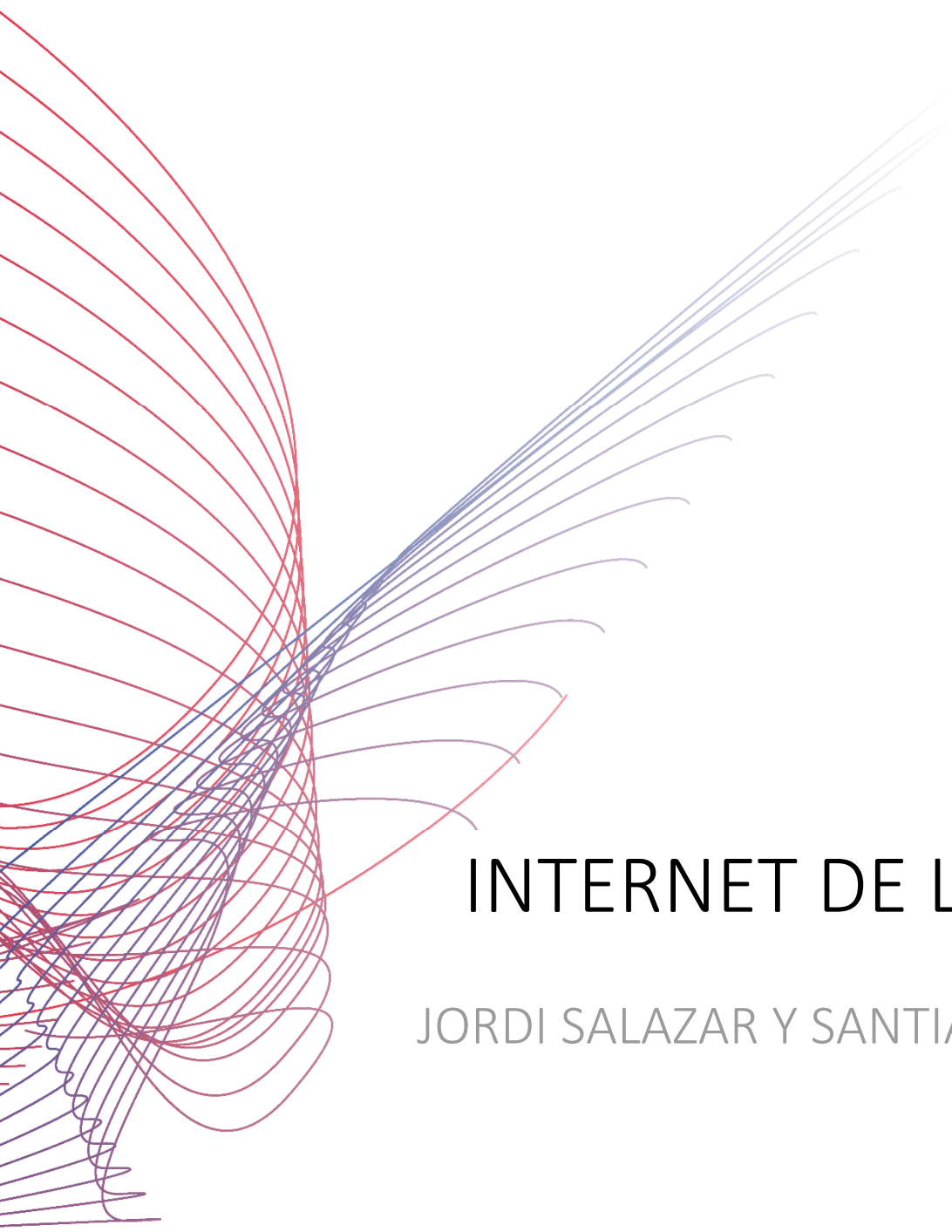
en cs de sk es

TECH pedia



INTERNET DE LAS COSAS

JORDI SALAZAR Y SANTIAGO SILVESTRE

Título: Internet de las cosas
Autor: Jordi Salazar y Santiago Silvestre
Publicado por: České vysoké učení technické v Praze
Fakulta elektrotechnická
Dirección de contacto: Technická 2, Praha 6, Czech Republic
Número de teléfono: +420 224352084
Print: (only electronic form)
Número de páginas: 34
Edición: Versión de prueba

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea.
Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

NOTAS EXPLICATIVAS

	Definición
	Interesante
	Nota
	Ejemplo
	Resumen
	Ventajas
	Desventajas

ANOTACIÓN

Este es un curso de introducción a la IoT (Internet de las cosas). En los capítulos primeros capítulos se introducen los conceptos básicos sobre la IoT. Seguidamente se presentan nociones básicas sobre el protocolo de internet IPv6 que es el más utilizado en el entorno de la IoT y se describen las principales aplicaciones, el estado actual del mercado y las tecnologías que permiten la existencia de la IoT. Finalmente se analizan los retos de futuro que se consideran más importantes.

OBJETIVOS

Al final del estudio de este curso el alumno será capaz de entender los conceptos básicos sobre IoT y hacerse una idea de las posibilidades que ofrecen las aplicaciones basadas en este entorno.

LITERATURA

[1] R. H. Weber, (2010). "Internet of Things - New Security and Privacy Challenges". Computer Law & Security Review 26: 23-30.

[2] Dave Evans. (2011). How the Next Evolution of the Internet Is Changing Everything. Cisco Internet of Things White Paper.

[3] Stephen E. Deering and Robert M. Hinden (1998). RFC 2460, Internet Protocol, Version 6 (IPv6) Specification.

[4] Charith Perera et. al. (2014). Sensing as a Service Model for Smart Cities Supported by Internet of Things. Transactions on Emerging Telecommunications Technology 25 (1): 81–93.

[5] Ma HD. (2011). “Internet of things: Objectives and scientific challenges”. Journal of computer science and technology 26 (6): 919-924.

[6] In Lee and Kyoochun Lee (2015) “The Internet of Things (IoT): Applications, investments, and challenges for enterprises, *Business Horizons*, 58, 431-440.

[7] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.

[8] Ala Al-Fuqaha et al. (2015) “Internet of Things: A survey on enabling technologies, protocols and applications”, *IEEE Communications Surveys & Tutorials*. DOI 10.1109/COMST.2015.2444095

[9] The European Technology Platform on Smart Systems Integration (2008). "Internet of Things in 2020: A Roadmap for the future"

Indice

1 ¿A qué nos referimos con el término IoT? Definición, historia y características de la IoT.

Este capítulo describe algunos aspectos destacados importantes en la historia de la **IoT (*Internet de las cosas*)**. Hoy en día, la arquitectura de la información basada en Internet permite el intercambio de bienes y servicios entre todos los elementos, equipos y objetos conectados a la red. La IoT se refiere a la interconexión en red de todos los objetos cotidianos, que a menudo están equipados con algún tipo de inteligencia. En este contexto, Internet puede ser también una plataforma para dispositivos que se comunican electrónicamente y comparten información y datos específicos con el mundo que les rodea. Así, la IoT puede verse como una verdadera evolución de lo que conocemos como Internet añadiendo una interconectividad más extensa, una mejor percepción de la información y servicios inteligentes más completos. En su mayor parte, se utilizó la Internet para protocolos orientados a la conexión de aplicaciones como **HTTP** (***Protocolo de transferencia de hipertexto)*** y **SMTP** (***Simple Mail Transfer Protocol***). Sin embargo, hoy en día un gran número de dispositivos inteligentes se comunican entre ellos y con otros sistemas de control. Este concepto se conoce como **M2M** (***comunicaciones de máquina a máquina***).

IoT (***Internet of things/Internet de las cosas***) es una arquitectura emergente basada en la Internet global que facilita el intercambio de bienes y servicios entre redes de la cadena de suministro y que tiene un impacto importante en la seguridad y privacidad de los actores involucrados [1].

Algunos aspectos destacados en la historia de la IoT son los siguientes:

- El término: Internet de las Cosas fue utilizado por primera vez por Kevin Ashton en 1999 que estaba trabajando en el campo de la tecnología **RFID** en red (***identificación por radiofrecuencia***) y tecnologías de detección emergentes.
- Sin embargo, la IoT "nació" en algún momento entre 2008 y 2009 [2].
- En 2010, el número de objetos físicos cotidianos y dispositivos conectados a Internet fue de alrededor de 12,5 mil millones. En la actualidad hay cerca de 25 mil millones de dispositivos conectados a la IoT. Más o menos un dispositivo inteligente por persona [2].
- Se espera que el número de dispositivos inteligentes o "cosas" conectados a la IoT será de más de 50 mil millones en 2020.

La IoT introduce un cambio radical en la calidad de vida de las personas, ofreciendo una gran cantidad de nuevas oportunidades de acceso a datos, servicios específicos en la educación, en seguridad, asistencia sanitaria o en el transporte, entre otros campos. Por otra parte, será la clave para aumentar la productividad de las empresas, ofreciendo una amplia distribución de la red, redes locales inteligentes de dispositivos inteligentes y nuevos servicios que pueden ser personalizados según las necesidades del cliente. La IoT trae beneficios de mejora de la gestión y el

seguimiento de los activos y de los productos, aumenta la cantidad de datos de información y permite la optimización de equipos y uso de los recursos que puede traducirse en ahorro de costes. Además, ofrece la oportunidad de crear nuevos dispositivos interconectados inteligentes y explorar nuevos modelos de negocio.

2 Introducción a IPv6

Este capítulo ofrece una introducción básica a IPv6: Protocolo de Internet versión 6, que es necesaria para la IoT.

2.1 Introducción a IPv6

Cuando utilizamos Internet para cualquier actividad, ya sea por correo electrónico, transmisión de datos, navegación web, descarga de archivos, imágenes o vídeos o cualquier otro servicio o aplicación, la comunicación entre los diferentes elementos de la red y nuestro propio ordenador, portátil o teléfono inteligente, utiliza un protocolo: El **IP *(protocolo de Internet)*** que especifica el formato técnico de los paquetes y el esquema de direccionamiento para que las computadoras se comunican a través de una red.

IPv6 (***Internet protocol version 6***) es la versión más reciente del IP, el protocolo de comunicaciones que proporciona un sistema de identificación y la ubicación de los equipos en las redes y las rutas de tráfico a través de Internet.

Con el fin de conectar cualquier dispositivo a Internet es necesario proporcionar una dirección IP al dispositivo. La primera versión de un Protocolo de Internet utilizado públicamente era **IPv4** ***(protocolo de Internet versión 4)***. Este protocolo fue creado por la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA). DARPA es una agencia del Departamento de Defensa de Estados Unidos responsable del desarrollo de las tecnologías emergentes, principalmente para aplicaciones militares creada en 1958. IPv4 incluyó un sistema de direccionamiento que utiliza identificadores numéricos que constan de 32 bits. El uso de direcciones con una longitud de 32 bits limita el número total de posibles direcciones a un número de aproximadamente 4,3 mil millones de direcciones para los dispositivos conectados a Internet en todo el mundo. El número de dispositivos conectados a Internet será pronto más grande que el número de direcciones proporcionadas por IPv4. Por esta razón, y en previsión de la situación, el organismo responsable de la estandarización de los protocolos de Internet: El **IETF *(Internet Engineering Task Force*)** ha estado trabajando en una nueva versión de IP desde 1998: El IPv6, el protocolo sucesor que está destinado a sustituir IPv4, fue descrito formalmente en el documento estándar de Internet RFC 2460 [3].

IPv6 utiliza un formato de dirección de 128 bits, lo que permite 2^{128}, o aproximadamente 3,4 10^{38} direcciones, aproximadamente 8 10^{28} veces más que IPv4. Si bien el aumento del conjunto de direcciones es uno de los beneficios más importantes de IPv6, hay otros cambios importantes tecnológicos en IPv6 que mejoran el protocolo IP: administración más fácil, mejor enrutamiento, un formato de cabecera más simple y enrutamiento más eficiente, integración de la autenticación y la privacidad de apoyo entre otros.

IPv6 coexistirá con IPv4 durante algún tiempo. El despliegue de IPv6 se hará gradualmente en una convivencia ordenada con IPv4. Los dispositivos cliente, equipos de red, aplicaciones, contenidos y servicios han de adaptarse a la nueva versión del protocolo de Internet IPv6. Por otra parte, la transición de IPv4 a IPv6 establecerá un conjunto común de normas entre las empresas, los sistemas educativos, etc. en todo el mundo.

Las direcciones IPv6 se representan como ocho grupos de cuatro dígitos hexadecimales. Estos grupos están separados por dos puntos, pero existen métodos

para abreviar esta notación completa. El formato de la cabecera IPv6 se muestra en la figura. 1.

Fig. 1. Formato de cabcera IPv6 [3]

Estructura de cabecera de IPv6	
Versión	4-bit Internet Protocol version = 6.
Clase de Tráfico	8-bit campo de clase de tráfico.
Nivel de flujo	20-bit de nivel de flujo.
Longitud de carga	16-bit enteros sin signo. Longitud de la carga útil IPv6, es decir, el resto del paquete que sigue esta cabecera IPv6, en octetos.
Siguiente cabecera	8-bit selector. Identifica el tipo de cabecera inmediatamente después de la cabecera IPv6. Utiliza los mismos valores que el campo de protocolo IPv4.
Salto de Límite	8-bit enteros sin signo. Disminuye en 1 por cada nodo que reenvía el paquete. El paquete se descarta si se reduce a cero.
Dirección remitente	128-bit dirección del remitente del paquete
Dirección de destino	Address 128-bit dirección del destinatario del paquete (posiblemente no es el destinatario final si un encabezado de enrutamiento está presente).

Las nuevas características introducidas con el protocolo IPv6 son básicamente las siguientes: Un nuevo formato de cabecera, una infraestructura eficiente y jerárquica de direccionamiento y enrutamiento, un espacio de direcciones mucho más grande y sin estado y la configuración de direcciones firewall, seguridad IP, extensibilidad, una mejor calidad de servicio (QoS) y un nuevo protocolo para la interacción con nodos cercanos.

El protocolo IPv6 ha resuelto algunos de los problemas de seguridad que se encuentran en las redes IPv4 mediante la adición obligatoria del **IPsec** ***(seguridad IP)***. Como resultado, IPv6 es más eficiente. IPsec mejora el protocolo IP original al proporcionar la autenticidad, integridad, confidencialidad y control de acceso a cada paquete IP a través de la utilización de dos protocolos: **AH** (***encabezamiento de autenticación***) y **ESP** (***carga útil de seguridad de encapsulación***). Por otra parte, la expansión del número de bits en el campo de dirección de 128 bits que ofrece IPv6 crea una barrera significativa para los atacantes que desean realizar el escaneo de puertos completo. Además, es posible vincular una clave pública de firma a una dirección IPv6: **CGA** (***Dirección generada criptográficamente***).

IPv6 ofrece también mejoras en la seguridad de la movilidad. A pesar de que el protocolo de Internet MobileIP está disponible en IPv4 e IPv6, en IPv6 fue construido en el protocolo en lugar de ser añadido como una nueva función en IPv4. Esto significa que cualquier nodo IPv6 puede utilizar una IP móvil tanto como sea necesario. Mobile IPv6 utiliza dos extensiones titulares: Una cabecera de enrutamiento para el registro y un objetivo principal para la entrega de datos entre nodos móviles y sus nodos fijos correspondientes.

3 Aplicaciones IoT

En este capítulo, se describen algunas aplicaciones importantes relacionadas con el campo de la IoT. Se introducen los principales elementos de la arquitectura de la IoT y se analiza la evolución prevista del mercado.

3.1 Introducción

IoT puede ser visto como una combinación de sensores y actuadores que son capaces de proporcionar y recibir información digitaliza y colocarla en redes bidireccionales capaces de transmitir todos los datos para ser utilizados por una gran cantidad de diferentes servicios y usuarios finales [4].

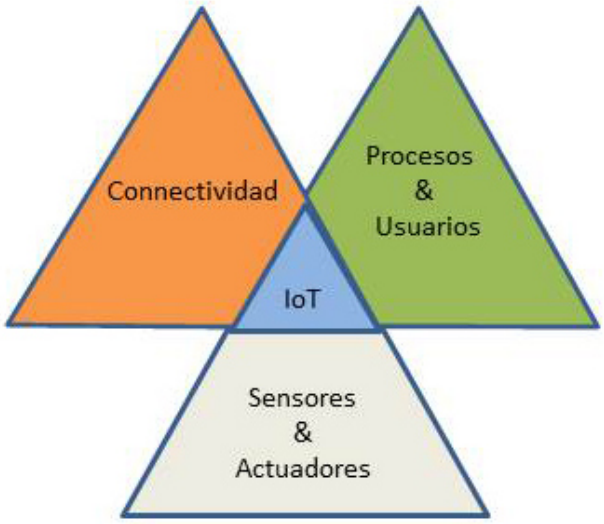


Fig. 2. Concepto de IoT.

Múltiples sensores se pueden unir a un objeto o dispositivo para medir una amplia gama de variables físicas o fenómenos y luego transmitir todos los datos a la nube. La detección puede ser entendida como un modelo de servicio.

Clasificación de Sensores	
Proveedores de datos del sensor	Las entidades empresariales que implementan y administran por sí mismos sensores.
Organizaciones	Público o Privado. Infraestructuras públicas. Las organizaciones comerciales. Corporaciones privadas: los proveedores de tecnología y servicios.
Personal y Hogares	Los teléfonos móviles, relojes inteligentes, giroscopios, cámaras, GPS, acelerómetros micrófonos, ordenadores portátiles, alimentos y artículos para el hogar, tales como televisores, cámaras, congeladores, hornos de microondas, lavadoras, electrodomésticos inteligentes, etc.

Hoy en día, el estado de la técnica de los dispositivos, tales como artículos convencionales de los hogares como refrigeradores o televisores, comprenden capacidades de comunicación y de detección. Estas capacidades serán cada vez mayores con la incorporación de la comunicación más inteligentes y herramientas de detección.

Productos con capacidades inteligentes conectados	
Monitorización	El entorno externo. Condición del producto,de las operaciones y de su uso.
Control	Controlar las funciones del producto. Personalización de la experiencia del usuario. Programación.
Optimización	Diagnóstico predictivo. El rendimiento del producto de optimización. Reducción de costos.
Autonomía	Mejora autónoma de productos y personalización. Autodiagnóstico y reparación. Operación en coordinación con otros productos
Proceso de toma efciente de decisiones.	Datos en tiempo real para la toma de decisiones.

La arquitectura de sistemas de IoT se puede dividir en cuatro capas: capa de detección de objetos, la capa de intercambio de datos, capa de integración de la información, y la capa de servicios de aplicaciones [5].

Los dispositivos inteligentes pueden estar ya conectados a través de Internet tradicional. Sin embargo, la IoT incorpora la capa de detección que reduce los requisitos de la capacidad de esos dispositivos y permite su interconexión. Sensores consumidores de datos se comunican con sensores o propietarios de los mismos a través de la capa de integración de la información que es responsable de toda la comunicación y las transacciones. Mientras tanto surgen nuevos requerimientos y desafíos para el intercambio de datos, el filtrado y la integración de la información, la definición de nuevos servicios para los usuarios, así como un incremento de la complejidad de la arquitectura de la red. Por otra parte, el uso de las tecnologías en nube está creciendo de manera exponencial. Nuevas plataformas de infraestructuras y aplicaciones de software se ofrecen en el marco de la IoT. Algunas de las principales ventajas y beneficios de la IoT serán la creación de servicios innovadores con un mejor rendimiento y soluciones de valor añadido, junto con la reducción de los costos de adquisición de datos de los servicios existentes y la oportunidad de crear nuevas fuentes de ingresos en un contexto de un modelo de negocio sostenible Estas aplicaciones se pueden orientar a los consumidores, negocios, comerciales, y actividades de encuestas, a la comunidad industrial y científica mediante el aprovechamiento de los desarrolladores de aplicaciones.

Arquitectura IoT de cuatro capas.	
Capa de detección	Sensores, los objetos físicos y la obtención de datos.
Capa de Intercambio de Datos	Transmisión transparente de datos a través de redes de comunicación.
Capa de integtración de la información	El procesamiento de la información incierta adquirida de las redes, filtrado de datos no deseados e integración de información principal en conocimiento útil para los servicios y los usuarios finales.
Capa de servicio de aplicación	Da servicios de contenido a los usuarios.

3.2 El Mercado IoT

La IoT es una arquitectura emergente basada en la Internet global técnica facilitando el intercambio de mercancías en una red de cadena de suministro mundial [1]. A medida que la tendencia de la tecnología se desplaza a velocidades de datos más rápidas y menor latencia de conectividad, se espera que Internet duplique su tamaño cada 5,3 años y la computación en nube puede jugar un papel clave en ese crecimiento. La computación en la nube es una de las plataformas que permiten apoyo a la IoT. La mayoría de las "cosas" del mundo real se integrarán en el mundo virtual, permitiendo en cualquier momento y en cualquier lugar conectividad completa.

La computación en la nube es un modelo para permitir el acceso a un conjunto compartido de recursos informáticos configurables, permitiendo a los usuarios beneficiarse de todas las tecnologías existentes, sin necesidad de profundos conocimientos o experiencia con cada uno de ellos.

En 2010, el número de objetos físicos cotidianos y los dispositivos conectados a Internet fue de alrededor de 12,5 mil millones. Se espera que este número se duplique hasta 25 mil millones en el año 2015 con lo que el número de dispositivos inteligentes por persona aumenta, y otros 50 millones en 2020 [2].

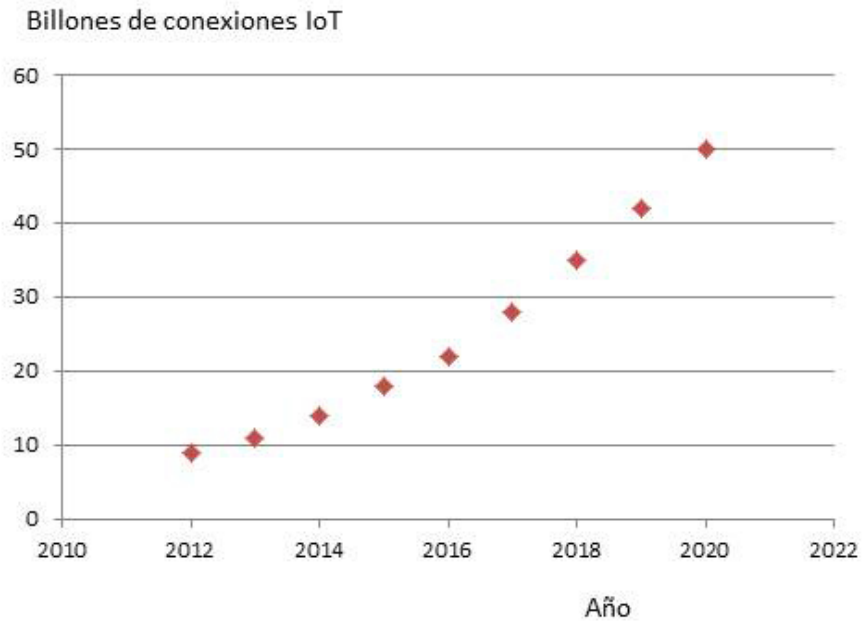


Fig. 1. Número de conexiones en IoT [2].

Mundo conectado.	
31 %	Teléfonos.
29%	Notebooks.
10%	Teléfonos inteligentes.
8%	TV inteligente.
5%	Tabletas.
5%	Usuarios de juegos.
5%	Media Players.
5%	eReaders.
3%	Otros.

Asia cuenta actualmente con la mayor cantidad de conexiones M2M debido al gran esfuerzo llevado a cabo en algunos países como Japón y China. Sin embargo, las empresas de tecnología de América y Europa están haciendo un progreso importante en la IoT y traerán al mercado a un considerable crecimiento en estos países. Con la aparición importante de la IoT, nuevos enfoques normativos para garantizar la privacidad y seguridad de los usuarios y los datos deben ser definidos.

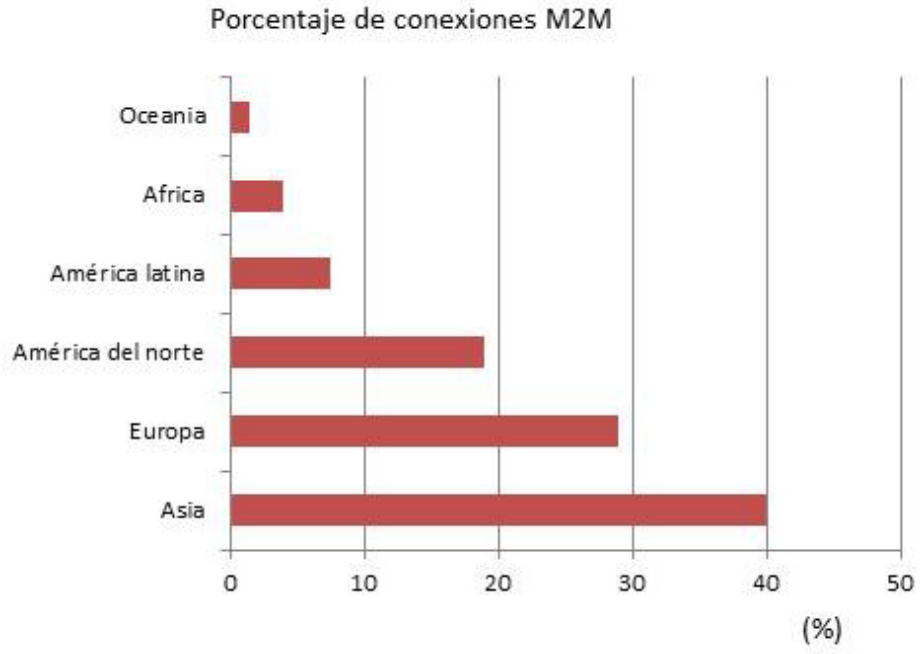


Fig. 1. Porcentaje de conexiones M2M [2].

3.3 Aplicaciones

El número de aplicaciones y servicios que pueden proporcionar es prácticamente ilimitado y se puede adaptar a muchos campos de la actividad humana, facilitando y mejorando su calidad de vida en múltiples formas. En este capítulo se da una breve lista de aplicaciones y servicios basados en la IoT. Sin embargo, es sólo una descripción limitada para comprender todas las posibles nuevas aplicaciones y servicios que la IoT podría proporcionar. Se espera alcanzar un valor estimado aproximadamente 19 billones de dólares para el 2020 por las aplicaciones y servicios de la IoT.

Aplicaciones y servicios IoT:

- Safety for all family members. Edificios inteligentes conectados: Las mejoras en la eficiencia (gestión de la energía y el ahorro) y de seguridad (sensores y alarmas). Aplicaciones domóticas incluyendo sensores y actuadores inteligentes para controlar electrodomésticos. Los servicios de salud y educación en el hogar. Control remoto de los tratamientos para los pacientes. Servicios de cable / satélite. Sistemas de almacenamiento / generación de energía. Apagado automático de la electrónica cuando no esté en uso. Termostatos inteligentes. Los detectores de humo y alarmas. Aplicaciones de control de acceso. Cerraduras inteligentes. Los sensores incorporados en la construcción de infraestructura para guiar a los primeros auxilios y asistencias. Seguridad para todos los miembros de la familia.

- Ciudades inteligentes y transporte: Integración de los servicios de seguridad. Optimización del transporte público y privado. Sensores de aparcamiento. Gestión inteligente de los servicios de estacionamiento y el tráfico en tiempo real. Gestión inteligente de semáforos en función de las colas de tráfico. Localización de los coches que han sobrepasado el tiempo de estacionamiento. Las redes energéticas inteligentes. Seguridad (cámaras, sensores inteligentes, información a los ciudadanos). Administración del Agua. Riego de parques y jardines. Contenedores de basura inteligentes. Controles de contaminación y movilidad. Obtener una respuesta inmediata y conocer las opiniones de los ciudadanos. Gobernanza inteligente. Sistemas de Votación. Monitoreo de accidentes, la coordinación acciones de emergencia.

Fig. 1. Ejemplo de aplicaciones IoT: Smart cities/Ciudades inteligentes.

- Educación: Vinculación de aulas virtuales y físicas para el aprendizaje, e-learning más eficiente y accesible. Servicios de acceso a bibliotecas virtuales y portales educativos. Intercambio de informes y resultados en tiempo real. El aprendizaje permanente. Aprendizaje de idiomas extranjeros. Gestión de la asistencia.

- Electrónica de consumo: Teléfonos inteligentes. Televisión inteligente. Laptops, computadoras y tabletas. Refrigeradores, lavadoras y secadoras inteligentes. Sistemas de cine en casa inteligentes. Aparatos inteligentes. Sensores para el collar del animal doméstico. Personalización de la experiencia del usuario. El funcionamiento del producto autónomo. Localizadores personales. Gafas inteligentes.

- Salud: Monitoreo de las enfermedades crónicas. Mejora de la calidad de la atención y la calidad de vida de los pacientes. Trackers de Actividad. Diagnóstico remoto. Pulseras conectadas. Cinturones interactivos. Deporte y monitoreo de actividades de fitness. Etiquetas inteligentes para fármacos. Seguimiento del uso de drogas. Los biochips. Interfaces cerebro-ordenador. Monitoreo de los hábitos alimenticios.

- Automoción: Smart Cars. Control de tráfico. Avanzar en la información sobre lo que está roto. Monitoreo inalámbrico de presión de los neumáticos de coche. La gestión inteligente de la energía y el control. Auto diagnóstico. Los acelerómetros. Sensores de posición, de presencia y de proximidad. Análisis de la mejor manera de ir en tiempo real a un sitio. Localización por GPS. Control de la velocidad del vehículo. Vehículos autónomos que utilizan los servicios de la IoT.

- Agricultura y medio ambiente: Medición y control de la contaminación del medio ambiente (CO_2, el ruido, los elementos contaminantes presentes en el

ambiente). Pronosticar cambios climáticos basados en el monitoreo de sensores inteligentes. Las etiquetas RFID pasivas asociadas a los productos agrícolas. Sensores en palets de productos. Gestión de residuos. Cálculos de Nutrición.

- Los servicios de energía: Datos precisos sobre el consumo de energía. La medición inteligente. Redes inteligentes. Análisis y predicción de comportamientos de consumo de energía y patrones. Pronosticar las tendencias y necesidades futuras de energía. Redes de sensores inalámbricos. La producción de energía y el reciclaje.

- Conectividad inteligente: Gestión de datos y prestación de servicios. El uso de medios de comunicación social y las redes sociales. El acceso a los servicios de correo electrónico, voz y video. La comunicación de grupo interactiva. En streaming en tiempo real. Juegos interactivos. Realidad aumentada. Supervisión de la seguridad de la red. Interfaces de usuario disponibles. La computación afectiva. Métodos de autenticación biométrica. Telemática de consumo. Servicios de comunicación M2M. Análisis de grandes datos. Realidad virtual. Servicios de computación en nube. Computación ubicua. Visión por computador. Antenas inteligentes.

- Fabricación: Gas y sensores de flujo. Sensores inteligentes de humedad, temperatura, movimiento, fuerza, carga, fugas y niveles. Visión de máquinas. Detección acústica y de vibraciones. Aplicaciones compuestas. Control inteligente de robots. Control y optimización de los procesos de fabricación. Reconocimiento de patrones. Aprendizaje automático. El análisis predictivo. Logística móvil. Gestión de almacenes. Prevenir la sobreproducción. Logística eficiente.

- Compras: Compras inteligentes. RFID y otras etiquetas electrónicas y lectores. Los códigos de barras en el comercio minorista. Inventarios. Control de la procedencia geográfica de los alimentos y productos. Control de calidad de los alimentos y de la seguridad.

4 Tecnologías subyacentes

La aplicación con éxito del concepto IoT en el mundo real es posible gracias a los avances en las tecnologías subyacentes. En este apartado se indicarán las tecnologías subyacentes más relevantes con el objetivo de proporcionar una visión del papel que probablemente jugarán en la IoT [6, 7].

4.1 Energía

Las tecnologías de almacenamiento de energía y de potencia son claves para el despliegue de aplicaciones de la IoT. Las cuestiones energéticas, en todas sus fases, desde la generación hasta la conservación y el uso, son fundamentales para el desarrollo de la IoT. Estas tecnologías tienen que ofrecer generación de energía de alta densidad de potencia y soluciones de generación, que, cuando se usen con una nanoelectrónica actual de baja potencia, nos permitirá diseñar el dispositivo de identificación autoalimentado basado en sensores inteligentes inalámbricos. Todavía hay una necesidad de investigar y desarrollar soluciones en esta área (nanoelectrónica, semiconductores, tecnología de sensores, integración de micro sistemas) que tienen como objetivo dispositivos más eficientes y compactos de ultra bajo consumo de energía y de almacenamiento de energía como baterías, pilas de combustible, y baterías de polímero / impresas, ya que los dispositivos actuales parecen insuficientes teniendo en cuenta la potencia de procesado necesaria y las limitaciones de energía del futuro. Además, la integración de sistemas aumentará la eficiencia de los sistemas actuales y proporcionará varias soluciones para las necesidades futuras.

4.2 Sensores

Los sensores son uno de los pilares constructivos del Internet de las cosas. Como sistemas ubicuos pueden implementarse en todas partes. También pueden ser implantados bajo la piel humana, en un bolso o en una camiseta. Algunos pueden ser tan pequeños como de cuatro milímetros de tamaño, pero los datos que recogen pueden ser recibidos a cientos de millas de distancia. Complementan los sentidos humanos y se han vuelto indispensables en un gran número de industrias, desde la salud hasta la construcción. Los sensores poseen la ventaja clave de poder anticiparse a las necesidades humanas en base a la información recopilada sobre su entorno. Su inteligencia multiplicada por numerosas redes les permite no sólo informar sobre el entorno, sino también tomar medidas sin la intervención humana.

Chips de silicio miniaturizados son diseñados con nuevas capacidades en factores de forma cada vez más pequeños y con mejor rendimiento en procesado y eficiencia. Los costes están bajando, siguiendo la Ley de Moore. El coste del ancho de banda también ha disminuido y de igual modo los costes de procesado, permitiendo que más dispositivos estén no únicamente conectados, sino que sean lo suficientemente inteligentes como para saber qué hacer con todos los nuevos datos que se generan o reciben.

Capacidades como el conocimiento del entorno y la comunicación entre máquinas son consideradas de alta prioridad para la IoT. Prioridades adicionales son la integración de memoria y la potencia de procesado, la capacidad de resistir a entornos severos, y una seguridad asequible. Por otra parte, el desarrollo de núcleos de procesadores/microcontroladores de ultra bajo consumo de energía diseñados específicamente para dispositivos móviles de la IoT y una nueva clase de sistemas inteligentes céntricos de la IoT simples y asequibles serán un factor clave. Las soluciones a este respecto van desde máquinas de estado finito micro programadas al uso de microcontroladores. La elección es un equilibrio entre la flexibilidad, la capacidad de programación, el área de silicio y el consumo de energía. Los dispositivos requieren alguna forma de almacenamiento no volátil (EEPROM/FRAM/Polímero), independientemente de si se trata de una memoria de máscara, programable una sóla vez, o bien regrabable eléctricamente. La memoria no volátil regrabable es claramente la preferida para lograr un alto rendimiento durante la fase de producción y al mismo tiempo servir como memoria de usuario, pudiendo ser programada y almacenar datos del sensor.

4.3 Computación en la nube

La computación en nube es un modelo para el acceso bajo demanda a un conjunto compartido de recursos configurables (por ejemplo, ordenadores, redes, servidores, unidades de almacenamiento, aplicaciones, servicios, software) que pueden ser proporcionados en la modalidad de Infraestructura como Servicio (*Infrastructure as a Service* - IaaS) o Software como Servicio (*Software as a Service* - SaaS). Uno de los resultados más importantes de la IoT es la enorme cantidad de datos generados a partir de dispositivos conectados a Internet [7]. Muchas aplicaciones IoT requieren almacenamiento masivo de datos, gran velocidad de procesamiento para permitir la toma de decisiones en tiempo real y redes de banda ancha de alta velocidad para transmitir datos, audio o vídeo. La computación en la nube ofrece la solución ideal para el manejo de los flujos enormes de datos y su procesado para un número sin precedentes de dispositivos IoT y de seres humanos en tiempo real.

4.4 Comunicación

Las nuevas antenas inteligentes multi-banda, integradas en el propio chip y hechas de materiales nuevos son los medios de comunicación que permitirán a los dispositivos comunicarse. Estas antenas deben ser optimizadas en tamaño, coste y eficiencia, y pueden ser de diversos tipos, como una bobina, una antena impresa, una antena embebida o una antena múltiple utilizando diferentes sustratos y estructuras 3D. Los esquemas de modulación y la velocidad de transmisión son también cuestiones importantes que deben abordarse para permitir protocolos de comunicación y velocidades de transmisión en multiple frecuencias y eficientes energéticamente. Los protocolos de comunicación estarán diseñados para arquitecturas orientadas a plataformas Web de la IoT donde todos los objetos, dispositivos inalámbricos, cámaras, ordenadores, etc. se combinen para analizar ubicación, la intención e incluso las emociones a través de una red. Se necesitarán nuevos métodos de gestión eficaz del consumo de energía en los diferentes niveles del diseño de la red, desde el enrutamiento a la arquitectura de los diferentes dispositivos.

4.5 Integración

La integración de dispositivos inteligentes en los envases, o mejor, en los propios productos permitirá un ahorro de costes significativo y aumentar la simpatía de los productos Eco. Se continuará con el uso de chips y antenas integrados en sustratos no convencionales como los tejidos téxtiles y el papel, y el desarrollo de nuevos sustratos, conductores y materiales de unión adecuados para ambientes hostiles y para la eliminación de residuos ecológicamente. La tecnología *System-in-Package* (SiP) permite la integración flexible y 3D de diferentes elementos como antenas, sensores activos y componentes pasivos en el envase, mejorando el rendimiento y reduciendo el coste de la etiqueta. Incrustaciones RFID con estructura de acoplamiento por tiras se utilizan para conectar el chip del circuito integrado y la antena con el fin de producir una variedad de formas y tamaños de etiquetas, en lugar de montaje directo.

4.6 Estándares

Los dispositivos IoT son muy diversos y miden diferentes parámetros y con diferentes convenciones y unidades de medida. Aunque los protocolos en propiedad siguen compitiendo, es probable que los estándares de código abierto serán una de las formas de obtener estos datos para interoperar.

Claramente, los estándares abiertos son la herramienta clave para el éxito de las tecnologías de comunicación inalámbrica y, en general, para cualquier tipo de comunicación de máquina a máquina. Sin embargo, se ha reconocido como un elemento importante para el despliegue de aplicaciones IoT la necesidad de una configuración más rápida de las normas de interoperatibilidad. Es necesario aclarar los requisitos para una identificación global única, denominación y DNS. Un reto que debe abordarse en el futuro es la falta de convergencia en la definición de modelos de referencia comunes, arquitecturas de referencia para las futuras redes, la Internet del Futuro y la IoT, y la integración de sistemas y redes heredadas.

5 Retos y barreras de la IoT

Muchas cuestiones difíciles necesitan ser abordadas aún. Hacer frente a estos retos permite a los proveedores de servicios y a los programadores de aplicaciones implementar sus servicios de manera eficiente. En los siguientes párrafos, se proporciona un breve análisis de los principales desafíos a que se enfrentan las fases de desarrollo y de despliegue de la IoT [8].

5.1 Retos

Fiabilidad

La fiabilidad tiene como objetivo aumentar la tasa de éxito de la prestación del servicio de IoT. Tiene una estrecha relación con la disponibilidad puesto que por fiabilidad garantizamos la disponibilidad de información y servicios a través del tiempo. La fiabilidad es aún más crítica y tiene requisitos más estrictos en lo que respecta al campo de las aplicaciones de respuesta de emergencia. En estos sistemas, la parte crítica es la red de comunicación que debe ser resistente a fallos a fin de realizar la distribución de información fiable. La fiabilidad debe ser implementada en software y hardware en todas las capas de la IoT. Con el fin de tener una IoT eficiente, la comunicación subyacente debe ser fiable, ya que por ejemplo, por una percepción poco fiable, la recopilación de datos, el procesamiento y la transmisión puede dar lugar a retrasos, pérdida de datos, y a decisiones finales equivocadas, lo que puede conducir a escenarios desastrosos y, en consecuencia, hacer la IoT menos fiable.

La **fiabilidad** se refiere al funcionamiento apropiado del sistema basado en su especificación.

Rendimiento

La evaluación del rendimiento de los servicios de la IoT es un gran reto, ya que depende del rendimiento de muchos componentes, así como del rendimiento de las tecnologías subyacentes. La IoT, al igual que otros sistemas, tiene que desarrollar y mejorar continuamente sus servicios para satisfacer las necesidades de los clientes. Los dispositivos de la IoT deben ser supervisados y evaluados para proporcionar el mejor rendimiento posible a un precio asequible para los clientes. Pueden usarse muchas métricas para evaluar el rendimiento de la IoT incluyendo la velocidad de procesado, la velocidad de comunicación, el factor de forma del dispositivo y el coste.

La evaluación del rendimiento de cada uno de los protocolos y las tecnologías subyacentes, los protocolos de la capa de aplicación y de calidad de servicio se han publicado en la literatura, pero la falta de una evaluación a fondo del rendimiento para las aplicaciones de la IoT es todavía una cuestión abierta.

La **calidad de servicio** (*Quality of Service* - QoS) es el rendimiento global de una red de telefonía o de ordenadores percibido por los usuarios de la red.

Interoperability

La interoperabilidad de extremo a extremo es otro reto para la IoT debido a la necesidad de manejar un gran número de cosas heterogéneas que pertenecen a diferentes plataformas. La interoperabilidad debería ser considerada por los desarrolladores de aplicaciones y fabricantes de dispositivos IoT para garantizar la

prestación de servicios a todos los clientes, independientemente de las especificaciones de la plataforma de hardware que utilicen. Por ejemplo, hoy en día la mayoría de los teléfonos inteligentes soportan tecnologías de comunicación comunes, tales como WiFi, NFC, y GSM para garantizar la interoperabilidad en diferentes escenarios. También, los programadores de la IoT deben construir sus aplicaciones para que permitan añadir nuevas funciones sin causar problemas o perder funciones mientras se mantiene la integración con las diferentes tecnologías de comunicación. En consecuencia, la interoperabilidad es un criterio importante en el diseño y la construcción de servicios de la IoT para satisfacer las necesidades de los clientes. Junto con la variedad de protocolos, las diferentes interpretaciones del mismo estándar aplicado por partes diferentes presentan un desafío para la interoperabilidad. Para evitar este tipo de ambigüedades, serían útiles pruebas de interoperabilidad entre los diferentes productos en un banco de pruebas como los ETSI Plugtests. PROBE-IT es un proyecto de investigación que tiene como objetivo garantizar la interoperabilidad de soluciones de IoT validadas que se llevaron a cabo en pruebas de interoperabilidad como COAP, 6LoWPAN e interoperabilidad semántica en IoT.

Es un hecho conocido que dos dispositivos diferentes pueden no ser interoperables, incluso si ambos siguen la misma norma. Esta es la excusa más importante para la amplia adopción de las tecnologías IoT. Las etiquetas del futuro deberán integrar los diferentes estándares de comunicación y protocolos que operen a frecuencias diferentes y permitir diferentes arquitecturas, centralizadas o distribuidas, y ser capaces de comunicarse con otras redes a menos que emergan estándares globales y bien definidos.

Seguridad y Privacidad

La seguridad presenta un reto importante para las implementaciones de la IoT debido a la falta de un estándar y arquitectura común para la seguridad de la IoT. En redes heterogéneas como en el caso de la IoT, no es fácil garantizar la seguridad y privacidad de los usuarios. La funcionalidad principal de la IoT se basa en el intercambio de información entre los miles de millones o incluso billones de objetos con conexión a Internet. Uno de los problemas de seguridad en la IoT que no ha sido considerado en los estándares es la distribución de las claves entre dispositivos. Por otra parte, las cuestiones de privacidad y las operaciones de acceso a perfil entre los dispositivos IoT sin interferencias son extremadamente críticas. Aún así, asegurar el intercambio de datos es necesario para evitar perder o comprometer la privacidad. El aumento del número de cosas inteligentes que nos rodean con datos sensibles requiere una gestión de control de acceso transparente y fácil de manera tal que, por ejemplo, un proveedor sólo pueda leer los datos, mientras que a otro se le permita controlar el dispositivo. En este sentido, se han propuesto algunas soluciones tales como la agrupación de dispositivos integrados en redes virtuales y solamente aquellos dispositivos deseados existentes dentro de cada red virtual. Otro enfoque es mantener un control de acceso en la capa de aplicación en función de cada vendedor.

Gestión

La conexión de miles de millones o billones de dispositivos inteligentes representa para los proveedores de servicios un problema de enormes proporciones a la hora de gestionar aspectos de fallo, configuración, contabilidad, rendimiento y seguridad (*Fault, Configuration, Accounting, Performance and Security* - FCAPS) de estos dispositivos. Este esfuerzo de gestión requiere el desarrollo de nuevos y ligeros protocolos de gestión para manejar la pesadilla de gestión que potencialmente se deriva de la implantación de la IoT en los próximos años. La gestión de dispositivos y aplicaciones IoT puede ser un factor eficaz para el crecimiento de la implantación de la IoT. Por ejemplo, el control de la comunicación M2M de los objetos IoT es importante para asegurar conectividad en todo momento para proporcionar servicios bajo demanda. *Light-weight* M2M (LWM2M) es un estándar que está siendo desarrollado por la Open Mobile Alliance para proporcionar la interfaz entre los dispositivos M2M y los servidores M2M para construir un esquema independiente de aplicación para la gestión de una gran variedad de dispositivos. Su objetivo es ofrecer aplicaciones M2M con capacidades de administración remota de dispositivos, servicios y aplicaciones M2M. El protocolo NETCONF Light es un esfuerzo de la *Internet Engineering Task Force* (IETF) para la gestión de dispositivos restringidos que proporciona mecanismos para instalar, manipular y eliminar la configuración de dispositivos de red. Es capaz de manejar una amplia gama de dispositivos desde dispositivos con recursos limitados a dispositivos ricos en recursos. La plataforma MASH IoT, desarrollada de forma independiente, es un ejemplo de plataforma que facilita la gestión (seguimiento, control y configuración) de los activos de la IoT en cualquier lugar y en tiempo real a través de un panel de control IoT en teléfonos inteligentes. El mantenimiento de la compatibilidad entre las capas de la IoT también debe gestionarse para mejorar la velocidad de conectividad y garantizar la prestación de servicios. El grupo de trabajo de administración de dispositivos Open Mobile Alliance (OMA) especifica los protocolos y mecanismos para la gestión de dispositivos y servicios móviles en entornos con recursos limitados.

Fabricación

Los retos de fabricación deben ser resueltos de manera convincente. Los costes deben bajar a menos de un centavo por cada etiqueta RFID pasiva, y la producción debe alcanzar volúmenes extremadamente altos, mientras que todo el proceso de producción debe tener un impacto muy limitado sobre el medio ambiente, basado en estrategias para la reutilización y el reciclaje, considerando el ciclo de vida completo de dispositivos digitales y de otros productos que podrían ser etiquetados o activados por un sensor.

5.2 Barreras

Pero también existen barreras para la IoT, especialmente en el ámbito de las normativas, la seguridad y la protección. El objetivo principal es proteger de la mejor forma posible la privacidad de las personas y forzar a las empresas a establecer formas seguras de manejar los datos y la información [8, 9].

Ausencia de Gobernabilidad

Una de las principales barreras para la adopción generalizada de la tecnología de la Internet de las cosas es la ausencia de gobernabilidad. Sin una autoridad de gobierno imparcial será imposible tener una IoT verdaderamente global, aceptada por los estados, empresas, organizaciones profesionales y la gente. Hoy en día no hay un único esquema de numeración universal: EPCglobal y Ubiquitous Networking Lab proponen dos formas diferentes, no compatibles, de identificación de objetos y existe el riesgo de tenerlos en competencia en un futuro próximo en el mercado global. También existe la necesidad de mantener la gobernabilidad tan genérica como sea posible, ya que tener una autoridad por campo de aplicación dará lugar sin duda a solape, confusión y competencia entre normas. Los objetos pueden tener identidades diferentes en diferentes contextos por lo que tener múltiples autoridades crearía una especie de *multi-homing*, que puede conducir a resultados desastrosos.

Privacidad y Seguridad

Con el fin de tener una adopción generalizada de cualquier sistema de identificación de objetos, existe una necesidad de disponer de una solución técnicamente sólida para garantizar la privacidad y la seguridad de los clientes. Si bien en muchos casos, la seguridad se ha hecho como un añadido, la sensación es que la aceptación pública de la IoT ocurrirá sólo cuando se apliquen soluciones de seguridad y privacidad sólidas. En particular, los ataques deben ser interceptados, los datos autenticados, el acceso controlado y la privacidad de los clientes (personas físicas y jurídicas) garantizado. Podría tratarse de mecanismos de seguridad híbridos que combinen, por ejemplo, la seguridad del hardware con la diversificación clave para ofrecer una seguridad superior que haga que los ataques sean significativamente más difíciles o incluso imposibles. La selección de las características de seguridad y mecanismos continuará siendo determinado por el impacto en los procesos de negocio; y las contrapartidas estarán entre el tamaño del chip, el coste, la funcionalidad, la interoperabilidad, la seguridad y la privacidad.

Las cuestiones de seguridad y privacidad deberían ser abordadas por las futuras normas que deben definir las diferentes funciones de seguridad para proporcionar servicios de confidencialidad, integridad o disponibilidad.

También hay una serie de cuestiones relacionadas con la identidad de las personas. Estas deben ser tratadas en política y legislación, siendo de vital importancia para las eficientes administraciones públicas del futuro.

6 Futuro de la IoT

Es posible identificar, en los años venideros, cuatro distintas macro-tendencias que darán forma al futuro de las tecnologías de Internet, junto con la explosión de dispositivos ubicuos que constituyen el futuro de la Internet de las Cosas [9]:

1. La primera de ellas, a veces conocida como "*exaflood*" o "*data deluge*", es la explosión de la cantidad de datos recopilados e intercambiados. Existe la necesidad por parte de todos los actores de repensar las actuales arquitecturas de red y de almacenamiento debido a que las redes actuales no son adecuadas para este crecimiento exponencial del tráfico. Será imprescindible encontrar nuevas formas y mecanismos que permitan localizar, traer, y transmitir datos. Una razón importante para este diluvio de datos es la explosión en el número de dispositivos de recogida e intercambio de información como se prevé cuando la Internet de las cosas se convierta en una realidad.

El término ***exaflood***, acuñado por Bret Swanson de la Fundación Progreso y Libertad, se refiere al creciente torrente de datos en Internet.

2. La energía necesaria para hacer funcionar los dispositivos inteligentes disminuirá dramáticamente. Ya hoy en día, muchos centros de datos han alcanzado el nivel máximo de consumo de energía y la adquisición de nuevos dispositivos necesariamente tiene que continuar con la retirada de los más viejos. Por lo tanto, la segunda tendencia que se puede identificar cubre a todos los dispositivos y sistemas desde el más pequeño al más grande de los centros de datos: la búsqueda de un nivel cero de entropía en el que el dispositivo o sistema tendrán que generar su propia energía.

3. La miniaturización de los dispositivos también está teniendo lugar de forma increíblemente rápida. El objetivo de un transistor nanométrico de un solo electrón está cada vez más cerca, que parece ser el último límite, al menos hasta que se produzcan nuevos descubrimientos de la física

4. Otra tendencia importante es avanzar hacia los recursos autonómicos. La creciente complejidad de los sistemas será inmanejable y dificultará la creación de nuevos servicios y aplicaciones a menos que los sistemas muestren auto propiedades, como la autogestión, la autorecuperación y la autoconfiguración.

Como tendencia general, al ser menos costoso integrar la tecnología en objetos físicos, vamos a ver más aplicaciones y la adopción de la IoT. En consecuencia, la IoT tendrá implicaciones importantes en compañías de negocio a negocio y de negocio a consumidor en los próximos años.