivo a emplearse. FIWARE hace uso de las interfaces NGSI-9 y NGSI-10 [52].

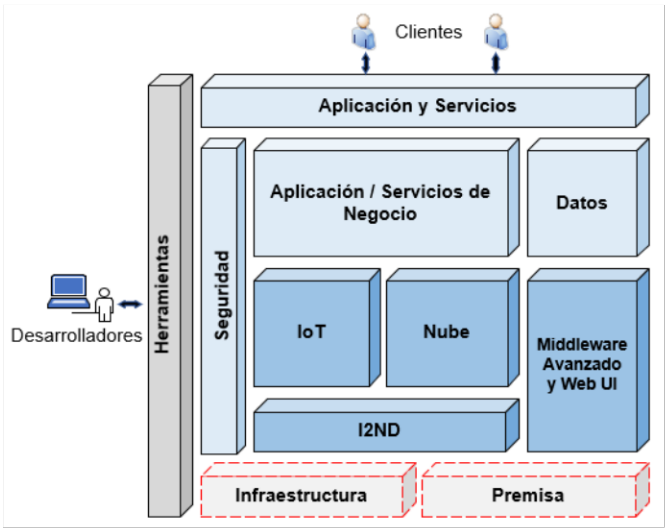


Figura 2.23. Arquitectura FI-WARE [50]

El proyecto FIWARE presenta una arquitectura avanzada y compleja, organizada en capítulos de acuerdo con los GE (Figura 2.23). Estos capítulos son: Nube, Datos, Aplicación y Servicios, IoT, Interfaz para Red y Dispositivos (I2ND), Seguridad y Gestión de Datos. En el presente trabajo se pondrá énfasis en el capítulo de IoT, el cual es visto

como un puente mediante el cual servicios FIWARE (*FI Services*) interactúan con dispositivos heterogéneos y con recursos limitados [52].

En lo relacionado a IoT, FIWARE define una arquitectura, donde los GE son una parte fundamental. Los GE se clasifican en 2 dominios: 1) IoT *Back End*: proporciona un conjunto de funciones, servicios y recursos almacenados en la nube; y 2) IoT *Edge*: contiene todos los elementos necesarios para la interconexión de dispositivos inteligentes con las FIApps. Esta arquitectura se muestra en la Figura 2.24, y tiene los siguientes bloques [7] y [53]:

- **Broker IoT:** permite agregar y recuperar información de los dispositivos mediante las interfaces NGSI.
- **Descubrimiento de IoT:** proporciona un mecanismo para descubrir servicios; además, de ser el encargado de registrar la disponibilidad del contexto.
- **Administración de Dispositivos IoT:** capacidades de comunicación básicas, tales como conectividad IP o de manera general, traduce la comunicación de protocolo específica de un dispositivo a Gateway a NGSI.
- **Broker de Contexto de Datos:** encargado de manejar las entidades de contexto (Dispositivos IoT).
- **Gateway IoT:** controla el API Edge y la conexión Gateway a Gateway (GW2GW).

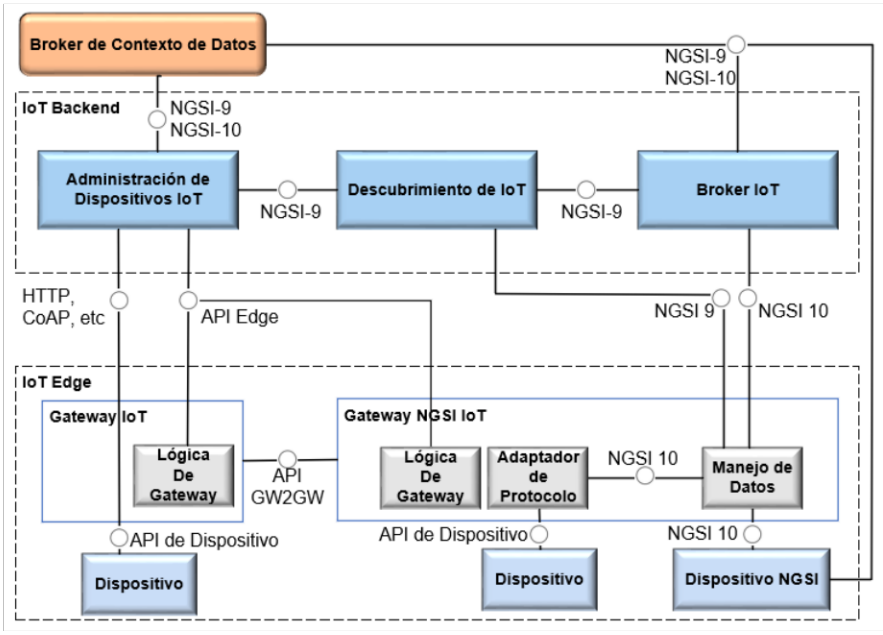


Figura 2.24. Arquitectura IoT de FIWARE, reconstruida en base a [7]

2.1.8.3 IoT-A

El objetivo de este proyecto es el de proveer un Modelo de Referencia para Arquitecturas (ARM) lo más genérico posible, mediante el cual se puedan derivar arquitecturas para

sistemas IoT. El proyecto IoT-A se encarga de proveer modelos, vistas, perspectivas y una serie de buenas prácticas para la implementación de una arquitectura IoT [54].

ARM consiste en tres partes interconectadas que son:

- **Modelo de Referencia IoT (RM):** conjunto de modelos usados para definir aspectos de la perspectiva de cada arquitectura.
- **Arquitectura de Referencia IoT (RA):** conjunto de perspectivas que incluye diferentes aspectos como seguridad, escalabilidad, entre otros.
- **Set Guía:** guía de buenas prácticas para el desarrollo e implementación de una arquitectura para sistemas IoT.

Una de las perspectivas más importantes del proyecto IoT-A, es la Vista Funcional (Figura 2.25). Propone un modelo en capas de grupos funcionales, integrados con un conjunto de componentes e interfaces que un sistema IoT debe poseer. Estos grupos son [54] y [55]:

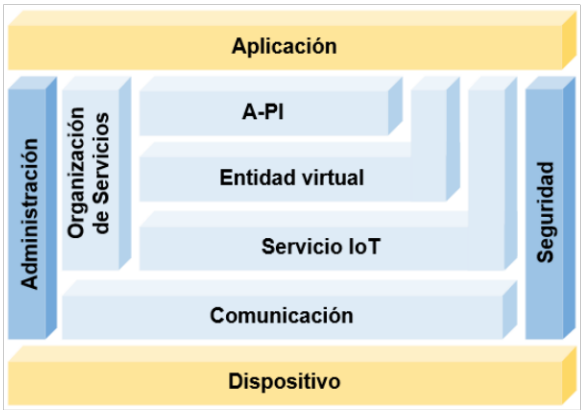


Figura 2.25. Vista Funcional IoT-A ARM, basada en [55]

- **Aplicación y Dispositivo:** se encuentran colocadas en el diagrama a modo de referencia; sin embargo, en la presente perspectiva no son tomadas en cuenta.
- **Administración y Seguridad:** grupos transversales que afectan a todos los demás grupos.
- **Organización de Servicios:** grupo encargado de elaborar y gestionar servicios de diferentes niveles de abstracción.
- **Administración de Procesos IoT (A-PI):** permite la integración de los sistemas de administración de negocios tradicionales con la arquitectura IoT-A ARM.
- **Entidad Virtual:** grupo compuesto de funcionalidades que permitan abstraer los requerimientos del Servicio IoT.
- **Servicio IoT:** relacionado con la Aplicación IoT.

- **Comunicación:** grupo fundamental dentro de esta perspectiva, incluye funciones relacionadas con el enrutamiento, detección y corrección de errores, control de flujo de la información, confiabilidad, QoS y Optimización de energía.

2.1.8.4 Modelo de Referencia James-Smith

En [55] se realiza un estudio sobre diferentes modelos de referencia para sistemas IoT, en los cuales se puede observar al modelo propuesto por James-Smith en 2005. Este modelo representa un diseño para redes de dispositivos inteligentes. Además, se encuentra apoyado en una Arquitectura Basada en Servicios (SOA) ya que emplea servicios web.

Las 3 capas del modelo son: Conexión, Abstracción y Aplicación. Estas capas son realmente básicas por lo que trabajos como [28], [30] y [31] adaptan el modelo para definir una arquitectura acorde a las necesidades del sistema IoT que plantean cada una de ellas.

2.1.8.5 Recomendación ITU-T Y.4000/2060: Arquitectura de Referencia IoT

Esta arquitectura fue propuesta en la Recomendación ITU-T Y.2060 en el 2012, luego en 2016 se realizó una revisión y se publicó la ITU-T Y.4000/2060. Esta recomendación define una arquitectura IoT de referencia compuesta de 4 capas y capacidades de seguridad y de gestión verticales a las 4 capas representadas en la Figura 2.26 [56]:

- **Dispositivo:** incluye las funcionalidades y capacidades de un dispositivo, éstas a su vez se ven clasificadas en dos: 1) Capacidades de dispositivo: incluye la comunicación directa o indirecta con la red de comunicación; y 2) Capacidades de Gateway: soporta múltiples interfaces y realiza la conversión de protocolo.
- **Red:** incluye capacidades que ofrecen conectividad con la red, control de acceso, autorización, autentificación y trazabilidad (AAA), y capacidades de transporte de datos e información de gestión relacionadas con aplicaciones IoT.
- **Soporte de Servicio y Aplicación (SSA):** consta de dos tipos de capacidades, la primera que son capacidades generales como el procesamiento y almacenamiento de datos que se dan en varias aplicaciones IoT, y capacidades de soporte específico, las cuales suplen necesidades específicas de una aplicación IoT.
- **Aplicación:** engloba a las aplicaciones IoT.

Las capacidades de seguridad se dividen en genéricas y específicas, las primeras no dependen de la aplicación e incluyen la autorización, confidencialidad e integridad de los datos, autentificación, control de acceso, entre otras. Por otra parte, las capacidades específicas suplen necesidades puntuales requeridas por una aplicación; por ejemplo, requisitos de seguridad para realizar transacciones a través del celular.

Las capacidades de gestión cubren gestión de fallos, de seguridad, y de configuración. Se clasifican en genéricas y específicas. Las capacidades genéricas abarcan la gestión remota de dispositivos, de tráfico en la red, entre otros. Las capacidades específicas se relacionan con requisitos puntuales de cada aplicación IoT.

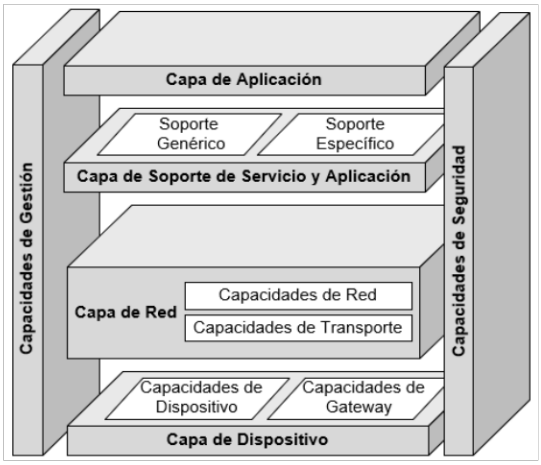


Figura 2.26. Arquitectura IoT de Referencia de acuerdo con la ITU-T [56]

A pesar de que la recomendación fue publicada en el año 2012, se puede observar que recomendaciones recientes como ITU-T Y.4474, publicada en el 2020, hace uso de esta recomendación y adapta su arquitectura de referencia para incorporar servicios basados en comunicaciones de luz visible (VLC) [57]. Las capas y capacidades verticales son similares, pero con diferentes funciones. Esta arquitectura se muestra en la Figura 2.27.

Una vez revisadas las arquitecturas y modelos de referencia, considerando el número de capas y sus funcionalidades, se realiza una tabla comparativa de estas arquitecturas (ANEXO II), donde consta información relevante que aporta al presente estudio.

Las arquitecturas más básicas de 3 capas presentan grandes similitudes en las funcionalidades de cada una de sus capas; este patrón cambia conforme la arquitectura o modelo de referencia aumenta su complejidad y número de capas. Para la comparación se tomaron en cuenta 12 parámetros o funcionalidades, repartidas en diferentes capas de la arquitectura o modelo de referencia analizado. Los parámetros que se consideran son:

- **Detección:** relacionada al dispositivo IoT (“Cosa”) que se encarga de sensar el entorno para una posible recolección de datos.
- **Recolección:** propiedad que permite al dispositivo IoT recopilar datos sin necesidad de esperar una condición que active esta funcionalidad.
- **Integración:** concerniente a la integración de dispositivos IoT, adaptación de protocolos e integración de datos.

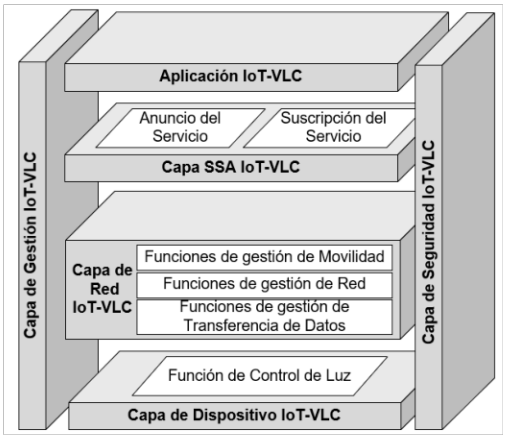


Figura 2.27. Arquitectura de Referencia IoT-VLC de acuerdo con la ITU-T [57]

- **Comunicación:** creación de rutas que posibiliten la transmisión de los datos.
- **Almacenamiento:** provisión de funcionalidades de almacenamiento de datos.
- **Preprocesamiento:** relacionada con la limpieza de datos inconsistentes, eliminación o reducción del ruido en los datos y normalización de los datos.
- **Procesamiento:** técnicas (*Machine Learning*, Aprendizaje Automático, entre otros) que usan datos preprocesados para extraer Conocimiento (Información).
- **Seguridad:** aplicación de métodos que añadan seguridad en el sistema IoT.
- **Calidad de Servicio:** relacionada con capas que recopilen información sobre las condiciones de hardware y software de los dispositivos del sistema IoT, con el fin de generar esquemas de configuración que garanticen un eficiente y correcto funcionamiento del sistema.
- **Administración:** relacionada con las capacidades de gestión del sistema IoT.
- **Apoyo en la toma de decisiones:** mediante el conocimiento extraído se realiza la creación de *Dashboards*, planes de mejora o ideas que faciliten la toma de decisiones.
- **Provisión de Aplicaciones y Servicios:** relacionada con el desarrollo y provisión de aplicaciones y servicios a los usuarios finales.

Para observar el avance y la evolución de las arquitecturas y modelos de Referencia para sistemas IoT de los últimos 5 años, se realizó una gráfica con la Línea de Tiempo, ésta puede ser observada en la Figura 2.28. Se incluyen fechas previas a los 5 últimos años para hacer referencia a fechas de creación de un modelo o arquitectura, ya que el análisis se realizó en base de publicaciones. Tal es el caso del *Survey* publicado en noviembre 2019 en [55], donde se hace una revisión de modelos de referencia para sistemas IoT como: 1) El modelo James-Smith; y 2) El Proyecto IoT-A, los cuales fueron originalmente publicados en 2005 y 2013, respectivamente.

Se puede destacar que se inicia con el modelo de Referencia James-Smith, ya que es uno de los más básicos y define únicamente 3 capas. Desde este punto en adelante se comenzaron a desarrollar arquitecturas de 3 capas como las planteadas en [29]–[31].

Debido al desarrollo de la tecnología y a las exigencias recibidas para los sistemas IoT, las arquitecturas de 3 capas comenzaron a modificarse para incluir una nueva capa que ejecute funcionalidades de preprocesamiento e integración de datos, con el fin de aliviar la carga computacional de la última capa, generalmente denominada capa de aplicación. Esta nueva capa en publicaciones revisadas como [35] y [36] se denomina “Computación” y “Middleware”, respectivamente. A partir de este punto se puede mencionar que cada desarrollador de sistemas IoT comenzó a incluir el número de capas que satisfacían las necesidades para un determinado sistema, llegando a observar arquitecturas de 5, 6, 7 o hasta 8 capas como la observada en [41].

Tras observar que el desarrollo de sistemas IoT no seguía un estándar común, surgen proyectos como IoT-A o FIWARE, cuyo objetivo inicial fue similar, proveer un modelo de referencia para el desarrollo de arquitecturas de sistemas IoT [50] y [54], de los cuales el proyecto IoT-A fue finalizado en el año 2013, mientras que FIWARE siguió la visión de mantenerse como una plataforma de desarrollo para sistemas IoT centrada en 4 dominios. También, se observa en la Figura 2.28, la aparición de la Recomendación ITU-T Y. 4000/2060, que sigue vigente, en base a la que se han desarrollo varios sistemas. Tal es el caso de llegar a desplegar otra recomendación que combina IoT con VLC [57].

Finalmente, en esta línea de tiempo se observa cómo la complejidad estructural de las arquitecturas se incrementa, va de una arquitectura de 3 capas simple a implementaciones de microservicios, o sistemas basados en la nube e implementar Blockchain. Este último punto surge como una solución de incrementar el nivel de seguridad en los sistemas IoT, pues ante cualquier integración de datos o modificación de la información del sistema, se debe actualizar cada nodo de la red Blockchain, de modo que, esta tecnología puede verse como la manera de incorporar una base de datos segura y distribuida en las aplicaciones para sistemas IoT [58]. Al final de la Figura 2.28 se observa el estándar desarrollado por la IEEE para la gestión de datos de sistemas IoT basados en Blockchain [47].

2.2 ANÁLISIS COMPARATIVO

Tras analizar cada arquitectura y modelo de referencia IoT ha quedado evidenciada la existencia de una gran variedad de éstas, y la falta de un estándar comúnmente aceptado para el desarrollo de sistemas IoT. Cada autor en sus publicaciones prácticamente plantea una arquitectura IoT de acuerdo con las necesidades, que ayudan a cumplir el objetivo de

una aplicación en específico, por lo que a modo general se puede mencionar que en su mayoría las arquitecturas para sistemas IoT analizadas no se encuentran estandarizadas.

Otro factor que provoca que exista una gran diversidad de arquitecturas para sistemas IoT, es variedad de dispositivos disponibles en el mercado, por lo que la falta de estandarización va de la mano con problemas de interoperabilidad entre diferentes sistemas IoT. Se considerarán como arquitecturas estandarizadas a aquellas que han sido generadas mediante un proyecto (IoT-A, FIWARE) o publicadas por órganos normalizadores (ITU-T); mientras que aquellas que han sido planteadas en publicaciones por varios investigadores con el fin de proponer un diseño o satisfacer necesidades de ciertas aplicaciones IoT, son consideradas como arquitecturas no estandarizadas. La Tabla 2.1 muestra una clasificación entre arquitecturas y modelos de referencia estandarizadas y no estandarizadas. Queda evidenciado que tras realizar una búsqueda gruesa (y su respectiva filtración) de publicaciones relacionadas con arquitecturas y modelos de referencia para sistemas IoT, la cantidad de estas arquitecturas o modelos de referencia que se encuentran estandarizados es escasa. En la presente investigación se obtuvo un total de 7 arquitecturas o modelos de referencia para sistemas IoT estandarizados.

Una vez revisada cada una de las publicaciones sobre arquitecturas o modelos de referencia detalladas en la sección 2.1 se ha realizado una comparación gráfica, asociando cada modelo o arquitectura con un área de aplicación de sistemas IoT. Este resultado puede ser observado en la Tabla 2.2. De manera general se resalta que sin importar el número de capas que posea una arquitectura o modelo de referencia, las áreas de aplicación más desarrolladas son el Cuidado de la Salud y Ciudad Inteligente, con un total de 5 y 6 publicaciones para cada área, respectivamente.

Según la revista McKinsey's global Economic, para el 2025, el desarrollo de dispositivos para el cuidado de la salud ocupará un 41% del total de dispositivos IoT desarrollados para dicho año [11]. Se puede observar una concordancia con lo expuesto en el presente trabajo, pues en los últimos 5 años se han presentado una gran cantidad de arquitecturas para sistemas IoT orientados al Cuidado de la Salud, tal como arquitecturas de 3 y 4 capas, basadas en la nube, uso de Blockchain y proyectos tales como FIWARE e IoT-A.

Con respecto al área de aplicación Ciudad Inteligente, según el análisis realizado se cuenta con la mayoría de las arquitecturas para sistemas IoT relacionadas. Según [59], las ciudades cada vez presentan un desarrollo importante, por lo que su densidad poblacional aumenta de igual manera. Con esto se presentan desafíos en el control ambiental, gestión de residuos, urbanización, entre otros.

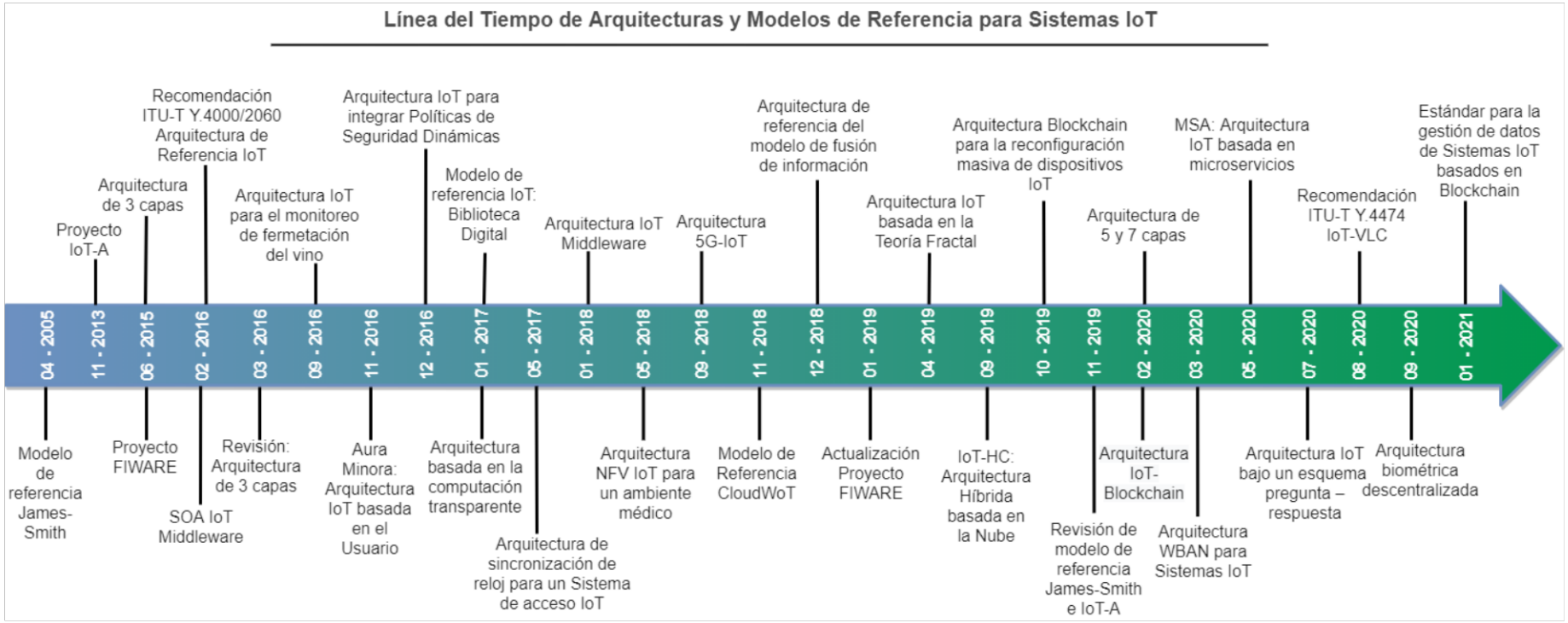


Figura 2.28. Línea del Tiempo de las Arquitecturas y Modelos de Referencia para Sistemas IoT de los últimos 5 años

Tabla 2.1. Arquitecturas y Modelos de Referencia para Sistemas IoT Estandarizados y No Estandarizados

Nombre de la Arquitectura / Modelo de Referencia para Sistemas IoT	Estandarizado	No Estandarizado
Arquitectura de 3 Capas (*Survey*)		✓
Arquitectura de Sincronización de Reloj para un Sistema de Acceso IoT		✓
Arquitectura Biométrica Descentralizada		✓
Arquitectura IoT bajo un Esquema Pregunta – Respuesta		✓
Arquitectura NFV IoT para un Ambiente Médico		✓
Arquitectura IoT basada en la Teoría Fractal		✓
Arquitectura IoT para Integrar Políticas de Seguridad Dinámicas		✓
Arquitectura WBAN para Sistemas IoT		✓
Arquitectura IoT para el Monitoreo de Fermentación del Vino		✓
Arquitectura 5 Capas (*Survey*)		✓
Arquitectura IoT Middleware		✓
Aura Minora: Arquitectura IoT basada en el Usuario		✓
Arquitectura 7 capas		✓
Arquitectura 5G-IoT		✓
MSA: Arquitectura IoT basada en Microservicios		✓
SOA IoT Middleware		✓
Arquitectura CloudWoT		✓
IoT-HC: Arquitectura Híbrida basada en la Nube		✓
Arquitectura basada en la Computación Transparente		✓
Arquitectura IoT-Blockchain		✓
Estándar para la Gestión de Datos de Sistemas IoT con Blockchain	✓	
Arquitectura Blockchain para la Reconfiguración Masiva de Dispositivos IoT		✓
Arquitectura de Referencia del Modelo de Fusión de Información	✓	
Proyecto FIWARE	✓	
IoT-A	✓	
Modelo de referencia James-Smith	✓	
Recomendación ITU-T Y.4000/2060: Arquitectura de Referencia IoT	✓	
Recomendación ITU-T Y.4474: Arquitectura IoT-VLC	✓	

Por ende, el área de aplicación de Ciudad Inteligente, en un futuro llegará a tener gran importancia y se buscará desarrollar sistemas IoT que suplan las necesidades expuestas.

De acuerdo a la clasificación realizada en la Tabla 2.2, se observa que las arquitecturas para sistemas IoT basadas en la Nube poseen una gran variedad de aplicaciones en diferentes áreas (Cuidado de la Salud, Transporte, Ciudad Inteligente, Agricultura y Cuidado Ambiental); esto se puede explicar debido a los recursos y capacidades ilimitadas

que ofrece la nube en las aplicaciones IoT, tales como mejora de procesamiento, almacenamiento y comunicación [24]. Finalmente, se puede mencionar que trabajos tales como [28], [38], [60], entre otros, únicamente plantean una arquitectura más no definen una aplicación para ésta. Este hecho refleja la falta de madurez de dichas arquitecturas.

Como se presentó en la sección 2.1, de los trabajos analizados, en algunos de ellos los autores mencionan un uso de la arquitectura, como en [31], donde se plantea un arquitectura biométrica descentralizada de 3 capas orientada a aplicaciones del Cuidado de la Salud. También existen autores que sólo definen una arquitectura a modo de diseño y no dan referencias sobre posibles usos.

En la Figura 2.29 con ayuda de la clasificación realizada en la Tabla 2.2 se realiza un mapa conceptual, donde se pueden apreciar únicamente las arquitecturas y modelos de referencia para sistemas IoT que definen una determinada área de aplicación. Donde se puede notar que las áreas de aplicación de sistemas IoT con una mayor acogida son el Cuidado de la Salud y Ciudad Inteligente.

Tras revisar documentación sobre los modelos de referencia para sistemas IoT, se puede decir que el Proyecto FIWARE define su despliegue sobre 4 dominios: *Smart City, Smart AgriFood, Smart Energy* y *Smart Industry* [50], los cuales tendrían su equivalente en la taxonomía de Áreas de aplicación para sistemas IoT presentada en el presente trabajo (Figura 1.3), que son Ciudad Inteligente, Agricultura y Cuidado Ambiental e Industria. Esto refleja que FIWARE no se extiende en todos los dominios de los sistemas IoT, y proyecta las aplicaciones a futuro en los 4 dominios mencionados.

Con respecto al proyecto IoT-A, en [61] se puede observar una lista de proyectos para sistemas IoT que tienen como base a IoT-A, en dicha lista se puede evidenciar que en su mayoría los proyectos desarrollados se aplican a 3 áreas como lo son el Cuidado de la Salud, Transporte y Ciudad Inteligente. Cabe mencionar que el proyecto IoT-A finalizó el 30 de noviembre de 2013, fijando como objetivo el desarrollo de un modelo de referencia para la interoperación de sistemas IoT [54]. Esto es importante, pues permite comparar las áreas de aplicación de sistemas IoT mayormente utilizadas en dicho año, con las del periodo comprendido en los último 5 años. Permitiendo así marcar una tendencia en el desarrollo de aplicaciones para sistemas IoT en las áreas del Cuidado de la Salud y Ciudad Inteligente, pues tanto en [61] como en la Tabla 2.2 estas áreas cuentan con el mayor número de proyectos realizados. Los demás proyectos de referencia (ITU-T, James-Smith y Fusión de Información) presentan un amplio campo de integración en diferentes áreas de aplicación, por lo cual no se incluyen en la Figura 2.29

Tabla 2.2. Arquitecturas y Modelos de Referencia para Sistemas IoT según su Área de Aplicación

Clasificación	Referencia	N. Capas	Área de Aplicación								
			Cuidado de la Salud	Transporte	Hogar Inteligente	Ciudad Inteligente	Agricultura y Cuidado Ambiental	Comercio	Industria	General	No Especifica
Arquitecturas de 3 capas	Arquitectura de 3 capas (Survey) [28]	3									✓
	Arquitectura de 3 capas [29]										✓
	Arquitectura de sincronización de reloj [30]			✓							
	Arquitectura biométrica [31]		✓			✓					
	Arquitectura IoT pregunta – respuesta [32]					✓					
Arquitecturas de 4 capas	Arquitectura NFV IoT [33]	4	✓								
	Arquitectura IoT Teoría Fractal [34]										✓
	IoT-Políticas de Seguridad Dinámicas [35]										✓
	Arquitectura WBAN [36]		✓								
	Arquitectura IoT-monitoreo de vino [37]								✓		
Arquitectura 5 capas	Arquitectura de 5 capas (Survey) [29]	5									✓
Arquitecturas de 6 capas o superior	Arquitectura IoT Middleware [38]	6									✓
	Aura Minora: Arquitectura IoT [39]	6				✓					
	Arquitectura de 7 capas [40]	7									✓
	Arquitectura 5G-IoT [41]	8				✓					
Arquitecturas basadas en Microservicios	MSA: Arquitectura IoT-microservicios [42]	3				✓					
	SOA IoT Middleware [43]	5									✓
Arquitecturas basadas en la Nube	Arquitectura CloudWoT [44]	4		✓			✓				
	IoT-HC: Arquitectura Híbrida-Nube [45]	3				✓	✓				
	Arquitectura-Comp. Transparente [46]	5	✓								
Uso de Blockchain	Arquitectura IoT-Blockchain [29]	5	✓		✓			✓			
	Estándar Gestión Datos-Sistemas IoT [47]	4								✓	
	Arquitectura reconfiguración IoT [48]	3									✓
Modelos de referencia y proyectos de desarrollo para Sistemas IoT	Modelo de Fusión de la Información [49]	6								✓	
	Proyecto FIWARE [50]	5								✓	
	IoT-A [54]	9								✓	
	Modelo de referencia James-Smith [55]	3								✓	
	Recomendación ITU-T Y.4000/2060 [56]	4								✓	

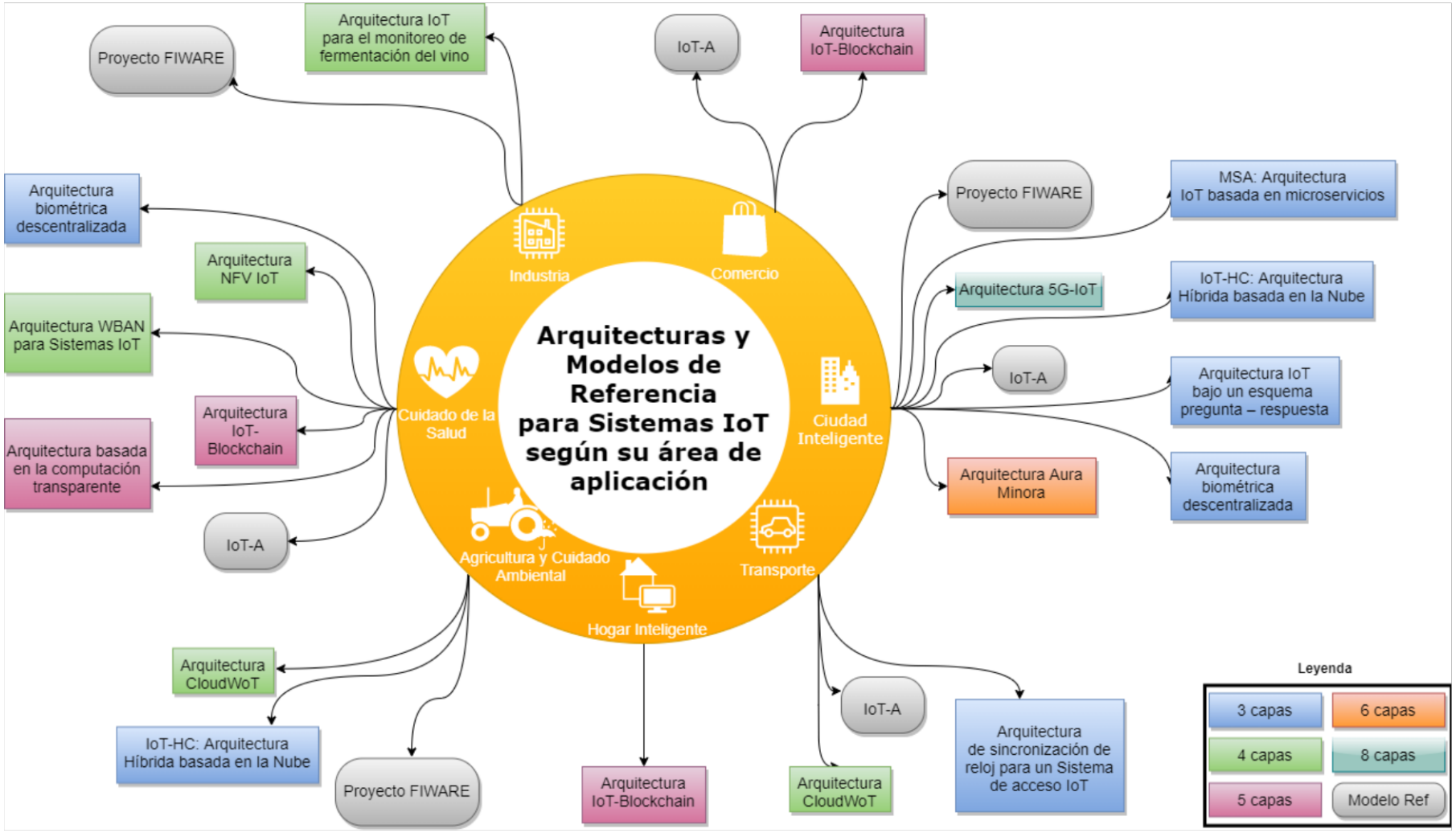


Figura 2.29. Arquitecturas y Modelos de Referencia para Sistemas IoT según su área de aplicación

3 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

3.1 RESULTADOS

Luego de analizar diferentes arquitecturas y modelos de referencia para sistemas IoT, así como realizar una comparación de las funcionalidades de las capas que integran cada una de ellas, se puede observar una gran variedad en cuanto a las mismas. Esto surge como consecuencia de la falta de un estándar común. Como se ha evidenciado en la presente investigación, la Tabla 2.1 refleja la escasa existencia de arquitecturas estandarizadas. La falta de un estándar común provoca que los desarrolladores de sistemas IoT planteen y desplieguen nuevas arquitecturas en cada aplicación IoT desarrollada, las cuales pueden llegar únicamente a quedar planteadas como propuesta, a ser implementadas por un uno o varios desarrolladores, y en el mejor de los casos a ser usadas como referencia por otros autores para mejorar o desarrollar otra arquitectura.

3.1.1 DEFINICIÓN DEL NIVEL DE MADUREZ DE LAS ARQUITECTURAS Y MODELOS DE REFERENCIA PARA SISTEMAS IOT

Para establecer el nivel de madurez de cada arquitectura o modelo de referencia IoT, se ha generado un mecanismo de asignación de puntos, en donde se asumen las siguientes puntuaciones para realizar un análisis de madurez de cada una de ellas:

- A: Publicado netamente como propuesta: 1 punto.
- B: Implementado sólo por quién hace la propuesta de la arquitectura: 2 puntos.
- C: Contribución como referencia para que otros autores puedan continuar, mejorar o implementar la propuesta de la arquitectura: 3 puntos.
- D: Publicado por una organización certificada en desarrollo de proyectos o entidad de estandarización: 4 puntos.

Estas puntuaciones se suman, se puede obtener hasta máximo 10 puntos. Se definen 3 niveles de madurez: Alto (mayor a 8 puntos), Medio (6 y 7 puntos) y Bajo (1 a 5 puntos). Cada letra de la puntuación se coloca entre paréntesis junto al texto que justifique su asignación. A continuación, se detallará el proceso de cálculo del nivel de madurez de cada arquitectura y modelo de referencia para sistemas IoT revisados en la sección 2.1.

Arquitectura de 3 Capas (Survey)

Lao en [29] realiza un estudio de las arquitecturas para sistemas IoT (A), en donde hace referencia a una publicación popular realizada por Al-Fuqaha [62], aquí se puede observar

que la arquitectura de 3 capas fue realmente utilizada y aceptada en las fases iniciales del desarrollo de sistemas IoT. Esta arquitectura fue implementada en proyectos desplegados por *China Mobile* para la transmisión de información en cadenas de suministro [63] y revisada superficialmente por otros autores en [64] y [65] (C). Por los motivos antes expuestos, se puede concluir que esta arquitectura de 3 capas tuvo su acogida; sin embargo, ante la limitación de funcionalidades de sus 3 capas, se optó por migrar a una de 4 y posteriormente a 5 capas [29].

- Nivel de madurez: Bajo (A y C → 4 puntos)

Arquitectura de Sincronización de Reloj de un Sistema de Acceso IoT

Tal como se expone en [30], la presente arquitectura fue diseñada e implementada con el objetivo de realizar el monitoreo de vehículos en tiempo real (A y B). La arquitectura ha sido referenciada por otros autores un total de 7 veces; sin embargo, en ninguna de las publicaciones se realiza la implementación de esta arquitectura, tal es el caso de [66], en donde se hace una revisión teórica de la presente arquitectura. Por ende, la arquitectura de sincronización de reloj únicamente se limita a ser un proyecto de autor, tanto en propuesta como implementación.

- Nivel de madurez: Bajo (A y B → 3 puntos)

Arquitectura Biométrica Descentralizada de 3 capas

En [31] se presenta una arquitectura biométrica de 3 capas descentralizada, la cual ha sido planteada para el monitoreo y detección de personas durante las temporadas de restricción de circulación en las ciudades (A). También se menciona que esta arquitectura ha sido validada con un conjunto de pruebas (rostros) para evaluar la eficiencia en la detección de rostros de la aplicación (B). Esta arquitectura ha sido referenciada en un total de 35 publicaciones, ya que el tema del COVID-19 se encuentra en la mira de la investigación. Sin embargo, en estas publicaciones no se realiza una referencia sobre el uso directo de la arquitectura presentada en [31]; tales son los casos de: [67] en donde se realiza una revisión de aplicaciones biométricas en el dominio de IoT, así como en [68] y [69], en donde se realiza una comparación de esta arquitectura biométrica con las propuestas por cada uno de sus autores.

- Nivel de madurez: Bajo (A y B → 3 puntos)

Arquitectura IoT Bajo un Esquema Pregunta – Respuesta

En [32] se propone y se evalúa una arquitectura IoT para el aprendizaje ubicuo (A y B). La presente arquitectura ha sido referenciada un total de 9 veces, sin embargo, no se refleja

un uso o aplicación de esta arquitectura por parte de otros autores. Tal es el caso de [70], en donde se propone un marco de trabajo para aplicaciones de aprendizaje inteligente, y se usa la arquitectura IoT bajo un esquema de pregunta y respuesta para validar la necesidad de proponer el marco de trabajo.

- Nivel de madurez: Bajo (A y B → 3 puntos)

Arquitectura NFV IoT para un Ambiente Médico

La arquitectura presentada en [33] se encuentra desarrollada a modo de propuesta e implementada en un Ambiente OPIC (A y B). La arquitectura se encuentra referenciada un total de 16 veces. En la mayoría de estos artículos únicamente se hace referencia de manera teórica para dar una introducción a aplicaciones IoT para el Cuidado de la Salud. Sin embargo, en [71] se puede observar una implementación de una arquitectura IoT de 4 capas similar a la arquitectura NFV IoT, por lo que se puede decir que la presente arquitectura cuenta con una implementación aparte de la del propio autor (C).

- Nivel de madurez: Medio (A, B y C → 6 puntos)

Arquitectura IoT basada en la Teoría Fractal

La arquitectura IoT basada en la Teoría Fractal [34] únicamente se encuentra desarrollada a manera de propuesta netamente teórica (A), pues no se realiza una implementación de ésta. La presente arquitectura se encuentra referenciada un total de 2 veces, sin embargo, en ninguna de estas publicaciones se realiza una implementación o modificación de la arquitectura.

- Nivel de madurez: Bajo (A → 1 punto)

Arquitectura IoT para Integrar Políticas de Seguridad Dinámicas

En [35] se presenta una propuesta e implementación de arquitectura IoT (A y B), la cual maneja políticas de seguridad dinámicas. Esta arquitectura ha sido referenciada 10 veces. Por ejemplo, en [72] se presenta una arquitectura simplificada orientada a la agricultura, ésta se basa en la arquitectura IoT para el manejo de Políticas de seguridad (C). Por otra parte, en [73] se hace referencia a la presente arquitectura para ejemplificar soluciones que requieren de un poder computacional alto y consumen una gran cantidad de energía.

- Nivel de madurez: Medio (A, B y C → 6 puntos)

Arquitectura WBAN para Sistemas IoT

La arquitectura WBAN detallada en [36] fue desarrollada a modo de propuesta (A) y posteriormente implementada para validar su funcionamiento (B). No se han realizado referencias a la presente arquitectura por parte de otros autores.

- Nivel de madurez: Bajo (A y B → 3 puntos)

Arquitectura IoT para el Monitoreo de Fermentación del Vino

La arquitectura presentada en [37] ha sido desarrollada a modo de propuesta (A), no se llega a implementar. Sin embargo, ha sido referenciada un total de 7 veces; por ejemplo, en [74] se trata a la arquitectura como trabajo relacionado y se calcula que su implementación rondaría los 300 euros. En [75] se trata a esta arquitectura como trabajo relacionado, la cual es modificada levemente e implementada (C). Finalmente, en [76] se hace una comparación de esta arquitecta y otras relacionadas con el monitoreo del proceso de fermentación del vino.

- Nivel de madurez: Bajo (A y C → 4 puntos)

Arquitectura IoT Middleware

La arquitectura IoT Middleware se presenta únicamente como una propuesta teórica (A), no se llega a implementar. Ha sido citada un total de 212 veces, se revisaron las publicaciones más relevantes, en donde se utiliza la presente arquitectura únicamente para introducir conceptos de la incorporación de Middleware en plataformas IoT, tal como en [77] y [78]. Por otra parte, Da Cruz en [79] realiza pruebas de rendimiento en diferentes plataformas IoT que integren un Middleware, entre las que se encuentra la presente Arquitectura IoT Middleware (C).

- Nivel de madurez: Bajo (A y C → 4 puntos)

Aura Minora: Arquitectura IoT basada en el Usuario

Aura Minora ha sido realizada netamente como una propuesta teórica (A), no se llegar a implementar por su autor [39]. La arquitectura Aura Minora ha sido referenciada un total de 7 veces, por ejemplo, en [80] se realiza una comparación de arquitecturas IoT orientadas a ciudades inteligentes en donde se contrasta esta arquitectura. En general la arquitectura Aura Minora ha sido referenciada para introducir conceptos de la integración de IoT con servicios ofrecidos en las ciudades, mas no se ha llegado a implementar por otros autores.

- Nivel de madurez: Bajo (A → 1 punto)

Arquitectura de 7 capas

La arquitectura ha sido referenciada 89 veces, de las citas relevantes que han sido revisadas no se han encontrado arquitecturas que tomen como referencia a la arquitectura de 7 capas, o aplicaciones que implementen este tipo de arquitectura, esto puede ser justificado debido a que en [40] aparte de desarrollar la arquitectura de 7 capas (A), se realiza un estudio de arquitecturas para sistemas IoT que van desde 3 hasta 7 capas, motivo por el cual el artículo es referenciado por un gran número de publicaciones. Por ejemplo, Kumar en [81] referencia a la arquitectura de 7 capas para introducir teoría de sensores en su propuesta de una aplicación de monitoreo de residuos en las ciudades.

- Nivel de madurez: Bajo (A → 1 punto)

Arquitectura 5G-IoT

En [41] se presenta la arquitectura 5G-IoT y las potenciales brechas de seguridad que poseen cada una de sus capas, en esta publicación Rahimi, revisa esta arquitectura y no se da una propuesta de implementación (A). La arquitectura ha sido referenciada 13 veces, tal como en [82], en donde se recalca la importancia de la tecnología 5G para las aplicaciones IoT. Además, se toma como referencia a la arquitectura 5G-IoT para proponer una nueva arquitectura denominada SDNFV 5G-IoT la cual combina redes SDN y Funciones de virtualización de red (NFV) (C). Otras publicaciones tal como [83] realizan estudios comparativos de arquitecturas para sistemas IoT que implementen tecnologías de nueva generación como 5G.

- Nivel de madurez: Bajo (A y C → 4 puntos)

MSA: Arquitectura IoT basada en Microservicios

De Sanctis en [42] presenta la arquitectura MSA desarrollada únicamente a modo de propuesta (A), el mismo autor en [84] realiza la mejora e implementación de su arquitecta (B), para una aplicación NdR (*Network detection and Response*). También se puede mencionar que la arquitectura MSA ha sido referenciada 10 veces, tal es el caso de [85], en donde se revisa esta arquitectura como trabajo relacionado, para dar paso a la propuesta de una nueva arquitectura “SEnviro” que a la vez funcione como plataforma IoT (C).

- Nivel de madurez: Medio (A, B y C → 6 puntos)

SOA IoT Middleware

En [43] se realiza un estudio sobre diferentes arquitecturas para sistemas IoT, entre las cuales se propone la arquitectura SOA IoT Middleware (A), sin embargo, no se presenta una implementación de dicha arquitectura. El artículo posee un total de 94 citas, pese a tener una gran cantidad de publicaciones que usan como referencia a esta arquitectura, únicamente la usan para introducir conceptos sobre middleware o arquitecturas basadas en servicios, tal es el caso de [86].

- Nivel de madurez: Bajo (A → 1 punto)

Arquitectura CloudWoT

Pese a tener 11 referencias de la arquitectura CloudWoT en otras publicaciones, en ninguna de estas se ha podido observar que se lleve a cabo una implementación de ésta. Por ejemplo, en [87] y [88] se hace referencia a la arquitectura CloudWoT únicamente para introducir conceptos de Computación en la Nube. Es así que, la arquitectura CloudWoT planteada en [44], se considera únicamente como una propuesta teórica de arquitectura (A).

- Nivel de madurez: Bajo (A → 1 punto)

IoT-HC: Arquitectura Híbrida basada en la Nube

Esta arquitectura únicamente ha sido planteada a modo de propuesta, no se ha llegado a implementar y tampoco se ha referenciado a la arquitectura en trabajos de otros desarrolladores.

- Nivel de madurez: Bajo (A → 1 punto)

Arquitectura basada en la Computación Transparente

En [46] se presenta a la Arquitectura IoT basada en la computación transparente (A). También, se realiza la implementación de esta arquitectura en una aplicación para relojes inteligentes denominada TCwatch (B). La arquitectura se encuentra referenciada un total de 356 veces, tras revisar las publicaciones más relevantes, se pudo observar casos como [89], en donde en base a la presente arquitectura se realiza la implementación de una aplicación que combine aprendizaje profundo con la computación en la nube (C) Existen otras publicaciones en donde se usa esta arquitectura únicamente para introducir conceptos de computación en la nube, tales como [90] y [91].

- Nivel de madurez: Medio (A, B y C → 6 puntos)

Arquitectura IoT-Blockchain

Lao en [29] realiza una revisión de aplicaciones IoT para sistemas Blockchain , en donde plantea la Arquitectura IoT-Blockchain pero no realiza una implementación de ésta (A). Blockchain al ser una tecnología emergente en los últimos años que puede ser vista como una base de datos distribuida ha pasado a ser considerada en la parte concerniente a la seguridad de sistemas IoT. La presente arquitectura ha sido referenciada un total de 113 veces, sin embargo, no se ha observado que otros autores hagan uso de la arquitectura IoT-Blockchain para implementar sistemas IoT. Casos como [92] y [93] emplean la publicación de Lao para introducir conceptos sobre mecanismos de conceso en Blockchain.

- Nivel de madurez: Bajo (A → 1 punto)

Estándar para la Gestión de Datos en Sistemas IoT con Blockchain

El estándar IEEE 2144.1 ofrece un marco de trabajo para el manejo de datos en sistemas IoT con Blockchain [47] (D). Pese a ser un área interesante, porque el manejo de datos es un factor sensible a considerar, en torno a la privacidad del usuario final, no se han encontrado publicaciones en donde se aplique el estándar para implementar un sistema IoT. En [94] y [95] solo se hace referencia a este estándar para dar a conocer la existencia de un marco de referencia para el manejo de datos con Blockchain en sistemas IoT.

- Nivel de madurez: Bajo (D → 4 puntos)

Arquitectura Blockchain para la Reconfiguración Masiva de Dispositivos IoT

En [48], Le-Dang propone una arquitectura basada en Blockchain para la reconfiguración masiva de dispositivos IoT (A); además, realiza una prueba de concepto de la arquitectura (B). Esta publicación ha sido referenciada un total de 9 veces, sin embargo, no se ha podido encontrar una continuación o implementación de este trabajo. Existen publicaciones tales como [96], en donde se menciona a la arquitectura de reconfiguración masiva de dispositivos IoT únicamente para introducir conceptos de escalabilidad en sistemas IoT.

- Nivel de madurez: Bajo (A y B → 2 puntos)

Arquitectura de Referencia del Modelo de Fusión de Información

El modelo de fusión de la información desarrollado a modo de propuesta en [49] (A), ha sido referenciado por otros autores un total de 7 veces; sin embargo, en ninguno de estos se da una continuación o seguimiento de la propuesta. Por ejemplo, en [97] se revisa al modelo, mencionando la importancia de la integración de la información médica para aplicaciones IoT orientadas al Cuidado de la Salud. En [98] se propone una arquitectura

IoT para un sistema inteligente de detección de pacientes con COVID-19, en donde el modelo de fusión de la información únicamente es revisado para introducir conceptos de recolección de datos médicos en ambientes IoT.

- Nivel de madurez: Bajo (A → 1 punto)

Proyecto FIWARE

FIWARE es un proyecto que tiene por objetivo construir una Plataforma Central para el Internet del Futuro (D). Este proyecto, posee una gran aceptación pues cuenta incluso con una comunidad de miembros bajo suscripción. La plataforma se centra en 4 dominios que son: *Smart AgriFood, Smart City, Smart Energy* y *Smart Industry*. Cuenta con aproximadamente 8000 desarrolladores que usan tecnologías FIWARE, 180 soluciones IoT en el mercado impulsadas por soluciones FIWARE (C) y 150 proyectos de Código abierto propuestos e implementados por desarrolladores FIWARE (A y B) [50].

- Nivel de madurez: Alto (A, B, C y D → 10 puntos)

IoT-A

El proyecto IoT-A creó un modelo de referencia para sistemas IoT (D) y concluyó en el 2013 [54]. En el presente proyecto de integración curricular se va a considerar al proyecto IoT-A con un nivel de madurez alto, pues varios proyectos de IoT emplearon este modelo de referencia. En [61] se puede observar una lista de 92 proyectos que adoptaron el modelo de IoT-A en diferentes áreas de aplicación como Ciudad Inteligente, Cuidado de la Salud, Transporte y Comercio (C). Cabe mencionar que esta lista forma parte de la documentación provista al público por parte del proyecto IoT-A (A y B).

- Nivel de madurez: Alto (A, B, C y D → 10 puntos)

Modelo de Referencia James-Smith

Este modelo de referencia cuenta realmente con poca madurez, por lo que puede ser observado como un intento de estandarización de la arquitectura de 3 capas para sistemas IoT (A). Sin embargo, no contó con el suficiente apoyo para que desarrolladores lo adopten en soluciones de aplicaciones IoT [55].

- Nivel de madurez: Bajo (A → 1 punto)

Recomendación ITU-T Y.4000/2060: Arquitectura de Referencia IoT

Esta recomendación realiza una revisión general sobre IoT, en donde se plantea el modelo de referencia para sistemas IoT (D). La documentación provista por la ITU para la línea de

recomendaciones Y.4000 cuenta con propuestas novedosas y revisadas con detalle (A y B). Este estándar puede verse como uno de los esfuerzos más significativos para lograr una estandarización en arquitecturas para sistemas IoT. A partir de este estándar se han desarrollado otros tales como, la arquitectura funcional para servicios IoT basada en VLC [57], el modelo de referencia IoT basada en Blockchain "BoT" (*Blockchain of Things*) [99] y la arquitectura para IoT ICS (*Identity Correlation Service*) [100] (C).

- Nivel de madurez: Alto (A, B, C y D → 10 puntos)

Una vez finalizada la asignación del nivel de madurez para cada arquitectura y modelo de referencia para sistemas IoT, se presenta la Figura 3.1, donde se pueden observar los porcentajes de los niveles de madurez. Se observa que la mayoría de las arquitecturas poseen un nivel bajo de madurez, pues éstas únicamente son planteadas a modo de propuesta, y en el mejor de los casos implementadas por sus propios autores, de modo que no contribuyen en futuros trabajos por parte de otros desarrolladores. Le siguen las arquitecturas con un nivel de madurez medio, las cuales han servido como contribución para generar otras arquitecturas o han sido mejoradas o reestructuradas por otros autores, permitiendo que se tenga una continuación y desarrollo a futuro de una determinada aplicación. Finalmente, se puede observar que el nivel de madurez alto posee el porcentaje más bajo, pues únicamente está comprendido por modelos de referencia, ya que estos son desarrollados por entidades normalizadoras u organizaciones centradas en el desarrollo de sistemas IoT, tal es el caso de ITU-T y FIWARE *Foundation*.

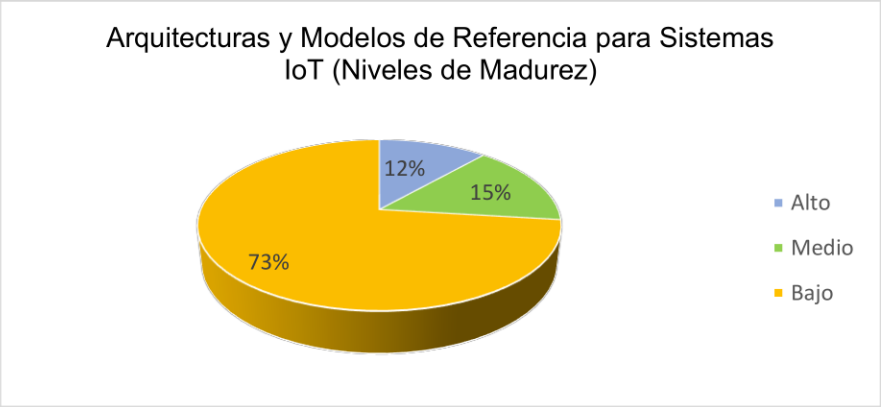


Figura 3.1. Porcentajes de arquitecturas y modelos de referencia para sistemas IoT según su nivel de madurez

3.1.2 DESAFIOS PRESENTES PARA TRABAJAR CON DISPOSITIVOS HETEROGÉNEOS

Hasta el momento, se han revisado diferentes arquitecturas y modelos de referencia para sistemas IoT, se los ha comparado a nivel de sus capas y funcionalidades que ofrecen, y

se ha definido un nivel de madurez para cada uno de ellos. De todo el análisis realizado, ha quedado claro que existe una gran cantidad de sistemas IoT que son desarrollados para diferentes tipos de aplicaciones, por ende, pueden hacer uso de diferentes tipos de dispositivos, generando así varios desafíos al trabajar con dispositivos heterogéneos. Se definirán tres principales desafíos: seguridad, escalabilidad y estandarización.

3.1.2.1 Seguridad

Los sistemas IoT pueden estar formados por dispositivos de diferentes tipos, los cuales en su mayoría cuentan con capacidades limitadas tanto en hardware como software, esto se debe a la alta competitividad entre los proveedores, los cuales en el afán de incrementar las ventas no invierten en la seguridad de los dispositivos y lanzan al mercado un dispositivo con varias vulnerabilidades de seguridad, ejemplos de estos dispositivos son monitores de casa, electrodomésticos, radios, drones, entre otros.

Estos dispositivos se encargan de la recolección de datos, y debido a sus limitaciones, los algoritmos de seguridad empleados en los sistemas IoT no suelen ser complejos, creando brechas de seguridad, por ejemplo, atacantes mal intencionados realizan escaneos de una gran cantidad de direcciones IP, en los resultados se suele obtener un detalle mínimo de los dispositivos conectados en cada red, como el nombre del fabricante; el atacante gracias a esta información infiere que se trata de un dispositivo IoT cotidiano y procede a intentar autenticarse con usuarios y claves por defecto manejados por los fabricantes, o realizar un ataque de diccionario para intentar descifrar la contraseña que le otorgue acceso al dispositivo IoT. De este modo los datos recolectados por los dispositivos IoT se pueden ver expuestos a modificación y extracción no autorizadas, incumpliendo así objetivos de la seguridad como integridad y confidencialidad, lo que afecta directamente a la privacidad del usuario y al funcionamiento de la aplicación del sistema IoT.

Los dispositivos IoT y los sistemas que los manejan deben contar con mecanismos de seguridad que protejan la privacidad del usuario. La autenticación en los dispositivos IoT puede manejarse mediante una autenticación de doble factor, que permita al usuario recibir en su dispositivo celular alertas de ingreso al dispositivo IoT. Otra medida de seguridad que puede aplicarse en el sistema IoT es la de implementar Blockchain, pues esta medida ayudaría a controlar que cada interacción en el sistema sea válida; sin embargo, se debe tomar en cuenta que la capacidad computacional en todo el sistema aumenta significativamente.

3.1.2.2 Escalabilidad

Con el crecimiento de los dispositivos conectados a Internet, los desarrolladores de sistemas IoT pueden optar por integrar éstos a los sistemas existentes. Sin embargo, cada nuevo dispositivo, de acuerdo con su fabricante únicamente admite el uso de ciertas tecnologías, por lo que el acoplar este nuevo dispositivo IoT a un sistema ya existente implica verificar que el dispositivo sea compatible con las tecnologías manejadas en el sistema.

El hecho antes mencionado, provoca que cada desarrollador se mantenga atado a una casa fabricante que le ofrezca dispositivos que cumplan con los parámetros utilizados en su sistema, esta acción limitaría que los dispositivos de diferentes fabricantes puedan trabajar entre sí, impidiendo así la posibilidad de escalar el sistema IoT. El hecho de que un dispositivo IoT no cumpla con los requisitos del sistema genera problemas al momento de acoplarlo, pues los datos generados poseen diferentes formatos y la tecnología de transmisión de datos que emplee el dispositivo puede tener diferentes tipos de solicitud o publicación de datos de las que maneje el sistema, o inclusive se pueden generar incompatibilidades al trabajar con diferentes protocolos de comunicación.

Los problemas de escalabilidad en sistemas IoT se podrían solucionar mediante la inclusión de un Gateway, el cual soporte múltiples interfaces y realice la conversión de protocolos usados en los dispositivos IoT al protocolo manejado por el sistema. También se debería considerar el manejar una capa de Middleware en donde se tenga la capacidad computacional necesaria convertir el formato de todos los datos recolectados en un único formato estandarizado por el sistema IoT.

3.1.2.3 Estandarización

Este es uno de los principales desafíos presentes al momento de desplegar sistemas IoT. Los desarrolladores de estos sistemas en función de la aplicación que busquen implementar usarán la arquitectura que cumpla con sus requerimientos, o incluso estos pueden llegar a desarrollar una por sí mismos y aplicarla. La falta de un estándar común y sobre todo aceptado en el campo de IoT provoca que los hechos antes mencionados sucedan.

La falta de estandarización en los sistemas IoT también provoca que la interacción de varios sistemas IoT no sea posible, pues cada proyecto al hacer uso de una diferente arquitectura provoca que no exista compatibilidad entre estos y por ende la integración de los sistemas no sea posible. Los esfuerzos por estandarizar las arquitecturas

implementadas en sistemas IoT han ido incrementando, pues organismos como la ITU han desarrollado recomendaciones para trabajar con arquitecturas de sistemas IoT tal como la recomendación ITU-T Y. 2060/4000 o se han realizado proyectos tal como FIWARE, la cual es una plataforma para el desarrollo de sistemas IoT; sin embargo, es necesario que estos esfuerzos se realicen en conjunto, generando una arquitectura estandarizada común, o se llegue a un consenso entre entes normalizadores para definir una arquitectura como estándar, la cual debe ser socializada con los desarrolladores de sistemas IoT.

3.2 CONCLUSIONES

En el presente trabajo de integración curricular se ha podido observar la existencia de una amplia gama de arquitecturas para sistemas IoT, éstas en un inicio fueron realmente simples, llegando a contar únicamente con 3 capas, limitando sus funcionalidades a la recolección y transmisión de los datos para su uso en una aplicación IoT. Con el avance de la tecnología, las arquitecturas para sistemas IoT incrementaron su complejidad, incorporando capas que expandan las funcionalidades del sistema, tales como, procesamiento de datos, administración, integración de datos y dispositivos (Gateway), funcionalidades de la nube, seguridad, entre otras, que de acuerdo con el desarrollador serán o no incorporadas. De modo que, mediante la línea de tiempo generada en la Figura 2.28 se ha evidenciado una gran evolución de las arquitecturas para sistemas IoT en los últimos 5 años.

Otro punto importante en el presente trabajo es el de las arquitecturas IoT estandarizadas, éstas son realmente son escasas y en su gran mayoría cada desarrollador opta por generar su propia arquitectura IoT. Este hecho refleja la falta de estandarización existente en los sistemas IoT, pues entre las arquitecturas revisadas en este trabajo no se encontró ninguna arquitectura que siga un estándar, éstas únicamente formaban parte de propuestas realizadas por los autores, creadas bajo su propio criterio y sin una base estandarizada.

De las arquitecturas y modelos de referencia para sistemas IoT desarrollados en los últimos 5 años, se ha podido observar que estos sistemas se encuentran desplegados en su mayoría sobre áreas de aplicación como Cuidado de la Salud, Transporte y Ciudad Inteligente. El proyecto IoT-A finalizado en el año 2013 comparte las mismas tres áreas de aplicación en la mayoría de sus proyectos realizados, esto permite dejar en evidencia que desde el año 2013 hasta el periodo comprendido en los últimos 5 años se ha mantenido una tendencia sobre las áreas de aplicación más desarrolladas en los sistemas IoT.

El nivel de madurez de las aplicaciones y modelos de referencia para sistemas IoT, es otro punto importante en el presente trabajo, pues se pudo observar que en su mayoría todas

las arquitecturas poseen un nivel de madurez bajo, ya que éstas no han sido tomadas como referencia por otros autores para mejorar o implementar dichas arquitecturas, quedando planteadas únicamente a modo de propuesta. Por otra parte, entre los proyectos de desarrollo y modelos de referencia para sistemas IoT analizados, se pudo observar que únicamente 3 poseen un nivel de madurez alto (IoT-A, FIWARE e ITU-T), y de estos se puede desatacar al proyecto FIWARE, pues se mantiene vigente y cuenta tanto con una estructura organizacional definida y con el apoyo de varios desarrolladores de sistemas IoT.

Tras observar la gran cantidad existente de arquitecturas para sistemas IoT, se pudo notar que la seguridad es un aspecto que en un inicio no fue tomado en cuenta, y con el avance de la tecnología pasó a ser esencial en todo tipo de sistema IoT desarrollado. Los sistemas IoT en los últimos años han incorporado Blockchain como una medida para agregar un nivel de seguridad, pues ésta permite asegurar cada interacción realizada en el sistema, ya sea desde la autenticación de un dispositivo IoT o hasta la manipulación de datos en el sistema, de modo que se mira a la seguridad como un desafío presente en el desarrollo de sistemas IoT y a Blockchain como la tendencia para agregar seguridad en los sistemas IoT.

Definir el nivel de madurez de una arquitectura IoT depende del punto de vista de cada autor, en el presente trabajo se generó un mecanismo de asignación de puntos, el cual permitió relacionar a cada arquitectura IoT con uno de los tres niveles de madurez definidos (Alto, Medio y Bajo). De modo que, se pudo observar que las arquitecturas IoT desarrolladas en los últimos 5 años no siguen un estándar común, por lo que la necesidad de poseer un arquitectura estandarizada y aceptada por los desarrolladores de sistemas IoT se convierte en un problema crítico a ser resuelto.

Las arquitecturas IoT desarrolladas en los últimos 5 años son numerosas y poseen una estructura de capas variada, así como distintas funcionalidades. Esto provoca que la interoperabilidad entre sistemas IoT sea compleja. Los esfuerzos para obtener una arquitectura estandarizada común deben aumentar y ser coordinados, pues diferentes organizaciones desarrollan su propio proyecto de estandarización de manera aislada, provocando una mayor división en el desarrollo aplicaciones IoT. Los sistemas IoT poseen un gran potencial de desarrollo a futuro, pero este solo será factible, siempre y cuando se desarrolle una arquitectura estándar común que facilite la interoperabilidad de los sistemas IoT, de manera que, las aplicaciones IoT mejoren los servicios que prestan a los usuarios finales.

3.3 RECOMENDACIONES

Para realizar un trabajo exploratorio de este tipo es importante filtrar las publicaciones a ser revisadas, esto se puede lograr ingresando palabras clave en los motores de búsqueda, las palabras usadas en el presente trabajo fueron: “Sistemas”, “IoT”, “Arquitecturas” y “Modelos de referencia”, y combinaciones de éstas, pues esto permitirá obtener publicaciones valiosas que aporten al estudio.

La cantidad de publicaciones manejadas en este tipo de trabajos suele ser extensa, por este motivo es importante manejar tablas en donde se resuman aspectos importantes de cada publicación, en este caso una tabla diseñada para arquitecturas IoT puede registrar el nombre de la arquitectura, la cantidad de capas (y sus nombres), el área de aplicación y el año de publicación de cada arquitectura IoT. Esta tabla en función de lo que se busque analizar ayudará a la clasificación y depuración de la información.

El presente trabajo puede dar pie a realizar un trabajo exploratorio centrado únicamente en arquitecturas y modelos de referencia para Sistemas IoT que integren Blockchain como mecanismo de autenticación de dispositivos IoT, pues se ha observado que esta clase de arquitecturas poseen un gran potencial, que ha sido explotado en los últimos años. El trabajo podría incluir aspectos de seguridad en sistemas IoT que no son cubiertos por Blockchain, con el fin de definir qué tan seguro es utilizar Blockchain como mecanismo de seguridad en los sistemas IoT.

Por otra parte, se ha observado que la plataforma de desarrollo para Sistemas IoT “FIWARE” posee un gran potencial y respaldo por parte del proyecto FIWARE Foundation, se podría realizar una investigación sobre este proyecto, con el fin de evidenciar sus ventajas y desventajas; y analizar si es posible que FIWARE se convierta en el estándar común para sistemas IoT.

4 REFERENCIAS BIBLIOGRÁFICAS

[1] J. Y. Khan, “Introduction to IoT Systems,” *Internet of Things (IoT)*, no. January, 2019, doi: 10.1201/9780429399084-1.

[2] K. Patel and Keyur, “Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges.,” *Univ. Iberoam. Ciudad México*, no. May, p. 6123,6131, 2016, [Online]. Available: http://www.opjstamnar.com/download/Worksheet/Day-110/IP-XI.pdf.

[3] A. Čolaković and M. Hadžialić, “Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues,” *Comput. Networks*, vol. 144, 2018, doi: 10.1016/j.comnet.2018.07.017.

[4] J. Clark, “What is the Internet of Things (IoT)?,” *IBM Business Operations Blog*, 2016. https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/ (accessed Nov. 21, 2021).

[5] Gartner, “Internet Of Things (iot),” *Gartner Glossary*. https://www.gartner.com/en/information-technology/glossary/internet-of-things.

[6] Oxford, “internet of things,” *Oxford Learners Dictionaries*. https://www.oxfordlearnersdictionaries.com/definition/english/internet-of-things.

[7] S. L. S. Maita, “NEW MODELS OF RELIABILITY IN THE NEW GENERATION OF INTERNET OF THINGS,” University of Coimbra, 2019.

[8] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, “Internet of Things applications: A systematic review,” *Comput. Networks*, vol. 148, pp. 241–261, 2019, doi: 10.1016/j.comnet.2018.12.008.

[9] N. Sharma, M. Shamkuwar, and I. Singh, “The history, present and future with iot,” *Intell. Syst. Ref. Libr.*, vol. 154, pp. 27–51, 2019, doi: 10.1007/978-3-030-04203-5_3.

[10] J. Manyika, M. Chui, and J. Bughin, “Disruptive technologies: Advances that will transform life, business, and the global economy,” *McKinsey Glob. …*, no. May, p. 163, 2013, [Online]. Available: http://www.mckinsey.com/insights/business_technology/disruptive_technologies%5Cnhttp://www.chrysalixevc.com/pdfs/mckinsey_may2013.pdf.

[11] R. Tiwari, N. Sharma, I. Kaushik, A. Tiwari, and B. Bhushan, “Evolution of IoT Data Analytics using Deep Learning,” *Proc. - 2019 Int. Conf. Comput. Commun. Intell.*

Syst. ICCCIS 2019, vol. 2019-Janua, pp. 418–423, 2019, doi: 10.1109/ICCCIS48478.2019.8974481.

[12] R. Lohiya and A. Thakkar, “Application Domains, Evaluation Data Sets, and Research Challenges of IoT: A Systematic Review,” *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8774–8798, 2021, doi: 10.1109/JIOT.2020.3048439.

[13] S. Kim and S. Kim, “User preference for an IoT healthcare application for lifestyle disease management,” *Telecomm. Policy*, vol. 42, no. 4, 2018, doi: 10.1016/j.telpol.2017.03.006.

[14] R. A. G. Salazar, “Sistema de telemedicina con monitoreo de signos vitales basado en Iot en un ambiente Smart TV,” 2021, [Online]. Available: http://repositorio.uta.edu.ec/handle/123456789/32315.

[15] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, “A review of machine learning and IoT in smart transportation,” *Futur. Internet*, vol. 11, no. 4, pp. 1–23, 2019, doi: 10.3390/FI11040094.

[16] E. Borgia, “The internet of things vision: Key features, applications and open issues,” *Comput. Commun.*, vol. 54, pp. 1–31, 2014, doi: 10.1016/j.comcom.2014.09.008.

[17] T. Malche and P. Maheshwary, “Internet of Things (IoT) for building Smart Home System,” pp. 65–70, 2017.

[18] M. Alvarez-Campana, G. López, E. Vázquez, V. A. Villagrá, and J. Berrocal, “Smart CEI moncloa: An iot-based platform for people flow and environmental monitoring on a Smart University Campus,” *Sensors (Switzerland)*, vol. 17, no. 12, 2017, doi: 10.3390/s17122856.

[19] G. Mois, S. Folea, and T. Sanislav, “Analysis of Three IoT-Based Wireless Sensors for Environmental Monitoring,” *IEEE Trans. Instrum. Meas.*, vol. 66, no. 8, pp. 2056–2064, 2017, doi: 10.1109/TIM.2017.2677619.

[20] M. R. M. Kassim, “IoT Applications in Smart Agriculture: Issues and Challenges,” *2020 IEEE Conf. Open Syst. ICOS 2020*, pp. 19–24, 2020, doi: 10.1109/ICOS50156.2020.9293672.

[21] J. Xu *et al.*, “Design of Smart Unstaffed Retail Shop Based on IoT and Artificial Intelligence,” *IEEE Access*, vol. 8, pp. 147728–147737, 2020, doi: 10.1109/ACCESS.2020.3014047.

[22] J. del Val Roman, “Industria 4.0. La Transformación Digital de la Industria Española,” *Coddiinforme*, p. 120, 2012, [Online]. Available: http://coddii.org/wp-content/uploads/2016/10/Informe-CODDII-Industria-4.0.pdf.

[23] A. Calatayud and R. Katz, “Cadena de suministro 4.0: Mejores prácticas internacionales y hoja de ruta para América Latina,” *Cadena Suminist. 4.0 Mejor. prácticas Int. y hoja ruta para América Lat.*, 2019, doi: 10.18235/0001956.

[24] F. Firouzi, K. Chakrabarty, and S. Nassif, *Intelligent Internet of Things: From Device to Fog and Cloud*. Springer US, 2020.

[25] K. Chopra, K. Gupta, and A. Lambora, “Future Internet: The Internet of Things-A Literature Review,” *Proc. Int. Conf. Mach. Learn. Big Data, Cloud Parallel Comput. Trends, Prespectives Prospect. Com. 2019*, pp. 135–139, 2019, doi: 10.1109/COMITCon.2019.8862269.

[26] S. A. Goswami, B. P. Padhya, and K. D. Patel, “Internet of Things: Applications, Challenges and Research Issues,” *Proc. 3rd Int. Conf. I-SMAC IoT Soc. Mobile, Anal. Cloud, I-SMAC 2019*, pp. 47–50, 2019, doi: 10.1109/I-SMAC47947.2019.9032474.

[27] Kanban, “¿Por qué utilizar la metodología Kanban?” https://kanbantool.com/es/metodologia-kanban.

[28] S. N. Swamy and S. R. Kota, “An empirical study on system level aspects of Internet of Things (IoT),” *IEEE Access*, vol. 8, pp. 188082–188134, 2020, doi: 10.1109/ACCESS.2020.3029847.

[29] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, “A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling,” *ACM Comput. Surv.*, vol. 53, no. 1, 2020, doi: 10.1145/3372136.

[30] S. Wang, Y. Hou, F. Gao, and S. Ma, “A novel clock synchronization architecture for IoT access system,” *2016 2nd IEEE Int. Conf. Comput. Commun. ICCC 2016 - Proc.*, pp. 1456–1459, 2017, doi: 10.1109/CompComm.2016.7924944.

[31] M. Kolhar, F. Al-Turjman, A. Alameen, and M. M. Abualhaj, “A three layered decentralized IoT biometric architecture for city lockdown during covid-19 outbreak,” *IEEE Access*, vol. 8, pp. 163608–163617, 2020, doi: 10.1109/ACCESS.2020.3021983.

[32] S. Y. Shapsough and I. A. Zualkernan, “A Generic IoT Architecture for Ubiquitous Context-Aware Learning,” *IEEE Trans. Learn. Technol.*, vol. 13, no. 3, pp. 449–464,

2020, doi: 10.1109/TLT.2020.3007708.

[33] I. Miladinovic and S. Schefer-Wenzl, “NFV enabled IoT architecture for an operating room environment,” *IEEE World Forum Internet Things, WF-IoT 2018 - Proc.*, vol. 2018-Janua, pp. 98–102, 2018, doi: 10.1109/WF-IoT.2018.8355128.

[34] J. Sun, S. Li, Q. Zhou, Y. Su, and Y. Fu, “Exploration and Research of Internet of Things Architecture Based on Fractal Theory,” *Proc. 2018 5th IEEE Int. Conf. Cloud Comput. Intell. Syst. CCIS 2018*, pp. 187–192, 2019, doi: 10.1109/CCIS.2018.8691200.

[35] Y. Li, F. Björck, and H. Xue, “IoT architecture enabling dynamic security policies,” *ACM Int. Conf. Proceeding Ser.*, pp. 50–54, 2016, doi: 10.1145/3026724.3026736.

[36] M. Boujrad, S. Lazaar, and M. Hassine, “Performance Assessment of Open Source IDS for improving IoT Architecture Security implemented on WBANs,” *PervasiveHealth Pervasive Comput. Technol. Healthc.*, 2020, doi: 10.1145/3386723.3387892.

[37] D. Tomtsis, S. Kontogiannis, G. Kokkonis, and N. Zinas, “IoT architecture for monitoring wine fermentation process of Debina variety semi-sparkling wine,” *ACM Int. Conf. Proceeding Ser.*, vol. 25-27-Sept, pp. 42–47, 2016, doi: 10.1145/2984393.2984398.

[38] M. A. A. Da Cruz, J. J. P. C. Rodrigues, J. Al-Muhtadi, V. V. Korotaev, and V. H. C. De Albuquerque, “A Reference Model for Internet of Things Middleware,” *IEEE Internet Things J.*, vol. 5, no. 2, pp. 871–883, 2018, doi: 10.1109/JIOT.2018.2796561.

[39] T. Shaikh, S. Ismail, and J. D. Stevens, “Aura Minora: A user centric IOT architecture for Smart City,” *ACM Int. Conf. Proceeding Ser.*, 2016, doi: 10.1145/3010089.3016028.

[40] N. M. Kumar and P. K. Mallick, “The Internet of Things: Insights into the building blocks, component interactions, and architecture layers,” *Procedia Comput. Sci.*, vol. 132, pp. 109–117, 2018, doi: 10.1016/j.procs.2018.05.170.

[41] H. Rahimi, A. Zibaeenejad, P. Rajabzadeh, and A. A. Safavi, “On the security of the 5G-IoT architecture,” *ACM Int. Conf. Proceeding Ser.*, 2018, doi: 10.1145/3269961.3269968.

[42] M. De Sanctis, H. Muccini, and K. Vaidhyanathan, “Data-driven Adaptation in

Microservice-based IoT Architectures," *Proc. - 2020 IEEE Int. Conf. Softw. Archit. Companion, ICSA-C 2020*, pp. 59–62, 2020, doi: 10.1109/ICSA-C50368.2020.00019.

[43] G. Misra, V. Kumar, A. Agarwal, and K. Agarwal, "Internet of Things (IoT) – A Technological Analysis and Survey on Vision, Concepts, Challenges, Innovation Directions, Technologies, and Applications (*An Upcoming or Future Generation Computer Communication System Technology*)," *Am. J. Electr. Electron. Eng. Vol. 4, 2016, Pages 23-32*, vol. 4, no. 1, pp. 23–32, 2016, doi: 10.12691/ajeee-4-1-4.

[44] A. M. Shaaban, A. Baith Mohamed, C. Schmittner, G. Quirchmayr, T. Gruber, and E. Schikuta, "CloudWoT - A reference model for knowledge-based IoT solutions," *ACM Int. Conf. Proceeding Ser.*, pp. 272–281, 2018, doi: 10.1145/3282373.3282400.

[45] C. De Napoli *et al.*, "IoT-HC: a novel IoT architecture for the hybrid cloud," *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*, vol. 2019-July, pp. 1–6, 2019, doi: 10.1109/ICCCN.2019.8847093.

[46] J. Ren, H. Guo, C. Xu, and Y. Zhang, "Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing," *IEEE Netw.*, vol. 31, no. 5, pp. 96–105, 2017, doi: 10.1109/MNET.2017.1700030.

[47] IEEE, "IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management," *IEEE Std 2144.1-2020*, pp. 1–20, 2021, [Online]. Available: https://ieeexplore-ieee-org.ezproxy.ugm.ac.id/document/9329260/metrics#metrics.

[48] Q. Le-Dang and T. Le-Ngoc, "Scalable Blockchain-based Architecture for Massive IoT Reconfiguration," *2019 IEEE Can. Conf. Electr. Comput. Eng. CCECE 2019*, pp. 1–4, 2019, doi: 10.1109/CCECE.2019.8861858.

[49] A. He, J. Shen, Y. Wang, and L. Liu, "Research on the Fusion Model Reference Architecture of Sensed Information of Human Body for Medical and Healthcare IoT," *Proc. - 2018 17th Int. Symp. Distrib. Comput. Appl. Bus. Eng. Sci. DCABES 2018*, pp. 162–164, 2018, doi: 10.1109/DCABES.2018.00049.

[50] FIWARE Foundation, "FIWARE Project." https://www.fiware.org/foundation/.

[51] F. Foundation, "5.2: FIWARE Go-to-market strategy Y2," pp. 1–39, 2019.

[52] F. Cirillo, G. Solmaz, E. L. Berz, M. Bauer, B. Cheng, and E. Kovacs, "A Standard-Based Open Source IoT Platform: FIWARE," *IEEE Internet Things Mag.*, vol. 2, no. 3, pp. 12–18, 2020, doi: 10.1109/iotm.0001.1800022.

[53] V. C. Pham, Y. Makino, and Y. Tan, “A FIWARE IoT Agent for ECHONET Lite Protocol,” *2020 IEEE 9th Glob. Conf. Consum. Electron. GCCE 2020*, pp. 235–239, 2020, doi: 10.1109/GCCE50665.2020.9291983.

[54] Lighthouse Project IoT-A, “IoT-A Project,” 2013. https://www.iot-a.eu/.

[55] D. Aksu and M. A. Aydin, “A Survey of IoT Architectural Reference Models,” *16th Int. Multi-Conference Syst. Signals Devices, SSD 2019*, pp. 413–417, 2019, doi: 10.1109/SSD.2019.8893170.

[56] ITU-T, “Rec. Y.2060/4000 Overview of the Internet of things,” *J. Adv. Res. Dyn. Control Syst.*, vol. 10, no. 9, pp. 659–665, 2012.

[57] ITU-T SG 20, “Rec. Y.4474 Functional architecture for Internet of things services based on visible light communication,” 2020.

[58] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[59] L. González, O. Sofía, D. Laguía, E. Gesto, and K. Hallar, “Internet del Futuro – Estudio de tecnologías IoT,” *Inf. Científicos Técnicos - UNPA*, vol. 12, no. 3, pp. 105–137, 2020, doi: 10.22305/ict-unpa.v12.n3.744.

[60] S. Wang, Y. Hou, F. Gao, and X. Ji, “A novel IoT access architecture for vehicle monitoring system,” *2016 IEEE 3rd World Forum Internet Things, WF-IoT 2016*, pp. 639–642, 2017, doi: 10.1109/WF-IoT.2016.7845396.

[61] A. Salinas, “Internet of Things Architecture Project Deliverable D6 . 1 - Requirements List,” *Architecture*, no. 257251, 2013.

[62] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[63] Y. Bo and H. Guangwen, “Supply chain information transmission based on RFID and internet of things,” *2009 Second ISECS Int. Colloq. Comput. Commun. Control. Manag. CCCM 2009*, vol. 4, pp. 166–169, 2009, doi: 10.1109/CCCM.2009.5267755.

[64] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future internet: The internet of things architecture, possible applications and key challenges,” *Proc. - 10th Int. Conf. Front.*

Inf. Technol. FIT 2012, pp. 257–260, 2012, doi: 10.1109/FIT.2012.53.

[65] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, “Study and application on the architecture and key technologies for IOT,” *2011 Int. Conf. Multimed. Technol. ICMT 2011*, pp. 747–751, 2011, doi: 10.1109/ICMT.2011.6002149.

[66] R. N. Gore, N. Elizabeth, D. Dzung, and S. Ashok, “Towards Robust Synchronization in IoT Networks,” *2019 11th Int. Conf. Commun. Syst. Networks, COMSNETS 2019*, vol. 2061, pp. 678–683, 2019, doi: 10.1109/COMSNETS.2019.8711343.

[67] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, “Biometrics for internet-of-things security: A review,” *Sensors*, vol. 21, no. 18, pp. 1–26, 2021, doi: 10.3390/s21186163.

[68] A. Rahman *et al.*, “SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic,” *Cluster Comput.*, vol. 4, 2021, doi: 10.1007/s10586-021-03367-4.

[69] Y. E. Oktian, E. N. Witanto, and S.-G. Lee, “A Conceptual Architecture in Decentralizing Computing, Storage, and Networking Aspect of IoT Infrastructure,” *IoT*, vol. 2, no. 2, pp. 205–221, 2021, doi: 10.3390/iot2020011.

[70] K. A. Demir, “Smart education framework,” *Smart Learn. Environ.*, vol. 8, no. 1, 2021, doi: 10.1186/s40561-021-00170-x.

[71] M. Krichen *et al.*, “A formal testing model for operating room control system using internet of things,” *Comput. Mater. Contin.*, vol. 66, no. 3, pp. 2997–3011, 2021, doi: 10.32604/cmc.2021.014090.

[72] C. Ramos, L. Nobrega, K. Baras, and L. Gomes, “Experimental NFT hydroponics system with lower energy consumption,” *Proc. 2019 5th Exp. Int. Conf. exp.at 2019*, vol. 500, pp. 102–106, 2019, doi: 10.1109/EXPAT.2019.8876479.

[73] K. Bajaj, B. Sharma, and R. Singh, “Implementation analysis of IoT-based offloading frameworks on cloud/edge computing for sensor generated big data,” *Complex Intell. Syst.*, no. 0123456789, 2021, doi: 10.1007/s40747-021-00434-6.

[74] W. D. Fang, W. He, W. Chen, L. H. Shan, and F. Y. Ma, “Research on the application-driven architecture in internet of things,” *Front. Artif. Intell. Appl.*, vol. 293, pp. 458–465, 2016, doi: 10.3233/978-1-61499-722-1-458.

[75] E. Cañete, J. Chen, C. Martín, and B. Rubio, “Smart winery: A real-time monitoring

system for structural health and ullage in fino style wine casks," *Sensors (Switzerland)*, vol. 18, no. 3, pp. 1–15, 2018, doi: 10.3390/s18030803.

[76] A. Cravero, D. Lagos, and R. Espinosa, "08408444," *IEEE Lat. Am. Trans.*, vol. 16, no. 5, pp. 1476–1484, 2018.

[77] S. Nižetić, N. Djilali, A. Papadopoulos, and J. J. P. C. Rodrigues, "Smart technologies for promotion of energy efficiency, utilization of sustainable resources and waste management," *J. Clean. Prod.*, vol. 231, pp. 565–591, 2019, doi: 10.1016/j.jclepro.2019.04.397.

[78] G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya, and B. Balusamy, "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," *Neural Comput. Appl.*, vol. 32, no. 3, pp. 639–647, 2020, doi: 10.1007/s00521-018-3915-1.

[79] M. A. A. da Cruz, J. J. P. C. Rodrigues, A. K. Sangaiah, J. Al-Muhtadi, and V. Korotaev, "Performance evaluation of IoT middleware," *J. Netw. Comput. Appl.*, vol. 109, pp. 53–65, 2018, doi: 10.1016/j.jnca.2018.02.013.

[80] M. G. Alvarez, J. Morales, and M. J. Kraak, "Integration and exploitation of sensor data in smart cities through event-driven applications," *Sensors (Switzerland)*, vol. 19, no. 6, 2019, doi: 10.3390/s19061372.

[81] S. Yerraboina, N. M. Kumar, K. S. Parimala, and N. Aruna Jyothi, "Monitoring the smart garbage bin filling status: An iot application towards waste management," *Int. J. Civ. Eng. Technol.*, vol. 9, no. 6, pp. 373–381, 2018.

[82] N. Gupta, S. Sharma, P. K. Juneja, and U. Garg, "SDNFV 5G-IoT: A Framework for the Next Generation 5G enabled IoT," *Proc. - 2020 Int. Conf. Adv. Comput. Commun. Mater. ICACCM 2020*, pp. 289–294, 2020, doi: 10.1109/ICACCM50413.2020.9213047.

[83] V. Vallois, F. Guenane, and A. Mehaoua, "Reference architectures for security-by-design iot: Comparative study," *2019 5th Int. Conf. Mob. Secur. Serv. MOBISECSERV 2019*, pp. 1–6, 2019, doi: 10.1109/MOBISECSERV.2019.8686650.

[84] H. Muccini, K. Vaidhyanathan, and M. De Sanctis, *A User-driven Adaptation Approach for Microservice-based IoT Applications; A User-driven Adaptation Approach for Microservice-based IoT Applications*, vol. 1, no. 1. Association for Computing Machinery, 2021.

[85] M. Parvizimosaed, M. Noei, M. Yalpanian, and J. Bahrami, “A Containerized Integrated Fast IoT Platform for Low Energy Power Management,” *2021 7th Int. Conf. Web Res. ICWR 2021*, pp. 318–322, 2021, doi: 10.1109/ICWR51868.2021.9443141.

[86] H. Bangui, S. Rakrak, S. Raghay, and B. Buhnova, “Moving to the edge-cloud-of-things: Recent advances and future research directions,” *Electron.*, vol. 7, no. 11, 2018, doi: 10.3390/electronics7110309.

[87] M. A. Alam and A. Saiyeda, “A Cloud Based Solution for Smart Education,” *Int. J. Smart Educ. Urban Soc.*, vol. 11, no. 2, pp. 28–37, 2020, doi: 10.4018/ijseus.2020040103.

[88] A. M. Shaaban, T. Gruber, and C. Schmittner, “Ontology-based security tool for critical cyber-physical systems,” *PervasiveHealth Pervasive Comput. Technol. Healthc.*, vol. B, pp. 7–10, 2019, doi: 10.1145/3307630.3342397.

[89] H. Li, K. Ota, and M. Dong, “Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing,” *IEEE Netw.*, vol. 32, no. 1, pp. 96–101, 2018, doi: 10.1109/MNET.2018.1700202.

[90] K. Wang, H. Yin, W. Quan, and G. Min, “Enabling Collaborative Edge Computing for Software Defined Vehicular Networks,” *IEEE Netw.*, vol. 32, no. 5, pp. 112–117, 2018, doi: 10.1109/MNET.2018.1700364.

[91] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, “Survey on Multi-Access Edge Computing for Internet of Things Realization,” *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 2961–2991, 2018, doi: 10.1109/COMST.2018.2849509.

[92] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, “A Survey on Blockchain Interoperability: Past, Present, and Future Trends,” *ACM Comput. Surv.*, vol. 54, no. 8, 2022, doi: 10.1145/3471140.

[93] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W. C. Hong, “A survey on decentralized consensus mechanisms for cyber physical systems,” *IEEE Access*, vol. 8, pp. 54371–54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

[94] S. Otoum, I. Al Ridhawi, and H. Mouftah, “A Federated Learning and Blockchain-enabled Sustainable Energy-Trade at the Edge: A Framework for Industry 4.0,” *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2022, doi: 10.1109/jiot.2022.3140430.

[95] I. Romashkova, M. Komarov, and A. Ometov, “Demystifying Blockchain Technology for Resource-Constrained IoT Devices: Parameters, Challenges and Future

Perspective," *IEEE Access*, vol. 9, pp. 129264–129277, 2021, doi: 10.1109/ACCESS.2021.3112228.

[96] S. Saxena, B. Bhushan, and M. A. Ahad, "Blockchain based solutions to secure IoT: Background, integration trends and a way forward," *J. Netw. Comput. Appl.*, vol. 181, no. September 2020, p. 103050, 2021, doi: 10.1016/j.jnca.2021.103050.

[97] S. Jusoh and S. Almajali, "A Systematic Review on Fusion Techniques and Approaches Used in Applications," *IEEE Access*, vol. 8, pp. 14424–14439, 2020, doi: 10.1109/ACCESS.2020.2966400.

[98] I. D. Sabukunze, D. B. Setyohadi, and M. Sulistyoningsih, "Designing An Iot Based Smart Monitoring and Emergency Alert System for Covid19 Patients," *2021 6th Int. Conf. Converg. Technol. I2CT 2021*, pp. 1–5, 2021, doi: 10.1109/I2CT51068.2021.9418078.

[99] ITU-T, "Rec. Y.4464 Framework of blockchain of things as decentralized service platform," pp. 1–23, 2020.

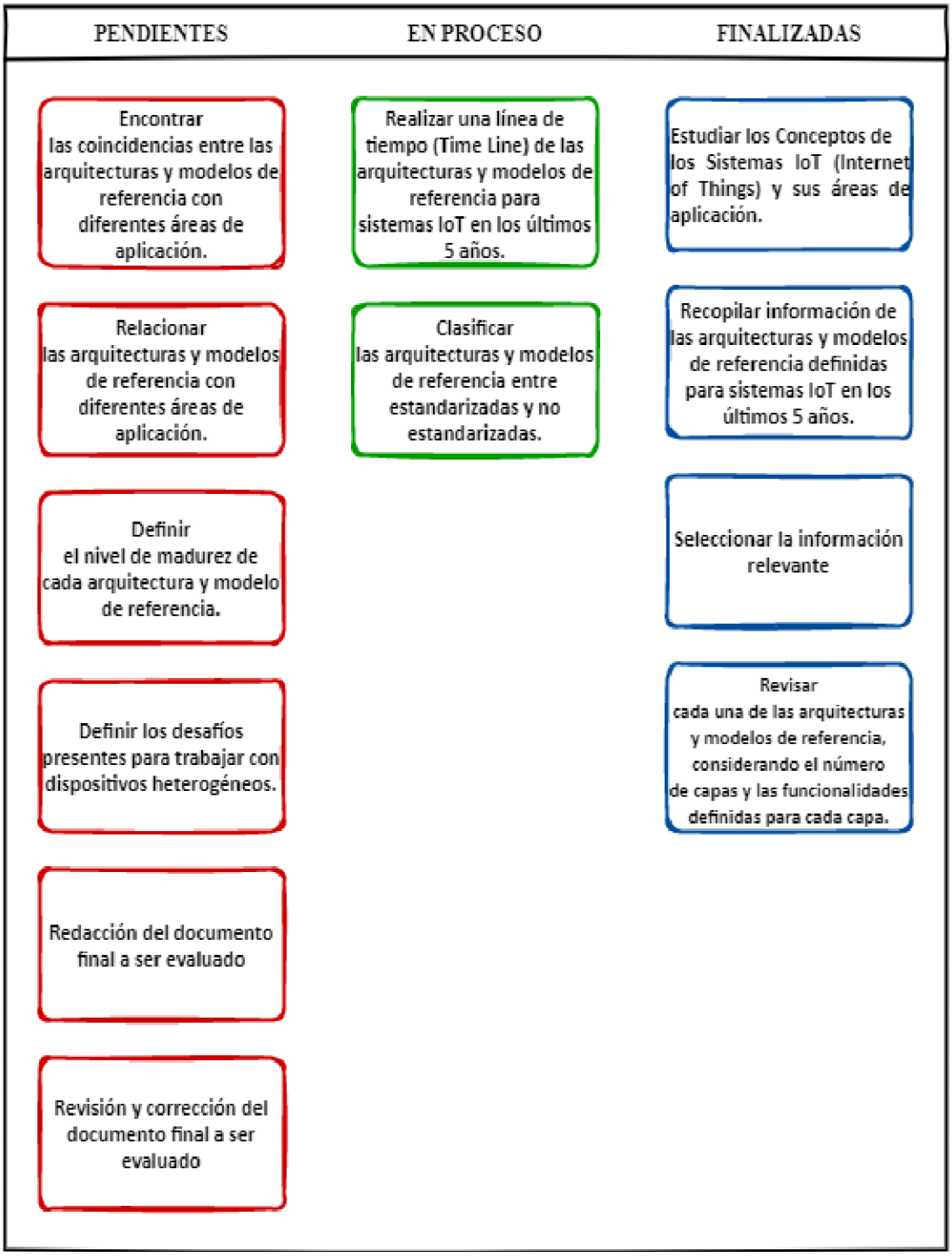
[100] ITU-T, "Rec. Y.4462 Requirements and functional architecture of open IoT identity correlation service," 2020.

5 ANEXOS

Anexo I. Tablero Kanban Simplificado (Semana 5)

Anexo II. Comparación de arquitecturas y modelos de referencia de Sistemas IoT

ANEXO I. Tablero Kanban Simplificado (Semana 5)



ANEXO II. Comparación de arquitecturas y modelos de referencia de Sistemas IoT

Clasificación	Referencia	N. Capas	Nombre de la Capa	Funcionalidades											
				Detección	Recolección	Integración	Comunicación	Almacenamiento	Preprocesamiento	Procesamiento	Seguridad	Calidad de Servicio	Administración	Apoyo en toma de decisiones	Provisión de Apps/Servicios
Arquitecturas de 3 Capas	[28]	3	Adquisición		✓										
			Mantenimiento					✓							
			Distribución				✓								
	[29]		Percepción	✓	✓										
			Transporte				✓								
			Aplicación												✓
	[30]		Dispositivo		✓										
			Borde				✓	✓		✓					
			Aplicación												✓
	[31]		Módulo de aprendizaje	✓	✓										
			Comunicaciones				✓								
			Aplicaciones de Front-end												✓
	[32]		Física	✓	✓										
			Red				✓								
			Aplicación												✓

ANEXO II. Comparación de arquitecturas y modelos de referencia de Sistemas IoT (Cont.)

Clasificación	Referencia	N. Capas	Nombre de la Capa	Funcionalidades											
				Detección	Recolección	Integración	Comunicación	Almacenamiento	Preprocesamiento	Procesamiento	Seguridad	Calidad de Servicio	Administración	Apoyo en toma de decisiones	Provisión de Apps/Servicios
Arquitecturas de 4 Capas	[33]	4	Sensores y Actuadores	✓	✓										
			Gateway IoT			✓									
			Red IP				✓								
			Centro de Datos					✓		✓			✓		✓
	[34]		Percepción		✓										
			Red				✓								
			Soporte						✓						
			Aplicación							✓					✓
	[35]		Dispositivo		✓										
			Red				✓								
			Computación								✓				
			Servicio								✓				✓
	[36]		Percepción		✓										
			Red				✓								
			Nube/Middleware					✓		✓					
			Aplicación												✓

ANEXO II. Comparación de arquitecturas y modelos de referencia de Sistemas IoT (Cont.)

Clasificación	Referencia	N. Capas	Nombre de la Capa	Funcionalidades											
				Detección	Recolección	Integración	Comunicación	Almacenamiento	Preprocesamiento	Procesamiento	Seguridad	Calidad de Servicio	Administración	Apoyo en toma de decisiones	Provisión de Apps/Servicios
Arquitecturas de 4 Capas	[37]	4	Sistema de Barril Inteligente	✓											
			Colector de datos		✓										
			Infraestructura de red inalámbrica				✓								
			Estación central					✓		✓			✓		✓
Arquitectura de 5 Capas	[29]	5	Detección	✓	✓										
			Red				✓								
			Middleware					✓		✓			✓		
			Aplicación							✓					✓
			Negocio											✓	
Arquitecturas de 6 Capas o Superior	[38]	6	Interoperabilidad			✓									
			Analítica y persistencia					✓		✓					
			Contexto							✓					
			Recursos y Eventos										✓		
			Interfaz gráfica de usuario										✓	✓	✓
			Seguridad								✓				

ANEXO II. Comparación de arquitecturas y modelos de referencia de Sistemas IoT (Cont.)

Clasificación	Referencia	N. Capas	Nombre de la Capa	Funcionalidades											
				Detección	Recolección	Integración	Comunicación	Almacenamiento	Preprocesamiento	Procesamiento	Seguridad	Calidad de Servicio	Administración	Apoyo en toma de decisiones	Provisión de Apps/Servicios
Arquitecturas de 6 Capas o Superior	[39]	6	Detección	✓	✓										
			Gateway			✓									
			Nube				✓								
			Servicio												✓
			Administración										✓		
			Plataforma												✓
	[40]	7	Entorno	✓											
			Hardware		✓	✓									
			Red						✓						
			Comunicación				✓								
			Servicios							✓					
			Soporte y gestión de Aplicación								✓		✓		
			Aplicación												✓

ANEXO II. Comparación de arquitecturas y modelos de referencia de Sistemas IoT (Cont.)

Clasificación	Referencia	N. Capas	Nombre de la Capa	Funcionalidades											
				Detección	Recolección	Integración	Comunicación	Almacenamiento	Preprocesamiento	Procesamiento	Seguridad	Calidad de Servicio	Administración	Apoyo en toma de decisiones	Provisión de Apps/Servicios
Arquitecturas de 6 Capas o Superior	[41]	8	Dispositivos físicos	✓	✓										
			Comunicación				✓								
			Computación de borde							✓					
			Almacenamiento de datos					✓							
			Administración de servicios				✓	✓		✓				✓	
			Aplicación												✓
			Colaboración y procesos												✓
			Seguridad								✓				
Arquitecturas Basadas en Servicios o Microservicios	[42]	3	Borde	✓	✓		✓					✓			
			Fog						✓	✓		✓			
			Nube					✓		✓			✓		✓
	[43]	5	Objetos	✓	✓										
			Abstracción de Objetos			✓				✓					
			Administración de servicios										✓		
			Composición de servicios												✓
			Aplicación												

ANEXO II. Comparación de arquitecturas y modelos de referencia de Sistemas IoT (Cont.)

Clasificación	Referencia	N. Capas	Nombre de la Capa	Funcionalidades											
				Detección	Recolección	Integración	Comunicación	Almacenamiento	Preprocesamiento	Procesamiento	Seguridad	Calidad de Servicio	Administración	Apoyo en toma de decisiones	Provisión de Apps/Servicios
Arquitecturas Basadas en la Nube	[44]	4	Campo	✓	✓						✓				
			Comunicación				✓				✓				
			Procesamiento de Datos					✓	✓	✓	✓		✓		
			Computación en la Nube							✓	✓				✓
	[45]	3	IoT	✓	✓										
			Borde				✓		✓						
			Nube					✓		✓					
	[46]	5	Usuario Final		✓										✓
			Servidor de Borde					✓		✓			✓		
			Red Central				✓								
			Nube					✓	✓						✓
			Administración e Interfaz										✓		✓

ANEXO II. Comparación de arquitecturas y modelos de referencia de Sistemas IoT (Cont.)

Clasificación	Referencia	N. Capas	Nombre de la Capa	Funcionalidades											
				Detección	Recolección	Integración	Comunicación	Almacenamiento	Preprocesamiento	Procesamiento	Seguridad	Calidad de Servicio	Administración	Apoyo en toma de decisiones	Provisión de Apps/Servicios
Uso de Blockchain	[29]	5	Física		✓										
			Red				✓								
			Blockchain				✓	✓			✓				
			Middleware								✓		✓		
			Aplicación												✓
	[47]	4	Transporte Seguro				✓				✓				
			Función					✓		✓	✓		✓		✓
			Servicio				✓			✓					
			Aplicación												✓
			Panel de Control y Administración										✓		
	[48]	3	Administradores										✓		
			Dispositivos IoT		✓										
			Red Blockchain								✓		✓		

ANEXO II. Comparación de arquitecturas y modelos de referencia de Sistemas IoT (Cont.)

Clasificación	Referencia	N. Capas	Nombre de la Capa	Funcionalidades											
				Detección	Recolección	Integración	Comunicación	Almacenamiento	Preprocesamiento	Procesamiento	Seguridad	Calidad de Servicio	Administración	Apoyo en toma de decisiones	Provisión de Apps/Servicios
Modelos de Referencia y Proyectos de Desarrollo para Sistemas IoT	[49]	6	Usuario												✓
			Control de detección	✓											
			Provisión de servicios							✓					
			Control de administración y operación										✓		
			Intercambio de recursos				✓								
			Objetivo		✓										
	FIWARE [50]	5	Broker IoT		✓										
			Descubrimiento de IoT										✓		
			Administración de dispositivos IoT										✓		
			Broker de contexto de datos										✓		✓
			Gateway IoT			✓	✓								

ANEXO II. Comparación de arquitecturas y modelos de referencia de Sistemas IoT (Cont.)

Clasificación	Referencia	N. Capas	Nombre de la Capa	Funcionalidades											
				Detección	Recolección	Integración	Comunicación	Almacenamiento	Preprocesamiento	Procesamiento	Seguridad	Calidad de Servicio	Administración	Apoyo en toma de decisiones	Provisión de Apps/Servicios
Modelos de Referencia y Proyectos de Desarrollo para Sistemas IoT	IoT-A [54]	9	Dispositivo												
			Comunicación				✓				✓	✓			
			Servicio IoT												✓
			Entidad Virtual				✓								
			Administración de procesos IoT										✓	✓	
			Organización de servicios												✓
			Aplicación												
			Seguridad								✓				
			Administración										✓		
	[55]	3	Detección	✓	✓										
			Red				✓								
			Aplicación												✓
	ITU-T [56]	4	Dispositivo	✓	✓	✓									
			Red				✓				✓				
			Soporte de servicio y aplicación					✓		✓					
			Aplicación												✓
			Capacidades de gestión										✓		
			Capacidades de seguridad								✓				