Documento de Investigación
17/2018

Programa de «Trabajo de Futuros»

«Panorama de tendencias geopolíticas»

-

Internet de las Cosas. Horizonte 2050

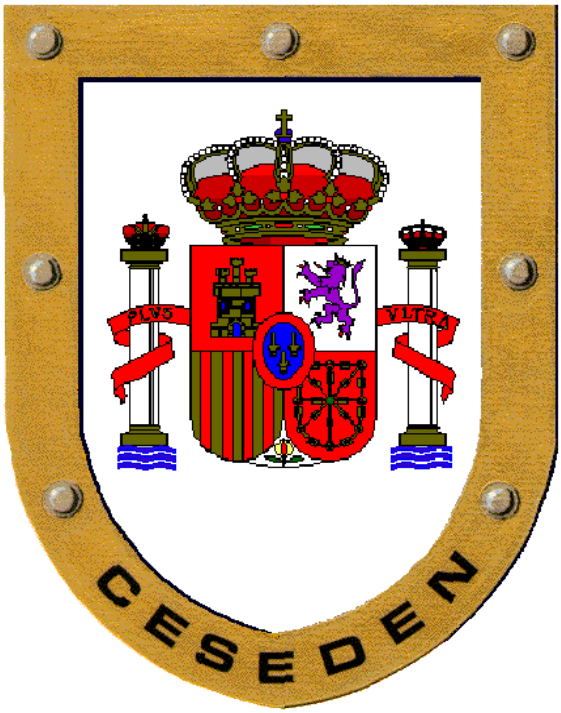
-

Internet of Things. Horizon 2050

Organismo solicitante del estudio:
Instituto Español de Estudios Estratégicos (IEEE)

Centro Superior de Estudios de la Defensa Nacional

(CESEDEN)



Trabajo maquetado, en julio de 2018, por el Instituto Español de Estudios Estratégicos (IEEE).

NOTA: Las ideas y opiniones contenidas en este documento son de responsabilidad del autor, sin que reflejen, necesariamente, el pensamiento del Ministerio de Defensa, del CESEDEN o del IEEE.

Internet de las Cosas. Horizonte 2050

Víctor Manuel Brea Sánchez
Centro Singular de Investigación en Tecnoloxías da Información (CiTIUS)

Resumen

Internet de las cosas (IoT) es un nuevo paradigma de Internet en el que todas las cosas están interconectadas. Se entiende por cosa cualquier elemento susceptible de conectarse a la red, sea éste un robot, un electrodoméstico, o una persona con su teléfono móvil. La ingente cantidad de cosas en la red de IoT genera lo que se denomina hiperconectividad. La hiperconectividad abre una serie de retos o desafíos tanto a nivel individual como a nivel de funcionamiento conjunto de las cuatro capas en las que se divide IoT, esto es, la capa de percepción o de sensado, la capa de redes y comunicación, la capa de servicios, y la capa de aplicaciones. A modo de resumen podemos decir que dos de los retos más importantes de IoT pasan por garantizar la capacidad de dar cobertura de red en un tiempo suficientemente corto ante la petición de un servicio y por mantener la seguridad y privacidad de los datos personales. Finalmente, decir que IoT abre nuevas aplicaciones en ámbitos tan diversos como el Internet de los Edificios, Internet de la Energía, Internet del Vehículo, salud y bienestar. Así mismo, IoT tendrá implicaciones socioeconómicas claras, con un claro ejemplo en la progresiva automatización de los procesos productivos, lo que con probabilidad llevará a un paulatino descenso de profesiones menos cualificadas o con trabajos más rutinarios, pero posiblemente también a una menor deslocalización de la industria hacia zonas de menor coste laboral. Todos estos aspectos se recogen en el presente documento.

Palabras clave

Internet de las Cosas (IoT), Nodos Sensores IoT, Redes y Comunicaciones, Aplicaciones, Servicios, Sistemas Ciber-Físicos.

Internet of Things. Horizon 2050

Abstract

Internet of Things (IoT) is a new paradigm by which all things are interconnected. Thing is defined as any element that can have network access. Robots, home appliances or people with their mobile phones are examples of things in IoT. The big amount of things in the IoT net yields the so-called hyperconnectivity. This leads to many challenges in every layer of IoT, this is, the perception or sensing layer, the network and communications layer, the service layer, and the application layer, as well as in their collective behavior. As a summary, we can state that two of the most difficult challenges in IoT lie in complying with both time response and network service for a given service request within a short enough time, and in guaranteeing security and privacy of personal data. Finally, it should be noted that IoT paves the way for new applications in fields as Internet of Buildings, Internet of Energy, Internet of Vehicles, wealth and well-being, etc. Also, IoT will have a clear socioeconomic impact. The increasingly automation of industrial processes with a likely cut of low-qualified jobs, but most likely with less outsourcing is a clear example of this. All these issues are addressed in this document.

Keywords

Internet of Things (IoT), IoT Sensing Nodes, Networks and Communications, Applications, Services, Cyber-Physical Systems.

Introducción- Definiciones

Según la agrupación europea Internet of Things European Research Cluster (IERC) [1, 2], Internet de las cosas, en inglés; Internet of Things (IoT), se define como una infraestructura global para la sociedad de la información, que permite la ejecución de servicios avanzados mediante la interconexión física y/o virtual de cosas mediante tecnologías de información y comunicación interoperativas que existen actualmente, pero que evolucionan a lo largo del tiempo.

IERC también define IoT como una infraestructura de red dinámica global capaz de auto configurarse basada en protocolos de comunicación estándar e interoperativos donde tanto las cosas físicas como virtuales tienen identidad propia, atributos físicos, personalidad virtual, e interaccionan de forma inteligente, y se integran de forma transparente, es decir, pasando desapercibidos, en la red de información.

El término cosa en IoT hace referencia a cualquier elemento susceptible de conectarse a Internet, sea éste un electrodoméstico, un mueble, un sensor o una red de sensores para monitorizar la temperatura y humedad de una plantación en un invernadero, un contador de energía eléctrica en una vivienda, una cámara de vídeo vigilancia en un aeropuerto, un robot software (*bot*), o simplemente una persona a través de los dispositivos que ésta pueda llevar encima, como teléfonos móviles o dispositivos vestibles (*wearables* en inglés), como pulseras o ropa inteligente, etc.

El término servicio hace referencia a una unidad funcional que se une a otras del mismo tipo a través de Internet para ejecutar una aplicación o suministrar información. El término aplicación hace referencia a lo local y a lo global. Así, la aplicación global que le suministra la ruta óptima a un vehículo autónomo en una ciudad inteligente implica la composición o unión de varias unidades funcionales o servicios web, incluyendo un servicio de navegación con mapas generados en tiempo real, servicios de GPS, así como sensores para adquirir información del entorno. En algunos casos, las aplicaciones son más locales, obteniendo los datos o servicios necesarios en el propio sistema. Así, los datos de temperatura recogidos por una red de sensores son suficientes para que el centro de datos del propio edificio tome la decisión de subir o bajar la misma.

La interoperatibilidad hace referencia a la conexión entre sistemas de forma transparente o desapercibida (*seamlessly* en inglés), tanto horizontal como verticalmente. La conexión vertical se da entre los diferentes componentes de un sistema cerrado. Pensemos por ejemplo en los sensores y actuadores de una plantación en un invernadero interconectados mediante una red inalámbrica que a su vez están conectados a la nube, donde una máquina o un operario toma decisiones y trasmite órdenes de vuelta a los actuadores situados en el invernadero. Este sistema con conexión vertical, técnicamente denominado sistema ciber-físico, en inglés, Cyber-Physical System (CPS), debería poder comunicarse e intercambiar información de forma transparente

con otros sistemas verticales o CPS como por ejemplo un sistema CPS para medir la energía consumida en la red eléctrica a través de la red global IoT.

La transformación de Internet en IoT lleva aparejada el aumento de la conectividad de dispositivos a la red, generando un nuevo concepto; hiperconectividad, que obliga a introducir nuevas tecnologías o transformar las existentes. Pensemos simplemente en el reto de la asignación de identidades a los miles de millones de dispositivos conectados a IoT, y en dotar a la red de seguridad contra ataques malignos, privacidad, confianza, y una respuesta temporal adecuada a la petición de un servicio. En este sentido, Gartner afirma que el número de dispositivos conectados a la red subirá de 5.000 a 50.000 millones del año 2015 al año 2020. Simplemente, doblar el número de cosas conectadas a IoT cada 5 años nos dejaría en 160000 millones en el horizonte 2050. En estas condiciones, y a modo de ejemplo, será un reto garantizar que un centro de datos en la nube proporcione un tiempo de respuesta suficientemente rápido y seguro a la petición de un servicio de planificación de una ruta para un conductor que circule en una ciudad con un volumen de tráfico significativo.

IoT- Estado del Arte

IoT suele dividirse en varias capas de abstracción; la capa física o de percepción, en donde se hace referencia a sensores y actuadores, la capa de red, que consta de los protocolos y tipos de comunicación y la infraestructura de red, la capa de servicios, y, finalmente, la capa de aplicaciones. IoT es por tanto un paradigma multidisciplinar que abarca desde la tecnología de fabricación de semiconductores o diseño y ensamblado de circuitos tanto micro como nanoelectrónicos, hasta la provisión de servicios web.

La capa física o de percepción obtiene datos del entorno, de la persona o del propio proceso o sistema sobre el que se actúa. Los elementos esenciales de esta capa son los sensores, qué, muchas veces se integran en nodos de procesamiento IoT capaz de subir a la nube los datos mediante servicios como Fiware o Amazon AWS [3, 4]. En este sentido, placas con procesadores Arduino y Raspberry Pi son las soluciones que mejor compromiso ofrecen entre precio y capacidad de procesamiento. Otras soluciones con más capacidad de cómputo, pero también más caras, incluyen tarjetas de procesamiento gráfico como Jetson o FPGA [5, 6].

Todas estas soluciones suelen conectarse a la red IoT mediante Ethernet o bien mediante comunicación inalámbrica. Otro punto importante en los nodos sensores IoT es la tecnología de identificación del nodo sensor IoT mediante soluciones como RFID (Radio Frequency Identifier), una solución muy extendida, ya que RFID se integra en una etiqueta pasiva, que no necesita alimentarse mediante baterías.

Las redes, protocolos y medios de comunicación de hoy en día han de adaptarse todavía a IoT. Estos cambios se centran en la hiperconectividad, que aumenta las

exigencias de velocidad de la red para satisfacer los requerimientos temporales de un usuario y obliga a redefinir cómo se identifican las cosas en IoT, y la interoperabilidad entre distintos sistemas o redes heterogéneas de manera imperceptible para el usuario. En la actualidad, gran parte de la interoperabilidad entre las distintas capas de IoT se lleva a cabo mediante el denominado *middleware*, que en el futuro IoT jugará un papel todavía más determinante. El software *middleware* permite escribir aplicaciones o servicios sin preocuparse de los dispositivos o los protocolos de comunicación que los sustentan. Obviamente, IoT ha de mantener la seguridad y la privacidad para ganarse la confianza de los usuarios.

Los retos señalados en el párrafo anterior se tratan de resolver de varias formas. Primero, reemplazando formatos de datos como HTML y XML por EXI, protocolos de comunicación como HTTP/TCP por CoAP, mucho más eficiente energéticamente, al igual que la sustitución de IPv4/IPv6 por 6LoWPAN, o protocolos de red mucho más sencillos [7, 8].

En cuanto a la capa de aplicaciones y servicios web, hay que decir que en la actualidad los usuarios de Internet cuando hacen una petición de información, como por ejemplo la solicitud de los vuelos y hoteles con mejor precio para un viaje, están ejecutando servicios web. Los servicios web habitualmente se ejecutan bajo demanda, de forma flexible y con poca latencia temporal mediante computación en la nube. La computación en la nube también suministra infraestructura como servicios de almacenamiento de datos remoto o aplicaciones. La base de la computación en la nube es un centro de datos. La llegada de IoT cambiará el paradigma de computación en la nube, ya que la hiperconectividad y la necesidad de respuestas rápidas en cualquier instante de tiempo y en cualquier lugar, especialmente con teléfonos móviles cuando la cobertura no es perfecta, hará que parte de la computación se desplace o se distribuya a los nodos de red de comunicaciones, creando lo que se denomina computación en la niebla (*fog computing*), o incluso en el nodo sensor IoT (*edge computing*) [1].

La inteligencia artificial es otro componente que irá ganando presencia en la computación en IoT, dando lugar a computación cognitiva. No sólo se buscan nodos IoT con inteligencia local, sino también inteligencia colectiva entre los distintos componentes de la red dinámica global IoT. La incorporación de inteligencia artificial en IoT permitiría adaptarse a datos cambiantes de manera mucho más efectiva que la implementación de un algoritmo.

En la actualidad, el potencial de IoT está por explotar, ya que la capa física y la capa de inteligencia habitualmente se encuentran desconectadas, requiriendo un gran esfuerzo manual para explotar los datos. La inteligencia artificial en IoT podría derivar en la toma de decisiones autónomas de sistemas sensores/actuadores, o en un análisis más efectivo y eficiente de los datos (*data analytics, big data*), acelerando la toma de decisiones mediante asesores virtuales inteligentes.

La seguridad y privacidad de datos es esencial para extender el uso de IoT. La tecnología denominada *blockchain* es la más prometedora para este fin. La clave de *blockchain* es que se descentraliza la seguridad, de manera que todos los nodos guardan copia de las transacciones y de las identidades de los usuarios, por lo que es posible determinar cuándo, quién y cómo realizó un ataque contra la seguridad de la red IoT. En este campo la inteligencia artificial colectiva jugará un papel fundamental.

Finalmente, en términos de aplicaciones, en la actualidad, la Unión Europea financia 5 grandes proyectos piloto de IoT con 100 millones de euros [1]. Estos cinco grandes proyectos son: i) Activage- centrado en IoT para crear ambientes inteligentes para personas mayores, ii) IoF2020- centrando en IoT para el procesamiento de comida y agricultura, iii) Monica- centrado en dispositivos vestibles IoT, iv)- Synchronicity- mercado único mediante IoT, y v) Autopilot- coche autonómo potenciado por IoT. Todos estos proyectos están desligados unos de otros, pero el hecho de que existan y dispongan de buena financiación da idea de la apuesta por IoT de las instituciones.

Además, existe un proyecto de IoT como prueba de concepto de ciudades inteligentes denominado Smart City Padova [7], donde se ejecutan acciones como aparcamiento inteligente, avisando a los conductores a través de GPS donde hay plazas de aparcamiento libres, alumbrado inteligente, con farolas o luces que se encienden sólo con transeúntes, etc. Así pues, la apuesta de la Unión Europea por IoT en la actualidad y de cara a futuro es clara.

IoT- Horizonte 2050

Nodos Sensores IoT

La evolución de la tecnología de nodos sensores IoT en el horizonte 2050 se encaminará hacia sensores más autónomos tanto energética, como computacionalmente, y con inteligencia incorporada.

1. Nodos sensores IoT con el suficiente poder de cálculo y almacenamiento para dotarlos de inteligencia artificial mediante aprendizaje máquina (*machine learning*), de manera que los nodos sensores IoT no sólo tendrían una determinada respuesta ante una entrada dada, sino que también podrían aprender de los datos y experiencias adquiridas para responder ante situaciones nuevas o inesperadas.

2. Nodos sensores IoT con un funcionamiento perpetuo en términos energéticos gracias a tecnologías de recolección de energía del ambiente como la fotovoltaica y su almacenamiento en baterías de alta calidad.

3. Nodos sensores IoT de menor tamaño, como circuitos integrados del orden de milímetros, típicamente 5 x 5 ó 10 x 10 milímetros, que podrían implementar el denominado polvo inteligente, pequeños circuitos integrados dotados de sensores que podrían esparcirse desde un drone o vehículo aéreo no tripulado para obtener variables en terrenos peligrosos o poco accesibles.
4. Incorporación de nuevas magnitudes que a día de hoy resultan difíciles en un espacio reducido, como por ejemplo procesamiento de vídeo mediante técnicas de aprendizaje profundo (*deep learning*).
5. Circuitos y baterías biodegradables.

El resultado de esta evolución sería una densidad de sensores IoT por unidad de área muy elevada desplegados en lugares insospechados. Una red de sensores para determinar el nivel de corrosión de los cimientos de una plataforma petrolífera, o redes de sensores capaces de recoger energía de reacciones químicas para medir ciertas variables del interior del cuerpo humano, son sólo dos ejemplos de aplicaciones derivadas del avance de nodos sensores IoT.

La industria de semiconductores y la nanoelectrónica son dos de las tecnologías que permiten dicho avance.

Redes y Comunicación

En cuanto a las comunicaciones, hoy en día las comunicaciones por fibra de banda ancha con las denominadas WLAN, junto a las comunicaciones sin cable de tipo WiFi y la móvil 4G son las tecnologías de comunicación dominantes. Sin embargo, en breve se prevé el paso de 4G a 5G, y en el horizonte 2050 se prevé una implantación más masiva de redes de bajo consumo de potencia.

En el horizonte 2050 este autor prevé una evolución en la tecnología de redes y comunicaciones de IoT hacia:

1. Redes inalámbricas de bajo consumo de potencia y corto alcance.
2. Redes de banda ancha de bajo consumo de potencia.
3. Cambio entre tecnologías de comunicación móvil de manera imperceptible (transparente) para el usuario, como por ejemplo entre 4G, 5G y WiFi.
4. Comunicación por satélite, sobre todo en zonas remotas.
5. Más flexibilidad en la configuración de redes mediante redes definidas por software (SDN) para garantizar servicios a través de IoT.
6. Redes de comunicación con capacidad de aprendizaje y repararse contra ataques de seguridad, o contra nodos IoT fallidos.

7. Identificación de las cosas de IoT mediante técnicas de ADN, y también mediante el contexto, que puede referirse tanto al espacial, como al temporal (acciones más comúnmente ejecutadas).

Computación- Aplicaciones y Servicios

La evolución en computación en el horizonte 2050 se encamina hacia:

1. Computación distribuida entre el nodo sensor IoT y el centro de datos de la computación en la nube, reduciendo así el tiempo de respuesta, que, en muchos casos, como la obtención de una ruta para un vehículo autónomo, o respuesta de semáforos ha de ser de ms, tiempo que en muchas ocasiones de poca cobertura no puede garantizarse, obligando a una computación más local, es decir, en el nodo sensor IoT.

2. Computación cognitiva, dotando de inteligencia a los distintos elementos de la red IoT, tanto a nivel de nodo sensor IoT, como a nivel de centro de datos.

3. Computación cognitiva colectiva (*swarm intelligence*) entre los distintos elementos de la red, tanto verticalmente (el caso de un determinado sistema CPS para una determinada aplicación, como por ejemplo la monitorización de cultivos en un invernadero), como horizontalmente (entre distintos sistemas CPS), formando así sistemas de sistemas. Este tipo de computación podría por ejemplo determinar un cuerpo extraño, como un nuevo nodo sensor IoT en una red de sensores para robar datos, o trazar de forma automática la trayectoria y las acciones de una persona sospechosa mediante la colaboración de la red de cámaras públicas en una ciudad inteligente ante una entrada descriptiva del tipo: varón calvo con barba, pantalones vaquero y chaqueta roja.

4. Computación o inteligencia de contexto, que podría servir para determinar qué individuos y qué acciones son las más comunes, anticipándose o acelerando así la toma de decisiones o la ejecución de acciones, y aumentando la seguridad de la red IoT ante elementos poco comunes.

5. Aprendizaje e interacción máquina-máquina, de manera que el aprendizaje no sólo podría realizarse con la supervisión de un humano experto que diseñaría los algoritmos y metodología de aprendizaje, sino que también podrían crearse inteligencias que creasen nuevas inteligencias, generando robots software, los denominados *bots*.

Aplicaciones

Salud, bienestar y envejecimiento activo

La salud, bienestar y envejecimiento constituyen una parte de IoT claramente centrada en el individuo. Los denominados dispositivos vestibles, *wearables* en inglés, constituyen la tecnología que permite IoT de la salud y el bienestar. En el futuro se prevé la incorporación de muchos más elementos de este tipo tanto como elementos externos, como integrados en la vestimenta. Muchos de estos dispositivos se alimentarán recogiendo energía del medio ambiente. Cuellos de camisa para medir el sudor y su composición, vestimentas para medir las calorías quemadas, el aliento, u otras variables como el ritmo cardíaco, o prendas que estimulen y que ayuden a la rehabilitación de un músculo o hueso dañado constituyen algunos ejemplos en el ámbito de la salud, bienestar y envejecimiento activo en IoT. Además, alrededor de estos dispositivos vestibles, habría otros complementarios, como por ejemplo cepillos de dientes que miden la cantidad de flúor, sensores que analizan los excrementos en inodoros, o pañuelos que analizan la composición de mocos o saliva. Todos estos datos podrían analizarse por un médico o experto en colaboración con técnicas de inteligencia distribuida entre el nodo sensor IoT, o en la nube. Finalmente, las personas actuarán con robots (Internet de los Robots; IoTR), continuamente, bien como elementos de ayuda a la decisión en procesos de negocio, bien como asistentes del hogar o en la fábrica, en la denominada Industria 4.0 actual.

Edificios Inteligentes (Internet de los Edificios; IoB)

La evolución de IoT en el horizonte de 2050 podría llevarnos a la transformación de edificios como elementos pasivos en elementos activos de una ciudad inteligente. Los edificios integrarían dispositivos de generación de energía, fundamentalmente fotovoltaica, que interaccionarían con la red de energía inteligente (*smart grid*), intercambiando paquetes de energía con el distribuidor de la misma de modo similar a como hoy en día se hace con paquetes de información o bits entre distintos servidores a lo largo y ancho de Internet. Los edificios también podrían interaccionar con otros elementos externos, formando parte de la ciudad inteligente, informando por ejemplo de la situación del tráfico. Obviamente, los edificios inteligentes facilitarán la vida de sus ocupantes y su interacción mediante aplicaciones y servicios como la localización e identificación de personas en edificios, dónde no hay cobertura GPS, o la interacción táctil o gestual para ejecutar determinadas acciones mediante dispositivos vestibles, o mediante cámaras que reconozcan acciones, o mediante entornos de realidad aumentada o virtual.

Energía Inteligente (Internet de la Energía; IoE)

Un aspecto importante de la red de energía en el futuro es la proliferación de mecanismos de recolección y almacenamiento de energía en el propio hogar. Esto cambiará tanto el papel de los consumidores, que se convertirán en prosumidores, como el de los distribuidores de energía, ya que habrá flujo de energía bidireccional; del hogar hacia la fuente de generación de energía, y viceversa. Se prevé que la energía fotovoltaica sea la dominante en el futuro, y que la red de energía se convierta en la denominada energía en la nube, *energy cloud* en inglés, en donde se analizarán el consumo y distribución de energía de forma similar a cómo se analiza el flujo de información en Internet. En este sentido, las técnicas de inteligencia artificial jugarán un papel determinante para toma de decisiones en procesos de optimización energética.

Transporte Inteligente (Internet del Vehículo; IoV)

Se prevé que el uso del automóvil en 2050 sea completamente diferente al actual, de manera que no se dispondrá de un vehículo para todo, trabajo, ocio, etc., sino que se dispondrá del vehículo como un servicio gestionado bajo demanda a través del móvil integrado en la red global IoT, sobre todo en entornos cada vez menos amigables para el vehículo, como las ciudades superpobladas. Otro elemento disruptivo será la llegada masiva del vehículo autónomo, sin conductor, lo que supondrá un reto en términos de toma de decisiones en ms mediante técnicas de inteligencia artificial, y en términos de la interacción del vehículo con la infraestructura del entorno y con otros vehículos, obligando a mapas actualizados en tiempo real, y a una red global IoT de bajo tiempo de respuesta, gracias, entre otros elementos a la computación distribuida entre nodo sensor IoT y la computación en la nube. Finalmente, también se hará un cambio total de vehículo alimentado por combustibles fósiles al vehículo eléctrico o de energía menos contaminante.

Agricultura Inteligente, Medio Ambiente

La agricultura de precisión es y será cada vez más frecuente, de manera que se extenderán aplicaciones como la previsión de plagas en cualquier plantación mediante la integración de modelos de inteligencia artificial con sensores sobre el terreno, avisando o recomendando el momento y la cantidad de insecticida necesarios. Así mismo, la trazabilidad de la comida desde su recogida hasta su consumo será un común denominador en la industria agroalimentaria. Este mismo modelo se aplicará al ganado. En medio ambiente y en la actividad pesquera, será muy importante evaluar la calidad del agua, o la previsión de riesgos naturales.

El despliegue desde drones de sensores de bajo tamaño, robustos a las inclemencias meteorológicas, y que recogen energía del ambiente será clave para abrir nuevas aplicaciones.

Ciudades Inteligentes

Las denominadas ciudades inteligentes son y serán la suma de interacciones entre las aplicaciones citadas con anterioridad, es decir, salud y bienestar, transporte inteligente, edificios inteligentes, energía inteligente, y medio ambiente.

Implicaciones IoT

Implicaciones Socioeconómicas

Todo lo expuesto con anterioridad nos hace intuir que las implicaciones de la introducción de IoT serán enormes a nivel socioeconómico, adentrándonos en una nueva sociedad digital. El cambio a nivel de organizaciones y relaciones de trabajo y personales serán muy importantes. Hoy en día, ya se vislumbra parte de este cambio en la denominada Industria 4.0, una fábrica o lugar de trabajo más eficiente, con hiperconectividad donde se automatizan todos los procesos de fabricación, y donde se registran todas nuestras acciones a través de flujos de trabajo. IoT llevará un paso más allá la evolución de la Industria 4.0, incorporando técnicas de inteligencia artificial más potentes tanto desde el punto de vista de modelo, como por ejemplo la inteligencia colectiva, como de computación, ya que ésta se distribuirá entre el nodo IoT sensor o dispositivo con el que interaccionamos y la computación en la nube. Las profesiones con trabajos más rutinarios y menos creativos, de baja o alta cualificación, se reducirán en gran medida, y la disminución de costes debido a la automatización podrá hacer que la industria prefiera decantarse por automatización y todos los servicios que ofrece IoT en lugar de la deslocalización.

Implicaciones de Seguridad, Privacidad y Confianza

La hiporconectividad asociada a IoT trae consigo inevitablemente más vulnerabilidad, de modo que IoT exige la implantación de protocolos de comunicación y software más seguros, incluyendo la privacidad de los datos, de manera que sólo el usuario y otros usuarios autorizados puedan acceder a estos datos. Uno de los ataques más comunes y directos en IoT será el denominado "negación de servicio" (Denial of Service; DoS),

debido a que será fácil inundar la red de datos debido a la hiperconectividad inherente a IoT. Evitar éste y otro tipo de ataques será clave para la aceptación de IoT tanto en la industria como en el público en general.

Referencias

[1] Ovidiu Vermesan, Joël Backquet. (2017). Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution. EU, Belgium: River Publishess.

[2] http://www.internet-of-things-research.eu/ (fecha de acceso 26/01/2018).

[3] https://www.fiware.org/ (fecha de acceso 26/01/2018).

[4] https://aws.amazon.com/es/ (fecha de acceso 26/01/2018).

[5] http://www.nvidia.es (fecha de acceso 26/01/2018).

[6] A. Nieto, D.L. Vilariño, V.M. Brea. (August, 2016). PRECISION: A reconfigurable SIMD/MIMD coprocessor for Computer Vision Systems-on-Chip. IEEE Transactions on Computers, 65, 2548-2561.

[7] Andrea Zanella et al. (February, 2014). Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1, 22-32.

[8] Jie Lin et al. (October, 2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, 4, 1125-1142.


ieee.es
Instituto Español de Estudios Estratégicos


USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA


CESEG
CENTRO DE ESTUDOS DE SEGURIDADE