**Towards Solving the IoT Standards Gap (Hacia la solución de la brecha de estándares de IoT)**

**Abstracto:**

Internet de las cosas (IoT) ha recibido una enorme atención en los últimos 5 años. En un futuro próximo, IoT se convertirá en una red de miles de millones de dispositivos inteligentes, sensores, vehículos y electrodomésticos que aparecen en la vida cotidiana de un usuario que recopila y comparte datos para facilitar su vida. En el año 2011, el número de dispositivos conectados a Internet superó la "población humana" en la tierra y se espera que crucen 50 mil millones de dispositivos en todo el mundo para 2020. Con esta explosión en el número de dispositivos, puntos de control y cantidad de datos, conectando estos dispositivos a entre sí y asegurar los datos se convierte en un gran desafío. Existe la necesidad de una estandarización de extremo a extremo de los modelos de recursos de dispositivos IoT, protocolos de conectividad y arquitectura para satisfacer las necesidades de las aplicaciones IoT. Muchos consorcios diferentes están trabajando en esta dirección desarrollando estándares de IoT impulsados ​​principalmente por gigantes de la industria y organismos gubernamentales. En este documento, discutimos los diversos esfuerzos de estandarización que ocurren en todo el mundo y también observamos los estándares específicos de la India. También presentamos nuestra perspectiva sobre la consolidación de estos diferentes estándares de IoT a través de la colaboración y enlaces para desbloquear un mayor potencial de ingresos a través de IoT.

**Publicado en:**[2018 Conferencia internacional sobre avances en informática, comunicaciones e informática (ICACCI)](https://ieeexplore.ieee.org/xpl/conhome/8536361/proceeding)

**Fecha de la conferencia:** 19-22 de septiembre de 2018

**Fecha añadida a IEEE *Xplore* :** 03 de diciembre de 2018

**Información del ISBN:**

**Número de acceso de INSPEC:** 18305792

**DOI:**[10.1109 / ICACCI.2018.8554506](https://doi.org/10.1109/ICACCI.2018.8554506)

**Editorial:**IEEE

**Lugar de la conferencia:** Bangalore, India

**SECCIÓN I.**

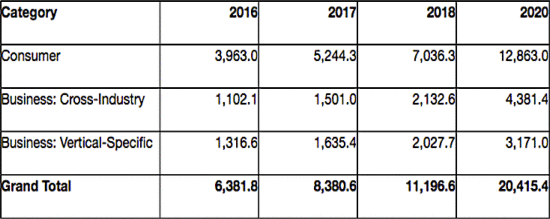
## **Introducción**

Internet de las cosas (IoT) se puede definir como una red de 'cosas' cotidianas que están conectadas / interconectadas en una LAN o una WAN distribuida. Un buen primer paso es pensar en lo que queremos decir cuando hablamos de IoT. En esencia, es la convergencia disruptiva de tecnología, telecomunicaciones, datos y personas. Es la humanización de la tecnología, la fusión de elementos y sistemas dispares en una plataforma unificada, lo que nos permite conectarnos más profundamente entre nosotros y con el mundo que nos rodea. Pero, sobre todo, el IoT es una oportunidad, una oportunidad de tomar mejores decisiones basadas en estas interconexiones, mejorando la calidad no solo de nuestras propias vidas, sino de la sociedad en general.

Todas las cosas conectadas comparten cinco componentes clave: “consumo de energía, almacenamiento y administración más inteligentes; salvaguardas más fuertes para la privacidad y seguridad; microcontroladores de alto rendimiento (MCU); sensores y actuadores; y la capacidad de comunicarse ". El término 'Cosas' puede comprender desde dispositivos pequeños como sensores, cámaras, dispositivos portátiles y teléfonos inteligentes hasta dispositivos enormes como electrodomésticos, automóviles y maquinaria industrial que se comunican entre sí para ofrecer un estilo de vida conveniente a los seres humanos. Las aplicaciones de IoT son amplias y van desde casos de uso simples como encontrar un lugar para estacionar automóviles, verificar el stock de comestibles en el refrigerador y ordenar por sí mismo el filtro de reemplazo de un dispensador de agua hasta la automatización industrial sofisticada más grande y el mantenimiento predictivo de máquinas .

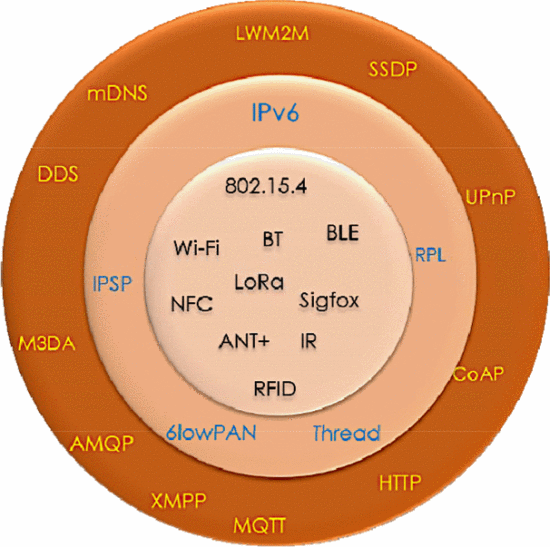
La cantidad de soluciones de IoT implementadas en el mercado ha experimentado un aumento exponencial del 31% en 2017 (con 8,4 billones de dispositivos IoT) en comparación con el año anterior. Se prevé que, en el sector de consumo, los principales productos / soluciones de IoT incluirán televisores inteligentes, electrodomésticos inteligentes y medidores eléctricos conectados. Y en el sector empresarial, incluirá soluciones de seguridad y control de acceso. IDC estima [2] que en 2018 se gastarán alrededor de $ 239 mil millones en la implementación de aplicaciones de IoT inteligentes, de los cuales el costo principal será para infraestructura / hardware (módulos físicos como sensores, actuadores, dispositivos inteligentes) y para asegurar la red de IoT. El gasto restante será para el desarrollo de aplicaciones de software, servicios y conectividad. Tabla 1. del informe Gartner 2017:

**Tabla 1.** Base instalada de IoT (millones de unidades)

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8536361/8554361/8554506/240-table-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8536361/8554361/8554506/240-table-1-source-large.gif)

IoT es muy similar a las computadoras y dispositivos de red tradicionales (enrutadores, conmutadores o módems) que tienen funciones de red con identidad y dirección únicas (MAC / IP) y ejecutan algún tipo de sistema operativo con memoria y potencia de procesamiento. Por lo tanto, las 'cosas' en IoT tienen todas las capacidades [3] de una computadora normal pero a nivel de miniatura. Los dispositivos IoT pueden monitorear, recopilar datos y enviar / recibir datos dentro de la red IoT o comunicarse a través de una red distribuida espacialmente a otro dispositivo, plataforma, servicio y aplicaciones IoT implementados en la nube. IoT es un concepto complejo que comprende varias tecnologías, protocolos y estándares de conectividad. Las siguientes capas proporcionan una abstracción de varios protocolos que existen hoy en día para satisfacer varias aplicaciones de IoT:

* "Infraestructura (por ejemplo: 6LowPAN, IPv4 / IPv6, RPL)
* Protocolos de datos (ej .: MQTT, CoAP, AMQP, Websocket, Node)
* Comunicación / Transporte (ej: Wi-Fi, Bluetooth, ZigBee, LPWAN)
* Semántica (ej .: JSON-LD, Web Thing Model)
* Identificación (por ejemplo: EPC, uCode, IPv6, URI)
* Descubrimiento (ej: Web físico, mDNS, DNS-SD)
* Marcos de varias capas (ej .: Alljoyn, IoTivity, Weave, Homekit) [4]
* Administración de dispositivos (por ejemplo: TR-069, OMA-DM) "



**Figura 1.** Complejidad de los estándares de IoT

Standards are the building blocks that form the IoT's foundation and ensure interoperability. If Cisco's estimate is “even close to the mark, keeping in mind there are some who feel that 50 billion devices by 2020 is even on the low side, then it's pretty clear that for the rapid adoption of the IoT, industry-wide agreements around the aforementioned components are crucial.” Creating wonderfully smart systems and devices will benefit no one if those things are unable to interoperate or communicate with one another. And with the IoT's multifaceted nature allowing it to cross over many disciplines and vertical markets, laying a path to true convergence and interoperability must be a top priority.

La explosión en la cantidad de dispositivos y aplicaciones de IoT que ahora se abren paso en el mercado significa que encontrar una forma de construir consenso en torno a arquitecturas e infraestructuras comunes es de vital importancia. En otras palabras, debemos aprender a caminar antes de poder correr. Una forma de hacerlo es a través del desarrollo y la adopción de estándares abiertos. Recientemente se han lanzado varios proyectos de estandarización, incluido el propio IEEE P2413 de IEEE, “Estándar IEEE para un marco arquitectónico para Internet de las cosas (IoT)”.

Cada uno de estos esfuerzos comparte un objetivo mutuo: tomar la multitud de comunicaciones discretas, procesamiento, programación y otros protocolos y enfoques que ahora compiten para obstruir el IoT y convertirlos en un enfoque único y unificado para desarrollar sus sistemas e infraestructuras fundamentales subyacentes.

Cualquier cambio tecnológico importante (y el IoT puede estar entre los más importantes de la historia) comienza con islas de innovación. Es común que varios grupos formen alianzas industriales donde los miembros aceleran sinérgicamente el progreso que ya comenzaron las compañías de ideas afines. Pero para que estas islas de innovación se conviertan en una vasta masa de tierra del futuro paisaje tecnológico, estas primeras actividades deben transformarse en estándares globales que permitan la economía de escala y ecosistemas vibrantes. Tenemos muchos ejemplos de tales transformaciones, “Actividades Zigbee / HomePlug / Wi-Fi en el área Smart Energy Profile 2.0 e IEEE 2030.5, entre otras”.

El desarrollo del núcleo común de estándares abiertos que incluye: "marcos arquitectónicos, modelos de referencia y planos de abstracción de datos", los componentes básicos del IoT, nos permitirá definir claramente las relaciones entre los numerosos mercados verticales del IoT, como el transporte, la atención médica y entretenimiento. A su vez, esto ayudará a minimizar la fragmentación de la industria y el mercado vertical, mejorar la interoperabilidad y nos permitirá construir ecosistemas de IoT que aprovechen con éxito y eficacia el poder de todas las cosas ". Debido a la disponibilidad de una amplia gama de estándares en la industria, una empresa o un desarrollador selecciona el protocolo o estándar que mejor se adapte a los requisitos inmediatos del proyecto. Y, por lo tanto, el mercado termina con múltiples soluciones patentadas. En tal escenario, Se necesita un 'estándar universal de IoT unificado' que permita una interoperabilidad perfecta entre proveedores y estándares a través de un esquema común de descubrimiento, direccionamiento y modelado de datos. Y solo un 'Estándar de colaboración abierto' puede impulsar a la industria hacia una adopción de estándares comunes.

El último ciclo de Gartner Hype sobre 'Estándares y protocolos de IoT' perfila 30 estándares sobre conectividad, seguridad, mensajería y sistemas operativos para Internet de las cosas. De los cuales, "15 han sido marcados para ofrecer un alto beneficio comercial y se espera que 6 se generalicen en los próximos cinco años", incluyendo:

* ***6LoWPAN*** : un grupo de trabajo bajo IETF que ofrece conectividad IPv6 a través de tecnologías de red que no son IP, como NFC y LoRa a una potencia extremadamente baja, de modo que los dispositivos compatibles pueden funcionar durante años con batería.
* ***Contiki*** : un sistema operativo de código abierto para microcontroladores IoT de bajo costo y bajo consumo.
* ***LiteOS*** : un sistema operativo tipo Unix para redes de sensores inalámbricos.
* ***oneM2M***: a Service layer standard focusing on Machine-to-Machine connectivity design & modules.
* ***RPMA*** (Random Phase Multiple Access): a proprietary standard for connecting IoT objects.
* ***Sigfox***: a proprietary low-power, low-throughput technology for IoT & M2M communications.

From the above list & the hype cycle, it is apparent that multiple IoT standards are trying to solve the same problem & have lot of overlapping functionalities. Also they target the same markets using different technological approaches. In fact, several multibillion-dollar battles are fought as competing vendors & standards organizations vie for IoT dominance & attempt to convince customers that their respective standards are the best way forward.

Some technologies are less proven than the others & so the goal of the standardisation effort is to legitimize such technologies & make customers feel safe that they can go ahead & use it, as opposed to it being proprietary & a closed system that may not be developed over time. A ‘Universal Unified IoT Standard’ is the key to success of IoT & also an innovation driver in the market, as there's little fear of infringement with a standard which is universally accepted & works well with even other competing standards. Such a standard promotes innovation as there are skills that exist & can be leveraged to integrate a new technology onto the existing platform/solution with the knowledge of the open standard.

Another part of the standards puzzle is security. In fact, Security is one of the biggest concerns when it comes to IoT & not only because of a series of security breach incidents involving unpatched IoT devices but because of the enormous amount of data that is generated from billions of connected IoT devices. According to Gartner, 25% of the known enterprise security attacks will target IoT networks by 2020 & yet only 10% of enterprise security budgets is devoted to IoT.

As billions of IoT devices come online in the next five years, the threat of a massive security breach increases exponentially. There have been incidents where companies have already been taken offline by attacks involving PLCs, video cameras & even industrial safety systems. Could new IoT security standards help protect corporate assets & critical infrastructure? Yes, we believe *pervasive security standards* could simplify the on-boarding of IoT devices & help protect IoT data.

The open standard that could seamlessly & securely connect new devices would speed-up the adoption of IoT by not only streamlining setup processes, but also by reassuring consumers & corporate users that devices & data will be protected. That said, there are multiple IoT solutions which are being deployed in the market today helping businesses to earn revenue with high risk of security breach. One of the primary limitations in IoT today is companies not having a clear strategy on Standards & Security. While some emerging IoT standards such as MatrixSSL address network security, others require security add-ons or additional implementation steps. For instance, Message Queuing Telemetry Transport (MQTT) transmits data in clear text, requiring additional security mechanisms for mission-critical IoT implementations.

And then there is the security gap when it comes to sensors, actuators & drives. While the network connecting these devices can be secured, there are no security standards at the device level securing each device leading to huge implications for solution integrity & also personnel safety. The International Society of Automation recently created a working group to better understand such gaps with an eye towards developing standards around the devices.

**SECTION II.**

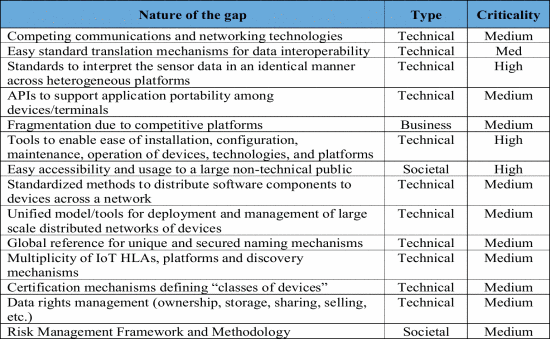
## **Gaps**

The identification and resolution of gaps is a clear concern for the IoT community. ETSI Technical Report on IoT Gaps [16], “Three categories of gaps have been addressed:

1. Technology gaps with examples such as communications paradigms, data models or ontologies, or software availability.
2. Societal gaps with examples such as privacy, energy consumption, or ease of use.
3. Business gaps with examples such as silo-ed applications, incomplete value chains, or missing investment.”

Once gaps have been identified, the actors in the technical community (standardisation in particular) may perceived differently the criticality depending on the role. The Table 2 lists these gaps and provides an average view of their criticality, that could be different with various roles (e.g., “users, service providers”). The characterization of gaps is a “work-in-progress” for the IoT Standardization forums.

**Table 2.**IoT standardization gaps



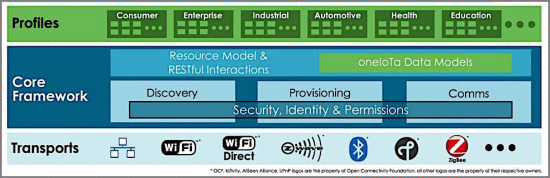
**SECTION III.**

## **IoT Standards: Key Consortiums & Alliances**

### A. Open Connectivity Foundation (OCF)

This organization was formed in 2014 as an “Open Internet Consortium” (OIC). With patronage and support from industry, mainly: Intel, Samsung, Dell, Atmel, and Wind River, the primary aim was to develop a framework for “Internet of Everything”. In 2017, with the partnership of Allseen Alliance and more industries including Qualcomm, Microsoft, and Electrolux, the organization changed the name to Open Connectivity Foundation (OCF). Currently, about 300 companies are supporting this initiative as active members.

OCF being the most active and one of the largest Industrial connectivity SDO in the IoT domain, their activities are designed to enumerate “security schemes, compliance standards, interoperability guidelines” for both consumers and enterprises. They strive to drive both functional and interoperability standards, for communication protocols and establish certification guidelines for IoT infrastructure and devices.



**Fig. 2.** OCF architecture

OCF sponsors the open source programs “IoTivity” and “AllSeen Alliance – AllJoyn” hosted at *Linux Foundation*. The architectural goal of IoTivity is “to interconnect both wired and wireless devices, with the Internet to ensure a protectable and resilient architecture for smart/lightweight devices”. AllJoyn's framework goal is “to build an open extensible design, to allow devices to communicate with peripheral devices and to connect to clouds by promoting proximal networks”. In October 2016, OCF merged both “AllJoyn and IoTivity” and ensured interoperability, backward compatibility support as well. To enable faster adoption, the license policy was changed from “Apache 2.0 to Apache 1.2.1” in the allied project [5].

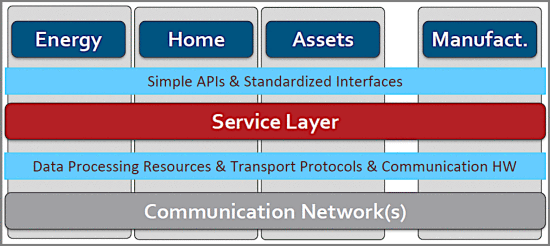
### B. Allseen Alliance

Allseen Alliance is an industry consortium founded by Qualcomm, Microsoft, Panasonic, Sony & LG. It offers an open development platform with an objective to enable the integration of IoT products, systems & services. Allseen's Alljoyn framework provides a unified standard communication protocol that is transport-layer/vendor agnostic & enables seamless interoperability to devices & applications in the network.

Allseen Alliance se fusionó con OCF en octubre de 2016, lo que representa un movimiento significativo hacia un ecosistema convergente que permite una plataforma operativa colaborativa escalable para IoT. Esta fusión también facilitó la colaboración en las sinergias entre las iniciativas de estandarización Allseen y OCF. El nuevo marco continúa admitiendo la interoperabilidad y ofrece compatibilidad para las funcionalidades de la generación anterior [7] .

### C. OneM2M

*Un* foro de estándares globales que cubre: "requisitos, arquitectura, API, seguridad, interoperabilidad" para M2M e IoT. *oneM2M,* fundada en 2012, abarca una amplia red de organizaciones activas populares de todo el mundo: “ARIB (Japón), ATIS (EE. UU.), CCSA (China), ETSI (Europa), TIA (EE. UU.), TSDSI (India), TTA ( Corea) y TTC (Japón) ". También trajo a su red, una serie de consorcios de la industria: "Foro de Banda Ancha, CEN, CENELEC, Plataforma Global, OMA)" e incluye más de "200 miembros".

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8536361/8554361/8554506/240-fig-3-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8536361/8554361/8554506/240-fig-3-source-large.gif)

**Fig. 3.** arquitectura oneM2M

La especificación oneM2M ha establecido un marco para soportar aplicaciones y servicios en “red inteligente, automóvil conectado, domótica, seguridad pública y salud”. Las alianzas OCF y oneM2M han firmado un acuerdo de enlace para colaborar para mejorar la interoperabilidad.

### D. Comisión de Estudio 20 del UIT-T (SG20)

Este grupo es uno de los organismos especiales de las Naciones Unidas para TI y comunicaciones. tecnologías. Bajo esta organización, el "Grupo de estudio 20" (SG20) se centra en la estandarización de IoT y las tecnologías aplicadas. SG20 coordina el desarrollo de estándares en IoT, M2M y tecnologías ubicuas de redes inalámbricas de sensores. La actividad principal es abordar los requisitos de las arquitecturas IoT "de extremo a extremo", la interoperabilidad de las aplicaciones y los conjuntos de datos empleados por varias verticales en la industria [11] .

### E. Grupo de subprocesos

Thread group [5] was formed by industry giants including Samsung, Nest, ARM, Silicon Labs & others with a primary objective to: a) develop secure, scalable network b) develop simple communication interfaces in mesh topology c) develop light weight mechanisms for low power efficient IoT operations d) use open network standards supporting IPv4/v6/6loWPAN protocols.

In the home automation space, there is a single gateway device around which all the other products in the home network communicate & operate. This leads to a single point of failure due to hacking or device failure. To address this problem, the Thread Group released the thread technology, which is scalable & resilient with modern authentication & encryption schemes. The design is inspired by Google Nest's technology & the network protocol offers secure & reliable communication interface to connect swarm of smart home devices/appliances, environment control, security/access, power/energy monitoring, lighting & safety control, with optimal battery burn rate. The OCF & Thread group have signed up a joint collaborative agenda, for enhancing interoperability across applications & IoT devices interconnectivity in smart homes.

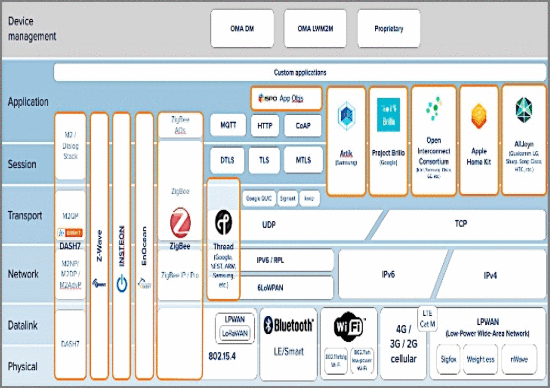
### F. Industrial Internet Consortium (IIC)

In 2014, IIC was established by Intel, IBM, GE, Cisco & AT&T, with an aim to drive the architectural frameworks for Industrial IoT: coordinating various ecosystem initiatives to connect objects using common architectures, interoperability & open standards – making it easier to adopt interconnected machines & intelligent analytics.

Over the years, IIC has unveiled up to nine test beds for real-world applications, such as the Track & Trace test bed – which helps manage handheld power tools in manufacturing environments & the Edge Intelligence test bed – which aims to accelerate the development of edge architectures & algorithms. These test beds guide & support the solution providers & system integrators who want to build Internet of Things solutions in the industrial space.

### G. Others

* IETF (“Internet Engineering Task Force”): Develops & promotes Internet standards that comprise of the Internet protocol suite. Key IoT standards groups – CoRE (“Constrained RESTful Environments”), 6lowpan (“IPv6 over Low power WPAN”), ROLL (“Routing Over Low power & Lossy networks”)
* ETSI (European Telecommunications Standards Institute): Standardization organization in the telecommunications industry of Europe. ETSI's ‘Connecting Things' cluster is developing standards & addressing an application-independent ‘horizontal’ service platform which is capable of supporting a very wide range of services including smart metering, smart grids, eHealth, city automation, consumer applications and connected vehicles.
* AIOTI (“Alliance for Internet of Things Innovation”): Initiated by the European Commission in order to develop & support the dialogue & interaction among the Internet of Things (IoT) players in Europe. The overall goal of the AlOTI is the creation of a dynamic European IoT ecosystem to unleash the potentials of the IoT. Working group WG03 focuses on IoT Standardization.
* IEEE (“Institute of Electrical & Electronics Engineers”): IEEE's IoT Innovation Space is a collaborative gathering place for technologists working on IoT to provide the platform where IoT professionals learn, share knowledge & collaborate on this sweeping convergence of technologies, markets, applications & the Internet to change the world
* IEC (“International Electro-technical Commission”) & ISO (“International Organization for Standardization”), JTC (“Joint Technical Committee”) SC41 (“Sub-Committee”) work on standardizing ‘Internet of things and related technologies’
* OMG/DDS (“Object Management Group/Data Distribution Service for real-time systems”): address the “machine-to-machine middleware standard to enable scalable, real-time, dependable, high-performance and interoperable data exchanges”.
* 3GPP:(“3rd Generation Partnership Project”) umbrella organization with seven-member groups (“ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC”)
* NB-IoT: (“Narrow Band radio technology to address the requirements of the IoT”) works on improving the various functional aspects, architectural requirements and characteristics to deliver low-operational and efficiency metrics.
* OASIS (“Organization for the Advancement of Structured Information Standards”): OASIS's MQTT Committee telemetry standards and light weight communication protocols.
* OGC (“Open Geospatial Consortium”): OGC's “Sensor Web for IoT” workgroup investigates the Sensor Web Enablement domain. It is tasked with “Web-friendly & efficient sensor interfaces/networks using the Representational State Transfer (REST)” model.
* IoT-A: (“European Lighthouse Integrated Project”) addresses IoT Architecture to create reference architectures and foundational definitions.
* OSIOT: develops & promotes licence-free, creative-common, free & open source for IoT.
* IoT-GSI (“Global Standards Initiative on Internet of Things”): worldwide organization involved in harmonizing the resulting standards, public deliverables and consolidating the IoT standards.
* W3C: Word Wide Web consortium
* SSNO: “Semantic Sensor Net Ontology”
* WTCG “Web of Things Community Group”
* ISA (International Society of Automation)
* RRG (“Routing research group”)
* HIPRG (“Host identity protocol research group”)



**Fig. 4.** IoT architecture, protocols & standards [6]

**SECTION IV.**

## **IoT Standards: Key Region Landscapes**

### A. North America

Un informe reciente sobre la estandarización de IoT del 'Instituto Nacional de Estándares y Tecnología (NIST)' [9] , concluyó: “Sin un conjunto estandarizado de requisitos de ciberseguridad, los actores maliciosos podrían explotar las brechas de seguridad y los sistemas de IoT podrían ser vulnerables a los ataques cibernéticos. Hay una necesidad de estándares de seguridad voluntarios, especialmente porque la industria de IoT es dinámica y está en un estado de cambio. Los esfuerzos legislativos están en marcha diseñados para regular ciertos estándares de seguridad de TI para los sistemas IoT en el gobierno ".

El informe afirmó además: “Las 11 áreas centrales de ciberseguridad enumeradas en este informe no son exhaustivas y proporcionan ejemplos de estándares relevantes. La ciberseguridad para IoT es única y sin estándares, los sistemas de IoT podrían tener lagunas en muchas áreas, incluidas las técnicas criptográficas, la gestión de incidentes cibernéticos, la seguridad de la red, los sistemas de gestión de seguridad de la información, la garantía de software y más. NIST recomienda que las agencias gubernamentales impongan el cumplimiento de los estándares en las adquisiciones, apoyen el desarrollo de esquemas de evaluación de conformidad adecuados a los requisitos de dichos estándares, citando la adopción del logotipo de Wi-Fi (alianza de certificación de Wi-Fi) para productos y dispositivos ".

El informe NIST llega en un momento en que varios organismos y foros internacionales han propuesto iniciativas para establecer estándares de IoT. El informe afirma además que: "Los esfuerzos de certificación de seguridad en curso en China y Europa, así como un aumento significativo este año en el uso de ataques de amplificación de botnets, han puesto a las agencias y a la industria de EE. UU. En una carrera para establecer estándares internacionales de seguridad de referencia para dispositivos conectados . "

### B. Europa

ETSI junto con varias otras organizaciones aliadas como CEN, CENELEC, ESMIG, CESI, Continua, ENISA, OMA están desarrollando estándares a través de su clúster 'Connected Things'. El "Grupo de Investigación Europea de Internet de las Cosas (IERC)" se estableció para impulsar las actividades de pre-estandarización en el dominio de IoT y la hoja de ruta de estandarización de IoT. También trabajan con varios grupos de la comunidad de pares, como los "grupos de EC" para los procesos de regulación y estandarización.

*ESPRESSO* ("enfoque de estandarización sistémica para empoderar a las ciudades y comunidades inteligentes") se crea para desarrollar el marco conceptual de Smart City para la región de la UE basado en estándares abiertos.

*Smart M2M* es el grupo clave en Europa que desarrolla una hoja de ruta técnica para ciudades inteligentes y el marco medioambiental de IoT. Han estado trabajando en varios mandatos de la Comisión Europea (CE) como el Mandato 441 sobre Medición Inteligente (M / 441 se refiere a funciones de interoperabilidad en medidores de servicios públicos para áreas como electricidad, agua, calefacción, gas) y el Mandato 490 que trata sobre Smart -Rejillas y servicios.

### C. India

Se estima que el mercado de IoT en India tocará 15Bnby2020 w i t h In di a a c c o u n t i n gFo r n e a r l y5 51Bn de inversión del gobierno indio cada año para construir 100 ciudades inteligentes, IoT será fundamental en la construcción de diversas aplicaciones como parte de Digital India. El marco de políticas de IoT para India propuesto por el Ministerio de Electrónica y Tecnología de la Información (MeiTy ​​India) emplea un enfoque de múltiples pilares que comprende 5 verticales y 2 horizontales, incluidas las normas. Se ha establecido un plan para designar una autoridad nodal para conducir y formalizar estándares con respecto a las tecnologías [1] . A continuación, discutimos algunas de las principales iniciativas de estándares de IoT que están trabajando para cumplir con los requisitos específicos de India.

#### "Sociedad de Desarrollo de Normas de Telecomunicaciones", India

TSDSI is chartered to promote technologies in the telecommunications & networking sectors & also steer the standardization of specific requirements in Indian context. TSDSI helps create the manufacturing processes in India & also provides regional leadership for neighboring developing nations in the domain of telecommunications. It also represents the interests & perspectives of India in standardization forums globally viz.: ITU, 3GPP, oneM2M & others.

#### Bureau of Indian Standards (BIS)

A recent report on ‘Smart Infrastructure Panel LITDC/P2’, published by Bureau of Indian Standards, concluded that “The last-mile communication technologies will need to connect heterogeneous devices with heterogeneous applications. A unified last-mile stack will enable the necessary interoperability across all such devices (irrespective of the diversity in the PHY & Link-Layer Technologies) & offer a seamless view to the application. It should also allow connectivity to existing infrastructures & to the Internet. In this regard, we need to thoroughly access the suitable candidate technologies, protocols & standards for unification of the last-mile communication for Smart Infrastructure needs” [10].

Through a common network-layer protocol, IP-based “last-mile” architecture enables interoperability at the levels:

* Among IEEE 802.11/IEEE 802.15.4 data link layer standards, cellular, Bluetooth or Powerline Communication (PLC) etc.
* Among heterogeneous applications such as web-based configuration systems, publish-subscribe protocols, etc.

Hence, it is imperative that India has to develop a Unified Last Mile Communication Standard in which:

* Layer 3-6 shall be immediately Unified & standardized.
* For all the prevalent communication technologies that support IP, Interfaces L1 - L2 & L3–L6 shall be defined.
* A comprehensive Framework and Directory for defining Data Semantics in a unified, harmonized & structured manner shall either be Identified (if it exists) or developed for Smart Infrastructure domain.

#### Experto Europeo en Normalización Secundario en India

SESEI es un proyecto conjunto indoeuropeo con sede en India, creado para promover la cooperación entre la Unión Europea / EFTA-India en materia de normas y otras tecnologías aliadas. Este proyecto se centra en actividades de estandarización para tecnologías en general, pero con un énfasis prioritario en los sectores de las TIC, automoción, electrónica de consumo e industria, ciberseguridad, ciudades inteligentes, etc. Actualmente, el proyecto SESEI se centra en áreas de impulso como: M2M, IoT, moderno diseños de red, ciberseguridad, 5G, SDN y NFV. Se espera que las recientes reuniones y talleres de colaboración celebrados en la India avancen las iniciativas de estandarización global tanto de la UE como de la India.

**SECCION V.**

## **Desafíos**

Todos los consorcios que trabajan en la estandarización de IoT hoy admiten membresía abierta en toda la industria, distribuyen el código de fuente abierta y la documentación técnica, protegen la IP y también proporcionan la certificación del dispositivo. Con todo el replanteamiento en curso, no existe (todavía) un único estándar de IoT común que permita una infraestructura de colaboración; de hecho, incluso los enfoques tradicionales de conectividad de IoT que utilizan dispositivos web y en la nube están siendo cuestionados con la aparición de peer to peer ( P2P) arquitecturas para aprovechar operaciones de baja potencia y más rápidas.

Thread, ZigBee, AllSeen, Open Connectivity Foundation han formulado especificaciones y estándares para construir conexiones entre varias áreas de IoT a través de diferentes formas de tecnologías y protocolos y para definir un estándar común para la conectividad y el descubrimiento de servicios para que las diferentes verticales de IoT puedan unirse. A medida que los proveedores luchan por dar sentido al Internet de las cosas, el mercado se está dando cuenta de la necesidad de estándares consistentes y una amplia interoperabilidad para un ecosistema conectado y transparente alrededor de IoT. Uno de los mayores desafíos que ha traído la fragmentación de los estándares es una gran cantidad de dispositivos, algunos de los cuales pueden estar en una ruta crítica, y algunos de los cuales se ven obligados a quedar obsoletos debido a la falta de estándares. Esto se combina con la vida impredecible de los estándares, sus cláusulas de licencia, debido a adquisiciones,

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8536361/8554361/8554506/240-fig-5-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8536361/8554361/8554506/240-fig-5-source-large.gif)

**Fig.5.** Paisaje de estándares y alianzas de IoT

La falta de estándares también tiene un gran impacto en el costo de la adaptación de IoT, ya que múltiples estándares no cooperativos obligan a los ODM a crear capas adicionales de abstracciones h / w & s / w para satisfacer estándares mutuamente excluyentes.

**SECCION VI.**

## **Marco estándar unificado de IoT propuesto**

We propose a ‘Unified IoT Standard’ framework which will interwork with various standards organizations by developing a common architecture utilizing the best implementations from each standard enabling seamless interaction across different frameworks. The proposed framework enables interoperability of standards by building smart connectors/bridges that translates the specifications into a common language. The connectors will be flexible across vertical markets & extensible to address new specifications for markets that are not there yet. Also, it will co-work with certification bodies of different standards organizations & provide intellectual property & branding protection as a benefit of certification. Additionally, it will also provide a platform/framework for the community to develop new IoT enabled services & to test if their applications are compliant & if the devices can share data securely.

Interoperability will be the key and critical element in ensuring “seamless communication and flow of data” across sectors and domains in the future IoT systems. We propose some steps that are necessary to arrive at common standards and solutions that will foster collaboration and reduce fragmentation:

* promote “horizontal standards” rather than “vertical specific”
* integrating “horizontal frameworks (e.g., oneM2M)” with open platform support;
* Address cross-layer solutions (e.g. data management, security) must be also supported by standards; and provided by the SDOs and SSOs;
* Efficient security, trust and privacy guarantee are essential to acceptance and faster adaption to the unified standards, covering holistic views(e.g., “security by design, privacy by design, user-centric and data-centric solutions”);

Algunas nuevas tendencias en el diseño de sistemas IoT (p. Ej., Virtualización de IoT) estarán respaldadas por una reutilización masiva de componentes OSS. Esto desafía el papel tradicional de los estándares. Por otro lado, los nuevos enfoques para el diseño de sistemas IoT también pueden requerir que algunos bloques de construcción existentes (y los estándares asociados) se reconsideren y, a su vez, promuevan el desarrollo de nuevos estándares.

El objetivo de lograr una verdadera 'interoperabilidad de todo' y desbloquear un mayor potencial de ingresos a través de IoT se basa en esta consolidación e interfuncionamiento de todos estos estándares. Un marco de 'estándar de IoT unificado' en todo el mundo logrado a través de colaboraciones y enlaces con organismos y consorcios de estándares existentes es la clave para permitir una interoperabilidad perfecta en miles de millones de cosas. El tiempo de comercialización de las soluciones de IoT se reducirá drásticamente con dicho marco y permitirá a las startups / PYME / desarrolladores de IoT que trabajan en IoT crear fácilmente soluciones plug and play al conectarse a varias plataformas de IoT, independientemente del estándar que adopte.

**SECCION VII.**

## **Conclusión**

Los consorcios de IoT se diferencian al establecer su valor agregado de manera diferente y promocionar sus rangos de membresía, pero el denominador común es que todos tienen una amplia representación de socios de la industria y han desarrollado una especificación para el descubrimiento confiable, la conectividad, la interoperabilidad y una implementación de referencia de lo mismo. Admiten un proyecto de código abierto y una base de código que distribuyen y administran a través de un modelo de gobierno de fuente. Los fabricantes de dispositivos pueden tomar el código y cambiarlo para satisfacer necesidades personalizadas. Pero el éxito y el crecimiento de IoT dependen en gran medida de la cooperación de todos estos estándares.

### RECONOCIMIENTO

Extendemos nuestros agradecimientos al "Decanato de Investigación" en la Universidad de Amrita, los laboratorios de I + D de Samsung e Intel.