Internet of Things: State-of-the-art, Computing Paradigms and Reference Architectures

B. Mazon-Olivo, A. Pan

***Abstract*—The Internet of Things (IoT) makes it possible to connect objects or things to the internet, with the purpose of collecting data and controlling processes or machines remotely. IoT enables the physical world to be integrated into the digital world in order to optimize time, save costs and facilitate human labor. An IoT system comprises a rich ecosystem of elements that make up its value chain, which includes a computational and communication architecture or model, components and technologies. IoT has evolved rapidly, producing an exuberant scientific literature. This document presents the state of the art of IoT, with updated sources, that guides the reader, who is entering the world of IoT, to have a starting point for future research. In addition to the review of IoT architectures, components of the IoT ecosystem, computational paradigms and, security and governance aspects. Our main contribution is focused on the analysis of the Middleware layer in IoT architectures, oriented to the storage and processing of data.**

***Index Terms*— Internet of Things, IoT, ecosystem components, computing paradigms, reference architecture, reference model, data management, middleware.**

I. INTRODUCCIÓN

EL Internet de las cosas (IoT) nace de la necesidad de extender el acceso y control remoto a través de internet a dispositivos no tradicionales considerados como objetos o cosas [1]. IoT consiste en un sistema de dispositivos de computación interrelacionados (como autos, casas, animales, máquinas, robots, personas, etc.), que cuentan con identificadores únicos y que pueden recopilar, analizar e intercambiar datos sin intervención humana explícita [2], [3].

IoT es una tecnología fundamental en la innovación y desarrollo de muchos sectores; está causando impacto en la vida cotidiana, en el ámbito social, la industria y los negocios. IoT ofrece una gran oportunidad de mercado para fabricantes de dispositivos electrónicos, objetos inteligentes, sensores, actuadores y gateways; para proveedores de servicios de internet y computación en la nube; y, para desarrolladores de aplicaciones IoT de dominios específicos. IoT es una tecnología transversal para aplicación como ciudades inteligentes, hogares y edificios inteligentes, medicina y salud inteligente, industria inteligente, transporte y logística inteligente, agricultura de precisión, etc. [1], [3], [4].

El documento está organizado en secciones: en I. Introducción, se describen los trabajos relacionados y contribuciones. En la sección II, se realiza una discusión de Arquitecturas de referencia para aplicaciones IoT y paradigmas computacionales, y, se identifican los componentes del ecosistema IoT. Las siguientes tres secciones se centran en las principales capas que se encuentran habitualmente en las arquitecturas de referencia. En la sección III. Capa de Percepción, se aborda: Redes de sensores, transductores, sensores y actuadores, dispositivo IoT. En la sección IV. Capa de Red, se destaca: redes de comunicación para IoT, protocolos y Gateway para IoT. En la sección V. Capa Cloud, middleware y aplicaciones, se discute el problema de almacenamiento y procesamiento de datos en aplicaciones IoT. En la sección VI, se trata aspectos de seguridad y gobernanza en IoT. Finalmente, en la sección VII, se describen las conclusiones.

A. Trabajos relacionados y contribuciones

Hay muchos trabajos de revisiones y encuestas de IoT, algunos con enfoque genérico y otros específicos. En la Tabla I, se presenta una comparación con los trabajos de revisión y encuestas, organizado por tópicos de IoT.

TABLA I
TRABAJOS DE REVISIÓN Y ENCUESTAS DE IOT

Tópico IoT	Referencias
Definiciones de IoT	[4], [5], [6], [7], [8], [9], [10], [11]
Evolución de IoT	[6]
Retos / problemas abiertos	[4], [5], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17],
Arquitecturas de referencia de IoT, Plataformas IoT	[4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [16], [18], [19], [20], [21], [22], [23], [24], [25], [26]
Elementos o componentes de IoT	[5], [9], [10], [11], [15], [20]
Redes de sensores inalámbricas, objetos IoT, dispositivos IoT	[4], [5], [6], [8], [9], [11], [13], [15], [16], [18], [22], [23], [27], [28]
Redes de comunicación, tecnologías, protocolos, Gateway IoT, Redes definidas por software, 5G	[4], [5], [6], [7], [9], [11], [13], [18], [20], [23], [29], [15], [16], [17]
Middleware IoT	[4], [5], [8], [15], [16]
Almacenamiento y Procesamiento de datos en IoT, Big data	[7], [9], [30], [31]
Dominios / aplicaciones IoT	[4], [7], [8], [9], [11], [12], [13], [14], [15], [16], [18], [21], [32], [33]
Seguridad y privacidad en IoT, Blockchain	[4], [5], [9], [10], [12], [13], [16], [20], [30],
Cloud Computing (CC)	[5], [8], [9], [13], [15], [21], [29], [34], [35],
Fog Computing	[8], [9], [13], [15], [18], [21], [29], [34]
Edge Computing	[13], [21], [34]
Mobile Edge Computing, Mobile cloud computing	[21], [29], [34]

El objetivo de este trabajo consiste en la revisión del estado del arte de IoT, con un lenguaje sencillo y orientador, para el

B. Mazon-Olivo. Grupo de investigación AutoMathTIC, Facultad de Ingeniería Civil, Universidad Técnica de Machala. Machala, El Oro, Ecuador. bmazon@utmachala.edu.ec

A. Pan. Facultade de Informática, Universidade da Coruña. A Coruña, España. apan@udc.es

lector que está incursionando en el mundo de IoT, tenga un punto de partida para futuras investigaciones. Nuestras principales contribuciones se centran en:

- Presentar una revisión, lo más completa posible, del estado del arte de IoT, con fuentes actualizadas y una estructura sistemática y orientadora.
- Realizar un análisis de los modelos de referencia de arquitecturas IoT y los paradigmas computacionales.
- En base al modelo de 3 capas (percepción, red, middleware / aplicación) adoptado por la mayoría de modelos de referencia, identificar los componentes del ecosistema IoT y, aspectos de seguridad y gobernanza.
- Nuestra mayor contribución se centra en el análisis de Middleware IoT, orientado al almacenamiento y procesamiento de datos. Además, proponemos una Arquitectura de Gestión de Datos en un Sistema IoT. Esto se debe a que, no se encontró un modelo que explique la complejidad del manejo de los datos y, los retos y problemas abiertos en este tipo de Middleware IoT.

A continuación, se describen brevemente los trabajos previos relacionados con el componente Middleware IoT. [4], [5], [8] y [16] contienen principalmente definiciones, características y una breve clasificación. Kassab y Darabkh [15], realizan una categorización/ clasificación, identificación de herramientas/ plataformas y destacan algunos desafíos a nivel de Middleware IoT. Además, en [36] y [37], plantean los requisitos funcionales y no funcionales, analizan las contribuciones existentes y plantean desafíos de la capa Middleware IoT, por ejemplo: descubrimiento y gestión de recursos, gestión de eventos, gestión de la seguridad y privacidad, entre otros. Los trabajos [7], [9], presentan una breve descripción de la gestión de datos en IoT. En [30], [31], se analizan con mayor profundidad las contribuciones de Big Data (BD) y BD Analytics (BDA) en IoT; también presentan desafíos importantes como: el manejo de grandes volúmenes de datos heterogéneos y en tiempo real, la integración de datos y la aplicación de técnicas de BDA.

Finalmente, en [38], se presenta un modelo de referencia para Middleware IoT; los módulos que describen brevemente son: interoperabilidad, persistencia y análisis de datos, contexto, recursos y eventos, interfaz gráfica de usuario y seguridad.

Sin embargo, ninguno de estos trabajos aborda de forma exhaustiva todos los problemas relacionados con la gestión de grandes volúmenes de datos en aplicaciones IoT ni proponen una arquitectura de referencia detallada para abordarlos.

B. Revisión de Literatura

Se aplicó una metodología de Revisión Sistemática de Literatura (RSL) similar al trabajo de Botta [8]. Se buscó trabajos en las bases datos: Web of Science, Scopus, ScienceDirect, MDPI, IEEE Xplore, Springer, Taylor and Francis, ACM y Google Scholar.

En Fig. 1, se observa el número de publicaciones indexadas en Google Scholar, relacionados con IoT, cloud computing y Big Data. Se aprecia un incremento considerable entre el año 2010 y 2020, y una aparente disminución de las publicaciones, a partir del 2019.

En Fig. 2, se resume la cantidad de publicaciones por tópicos relacionados con IoT, realizadas entre el 2019 y 2020. Las cadenas de búsqueda aplicadas en Google Scholar, fueron primero “Internet of things (IoT)”; y luego se armó cadenas combinadas con “Internet of things” y los tópicos descritos a continuación: “challenges”, “security”, “cloud computing”, “architecture” and “reference” and “model”, “evolution”, “platforms”, “domains”, “sensor network”, “definitions”, “gateway”, “WSN”, “components” and “ecosystem”, “edge computing”, “fog computing”, “mobile edge computing”, “mobile cloud computing”.

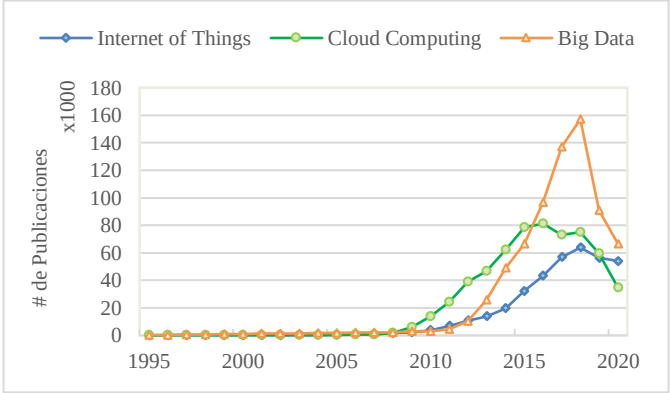

Fig. 1. # de publicaciones/año de IoT, cloud computing y Big Data

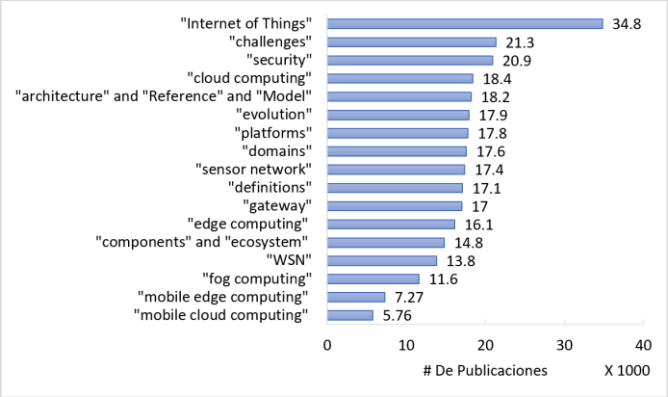

Fig. 2. # de publicaciones por tópicos de IoT, periodo 2019-2020.

II. ARQUITECTURAS DE REFERENCIA DE IOT Y PARADIGMAS COMPUTACIONALES

A. Modelos de Referencia de Arquitecturas (ARM) para Internet de las cosas

Existen varias arquitecturas, marcos de referencia o modelos conceptuales para IoT propuestos por organizaciones, comunidad académica y el sector empresarial.

En Fig. 3, se presenta una comparativa de algunos modelos basados en capas.

A continuación, se describen las capas más importantes:

La *capa de percepción* (Objetos/ Dispositivos/ Sensor-Actuador/ WSN/ Edge Computing/ Sensado), digitaliza y transfiere datos a la capa de red, a través de canales seguros [9]. Se localizan los objetos físicos, dispositivos sensores y actuadores utilizados para recopilar información del contexto.

La *capa de acceso* (Adaptación/ Observador), comprueba la información que recibe de la capa de percepción, si está

protegida o no contra intrusos y virus. Si hay algún ataque, no pasa los datos a la siguiente capa. También verifica la identidad y autenticación de los objetos [9], [10].

Nº DE CAPAS	REFERENCIAS
3 Capas	Gubbi [3], Al-Fuqaha [9] ,Burham [10], Omoniwa [13], Kassab [15], Aman [16], Muccini [19], Berrú-Ayala [25], Sharma [26]
4 Capas	Burham [10], Hassija [12],Omoniwa [13], Muccini [19], Aman [16]
5 Capas	Al-Fuqaha [9], Burham [10], Omoniwa [13], Muccini [19], Aman [16]
Basado en SOA	Atzori [4], Botta [8], Al-Fuqaha [9], Kassab [15]
Basado en Middleware	Al-Fuqaha [9]
6 CAPAS	Muccini [19]

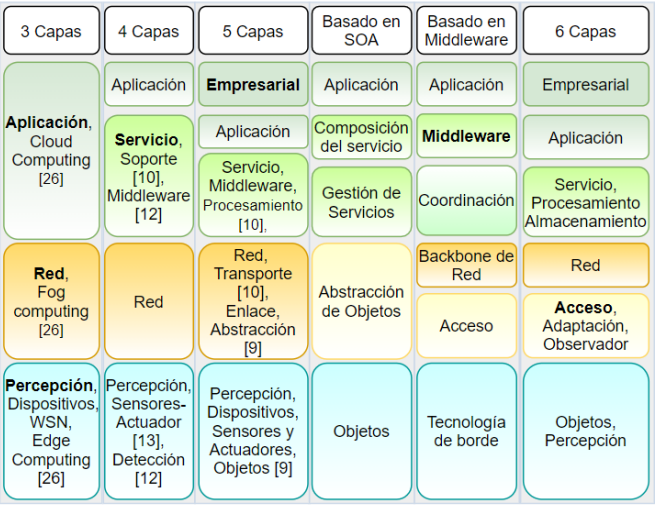

Fig. 3. Modelos de arquitecturas IoT basados en capas.

La *capa de Red* (Abstracción de Objetos/ Transporte/ Fog computing), transporta y transmite los datos, recopilados de la capa de percepción, hacia la cloud. Se localizan componentes de red (switch, router, Gateway, etc.), medios de comunicación y protocolos. También es responsable de aspectos de seguridad y el control de ataques [9], [10].

La *Capa Aplicación / Cloud Computing (CC)* en modelos de más de tres capas, puede dividirse en:

- *Capa de procesamiento y almacenamiento*, *Soporte*, o *Middleware*. Permite a los programadores de aplicaciones IoT trabajar con objetos heterogéneos sin tener en cuenta una plataforma de hardware específica. Se encarga de integrar, almacenar, procesar y analizar datos, tomar decisiones y ofrecer servicios de protocolos de conexión de red [9].
- *La capa de aplicación*, define los servicios y funciones que proporciona la aplicación IoT implementada (hogar inteligente, ciudad inteligente, salud inteligente, etc.) a los clientes. Los servicios pueden variar para cada aplicación y depende de la información que se recopilan de los sensores. También se consideran aspectos de seguridad [9], [10].
- *La capa empresarial*, tiene la responsabilidad de administrar y controlar el comportamiento de las aplicaciones, modelos de negocios y ganancias de IoT. También tiene la capacidad de determinar cómo se puede crear, almacenar y cambiar la información. Administra la privacidad del usuario y evita vulnerabilidades [9], [10].

A continuación, se listan varias propuestas de ARM para sistemas IoT:

ARM IoT de organizaciones: IoT: ITU-T Y.2060 (06/2012) IoT reference model [39], IoT Architectural Reference Model (ARM) del proyecto IoT-A [40], Internet of Things Reference Model (CISCO) [41], IEEE P2413, Standard for an Architectural Framework for the Internet of Things (IoT) [42], [43], Reference model for the IoT (CCSA) [44], Industrial Internet Reference Architecture (IIRA v1.8) [45], Reference Architecture Model Industrie 4.0 (RAMI) [46], ISO/IEC 30141 (IoT RA) [47], Web of Things Architecture (WoT-W3C) [48].

ARM IoT de la comunidad científica: Framework conceptual de IoT y CC [3], Arquitectura de interoperabilidad de nivel semántico para IoT [49], Nube logística basada en IoT y SaaS Cloud Computing [50], DIAT: una arquitectura distribuida y escalable para IoT [51], CEB: Cloud-Edge-Beneath [52], Arquitectura IoT de Vehículos (IoV) [53], ViSiT [54], IoT-ARM para ciudades inteligentes [55], SACA [26], Modelo de referencia para Middleware IoT [38], Arquitectura IoT para fabricación inteligente, aplicando Big Data y Edge Analytics [56], Blockchain Meets IoT, una arquitectura para la gestión de acceso escalable en IoT [57], IoT cognitiva (CIoT) [58], Arquitectura Fog Computing [59], entre otras.

ARM IoT del sector comercial: se han propuesto, a través de sus plataformas IoT, por ejemplo: Microsoft Azure IoT, AWS IoT, IBM Watson IoT Platform, Google IoT, Adafruit IO, Thingspeak, Sofia2, Altair Smart Works, PTC ThingWorx, Cisco Kinetic, Verizon Thingspace, Oracle IoT Cloud, AT&T M2X, SAP IoT, Huawei, C3 IoT, Bosch IoT Suite, etc. [8], [14].

B. *Paradigmas de Computación en IoT*

En la última década es notable la evolución de los paradigmas de computación. Cloud Computing es el más relevante y fundamental para el desarrollo de los servicios y aplicaciones de IoT. Sin embargo, debido a la cantidad masiva de datos producidos por los dispositivos IoT, han surgido otros paradigmas como: Fog Computing (FC) y Edge Computing (EC) (ver Fig. 4).

Cloud Computing. Para [35], es "la entrega de infraestructura y aplicaciones de TI como un servicio a pedido, para individuos y organizaciones, a través de plataformas de Internet". Se compone de: cinco características (autoservicio bajo demanda, acceso de red de servicios, agrupación de recursos, elasticidad rapidez y servicio medido), tres modelos de servicio (software como servicio (SaaS), plataforma como servicio (PaaS), e infraestructura como servicio (IaaS)) y, cuatro modelos de implementación de nube (privada, comunitaria, pública e híbrida) [60], [61]. Proveedores de CC son: Amazon Web Services, IBM, Microsoft Azure, Google Cloud Platform, Salesforce, SAP, Oracle, Alibaba Cloud, RackSpace, VMware etc. Una variante es la Computación móvil en la nube [62].

Fog Computing (FG), descentraliza los servicios de la cloud al borde de la red; puede ser una plataforma virtualizada en un micro data center, con servicios de computación, almacenamiento, comunicación y control de redes en un entorno localizado [59], [63]. En [64], mencionan un paradigma alternativo relacionado con la movilidad: Computación móvil en el borde (*MEC: Mobile or Multi-Access Edge Computing*), que proporciona a los clientes, una gama de medios y servicios de computación crítica, similares a la cloud, en la periferia de las redes de celulares; facilitando el control, almacenamiento, procesamiento y analítica del tráfico de datos en redes móviles.

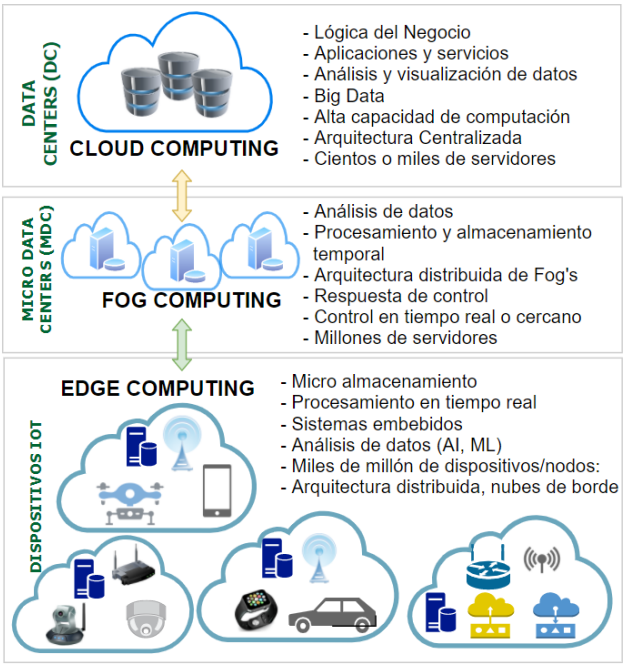

Fig. 4. Paradigmas de computación en IoT.

Edge Computing (EC), el procesamiento de datos se realiza en la periferia de una red cercana a las fuentes de datos; puede ser en dispositivos inteligentes, micro servidores, teléfonos inteligentes, etc., ubicados entre los dispositivos finales y la nube [21], [63]. Tiene el propósito de: minimizar la latencia y volúmenes de tráfico de red hacia la nube, lo que conlleva a una eficiencia energética y reducción de costos [59], [64], [65].

C. *Componentes del ecosistema IoT*

En Fig. 5, constan los componentes del ecosistema IoT, según el modelo de 3 capas.

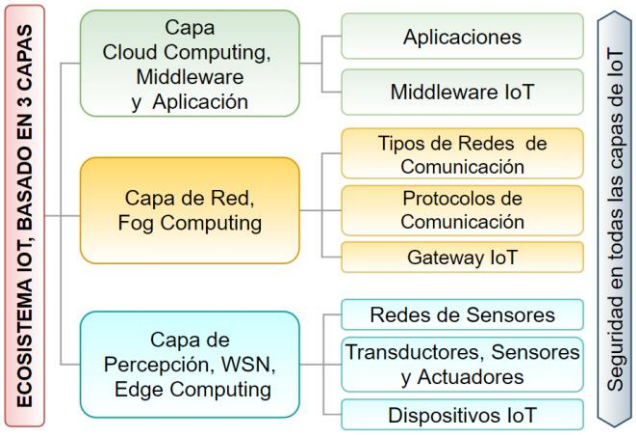

Fig. 5. Componentes del Ecosistema IoT basado en capas.

En la capa de Percepción se ubican las redes de sensores cableadas e inalámbricas, dispositivos IoT, transductores, sensores y actuadores. La capa de Red consta de: infraestructura de redes de comunicación, protocolos de comunicación IoT y Gateways IoT. Y, en la capa de aplicación: Middleware y aplicaciones IoT [3], [5], [20], [66]. La seguridad es un aspecto importante a considerar en todos los niveles de un sistema IoT. En las secciones III, IV, V y VI se describen estos componentes en detalle.

III. CAPA DE PERCEPCIÓN

A. *Rede de Sensores (SN: Sensors Network, WSN: Wireless Sensors Network o WSAN si incluye actuadores)*

Las SN incluyen múltiples dispositivos (motes o nodos) equipados con transductores, actuadores y sensores que interactúan según la aplicación IoT [63]. Una SN puede estar formada por cientos o miles de nodos que se comunican entre sí y transmiten datos a otros dispositivos como el Gateway y a través de este se envían a un sistema distribuido o centralizado para su almacenamiento y procesamiento [63], [66].

Clasificación de las redes de sensores (SN). Se pueden clasificarse según varios aspectos como se observa en Fig. 6. [27], [67].

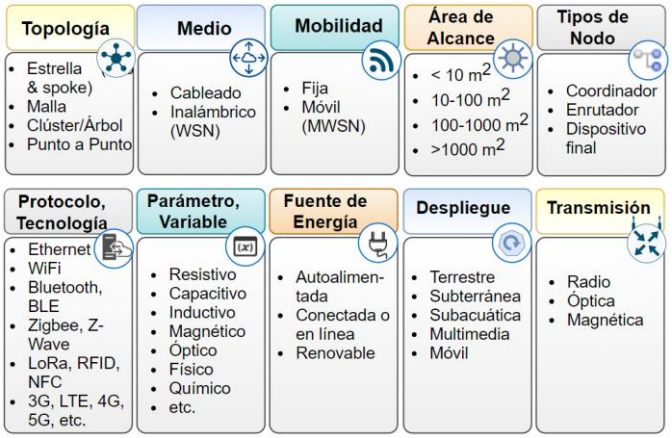

Fig. 6. Clasificación de las redes de sensores.

Componentes de una SN. Los componentes dependen del dominio o aplicación IoT. Estos son: hardware de los nodos, pila de comunicación, middleware y agregación segura de datos [3]; ver Tabla II.

TABLA II
COMPONENTES DE UNA WSN

Componente	Descripción
Hardware de los nodos	Dispositivos con: microcontrolador, interfaces de sensores, memoria interna/externa, unidades transceptoras, fuente de alimentación, convertidor analógico/digital e interfaces de comunicación.
Pila de comunicación	Los nodos necesitan comunicarse entre sí para transmitir datos en un solo salto o en múltiples saltos a una estación base. La pila de comunicación en el nodo receptor debe tener la capacidad de interactuar con el mundo exterior a través de Internet. Para mantener una red escalable y durable, es importante la interacción de varios protocolos de comunicación en la transmisión de datos desde los sensores hacia un sistema distribuido o centralizado.
Middleware	Facilita la comunicación entre componentes heterogéneos de un sistema IoT, permitiendo resolver los problemas relacionados con los sistemas distribuidos de una manera independiente del despliegue. Un ejemplo es Sensor Web Enabled (SWE) de Open Geospatial Consortium (OGC).
Agregación segura de datos	La agregación de datos debe ser eficiente y segura para extender la vida útil de la red y garantizar la recolección confiable desde los sensores. Por consiguiente, las fallas de los nodos suelen ser una característica común de las WSN, en consecuencia, la topología de red debe tener la capacidad de repararse.

B. Transductores, sensores y actuadores

Transductor, transforma o convierte una determinada energía de entrada, en otra de diferente naturaleza en la salida. Los transductores pueden ser sensores y actuadores [63].

Los sensores convierten estímulos físicos en señales eléctricas analógicas o digitales y según la señal se clasifican en acústicos, eléctricos, magnéticos, ópticos, térmicos y mecánicos [63]. También, se encargan de monitorear las características físicas, químicas o ambientales como: temperatura, humedad, movimiento, velocidad del viento, dirección del viento, nivel de Ph, electro conductividad, nivel de luz, etc. [66]. Para [3], los sensores son dispositivos eficientes de bajo consumo y costo, incorporados en aplicaciones de teledetección.

Los actuadores son capaces de transformar energía eléctrica, hidráulica o neumática en la activación de algún proceso u otro dispositivo, que afecta el medio ambiente como: abrir /cerrar válvulas, encender / apagar una bomba o foco, emitir sonido, generar ondas de radio, activar/desactivar un motor, etc.; permitiendo de esta forma que los objetos estén simultáneamente al tanto de su entorno e interactúen con las personas o cosas [63].

C. Dispositivo IoT

Considerado mote, nodo, objeto inteligente, transductor inteligente, entre otros. Por lo general son pequeños computadores con capacidad de monitorear información de sensores, controlar actuadores y comunicarse con otros nodos, con un Gateway o directamente con un servidor remoto [11], [68]. Los componentes de un mote son: batería de energía, entradas y/o salidas analógico/digitales, microprocesador (SoC: System on Chip) que incluye CPU, memoria e interfaces de comunicación (GPS, serial, Ethernet, Wireless, celular, etc.). También pueden incluir almacenamiento interno o externo, GPU e interfaces de audio y video. En cuanto al firmware, consta de un sistema operativo (SO), protocolos y algoritmos [11]. Las plataformas hardware para dispositivos IoT se clasifican en: 1) Sistemas embebidos y tarjetas: Ejemplo; Arduino (UNO, MEGA, Yun), Intel Galileo, Intel Edison, Beagle Bone Black, Orange Pi, Adafruit, Raspberry Pi, ARM mbed, ESP8266, Littlebits, Particle Photon, Pinoccio, RedBearLab, etc. Y, 2) Gadgest & Wareables; ejemplo de fabricantes: Apple, Xiaomi, Huawei, Samsung, Fitbit y otros [11], [22], [69]–[71]. Un mote requiere un SO liviano para su gestión y control; según [9], [28], los más destacados son: RiOT, TinyOS, Contiki, Mantis, Nano-RK, LiteOS, entre otros. Los SO dependen de los tipos de dispositivos, por ejemplo, para Raspberry Pi, son: FreeBSD, Raspbian, Kali Linux, etc.

D. Retos y problemas abiertos en la capa de percepción

Dada la creciente demanda de tecnologías de WSN y dispositivos IoT comerciales, un desafío importante es la interoperabilidad entre distintas tecnologías y estándares para lograr la convergencia de diversidad de servicios de extremo a extremo. El Gateway IoT, debe ser capaz de abstraer la diversidad de dispositivos finales e integrarlos en una arquitectura estándar. Además, una WSN enfrenta problemas relacionados con la comunicación a largo alcance, confiabilidad, fiabilidad, escalabilidad, compatibilidad, gestión de la calidad del servicio (QoS), direccionamiento IPv6, errores en los nodos (fallos en la comunicación inalámbrica, ruido en mediciones, fallos del hardware). También el uso óptimo de recursos como: eficiencia energética, capacidad de almacenamiento y procesamiento, nodos plug & play, bajos costes, etc. [15]. Cabe destacar que la seguridad y privacidad es uno de los factores más importantes en una WSN; ya que es más susceptible a amenaza y fallos, debido a la capacidad limitada de los nodos y al despliegue en áreas no protegidas [27], [72]. Otro problema es la movilidad en los nodos (ejm. vehículos autónomos conectados) [27].

Las investigaciones futuras, están relacionadas con el Internet de las Nano Cosas (IoNT), el uso de la Nanotecnología y nuevos materiales, para fabricación del hardware de los nodos y transductores [73], [74]. También en [75], mencionan las tecnologías memristivas y la Inteligencia Artificial embebida.

IV. CAPA DE RED

A. Redes de comunicación de datos para IoT

Las redes de comunicación en IoT incluyen componentes hardware, software, tecnologías y protocolos que permiten la conectividad entre objetos IoT y la infraestructura de un Data Center o cloud computing de un sistema IoT [5]. Las tecnologías de redes y protocolos tienen la responsabilidad de la comunicación de los datos recolectados de los diferentes dispositivos IoT [76]. Los dispositivos IoT se conectan con nodos de borde o Gateway IoT, utilizando una red de tipo PAN/WPAN o LAN/WLAN dentro de un área de corto alcance. Luego un Gateway IoT se comunica con los centros de datos remotos o cloud computing, utilizando redes MAN-NAM / WMAN-WNAN o WAN/ WWAN que cubren un área de mediano a largo alcance [77].

En la Tabla III, resume los tipos de redes de comunicación de datos según [5], [11].

TABLA III
TIPOS DE REDES DE COMUNICACIÓN DE DATOS UTILIZADAS EN IOT

Tipo de redes	Estándar	Distancia	Tecnologías
Redes de área personal (PAN/WPAN)	IEEE 802.15. (1, 3, 4, 6)	<10 m	UWB, NFC, RFID, Bluetooth, BLE, ZigBee, Z-Wave, 6LoWPAN, ETSI HiperPAN, LoRa, etc.
Redes de área Local (LAN/ WLAN)	IEEE 802.3, 3u, 3z/ IEEE 802.11 (a, b, g, n, ax)	<100 m	Ethernet, Wi-Fi, HaLow (Low-power WiFi), ETSI HiperLAN, etc.
Red de área metropolitana o Red de área de vecindario (MAN-NAN/ WMAN-WNAN)	IEEE 802.6 / IEEE 802.16	<10 Km	Wi-MAX, ETSI HiperMAN, ZigBee NAN, Wi-SUN, NWare
Wide Area Network (WAN/ WWAN)	IEEE 802.20, CDMA, GSM, UMTS, GPRS	>10Km	2G, 3G, 4G, 5G, LTE/MTC, UMTS, NB-IoT, Low Power Wide Area Network (LPWAN: LoRaWAN, Weightless, SigFox, DASH7), 3GPP, GSM/EDGE/GPRS, Comucación satelital

Las Tecnologías de comunicación inalámbricas para IoT, han tenido un rápido desarrollo, pasando de la red Infrarrojo para comunicación punto a punto (P2P) a las WPAN, redes inalámbricas multipunto y de corto alcance como Bluetooth o las redes de alcance medio y multi-saltos como las ZigBee y, redes de largo alcance como Long Range /LoRaWAN [1], [5], [78].

Los protocolos de comunicación, facilitan la interoperabilidad entre los componentes de un sistema de entornos diferentes. La pila de protocolos utilizados para la comunicación de datos en sistemas IoT, se basa en la arquitectura de protocolos TCP/IP [5], [23], [79]. La capa de aplicación se ejecuta en la parte superior de esta pila y se identifican protocolos para aplicaciones IoT: Constrained Application Protocol (CoAP), Message Queue Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), Extensible Messaging and Presence Protocol (XMPP), Data Distribution Service (DDS), HTTP, HTTPS, etc. [5], [9], [23], [79].

B. Gateway IoT

Es un dispositivo físico con un software de control que actúa como puerta de enlace, permitiendo que las redes de sensores tengan un acceso confiable a Internet. Facilita la conexión e interoperabilidad entre dispositivos IoT, las aplicaciones remotas y usuarios finales, a través de redes inalámbricas, cableadas o híbridas [80]. Un Gateway actúa como uno de los componentes clave en una arquitectura IoT, debido a que provee varias soluciones como: la conversión de protocolos y centralización de la conectividad, por un lado con diversas tecnologías de redes de sensores y, por el otro extremo, con el centro de procesamiento de datos remoto o CC [5], [81]. Un Gateway puede ser fijo (implementado en un pequeño computador, por ejemplo: Raspberry PI, micro-servidor o micro-data center), o puede ser móvil (implementado en un teléfono inteligente), en los dos casos tiene la capacidad de coordinar la comunicación entre los nodos sensores y una plataforma IoT. Un Gateway, además de recibir los datos de los nodos IoT ubicados en las WSN, los procesa y almacena temporalmente, para luego direccionar, enrutar y enviarlos, a través de un protocolo de comunicación, al escenario IoT; [63], [69].

Las características de un Gateway IoT son: el soporte de comunicación e interoperabilidad entre redes heterogéneas, control de movilidad y administración de nodos de redes de sensores dependientes, soporte de protocolos de red heterogéneos, enrutamiento de paquetes, reenvío de paquetes, procesamiento y almacenamiento temporal, soporte de convergencia y agregación de datos multimodales (de distinto: origen, volumen, velocidad y tiempo de llegada) y, seguridad y privacidad [20].

C. Problemas abiertos en la capa de red

Los problemas abiertos en la capa de red están relacionados con las redes celulares 5G [17], [82] y 6G [83], que proporcionan tecnologías habilitadoras clave para el despliegue ubicuo de la tecnología IoT. Los retos más destacados son: agregación de portadoras, múltiples entradas y múltiples salidas (MIMO), MIMO masivo (M-MIMO), red de acceso de radio centralizada (CRAN), procesamiento multipunto coordinado (CoMP), comunicaciones de dispositivo a dispositivo (D2D), redes definidas por software, (SDN), redes de sensores inalámbricos definidas por software (SD-WSN), virtualización de funciones de red (NFV), radios cognitivas (CR), etc. [29].

V. CAPA CLOUD, MIDDLEWARE Y APLICACIONES

En esta capa se localiza la infraestructura Cloud Computing para la gestión de: 1) los servicios Middleware de almacenamiento y procesamiento de datos y, 2) las aplicaciones IoT [3], [5], [20], [66].

A. Subcapa Middleware IoT: Almacenamiento y Procesamiento de datos

Los datos enviados por la capa de red no se encuentran en un formato en el que puedan ser directamente analizados. La subcapa de Middleware IoT de datos, solventa este problema para permitir la toma de decisiones en la subcapa de aplicación.

Las principales dificultades a las que debe enfrentarse esta subcapa son: 1) Las e*normes cantidades de datos,* generados muy rápidamente por las aplicaciones IoT, que deben ser almacenadas y procesadas a un coste razonable [84]. 2) *La integración de los datos* recolectados por los sensores con otras fuentes de información. 3) *Distintos tipos de análisis* que *requieren almacenar datos en formatos y niveles de agregación diferentes*; pueden también requerir diferentes sistemas de procesamiento [84]. Por ejemplo, una aplicación de agricultura de precisión que intente predecir el mejor uso posible para una parcela determinada, necesitará trabajar sobre datos agregados a nivel de tipo de suelo y tipo de cultivo en distintos intervalos temporales (ejm. medidas de producción por tipo de cultivo en distintos tipos de suelo y condiciones atmosféricas). Por el contrario, una aplicación que active automáticamente el riego en una parcela cuando las condiciones lo requieren puede necesitar responder de forma inmediata a eventos individuales sin agregar (ejm. cambios en la temperatura y humedad del suelo detectados por los sensores). Los sistemas de almacenamiento y procesamiento de datos necesarios para dar respuesta a estos dos tipos de necesidades son también muy diferentes.

En esta sección se presenta una arquitectura de referencia capaz de resolver estos problemas. También se identifican las herramientas más adecuadas para implementar cada uno de sus componentes. Finalmente, se describen algunos de los principales problemas abiertos en esta área. La Fig. 7 muestra las principales etapas por las que pasan los datos de las aplicaciones IoT.

El proceso comienza con la *captura y transmisión de datos*, cuando los datos son obtenidos a través de los sensores y se envían al Gateway IoT. Las primeras labores de preprocesamiento pueden hacerse en esta etapa; por ejemplo, se puede calcular la media de las mediciones de varios sensores cercanos y/o de las medidas tomadas por un sensor en varios instantes (por hora, día). Esto atenúa los efectos de errores de medición y disminuye los datos a procesar en etapas posteriores. Algunos análisis sencillos de datos pueden realizarse también en esta etapa, cuando sólo se precise de datos locales para tomar la decisión y el coste computacional sea pequeño. Un ejemplo en el ámbito de la agricultura de precisión sería cambiar las condiciones de riego en una parcela como respuesta a condiciones atmosféricas locales.

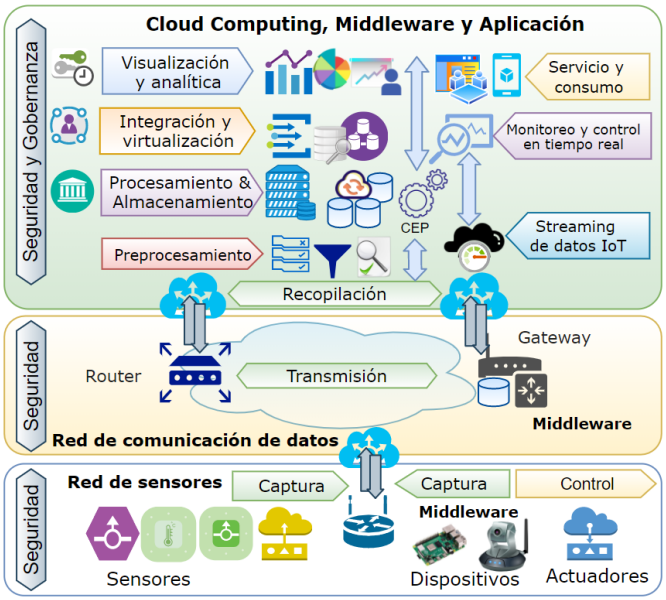

Fig. 7. Arquitectura propuesta de referencia para procesos de gestión de datos en un sistema de IoT

Al procesamiento de datos realizado en esta capa, se le llama a menudo 'Edge Computing' (ver Fig. 4). [59], [64], [65]

En la siguiente etapa, la capa de Red es responsable de enviar los datos preprocesados al sistema central de toma de decisiones, que suele ser un sistema de Cloud Computing [65], [85]. Estos sistemas están optimizados para el almacenamiento y procesamiento de grandes cantidades de datos con bajo coste.

A pesar del primer nivel de agregación de datos realizado en la capa de percepción, el volumen y rapidez de llegada de datos en las aplicaciones IoT puede ser muy elevado. Por lo tanto, el sistema debe permitir la *recopilación y preprocesamiento de datos* de forma rápida, barata, y tolerante a fallo. Sin embargo, el volumen de datos suele ser demasiado grande para almacenar permanentemente todos los datos sin agregar, por lo que es necesario eliminar los datos más antiguos.

La tecnología más popular para esta tarea es Apache Kafka [86], [87]. Esta herramienta utiliza una infraestructura distribuida y tolerante a fallos para actuar como un gran "buffer" que almacena temporalmente (normalmente durante unos pocos meses) los mensajes de los sensores, ya en un formato unificado. Esto permite desacoplar el ritmo de llegada de los eventos, del ritmo de procesamiento de los mismos, que puede ser muy diferente. Mantener almacenados los datos "crudos" durante unos meses también permite corregir posibles errores que se produzcan en etapas posteriores.

A partir de este momento, los datos pueden seguir dos caminos: 1) Para *aplicaciones de analítica y ciencia de datos*, los datos deben combinarse con información de dimensiones relevantes para el análisis. Por ejemplo, en una aplicación de agricultura de precisión, las medidas de sensores deben combinarse con información del tipo de cultivo, ubicación y clima de la parcela, tipo de suelo, etc. Los datos también se agregan a una granularidad superior, más adecuada para este tipo de análisis. Por ejemplo, es habitual utilizar medias temporales (por hora, día, etc.) de las medidas y/o agregar las medidas de tipos similares. Esto disminuye el volumen de datos a almacenar de forma permanente y facilita el análisis de tendencias y la creación de informes. Para este tipo de aplicaciones, los datos se almacenan en distintos sistemas de almacenamiento y procesamiento, descritos en el siguiente epígrafe. 2) Para *aplicaciones de monitoreo y control* en tiempo real [30], [88]–[90], los datos también se integran con información dimensional, pero no se agregan o lo hacen a una granularidad más fina. Estos datos se procesan en los módulos de *streaming / complex event processsing (CEP)*, que calculan métricas en tiempo real para alimentar cuadros de mando y/o generar respuestas automáticas [91].

Sistemas de almacenamiento y procesamiento de datos. Los datos agregados y transformados para aplicaciones de analítica y ciencia de datos (camino 1) pueden ser almacenados en tres tipos de sistemas gestores de bases de datos (DBMS) [92]: 1) *Gestores de bases de datos relacionales* (RDBMS), como: MySQL, PostgreSQL, SQLServer, etc.; se utilizan para datos estructurados y volúmenes de datos pequeños o medios como, por ejemplo, los datos de dimensiones utilizados para contextualizar las medidas recogidas por los sensores. 2) *Sistemas Big Data*, como Apache Spark, Impala o Presto. Se especializan en el almacenamiento de grandes cantidades de datos utilizando infraestructura de bajo coste, distribuida y tolerante a fallos. Estos sistemas tienen su origen en tecnologías como Hadoop y HDFS [30], [31], [93] pero han evolucionado para funcionar en entornos de cloud computing. En arquitecturas IoT estos sistemas se suelen utilizar para almacenar los datos procedentes de los sensores, integrados, transformados y agregados para permitir procesos de analítica y ciencia de datos. Son también adecuados para almacenar datos no estructurados (ejm. cartografías, audios, videos, etc.) 3) *Bases de datos no relacionales o NoSQL*, por ejemplo: MongoDB, Neo4j, Azure Cosmos DB, Google BigTable, Amazon DynamoDB, etc. [94]–[96]. Estos sistemas son adecuados para satisfacer requerimientos de almacenamiento especiales como: clave-valor, documentos, orientado a grafos, etc. [94]. En arquitecturas IoT se suelen utilizar para almacenar datos especiales dependientes del dominio (ejm. datos geoespaciales de cartografías, o grafos de dependencias entre componentes). 4) *APIs externas*, a menudo, las aplicaciones IoT se ven obligadas a acceder a APIs de proveedores externos (ejm. APIs de geolocalización, procesamiento de lenguaje natural o calidad de datos, entre otras).

Streaming de datos IoT, monitoreo y control en tiempo real. Las aplicaciones de monitoreo (camino 2) necesitan procesar los datos en tiempo real (o con retardo muy bajo), por lo que las transformaciones deben realizarse de forma muy eficiente. Para combinar datos y generar métricas en tiempo real pueden utilizarse sistemas de procesamiento de streams como Apache Storm [97], Flink [98], Spark Streaming [99] y también sistemas de *complex event processing* [91]. Ambos tipos de sistemas implementan reglas para fusionar los datos de los sensores con datos extraídos de otros sistemas. Pueden usarse para generar métricas que alimentan cuadros de mando en tiempo real, para generar alertas y/o para desencadenar respuestas automáticas a través de actuadores en la capa de percepción [30], [91].

Integración y virtualización de datos. Esta etapa es necesaria para integrar los datos procedentes de los sensores con información almacenada en todos los tipos de DBMS mencionados y también con APIs externas.

El enfoque tradicional de integración de datos se basa en la tecnología ETL (Extraction, Transformation and Load) [126]. En esta aproximación, cada vez que se necesita combinar y transformar los datos de múltiples fuentes para un nuevo tipo de análisis, se crea un nuevo repositorio de datos (data warehouse) en el que se vuelcan los datos necesarios, integrados y en el formato deseado. Algunas herramientas comerciales que siguen este enfoque son Pentaho Data Integration e Informática[100],

En el contexto de las aplicaciones IoT, esta aproximación plantea diversos problemas: 1) No es válida para la integración de datos en tiempo real requerida en las aplicaciones de monitoreo, 2) Incluso para aplicaciones de analítica/ciencia de datos, la creación de nuevas copias de datos para cada nueva necesidad resulta en tiempos de desarrollo muy largos, y 3) puede generar problemas de seguridad y gobernanza como resultado de las múltiples copias de los mismos datos.

Una aproximación alternativa cada vez más común en aplicaciones IoT es la Virtualización de Datos [126], que permite definir vistas unificadas de datos distribuidos en múltiples fuentes, sin necesidad de mover ni replicar los datos. El usuario puede ejecutar consultas sobre una "base de datos virtual" que expone una serie de tablas lógicas donde los datos aparecen al usuario integrados como si estuviesen realmente en un único sistema. Cuando el sistema de virtualización de datos recibe una consulta, es capaz de acudir en tiempo real a cada fuente de datos, extraer los datos necesarios para responder a la consulta, combinarlos y devolverlos al usuario.

Esta aproximación presenta varias ventajas: 1) Puede utilizarse tanto para aplicaciones de analítica/ciencia de datos como en aplicaciones de monitoreo en tiempo real. 2) Minimizar la replicación de datos; Gartner estima los ahorros de tiempo y costes conseguidos con esta tecnología en un 45% [100], [101]. 3) Proporciona una capa unificada para implementar políticas de seguridad y gobernanza, de forma que no es necesario implementarlas separadamente en cada sistema. Evita también la proliferación de copias de los mismos datos.

Algunas herramientas comerciales de virtualización de datos son Denodo, IBM Data Virtualization, Tibco Data Virtualization, entre otras [100].

Existen todavía importantes *problemas abiertos en la capa de middleware de datos*. En [102], se destacan algunos:

1. Cómo distribuir de manera óptima el procesamiento de datos entre Edge y Cloud [102].
2. Almacenamiento de datos. Cómo desarrollar métodos inteligentes para resumir la información de los sensores con la menor pérdida posible de granularidad [84].
3. Exploración y descubrimiento de datos. Cómo construir técnicas escalables de descubrimiento de datos, para tareas como data profiling o para encontrar fácilmente toda la información relevante para una tarea determinada [102].
4. Las aplicaciones de Machine Learning (ML) necesitan acceder a datos de formas novedosas, que no siempre se expresan bien con lenguajes clásicos como SQL. Es necesario desarrollar nuevas técnicas que automaticen lo más posible este trabajo [102].

B. Subcapa Aplicación

La subcapa de aplicación se encarga de utilizar la información integrada para la toma de decisiones. Los componentes de esta subcapa dependen del tipo de análisis:

1. Las aplicaciones de analítica de datos utilizan herramientas que permiten visualizar informes sobre información agregada. Algunos ejemplos de herramientas son Apache SuperSet [103], Tableau o Microsoft Power BI.
2. Las aplicaciones de ciencia de datos suelen utilizar algoritmos de Machine Learning para la construcción de modelos predictivos [30], [104].
3. Las aplicaciones de monitoreo permiten construir cuadros de mando en tiempo real. Para implementarlos se pueden usar plataformas IoT en modo SaaS; por ejemplo: Azure IoT, AWS IoT, Grafana, etc. [30], [105], [106].

Las características y funcionalidades de la subcapa aplicación dependen en gran medida del Dominio IoT implementado. A continuación, se describen con mayor detalle los *dominios de aplicación de IoT*:

Cuidado inteligente de la salud, Salud inteligente (Smart Healthcare, Smart Health). Consiste en el uso de las tecnologías de la información y comunicación (TICs) en la salud asistida o independiente. Para [73], es una red de servicios de asistencia sanitaria inteligente, para el diagnóstico, prevención o restablecimiento de la salud de los pacientes. Los escenarios de puede ser: emergencia, medicación, telemedicina, asistencia médica en el hogar, paquetes farmacéuticos inteligentes, dispositivos biomédicos, tele rehabilitación, etc. En [107], destacan el uso de wearables para detección de parámetros fisiológicos. Los retos son el uso de biosensores, monitoreo inteligente del estado del paciente, robots quirúrgicos que integran realidad aumentada [73]. También está la medicina de precisión a través de internet de las nano cosas (IoNT), nanosensores o nanorobots [73], [74].

Ciudades (Smart Cities). Debido al aumento de la población y la complejidad de las infraestructuras urbanas, se necesitan métodos para manejar los problemas de urbanización a gran escala; y, servicios que mejoren la calidad de vida de sus habitantes [108]. Las *Smart Cities*, integran las TICs en infraestructuras físicas, para una mejor interacción con las personas y organizaciones; con el propósito de aprovechar la inteligencia colectiva [109]. En [110], mencionan las interfaces basadas en voz (Voice User Interface (VUI)) e Interfaz de usuario basadas en gestos (Gesture-based user interface: GBUI) para el control de dispositivos en edificios. En [111], describen el uso de la realidad aumentada (AR) e IoT para mejorar la accesibilidad a las cosas, útil para personas con discapacidad. En [112], [113], describen el uso de Inteligencia Artificial (AI) y Machine Learning (ML) y Deep Learning (DL) junto con IoT, para resolver problemas sobre el uso inteligente y óptimo de recursos en: la gestión de redes de servicios públicos (agua, energía, alcantarillado, etc.), en edificios y hogares, en ambientes de ocio y turismo (parques, plazas, museos, etc.), en movilidad (gestión del tráfico, transporte, vehículos conectados, parqueo), en seguridad pública, economía y gobierno [7], [108], [109].

Edificios y hogares inteligentes (Smart Building and Home). Los edificios y hogares son componentes clave de las ciudades inteligentes [32], [114]. El propósito es la optimización de sus operaciones, mediante el monitoreo y control inteligente de: equipos, dispositivos y servicios; por ejemplo: sistema de iluminación, aire acondicionado y calefacción, elevadores, distribución y consumo de agua, energía eléctrica, televisión e internet, sistemas de video vigilancia, etc. [32], [114].

Agricultura y crianza de animales inteligente (Precision Agriculture, Smart Agriculture, Smart LiveStock). Consiste en la aplicación de las TICs (IoT, AI, ML, DL, etc.), junto a tecnologías mecanizadas, con el propósito de optimizar las labores agropecuarias y disminuir el consumo de recursos (materia prima, fertilizantes, agua, mano de obra, etc.); y, mejorar del rendimiento y calidad de la producción [18], [115]. Algunas ejemplos son: sensores remotos e inalámbricos, vehículos aéreos no tripulados (dron fumigador), agri-robots, tractor autónomo, cosechadora de precisión, sistemas inteligentes de riego y fertirriego, sistema de manejo integrado de plagas/maleza, sistema recomendador de la producción, sistemas de monitoreo del rendimiento, alimentadores inteligentes de animales, etc. [18], [115].

Industria 4.0 y fabricación inteligente (Industry 4.0, Smart Manufacturing). Comprende la integración de las TICs y tecnologías electromecánicas con el objetivo de mejorar la eficiencia y capacidad de respuesta de un sistema de producción [116]. Equipos en Industria 4.0 son: sensores de precisión, robots, máquinas industriales, impresoras 3D, dispositivos de inspección, montaje y almacenamiento logístico [117]. Los procesos son: digitalización de la producción, automatización de sistemas de adquisición de datos de línea de producción y uso de máquinas, vinculación a sistemas de suministros e intercambio automático de datos [116], [118] y modelos basados en datos, para la toma de decisiones automáticas en tiempo real [118], [119].

Movilidad Inteligente (Smart mobility). Es clave para la transportación sostenible de pasajeros y/o productos, en ciudades, industria, comercio, educación, salud, etc., tanto en ambientes urbanos como en rurales [33]. Los principales sectores son: sistemas viales, sistema de videovigilancia, monitoreo del tráfico y control de infracciones, señalización inteligente, sistemas de automatización de la conducción, e-ticket, e-parking, seguimiento en tiempo real del transporte público, etc. [33]. Los retos son la eficiencia en los sistemas, eco-sostenibilidad, disminución de accidentes de tránsito, vehículos autónomos (terrestres, aéreos y marítimos), etc. [120].

Comercio Minorista inteligente (Smart Retail). Consiste en el uso de las TICs [121], para mejorar la experiencia de los clientes; permitiéndoles escuchar o ver recomendaciones y ofertas personalizadas, en cualquiera de los casos, en una tienda en línea o en la física [121], [122]. La transacción de la compra y el pago siguen siendo en línea; el celular del cliente y la aplicación de la tienda pueden encargarse del proceso de forma autónoma. Los retos son transacciones y pagos automáticos y seguros; tecnologías como Blockchain y los contratos inteligentes pueden ser útiles [122]. Otros retos son las estanterías inteligentes que solicitan reposición de productos a un sistema de almacén e inventario inteligente; con esto lo que se busca es una tienda minorista inteligente con poca intervención de personal [121].

Otras aplicaciones IoT son las redes de energía inteligente (Smart Grid), gestión inteligente de la cadena de suministros (Smart Supply Chain), etc.

VI. SEGURIDAD Y GOBERNANZA EN IOT

A. *Seguridad en IoT*

A menudo la seguridad se descuida o se trata como una tarea tardía tanto por los fabricantes de hardware como por los desarrolladores de software de soluciones IoT. En la mayoría de los casos, los esquemas de protección se basan sólo en software, dejando al hardware vulnerable. Una plataforma de hardware no segura, conducirá inevitablemente a una pila de software no segura. En este caso, las *vulnerabilidades* pueden estar presentes en cualquier capa o componente de un sistema IoT. Estas debilidades son potenciales *amenazas*, que incluso pueden ser aprovechadas, por personas malintencionadas, para causar *ataques* que afectan negativamente el funcionamiento de todo el sistema IoT o, de una parte, como un dispositivo, servicio o aplicación. En este sentido, es importante identificar las posibles amenazas y *mecanismos de seguridad* para garantizar que un sistema IoT cumpla con los atributos de disponibilidad, integridad y confidencialidad.

Amenazas de seguridad y privacidad en IoT. Existen muchas amenazas que pueden ocurrir según [10], [12], [123]–[128], por ejemplo:

- *Forgery*, falsificación de datos identidades o perfiles para engañar al usuario o para saturar el consumo de recursos.
- *Tampering*, manipulación para degradar la eficiencia del servicio o de transmisión de datos.
- *Spamming*, envío de información no deseada.
- *Sybil*, manipulación de identidades múltiples a través de información de un usuario legítimo para el control ilegal de recursos.
- *Jamming*, interferencia malintencionada de la red de comunicación con datos ficticios, para perturbar la transmisión.
- Eavesdroping, espionaje o captura ilegal de paquetes para conseguir información.
- *DoS: Denial of Service*, ataque de Denegación de Servicio, que consiste en la sobrecarga de solicitudes para inhabilitar el uso de una aplicación o un dispositivo a los usuarios legítimos.
- *Botnet*, red de bots maliciosos usados para llevar a cabo otros tipos de ataques (DoS, Spamming, Phishing, etc.).
- *MiTM: Main-in-The-Middle* (Hombre en el Medio), una persona intercepta la comunicación entre dos dispositivos y manipula los datos que intercambian.
- *Phishing / Spoofing*, suplantación de identidad, servicios falsos e ingeniería social, para engañar a las víctimas, para hacerles descargar Malware y/o perpetrar robos de datos o de dinero.
- *Ataques relacionados con la privacidad*: privacidad de

identidad y datos (fuga de datos personales de usuarios, divulgación no autorizada), *privacidad de uso y ubicación*, (captura de patrones de uso del usuario y de información de ubicación), entre otros.

Luego de analizar los trabajos de [10], [12], [123]–[128], en la Tabla IV, se presenta una clasificación de posibles amenazas, según el modelo de tres capas de IoT.

TABLA IV
TIPOS DE AMENAZAS EN IOT

Capa	Amenazas
Percepción,	- Nodo Falso (Fake Node), Interrupción del nodo (Node Outage), Captura del nodo, daño físico, robo y/o pérdida - Eavesdropping, Jamming, Forgery, Tampering - Ataque de tiempo (Timing Attack) - Ataque de reproducción (Replay Attack), otros
Red,	- MiTM, DoS, DDoS (DoS Distribuido), *Botnet*, - Jamming, Eavesdropping, Tampering, Phishing, Malware, Forgery, Sybil, - Amenaza avanzada persistente (APT), - Ataques de Exploits (aprovechamiento de vulnerabilidades como: no encriptación en la transmisión, cifrado no adecuado, no autenticación, no autorización, claves inseguras, puertos abiertos, programación insegura, etc.) - Ataques de inyección de código malicioso (Code Injection) - Ataque de almacenamiento (Storage Attack) - Usuarios fantasmas (Rogue user), - Nodos fantasmas (Rogue edge), otros
Aplicación	- DDoS, Spamming, Sybil, Phishing, Spoofing - Ataque malicioso de información privilegiada - Ataque a la confidencialidad / privacidad - Ataques de Malware: spyware, virus, gusanos, troyanos, etc. - Agotamiento de recursos o servicios, como consecuencia de otros ataques - Secuestro de sesiones (Session Hijacking) - Ataques de manipulación de parámetros (Tampering) - Ataques de Exploits, Code Injection, Cross-Site Scripting (XSS), Sql Injection, otros

Así también, después de la revisión y análisis de varios trabajos [10], [12], [123]–[128], en la Tabla V, se presenta una clasificación de los mecanismos de seguridad o contramedidas. Existen varios aspectos de seguridad y privacidad a tener en cuenta, ante posibles ataques que pueden ocurrir en cualquier capa y componente de un sistema IoT (nodos sensores, actuadores, WSN, red de comunicación, Gateway, nodos Fog/Edge, capa cloud, middleware y aplicación).

En síntesis, se debe manejar frameworks de seguridad de autenticación y control de acceso (autorización), comunicación segura de extremo a extremo, claves seguras (cifrado y encriptado seguro), protocolos seguros, dispositivos o herramientas de seguridad (cortafuegos, control de acceso, etc.), soluciones anti-malware, sistema de prevención/ detección de intrusos (IPS/ IDS), programación segura en todas las capas, controles físicos (de hardware, control biométrico), entre otros. También es prometedor el uso de nuevas alternativas como Blockchain, algoritmos de ML/IA y Redes Definidas por Software (SDN). Sin embargo, los desafíos en seguridad aún persisten, las agencias de supervisión, control y de estandarización deben trabajar en conjunto para desarrollar estándares de seguridad sólidos y robustos para todos los componentes de un sistema IoT.

TABLA V
MECANISMOS DE SEGURIDAD EN IOT

Capa	Mecanismos de defensa/protección de seguridad
Percepción	- Protocolos seguros y ligeros (TLS, DTLS), infraestructura de claves públicas (PKI) - Autorización segura: Control de acceso basado en atributos (ABAC), Control de acceso basado en roles (RBAC) - Criptografía Ligera de clave simétrica (algoritmos: AES (Advanced Encryption Standard), DES (Data Encryption Standard)), clave pública (algoritmos: RSA (Rivest, Shamir y Adleman), ECC (Elliptic Curve Cryptography)) y Criptografía Hash - Framework de seguridad embebido en nodos, algoritmos ML/IA, - Controles de hardware, controles biométricos, otros
Red	- Protocolos seguros (TLS, DTLS, IPSec,), Redes virtuales privadas (VPN), Infraestructura de claves públicas (PKI) - Framework de gestión de identidad - Framework adaptativo basado en riesgos - Uso de dispositivos o herramientas software (Ejm. firewall), para contrarrestar ataques como DoS, bloquear accesos no autorizados, etc. - Sistema de prevención/detección de intrusos (IPS/ IDS) - Redes Definidas por Software (SDN) para IoT - Seguridad basada en Sistemas de Reputación - Soluciones anti-malware, - Frameworks de seguridad integrada en gateways, nodos fog/edge, microdatacenters - BlockChain, Algoritmos ML/IA, - Controles de hardware, controles biométricos, otros
Aplicación	- Framework de seguridad integrada para autenticación y control de acceso (autorización) - Políticas de seguridad para usuarios - Soluciones anti-malware, cortafuegos - Protección de privacidad (privacidad de identidad, de datos, de uso y de localización) - Programación segura: Codificación/ validación de entradas, codificación de salidas para evitar Code Injections. - BlockChain, Algoritmos ML/IA, otros

B. Gobernanza en IoT

Según Almeida y otros [129], la Gobernanza en IoT, es un tema poco tratado y es un reto muy importante por resolver. IoT debido a su naturaleza, guarda relación con la gobernanza de Internet ("el desarrollo y aplicación de principios, normas, reglas, procedimientos y programas, que regulan la evolución y el uso de Internet" [129]). Para [130], Gobernanza de IoT, es considerar la integridad de los mecanismos de control, como el establecimiento de los principios de privacidad, seguridad, ética y competencia para hacer cumplir los derechos de los ciudadanos y consumidores y proteger sus datos. Para [131], los elementos importantes de la gobernanza de IoT están orientados a: *gobernanza del espacio, gobernanza del tiempo, gobernanza de dispositivos y gobernanza de datos*. En este sentido, hay muchos problemas por resolver, relacionados con la seguridad y privacidad (en dispositivos, las comunicaciones, gestión de datos, acceso y uso de servicios y aplicaciones), estándares de

interoperabilidad, uso de espacios (ejm. control de tráfico aéreo de drones), manejo del tiempo (ejm. coordinación de robots en una fábrica), gestión de recursos, gestión de los datos, separación de ámbitos: físico y cibernético (separación de usuarios y dispositivos), entre otros aspectos.

VII. CONCLUSIONES

Este trabajo orienta al lector, que está incursionando en el mundo de Internet de las Cosas (IoT), a tener un punto de partida para futuras investigaciones. Se analizó la literatura relacionada con el estado del arte de IoT: arquitecturas de referencia, plataformas IoT y paradigmas computacionales (Cloud, Fog y Edge Computing). Además, se identificó los componentes del ecosistema de IoT basado en el modelo de referencia de 3 capas (Percepción, Red y Middleware/ Aplicación) y, los problemas abiertos para investigaciones futuras. Luego presentamos nuestra principal contribución, que se centra en el análisis de Middleware IoT, orientado al almacenamiento y procesamiento de datos, donde hemos propuesto una arquitectura para la gestión de datos en un sistema IoT. Finalmente, se analizaron trabajos sobre seguridad y gobernanza en IoT.

AGRADECIMIENTOS

Este trabajo recibió apoyo tanto de la Universidad Técnica de Machala, Ecuador, como de la Universidade da Coruña, España, a través de un acuerdo interinstitucional. Un especial agradecimiento a sus autoridades.

REFERENCIAS

[1] A. Khanna and S. Kaur, 'Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture', *Comput. Electron. Agric.*, vol. 157, pp. 218–231, Feb. 2019, doi: 10.1016/j.compag.2018.12.039.

[2] I. Yaqoob *et al.*, 'Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges', *IEEE Wirel. Commun.*, vol. 24, no. 3, pp. 10–16, Jun. 2017, doi: 10.1109/MWC.2017.1600421.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, 'Internet of Things (IoT): A vision, architectural elements, and future directions', *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.

[4] L. Atzori, A. Iera, and G. Morabito, 'The Internet of Things: A survey', *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[5] A. Čolaković and M. Hadžialić, 'Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues', *Comput. Netw.*, vol. 144, pp. 17–39, Oct. 2018, doi: 10.1016/j.comnet.2018.07.017.

[6] S. Madakam, R. Ramaswamy, and S. Tripathi, 'Internet of Things (IoT): A Literature Review', *J. Comput. Commun.*, vol. 03, no. 05, pp. 164–173, 2015, doi: 10.4236/jcc.2015.35021.

[7] B. N. Silva, M. Khan, and K. Han, 'Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities', *Sustain. Cities Soc.*, vol. 38, pp. 697–713, Apr. 2018, doi: 10.1016/j.scs.2018.01.053.

[8] A. Botta, W. De Donato, V. Persico, and A. Pescapé, 'Integration of Cloud computing and Internet of Things: A survey', *Future Gener. Comput. Syst.*, vol. 56, pp. 684–700, Mar. 2016, doi: 10.1016/j.future.2015.09.021.

[9] 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. Tutor.*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[10] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, 'IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey', *Sensors*, vol. 18, no. 9, p. 2796, Aug. 2018, doi: 10.3390/s18092796.

[11] P. P. Ray, 'A survey on Internet of Things architectures', *J. King Saud Univ. - Comput. Inf. Sci.*, Oct. 2016, doi: 10.1016/j.jksuci.2016.10.003.

[12] 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.

[13] B. Omoniwa, R. Hussain, M. A. Javed, S. H. Bouk, and S. A. Malik, 'Fog/Edge Computing-Based IoT (FECIoT): Architecture, Applications, and Research Issues', *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4118–4149, Jun. 2019, doi: 10.1109/JIOT.2018.2875544.

[14] P. P. Ray, 'A survey of IoT cloud platforms', *Future Comput. Inform. J.*, vol. 1, pp. 35–46, Dec. 2016, doi: 10.1016/j.fcij.2017.02.001.

[15] W. Kassab and K. A. Darabkh, 'A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations', *J. Netw. Comput. Appl.*, vol. 163, p. 102663, Aug. 2020, doi: 10.1016/j.jnca.2020.102663.

[16] A. H. M. Aman, E. Yadegaridehkordi, Z. S. Attarbashi, R. Hassan, and Y. Park, 'A Survey on Trend and Classification of Internet of Things Reviews', *IEEE Access*, vol. 8, pp. 111763–111782, 2020, doi: 10.1109/ACCESS.2020.3002932.

[17] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, 'Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios', *IEEE Access*, vol. 8, pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[18] J. M. Talavera *et al.*, 'Review of IoT applications in agro-industrial and environmental fields', *Comput. Electron. Agric.*, vol. 142, pp. 283–297, Nov. 2017, doi: 10.1016/j.compag.2017.09.015.

[19] H. Muccini and M. T. Moghaddam, 'IoT Architectural Styles: A Systematic Mapping Study', in *Software Architecture*, vol. 11048, C. E. Cuesta, D. Garlan, and J. Pérez, Eds. Cham: Springer International Publishing, 2018, pp. 68–85.

[20] S. Lee, M. Bae, and H. Kim, 'Future of IoT Networks: A Survey', *Appl. Sci.*, vol. 7, no. 10, p. 1072, Oct. 2017, doi: 10.3390/app7101072.

[21] R. K. Naha *et al.*, 'Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions', *IEEE Access*, vol. 6, pp. 47980–48009, 2018, doi: 10.1109/ACCESS.2018.2866491.

[22] K. J. Singh and D. S. Kapoor, 'Create Your Own Internet of Things: A survey of IoT platforms.', *IEEE Consum. Electron. Mag.*, vol. 6, no. 2, pp. 57–68, Apr. 2017, doi: 10.1109/MCE.2016.2640718.

[23] S. Sinche *et al.*, 'A Survey of IoT Management Protocols and Frameworks', *IEEE Commun. Surv. Tutor.*, pp. 1–1, 2019, doi: 10.1109/COMST.2019.2943087.

[24] M. Ammar, G. Russello, and B. Crispo, 'Internet of Things: A survey on the security of IoT frameworks', *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018, doi: 10.1016/j.jisa.2017.11.002.

[25] J. Berrú-Ayala, D. Hernandez-Rojas, P. Morocho-Díaz, J. Novillo-Vicuña, B. Mazon-Olivo, and A. Pan, 'SCADA System Based on IoT for Intelligent Control of Banana Crop Irrigation', *Appl. Technol. ICAT 2019 Commun. Comput. Inf. Sci.*, vol. 1193, pp. 243–256, 2020, doi: https://doi.org/10.1007/978-3-030-42517-3_19.

[26] V. Sharma, J. D. Lim, J. N. Kim, and I. You, 'SACA: Self-Aware Communication Architecture for IoT Using Mobile Fog Servers', *Mob. Inf. Syst.*, vol. 2017, pp. 1–17, 2017, doi: 10.1155/2017/3273917.

[27] Y.-G. Yue and P. He, 'A Comprehensive Survey on the Reliability of Mobile Wireless Sensor Networks: Taxonomy, Challenges, and Future Directions', *Inf. Fusion*, Mar. 2018, doi: 10.1016/j.inffus.2018.03.005.

[28] O. Hahm, E. Baccelli, H. Petersen, and N. Tsiftes, 'Operating Systems for Low-End Devices in the Internet of Things: A Survey', *IEEE Internet Things J.*, vol. 3, no. 5, pp. 720–734, Oct. 2016, doi: 10.1109/JIOT.2015.2505901.

[29] P. P. Ray and N. Kumar, 'SDN/NFV architectures for edge-cloud oriented IoT: A systematic review', *Comput. Commun.*, vol. 169, pp. 129–153, Mar. 2021, doi: 10.1016/j.comcom.2021.01.018.

[30] F. Ullah and M. Ali Babar, 'Architectural Tactics for Big Data Cybersecurity Analytics Systems: A Review', *J. Syst. Softw.*, vol. 151, pp. 81–118, May 2019, doi: 10.1016/j.jss.2019.01.051.

[31] S. Shadroo and A. M. Rahmani, 'Systematic Survey of Big Data and Data Mining in Internet of Things', *Comput. Netw.*, Apr. 2018, doi: 10.1016/j.comnet.2018.04.001.

[32] J. Al Dakheel, C. Del Pero, N. Aste, and F. Leonforte, 'Smart buildings features and key performance indicators: A review', *Sustain. Cities Soc.*, vol. 61, p. 102328, Oct. 2020, doi: 10.1016/j.scs.2020.102328.

[33] L. Butler, T. Yigitcanlar, and A. Paz, 'Smart Urban Mobility Innovations: A Comprehensive Review and Evaluation', *IEEE Access*, vol. 8, pp. 196034– 196049, 2020, doi:10.1109/ACCESS.2020.3034596.

[34] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, 'The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective', *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2586–2595, Nov. 2017, doi: 10.1109/JSAC.2017.2760478.

[35] P. K. Senyo, E. Addae, and R. Boateng, 'Cloud computing research: A review of research themes, frameworks, methods and future research directions', *Int. J. Inf. Manag.*, vol. 38, no. 1, pp. 128–139, Feb. 2018, doi: 10.1016/j.ijinfomgt.2017.07.007.

[36] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, 'Middleware for Internet of Things: A Survey', *IEEE Internet Things J.*, vol. 3, no. 1, pp. 70– 95, Feb. 2016, doi:10.1109/JIOT.2015.2498900.

[37] J. Zhang, M. Ma, P. Wang, and X. Sun, 'Middleware for the Internet of Things: A survey on requirements, enabling technologies, and solutions', *J. Syst. Archit.*, vol. 117, p. 102098, Aug. 2021, doi: 10.1016/j.sysarc.2021.102098.

[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, Apr. 2018, doi: 10.1109/JIOT.2018.2796561.

[39] ITU-T, 'Serie Y.2060: Global Information Infraestructure, Internet Protocol Aspects and Next - Generation Networks'. International Telecommunication Union, Jun. 2012, Accessed: Apr. 18, 2019. [Online]. Available: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-Y.2060-201206-I!!PDF-E&type=items.

[40] M. Bauer *et al.*, 'IoT Reference Model', in *Enabling Things to Talk*, A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. van Kranenburg, S. Lange, and S. Meissner, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 113–162.

[41] CISCO., 'The Internet of Things Reference Model.', 2014. http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf (accessed Apr. 24, 2018).

[42] IEEE P2413, 'Standard for an Architectural Framework for the Internet of Things (IoT) IEEE P2413.', 2016. http://grouper.ieee.org/groups/2413/Intro-to-IEEE-P2413.pdf (accessed Sep. 10, 2019).

[43] IEEE P2413, 'Standard for an Architectural Framework for the Internet of Things (IoT).', 2019. https://standards.ieee.org/develop/project/2413.html (accessed Sep. 10, 2019).

[44] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, 'A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective', *IEEE Internet Things J.*, vol. 1, no. 4, pp. 349–359, Aug. 2014, doi: 10.1109/JIOT.2014.2337336.

[45] IIC, 'The Industrial Internet of Things Volume G1: Reference Architecture.', *Industrial Internet Consortium*, 2017. https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf (accessed Apr. 25, 2018).

[46] VDI/VDE, 'Reference Architecture Model Industrie 4.0 (RAMI4.0).', 2015. https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/januar/GMA_Status_Report__Reference_Archtitecture_Model_Industrie_4.0__RAMI_4.0_/GMA-Status-Report-RAMI-40-July-2015.pdf (accessed Apr. 25, 2018).

[47] ISO/IEC, 'Information technology – Internet of Things Reference Architecture (IoT RA).', 2016. https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf (accessed Apr. 25, 2018).

[48] W3C, 'Web of Things (WoT) Architecture', 2019. https://w3c.github.io/wot-architecture/#sec-functional-requirement (accessed Sep. 12, 2019).

[49] J. Kiljander *et al.*, 'Semantic Interoperability Architecture for Pervasive Computing and Internet of Things', *IEEE Access*, vol. 2, pp. 856–873, 2014, doi: 10.1109/ACCESS.2014.2347992.

[50] C. Shang-Liang, C. Yun-Yao, and H. Chiang, 'A New Approach to Integrate Internet-of-Things and Software-as-a-Service Model for Logistic Systems: A Case Study', *Sensors*, vol. 14, no. 4, pp. 6144–6164, Mar. 2014, doi: 10.3390/s140406144.

[51] C. Sarkar, A. U. Nambi S. N., R. V. Prasad, A. Rahim, R. Neisse, and G. Baldini, 'DIAT: A Scalable Distributed Architecture for IoT', *IEEE Internet Things J.*, vol. 2, no. 3, pp. 230–239, Jun. 2015, doi: 10.1109/JIOT.2014.2387155.

[52] Y. Xu and A. Helal, 'Scalable Cloud–Sensor Architecture for the Internet of Things', *IEEE Internet Things J.*, vol. 3, no. 3, pp. 285–298, Jun. 2016, doi: 10.1109/JIOT.2015.2455555.

[53] O. Kaiwartya *et al.*, 'Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects', *IEEE Access*, vol. 4, pp. 5356–5373, 2016, doi: 10.1109/ACCESS.2016.2603219.

[54] P. A. Akiki, A. K. Bandara, and Y. Yu, 'Visual Simple Transformations: Empowering End-Users to Wire Internet of Things Objects', *ACM Trans. Comput.-Hum. Interact.*, vol. 24, no. 2, pp. 1–43, Apr. 2017, doi: 10.1145/3057857.

[55] V. Beltran, A. F. Skarmeta, and P. M. Ruiz, 'An ARM-Compliant Architecture for User Privacy in Smart Cities: SMARTIE—Quality by Design in the IoT', *Wirel. Commun. Mob. Comput.*, vol. 2017, pp. 1–13, 2017, doi: 10.1155/2017/3859836.

[56] P. K. Illa and N. Padhi, 'Practical Guide to Smart Factory Transition Using IoT, Big Data and Edge Analytics', *IEEE Access*, vol. 6, pp. 55162–55170, 2018, doi: 10.1109/ACCESS.2018.2872799.

[57] O. Novo, 'Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT', *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018, doi: 10.1109/JIOT.2018.2812239.

[58] J. Ploennigs, A. Ba, and M. Barry, 'Materializing the Promises of Cognitive IoT: How Cognitive Buildings Are Shaping the Way', *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2367–2374, Aug. 2018, doi: 10.1109/JIOT.2017.2755376.

[59] M. Aazam, S. Zeadally, and K. A. Harras, 'Fog Computing Architecture, Evaluation, and Future Research Directions', *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 46–52, May 2018, doi: 10.1109/MCOM.2018.1700707.

[60] P. Mell and T. Grance, 'The NIST Definition of Cloud Computing'. National Institute of Standards and Technology, 2011, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[61] G. Pallis, 'Cloud Computing: The New Frontier of Internet Computing', *IEEE Internet Comput.*, vol. 14, no. 5, pp. 70–73, Sep. 2010, doi: 10.1109/MIC.2010.113.

[62] R. Roman, J. Lopez, and M. Mambo, 'Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges', *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018, doi: 10.1016/j.future.2016.11.009.

[63] D. Hernández, Mazón-Olivo, Bertha, and Escudero, Carlos, 'Internet de las cosas (IoT)', in *Análisis de Datos Agropecuarios*, 1st ed., I. Ramírez-Morales and B. Mazón-Olivo, Eds. Machala-Ecuador: Universidad Técnica de Machala, 2018, pp. 74–100.

[64] K. Bilal, O. Khalid, A. Erbad, and S. U. Khan, 'Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers', *Comput. Netw.*, vol. 130, pp. 94–120, Jan. 2018, doi: 10.1016/j.comnet.2017.10.002.

[65] H. Elazhary, 'Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions', *J. Netw. Comput. Appl.*, vol. 128, pp. 105–140, Feb. 2019, doi: 10.1016/j.jnca.2018.10.021.

[66] I. Lee and K. Lee, 'The Internet of Things (IoT): Applications, investments, and challenges for enterprises', *Bus. Horiz.*, vol. 58, no. 4, pp. 431–440, Jul. 2015, doi: 10.1016/j.bushor.2015.03.008.

[67] O. Voitovych, L. Kupershtein, O. Shulyatitska, and V. Malyushytskyy, 'The authentication method in wireless sensor network based on trust model', in *2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, Kiev, May 2017, pp. 993–997, doi: 10.1109/UKRCON.2017.8100398.

[68] D. Hernández-Rojas, T. Fernández-Caramés, P. Fraga-Lamas, and C. Escudero, 'Design and Practical Evaluation of a Family of Lightweight Protocols for Heterogeneous Sensing through BLE Beacons in IoT Telemetry Applications', *Sensors*, vol. 18, no. 2, p. 57, Dec. 2017, doi: 10.3390/s18010057.

[69] D. Hernandez-Rojas, B. Mazon-Olivo, J. Novillo-Vicuña, C. Escudero-Cascon, A. Pan-Bermudez, and G. Belduma-Vacacela, 'IoT Android Gateway for Monitoring and Control a WSN', in *Technology Trends. Communications in Computer and Information Science*, vol. 798, M.

Botto-Tobar, N. Esparza-Cruz, J. León-Acurio, N. Crespo-Torres, and M. Beltrán-Mora, Eds. Cham: Springer International Publishing, 2018, pp. 18–32.

[70] J. Novillo-Vicuña, D. Hernández-Rojas, B. Mazón-Olivo, J. Molina Ríos, and O. Cárdenas-Villavicencio, *Arduino y el Internet de las Cosas*, Primera. Alicante, España: 3Ciencias, Área de Innovación y Desarrollo, S.L, 2018.

[71] J. P. Novillo-Vicuña, D. L. Hernandez-Rojas, B. Mazon-Olivo, and K. D. Correa-Elizaldes, 'Monitoreo inalámbrico de señales eléctricas de voltaje 110/220V a través de Arduino', *Alternativas*, vol. 19, no. 1, Jun. 2019, doi: 10.23878/alternativas.v19i1.198.

[72] R. Fantacci, T. Pecorella, R. Viti, and C. Carlini, 'A network architecture solution for efficient IOT WSN backhauling: challenges and opportunities', *IEEE Wirel. Commun.*, vol. 21, no. 4, pp. 113–119, Aug. 2014, doi: 10.1109/MWC.2014.6882303.

[73] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, 'The Future of Healthcare Internet of Things: A Survey of Emerging Technologies', *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 1121–1167, Secondquarter 2020, doi: 10.1109/COMST.2020.2973314.

[74] A. S. Albahri *et al.*, 'IoT-based telemedicine for disease prevention and health promotion: State-of-the-Art', *J. Netw. Comput. Appl.*, vol. 173, p. 102873, Jan. 2021, doi: 10.1016/j.jnca.2020.102873.

[75] N. Du, H. Schmidt, and I. Polian, 'Low-power emerging memristive designs towards secure hardware systems for applications in internet of things', *Nano Mater. Sci.*, Jan. 2021, doi: 10.1016/j.nanoms.2021.01.001.

[76] S. S. Dhanda, B. Singh, and P. Jindal, Eds., 'Wireless Technologies in IoT: Research Challenges', in *Engineering Vibration, Communication and Information Processing*, Lecture Notes in Electrical Engineering., vol. 478, Springer Singapore, 2018, pp. 229–239.

[77] Pareek, Mani and Buriya,Sushil, 'A Study of Link Layer Protocols in IOT', *Int. J. Future Revolut. Comput. Sci. Commun. Eng.*, vol. 4, no. International Journal on Future Revolution in Computer Science&Communication Engineering, pp. 355–359, Feb. 2018.

[78] I. Yaqoob, I. A. T. Hashem, Y. Mehmood, A. Gani, S. Mokhtar, and S. Guizani, 'Enabling Communication Technologies for Smart Cities', *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 112–120, Jan. 2017, doi: 10.1109/MCOM.2017.1600232CM.

[79] G. Durante, W. Beccaro, and H. E. M. Peres, 'ACPT IoT Protocols Comparison for Wireless Sensors Network Applied to Marine Environment Acoustic Monitoring', *IEEE Lat. Am. Trans.*, vol. 16, no. 11, Art. no. 11, 2018.

[80] Z. Sheng, C. Mahapatra, C. Zhu, and V. Leung, 'Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT', *Access IEEE*, vol. 3, pp. 622–637, 2015, doi: 10.1109/ACCESS.2015.2435000.

[81] Z. Sheng, C. Mahapatra, C. Zhu, and V. Leung, 'Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT', *Access IEEE*, vol. 3, pp. 622–637, 2015, doi: 10.1109/ACCESS.2015.2435000.

[82] T. Hoeschele, C. Dietzel, D. Kopp, F. H. P. Fitzek, and M. Reisslein, 'Importance of Internet Exchange Point (IXP) infrastructure for 5G: Estimating the impact of 5G use cases', *Telecommun. Policy*, vol. 45, no. 3, p. 102091, Apr. 2021, doi: 10.1016/j.telpol.2020.102091.

[83] Y. Wei, M. Peng, and Y. Liu, 'Intent-based networks for 6G: Insights and challenges', *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 270–280, Aug. 2020, doi: 10.1016/j.dcan.2020.07.001.

[84] M. Dadkhah, M. Lagzian, F. Rahimnia, and K. Kimiafar, 'What Do Websites Say about Internet of Things Challenges? A Text Mining Approach', *Sci. Technol. Libr.*, vol. 39, no. 2, pp. 125–141, Apr. 2020, doi: 10.1080/0194262X.2020.1715320.

[85] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, 'Secure integration of IoT and Cloud Computing', *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018, doi: 10.1016/j.future.2016.11.031.

[86] J. Kreps, N. Narkhede, and J. Rao, 'Kafka: a Distributed Messaging System for Log Processing', p. 7.

[87] 'Apache Kafka.', *Apache Kafka*. https://kafka.apache.org/ (accessed Apr. 12, 2018).

[88] K. Zhou, C. Fu, and S. Yang, 'Big data driven smart energy management: From big data to big insights', *Renew. Sustain. Energy Rev.*, vol. 56, pp. 215–225, Apr. 2016, doi: 10.1016/j.rser.2015.11.050.

[89] X. Nie, T. Fan, B. Wang, Z. Li, A. Shankar, and A. Manickam, 'Big Data analytics and IoT in Operation safety management in Under Water Management', *Comput. Commun.*, vol. 154, pp. 188–196, Mar. 2020, doi: 10.1016/j.comcom.2020.02.052.

[90] Y. Zhang, S. Ren, Y. Liu, T. Sakao, and D. Huisingh, 'A framework for Big Data driven product lifecycle management', *J. Clean. Prod.*, vol. 159, pp. 229–240, Aug. 2017, doi: 10.1016/j.jclepro.2017.04.172.

[91] B. Mazon-Olivo, D. Hernández-Rojas, J. Maza-Salinas, and A. Pan, 'Rules engine and complex event processor in the context of internet of things for precision agriculture', *Comput. Electron. Agric.*, vol. 154, pp. 347–360, Nov. 2018, doi: 10.1016/j.compag.2018.09.013.

[92] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, 'IoT-based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges', *IEEE Internet Things J.*, pp. 1–1, 2016, doi: 10.1109/JIOT.2016.2619369.

[93] A. L. Cravero, 'Arquitecturas de Big Data para el análisis del Cambio Climático: Mapeo Sistemático de Estudios', *IEEE Lat. Am. Trans.*, vol. 18, no. 10, Art. no. 10, 2020.

[94] A. Corbellini, C. Mateos, A. Zunino, D. Godoy, and S. Schiaffino, 'Persisting big-data: The NoSQL landscape', *Inf. Syst.*, vol. 63, pp. 1–23, Jan. 2017, doi: 10.1016/j.is.2016.07.009.

[95] A. Makris, K. Tserpes, V. Andronikou, and D. Anagnostopoulos, 'A Classification of NoSQL Data Stores Based on Key Design Characteristics', *Procedia Comput. Sci.*, vol. 97, pp. 94–103, 2016, doi: 10.1016/j.procs.2016.08.284.

[96] 'DB-Engines Ranking.' https://db-engines.com/en/ranking (accessed Apr. 12, 2018).

[97] 'Apache Storm'. https://storm.apache.org/ (accessed Feb. 16, 2021).

[98] 'Apache Flink: Stateful Computations over Data Streams'. https://flink.apache.org/ (accessed Feb. 16, 2021).

[99] 'Apache Spark™ - Unified Analytics Engine for Big Data'. https://spark.apache.org/ (accessed Feb. 16, 2021).

[100] Garnert, 'Magic Quadrant for Data Integration Tools', *Gartner*, 2020. https://www.gartner.com/en/documents/3955823/magic-quadrant-for-data-integration-tools (accessed Oct. 05, 2020).

[101] 'Market Guide for Data Virtualization', *Gartner*. https://www.gartner.com/en/documents/3893219/market-guide-for-data-virtualization (accessed Feb. 16, 2021).

[102] D. Abadi *et al.*, 'The Seattle Report on Database Research', *ACM SIGMOD Rec.*, vol. 48, no. 4, pp. 44–53, Feb. 2020, doi: 10.1145/3385658.3385668.

[103] 'Apache Superset'. https://superset.apache.org/ (accessed Feb. 16, 2021).

[104] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, 'Machine learning for Internet of Things data analysis: A survey', *Digit. Commun. Netw.*, Oct. 2017, doi: 10.1016/j.dcan.2017.10.002.

[105] P. Moens *et al.*, 'Scalable Fleet Monitoring and Visualization for Smart Machine Maintenance and Industrial IoT Applications', *Sensors*, vol. 20, no. 15, Art. no. 15, Jan. 2020, doi: 10.3390/s20154308.

[106] H. Sánchez, C. González-Contreras, J. E. Agudo, and M. Macías, 'IoT and iTV for Interconnection, Monitoring, and Automation of Common Areas of Residents', *Appl. Sci.*, vol. 7, no. 7, Art. no. 7, Jul. 2017, doi: 10.3390/app7070696.

[107] M. Ijaz *et al.*, 'Intelligent Fog-Enabled Smart Healthcare System for Wearable Physiological Parameter Detection', *Electronics*, vol. 9, no. 12, Art. no. 12, Dec. 2020, doi: 10.3390/electronics9122015.

[108] A. Kirimtat, O. Krejcar, A. Kertesz, and M. F. Tasgetiren, 'Future Trends and Current State of Smart City Concepts: A Survey', *IEEE Access*, vol. 8, pp. 86448– 86467, 2020, doi: 10.1109/ACCESS.2020.2992441.

[109] A. H. Alavi, P. Jiao, W. G. Buttlar, and N. Lajnef, 'Internet of Things-enabled smart cities: State-of-the-art and future trends', *Measurement*, vol. 129, pp. 589– 606, Dec. 2018, doi: 10.1016/j.measurement.2018.07.067.

[110] K. M. Rashid, J. Louis, and K. K. Fiawoyife, 'Wireless electric appliance control for smart buildings using indoor location tracking and BIM-based virtual environments', *Autom. Constr.*, vol. 101, pp. 48–58, May 2019, doi: 10.1016/j.autcon.2019.01.005.

[111] Z. Rashid, J. Melià-Seguí, R. Pous, and E. Peig, 'Using Augmented Reality and Internet of Things to improve accessibility of people with motor disabilities in the context of Smart Cities', *Future Gener. Comput. Syst.*, vol. 76, pp. 248–261, Nov. 2017, doi: 10.1016/j.future.2016.11.030.

[112] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, 'Applications of Artificial Intelligence and Machine learning in smart cities', *Comput. Commun.*, vol. 154, pp. 313–323, Mar. 2020, doi: 10.1016/j.comcom.2020.02.069.

[113] J. Salas, F. de B. Vidal, and F. Martínez-Trinidad, 'Deep Learning: Current State', *IEEE Lat. Am. Trans.*, vol. 17, no. 12, Art. no. 12, 2019.
[114] S. Ghosh, 'Smart homes: Architectural and engineering design imperatives for smart city building codes', in *2018 Technologies for Smart-City Energy Security and Power (ICSESP)*, Mar. 2018, pp. 1–4, doi: 10.1109/ICSESP.2018.8376676.
[115] U. Shafi, R. Mumtaz, J. García-Nieto, S. A. Hassan, S. A. R. Zaidi, and N. Iqbal, 'Precision Agriculture Techniques and Practices: From Considerations to Applications', *Sensors*, vol. 19, no. 17, p. 3796, Sep. 2019, doi: 10.3390/s19173796.
[116] 'An implementation for Smart Manufacturing Information System (SMIS) from an industrial practice survey', *Comput. Ind. Eng.*, vol. 151, p. 106938, Jan. 2021, doi: 10.1016/j.cie.2020.106938.
[117] R. P. Rolle, V. de O. Martucci, and E. P. Godoy, 'Architecture for Digital Twin implementation focusing on Industry 4.0', *IEEE Lat. Am. Trans.*, vol. 18, no. 5, Art. no. 5, Apr. 2020.
[118] V. Roblek, M. Meško, and A. Krapež, 'Una visión compleja de la industria 4.0', *SAGE Open*, vol. 6, no. 2, p. 2158244016653987, Apr. 2016, doi: 10.1177/2158244016653987.
[119] H. Ahuett-Garza and T. Kurfess, 'A brief discussion on the trends of habilitating technologies for Industry 4.0 and Smart manufacturing', *Manuf. Lett.*, vol. 15, pp. 60–63, Jan. 2018, doi: 10.1016/j.mfglet.2018.02.011.
[120] I. Docherty, G. Marsden, and J. Anable, 'The governance of smart mobility', *Transp. Res. Part Policy Pract.*, vol. 115, pp. 114–125, Sep. 2018, doi: 10.1016/j.tra.2017.09.012.
[121] 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.
[122] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, 'NormaChain: A Blockchain-Based Normalized Autonomous Transaction Settlement System for IoT-Based E-Commerce', *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4680–4693, Jun. 2019, doi: 10.1109/JIOT.2018.2877634.
[123] N. Tariq *et al.*, 'The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey', *Sensors*, vol. 19, no. 8, Art. no. 8, Jan. 2019, doi: 10.3390/s19081788.
[124] T. Nandy *et al.*, 'Review on Security of Internet of Things Authentication Mechanism', *IEEE Access*, vol. 7, pp. 151054–151089, 2019, doi: 10.1109/ACCESS.2019.2947723.
[125] S. Khanam, I. B. Ahmedy, M. Y. Idna Idris, M. H. Jaward, and A. Q. Bin Md Sabri, 'A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things', *IEEE Access*, vol. 8, pp. 219709–219743, 2020, doi: 10.1109/ACCESS.2020.3037359.
[126] M. M. Ogonji, G. Okeyo, and J. M. Wafula, 'A survey on privacy and security of Internet of Things', *Comput. Sci. Rev.*, vol. 38, p. 100312, Nov. 2020, doi: 10.1016/j.cosrev.2020.100312.
[127] R. Yugha and S. Chithra, 'A survey on technologies and security protocols: Reference for future generation IoT', *J. Netw. Comput. Appl.*, vol. 169, p. 102763, Nov. 2020, doi: 10.1016/j.jnca.2020.102763.
[128] M. Mahbub, 'Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics', *J. Netw. Comput. Appl.*, vol. 168, p. 102761, Oct. 2020, doi: 10.1016/j.jnca.2020.102761.
[129] V. A. F. Almeida, D. Doneda, and M. Monteiro, 'Governance Challenges for the Internet of Things', *IEEE Internet Comput.*, vol. 19, no. 4, pp. 56–59, Jul. 2015, doi: 10.1109/MIC.2015.86.
[130] S.-I. Chang, L.-M. Chang, and J.-C. Liao, 'Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach', *Inf. Manage.*, vol. 57, no. 6, p. 103335, Sep. 2020, doi: 10.1016/j.im.2020.103335.
[131] M. Maheswaran and S. Misra, 'Towards a social governance framework for Internet of Things', in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Dec. 2015, pp. 801–806, doi: 10.1109/WF-IoT.2015.7389156.

Bertha Mazon-Olivo, es Ingeniera en Sistemas y Magíster en Informática Aplicada por la Escuela Superior Politécnica de Chimborazo, de Ecuador. Profesora Titular en la Universidad Técnica de Machala. Es estudiante del programa doctoral en Tecnologías de la Información y las Comunicaciones en Universidade da Coruña, España. Sus líneas de investigación son: Internet de las Cosas y Ciencia de Datos. Cuenta con varias publicaciones indexadas.

Alberto Pan, es Director Técnico de Denodo y Profesor Titular de la Universidad de A Coruña, en España. Doctor en Ciencias de la Computación en la Universidad de A Coruña en 2002. Sus intereses de investigación se centran en la extracción e integración de datos y la automatización de la web. Ha dirigido varios proyectos a nivel nacional e internacional. Es autor de numerosas publicaciones en revistas científicas y actas de congresos.