#	TITLE
	Title
1	A Feasible Cellular Internet of Things: Enabling Edge Computing and the IoT in Dense Futuristic Cellular Networks.
2	Access control in Internet of Things: Big challengues and new opportunities.

3	Internet of Things: A Review of Surveys Based on Context Aware Intelligent Services.

4	Internet-of-Things-Based Smart Environments: State of the Art, Taxonomy, and Open Research Challenges.
5	Internet of Things and Business Models.

6	Security and privacy considerations for IoT application on smart grids: Survey and research challenges.
7	Security, privacy and trust in Internet of Things: A straight road?

8	L'integrazione delle infrastrutture urbane fisiche e digitali: il ruolo dei "Big Data".
	The evolution of the internet of things industry and

9	The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply.
10	Towards a Smart city based on cloud of things, a survey on the Smart city vision and paradigms.

ABSTRACT

Structured summary

En este artículo se muestran dos escenarios de despliegue típicos de Internet Celular de las Cosas (C-IoT) con Edge Computing (EC), por medio de este se identifican los desafíos cruciales y soluciones. Una de estas soluciones es el procedimiento RACH, que ayuda a que un millón de dispositivos puedan acceder a la red celular.

En este artículo se proporciona una revisión técnica de diversas soluciones de control de acceso en IoT dentro de la vía Objetivos, Modelos, Arquitectura y Mecanismos (OM-AM). Al mismo tiempo se realiza un análisis de los requisitos de seguridad y privacidad para los dominios de aplicaciones IoT más dominantes, además se resaltan pros y contras de los modelos de control de accesos tradicionales y los protocolos recientes desde la nueva perspectiva IoT. Otro factor es la evaluación cualitativa y cuantitativa de los proyectos relacionados con IoT relevantes que reflejan soluciones de investigaciones y comerciales propuestas en este campo de control de accesos. Y como última instancia los desafíos potenciales y las orientaciones futuras de investigación.

En este artículo se revisan las tecnologías, enfoques y modelos actuales de IoT con el fin de descubrir que desafíos necesitan para tener más sentido los datos. Además, se presenta un estado del arte del IoT desde la perspectiva del contexto que permite la integración de IoT y las redes sociales en el emergente Internet Social de las Cosas (SIoT).

En este artículo se examina los esfuerzos de investigación de vanguardia para permitir ambientes inteligentes basados en IoT, se clasifica la literatura diseñando una taxonomía basada en facilitadoras de comunicación, tipos de redes, tecnologías, estándares inalámbricas de área local, objetivos y características. Además el artículo destaca las oportunidades sin precedentes que provocan los entornos inteligentes basados en IoT y su efecto en la vida humana. También se presentan algunos estudios de casos reportados de diferentes empresas. Finalmente, se discuten desafíos de investigación abierta para habilitar entornos inteligentes basados en IoT.

En este trabajo se analiza el impacto de IoT en los modelos de negocio y fuentes de creación de valor aplicando un marco propuesto a ilustraciones empíricas.

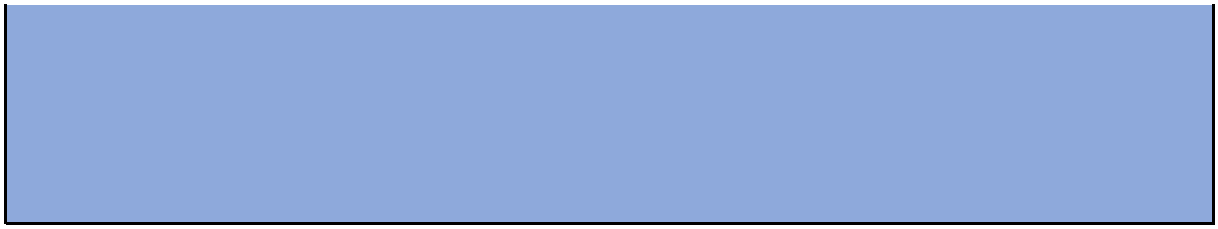
En este documento se ofrece una visión general de los desafíos de seguridad y privacidad de IoT en el despliegue y la gestión de la red inteligente. Además se abordan tres tipos de dominios de desafío: el dominio del cliente, el dominio de la información y la comunicación y el dominio de red.
En este artículo aborda las preocupaciones más importantes relacionadas con los problemas de seguridad en IoT. El principal factor habilitador de este paradigma prometedor es la integración de varias tecnologías y soluciones de comunicaciones con técnicas de seguridad y privacidad.

En este artículo se evaluó el análisis del papel de la información con respecto a la interacción entre el material y lo inmaterial, planteando una serie de cuestiones de interpretación que en el documento se describen.

Este documento pretende proporcionar alguna explicación sobre como los factores relacionados con la demanda, la oferta y las instituciones en China han afectado la creación y difusión de productos y servicios relacionados con Internet de Cosas. En cuanto a los factores de la demandas, el documento demuestra como

el tamaño del mercado potencial y la trayectoria tecnológica existente trabajan a favor de la difusión de IoT. Como factor relacionado con la demanda, el artículo sostiene que, en términos de la trayectoria tecnológica, China ha comenzado más lejos de la frontera que la mayoría de los países industrializados. En cuanto a los factores del lado de la oferta, el articulo promueve una comprensión de como las empresas de tecnología China han capitalizado en una enorme base de usuarios para desarrollar aplicaciones basadas en IoT.

Este documento examina la anotación semántica de los sensores en Cloud, y los servicios innovadores que pueden ser implementados y considerados para realizar la agregación de recursos heterogéneos mediante la definición del paradigma CoT. Se examina la visión inteligente de la ciudad, proporcionando información sobre los principales requisitos y destacando los beneficios de integrar diferentes ecosistemas de IoT dentro de Cloud bajo esta nueva visión CoT. También se analizan los retos relevantes en esta área de investigación.



INTRODU
Rationale
El Internet Celular de las Cosas (C-IoT) con Edge Computing (EC) es una tecnología prometedora en los sistemas celulares de quinta generación (5G), que permite conectar todo a Internet. Estos dispositivos se identifican por ser de baja potencia y soportar un rango de transmisión más largo, además de estar desarrollados para permitir IoT en áreas densas y remotas.
Esta es la era de Internet de las Cosas, donde las barreras entre los mundo real y cibernético son destruidas más rápidamente, convirtiendo cada día dispositivos físicos en objetos inteligentes, cuando esto comienza a pasar va a ser un gran motor para crear nuevos productos y nuevos servicios para mejorar el estilo de vida cotidiano de las personas, generar nuevos negocios, entre otras cosas, estos millones de dispositivos están siendo impregnados en nuestro entorno y nuestros cuerpos. Como consecuencia, frente al éxito o el fracaso de esta evolución revolucionaria estará determinado por dos desafíos clave: seguridad y privacidad.

Internet de las Cosas (IoT) ha permitido que los dispositivos de todo el mundo adquieran información y la almacenen, para poder utilizarla posteriormente. No obstante, esta oportunidad potencial a menudo no se explota debido al intervalo excesivamente grande entre la recopilación de datos y la capacidad de procesarla y analizarla.

Los rápidos avances en las tecnologías de la comunicación y el crecimiento explosivo de Internet de las Cosas han permitido al mundo físico interconectarse invisiblemente con actuadores, sensores y otros elementos computacionales, manteniendo la conectividad de red continua. El mundo físico conectado continuamente con elementos computacionales forma un ambiente inteligente. Un entorno inteligente apunta a apoyar y mejorar las habilidades de sus habitantes en la ejecución de sus tareas, como navegar a través de espacio desconocido y mover objetos pesados para los ancianos, por nombrar algunos. Los investigadores han llevado a cabo una serie de esfuerzos para utilizar IoT para facilitar nuestras vidas e investigar el efecto de los entornos inteligentes basados en IoT en la vida humana.

Las implicaciones de entendimiento en el rendimiento de la empresa desde la aparición de Internet de las Cosas (IoT) son fundamental para que las empresas tomen decisiones racionales sobre las configuraciones de modelos de negocio y las inversiones en IoT. Se espera que la transición entre el estado actual y la adopción y difusión generalizada de IoT sea compleja y la estandarización sea una de las múltiples barreras discutidas en la investigación sobre IoT. Con el fin de garantizar la interoperabilidad entre miles de millones de dispositivos heterogéneos, la normalización puede ser un factor significativo con un posible impacto en las inversiones de IoT.

La aparición y evolución de Internet de las Cosas (IoT) ofrece grandes ventajas para mejorar sustancialmente la gestión del consumo y distribución de electricidad en beneficio de los consumidores, proveedores y operadores de la red. Sin embargo, la introducción de dispositivos y tecnologías relacionadas con IoT en las redes inteligentes podría conducir a nuevos desafíos de seguridad y privacidad. Aunque se están desarrollando las innovaciones tecnológicas necesarias para garantizar una comunicación segura, se requiere aún más trabajo hacia normas más seguras para la comunicación entre dispositivos y redes inteligentes.

El Internet de las Cosas es casi un nuevo paradigma que está revolucionando la sociedad y la vida. Se pretende que todos los objetos que rodean a los seres humanos estén conectados a la web, que van desde dispositivos móviles a dispositivos; al mismo tiempo, el desarrollo de IoT da lugar a una serie de cuestiones éticas y de seguridad que cobran una nueva dimensión a la luz de la creciente complejidad de estas tecnologías. El mayor problema es que IoT no se refiere solo a objetos, sino que se trata de las relaciones entre los objetos cotidianos que rodean a los seres humanos. Es importante enfatizar que la mayoría de los objetos conectados no siempre son personales y están desatendidos, además su seguridad física no está garantizada y el control de los objetos puede ser perdido a veces

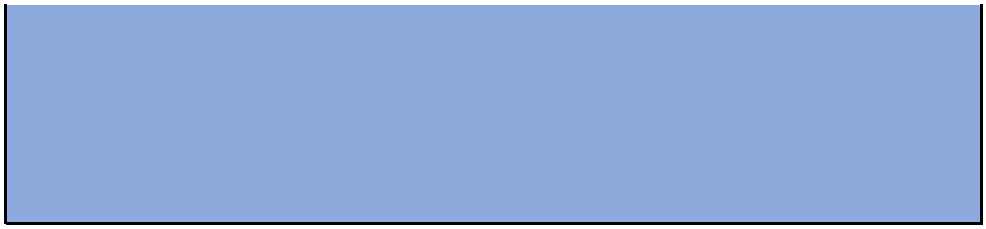
puede ser perdido a veces.

Los muchos desarrollos en el campo de la gestión de la información, el establecimiento de los conceptos de grandes volúmenes de datos y IoT, el desarrollo y la difusión de los sensores se están abriendo a escenarios innovadores y esbozar nuevos problemas con respecto a la cognitiva y la toma de decisiones, con formas especificas si se considera en relación con el ámbito de las infraestructuras, la construcción y la propiedad urbana.

Las tecnologías y los conocimientos especializados proporcionados por las multinacionales extranjeras han desempeñado un papel crucial. En cuanto a las instituciones formales, las políticas proactivas del gobierno han sido un factor importante en la evolución del IoT. También está en el interés del gobierno chino en desarrollar productos IoT para hacer más efectiva la censura y la vigilancia. Con respecto a las instituciones informales, los consumidores chinos están menos preocupados que

los occidentales por ser rastreados y monitoreados, lo que constituye una condición favorable para la adopción de dispositivos habilitados para IoT. Sin embargo, esta condición está cambiando debido al creciente abuso de la privacidad de los consumidores. China y Estados Unidos se comparan en términos de difusión, determinantes clave, indicadores de desempeño e impactos del IoT para entender las áreas en las que China supera a los Estados Unidos y los desempeña de manera insuficiente. Algunos indicadores se proponen para medir el desempeño relacionado con el IOT y los impactos de este.

En los últimos años el concepto de ciudad inteligente ha jugado un rol importante en los campos académicos y de la industria, con el desarrollo y despliegue de varias plataformas de middleware e infraestructuras basadas en IoT. Sin embargo, esta expansión ha seguido distintos enfoques creando, escenarios en el que diferentes ecosistemas IoT no son capaces de comunicarse entre ellos. Para llenar este vacío, es necesario volver a visitar la ciudad inteligente IoT semántica y ofrecer un enfoque global común.



ICTION
Objectives
Los dispositivos de comunicación tipo maquina (MTC) / C-IoT necesitan una conectividad ubicua, que es proporcionada por la infraestructura celular. En otras palabras, a medida que aumenta la densidad de estos dispositivos, se vuelve más difícil conectarlos a la red celular dentro de la cantidad estipulada de tiempo. Por esta razón este articulo tiene el objetivo de enfatizar en el procedimiento rápido RACH, el cual permite acceder a los dispositivos C-IoT realicen este procedimiento RACH con menos intentos y más ahorro de energía.
En este artículo se explora el área de control de acceso como no de los aspectos más claves de la seguridad y privacidad en IoT, este trabajo es el primero que muestra de manera extensa el control de acceso en entornos en IoT y presenta de manera integral los modelos, protocolos y soluciones de framework en IoT.

El objetivo principal de este trabajo es realizar un estudio completo de IoT, incluyendo los diferentes tipos de tecnologías para IoT; por medio de encuestas anteriores de IoT, incluyendo documentos que tratan de aplicaciones de IoT; y para indicar el número de servicio con el fin de insertar datos de contexto a la información obtenida por sensores y/o creada por el usuario para enriquecer y dar significado a datos de otra manera vacíos.

Las contribuciones de esta encuesta son: En primer lugar, se investiga clasificamos los esfuerzos de investigación de vanguardia realizados en el ámbito de entornos inteligentes y la taxonomía de los entornos inteligentes basados en IoT. Además, se presenta las oportunidades potenciales que la integración de IoT con entornos inteligentes puede contribuir a la sociedad humana. También se describen algunos casos de estudio de IoT basados en entornos inteligentes. Finalmente, se discuten los desafíos abiertos en la realización de la visión de la integración de IoT con varios entornos inteligentes como futuras direcciones de investigación.
El propósito de este trabajo es proponer un marco teórico que aumente la comprensión de aspectos importantes de los modelos de negocio y fuentes de creación de valor en el contexto de la IoT. Esta búsqueda se integra para mantener o recuperar la competitividad en el nuevo contexto de la IoT, es discutir lo que las empresas necesitan hacer para ser competitivas bajo estas nuevas condiciones. La creación de un marco propuesto para este fin puede contribuir así a la comprensión del entorno cambiante fuera de la empresa y aclarar las configuraciones en modelos de negocio que son más adecuadas para futuros cambios en las empresas que rodean el medio ambiente.

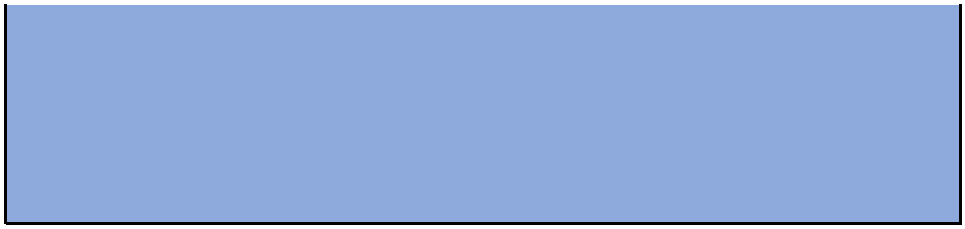
Este documento tiene como objetivo mostrar una visión general de la red inteligente y la tecnología IoT. Además revisar algunos problemas de privacidad y seguridad en las redes inteligentes y algunas implicaciones de seguridad y privacidad para aplicaciones de IoT en la gestión de redes inteligentes. Y por último, discutir algunos retos actuales sobre la adopción de IoT en las redes inteligentes.
En este documento tiene como objetivo discutir estos temas desde diferentes perspectivas: El punto de vista tecnológico, el punto de vista social, el punto de vista económico, el punto de vista cultural que plantean una gran numero de cuestiones de seguridad en Internet de las Cosas. En el mundo del IoT, las cosas físicas se conectan a otras cosas físicas, utilizando la comunicación inalámbrica y ofreciendo servicios contextuales.

El objetivo del documento es resumir el contexto actual de los factores de innovación tecnológica y proponer algunas hipótesis sobre los posibles escenarios futuros de servicios de apoyo a la gestión y desarrollo de la tierra y productos para la construcción de varias formas posibles la integración de la infraestructura urbana física y digital.

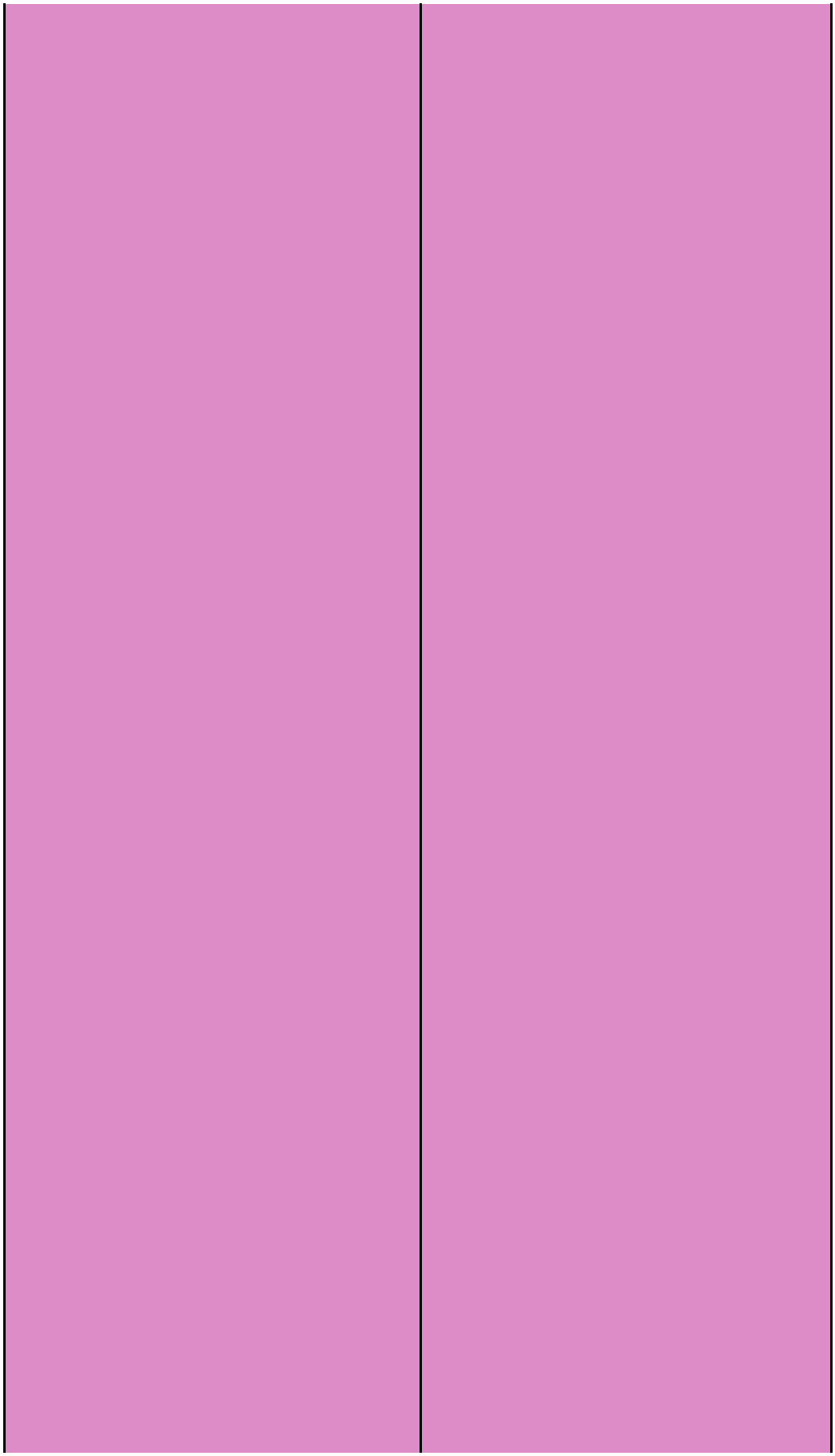
El objetivo de este trabajo es contribuir a la investigación sobre la creación y difusión de tecnologías mediante el examen de la interacción de las instituciones, la industria y

de tecnologías mediante el examen de la interacción de las instituciones, la industria y el mercado desde las perspectiva del IoT en China el cual puede servir como un banco de pruebas para otros mercados emergentes en el desarrollo y despliegue de productos IoT.

El objetivo de este artículo es explicar cómo la abstracción, virtualización y gestión de las cosas tienen que ser adecuadamente diseñadas e implementadas para desarrollar soluciones para la convergencia de diversas plataformas IoT y nubes. Un diseño preciso de estos mecanismos permitirá el desarrollo de una arquitectura tecnológica, donde la integración y despliegue de diversos dispositivos y objetos pueden ser considerados. Se presenta el proyecto VITAL como arquitectura basada en IoT, capaz de cumplir con requisitos críticos de una ciudad inteligente y mostrar cómo se puede considerar esta plataforma para unir diferentes y heterogéneos hilos IoT.

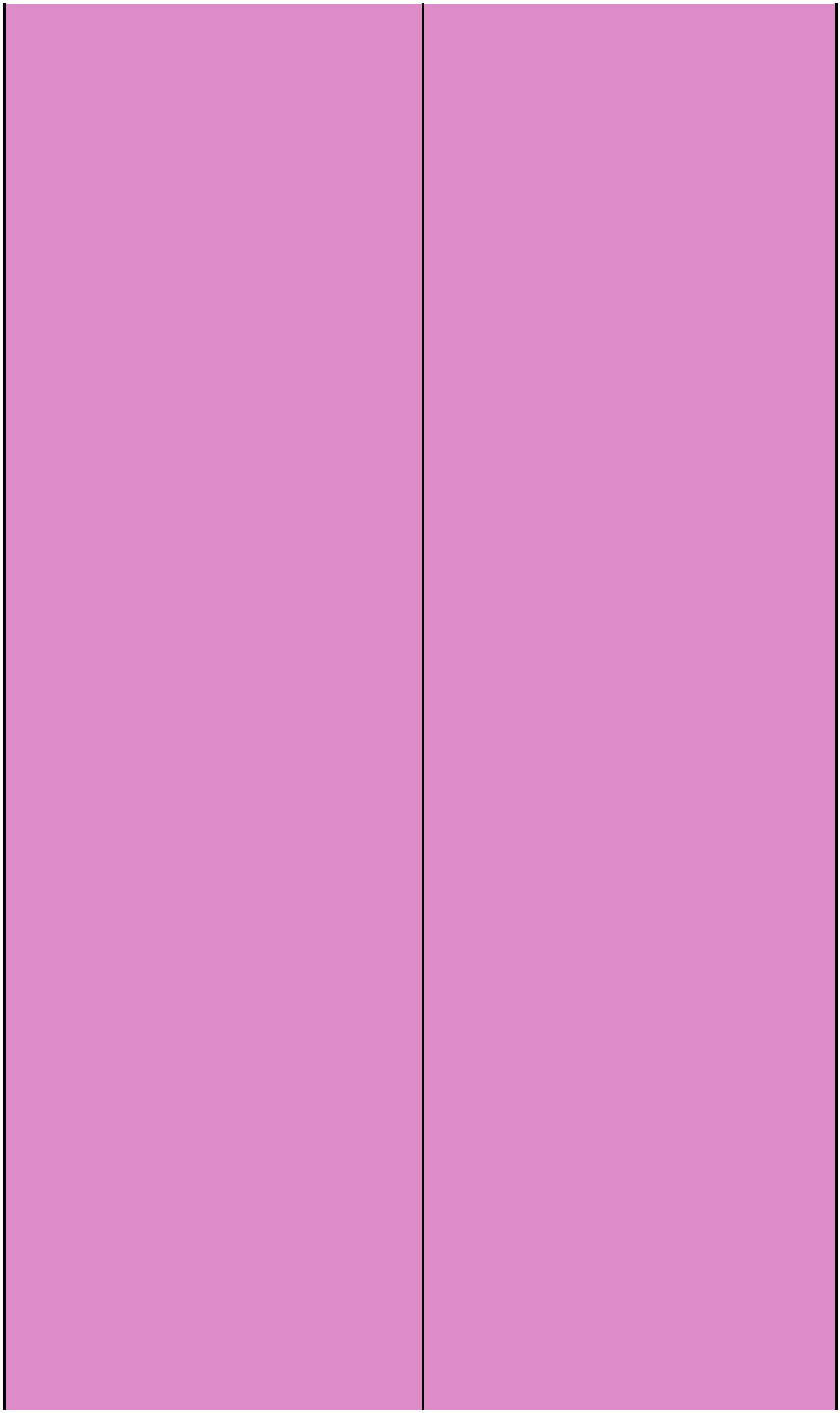


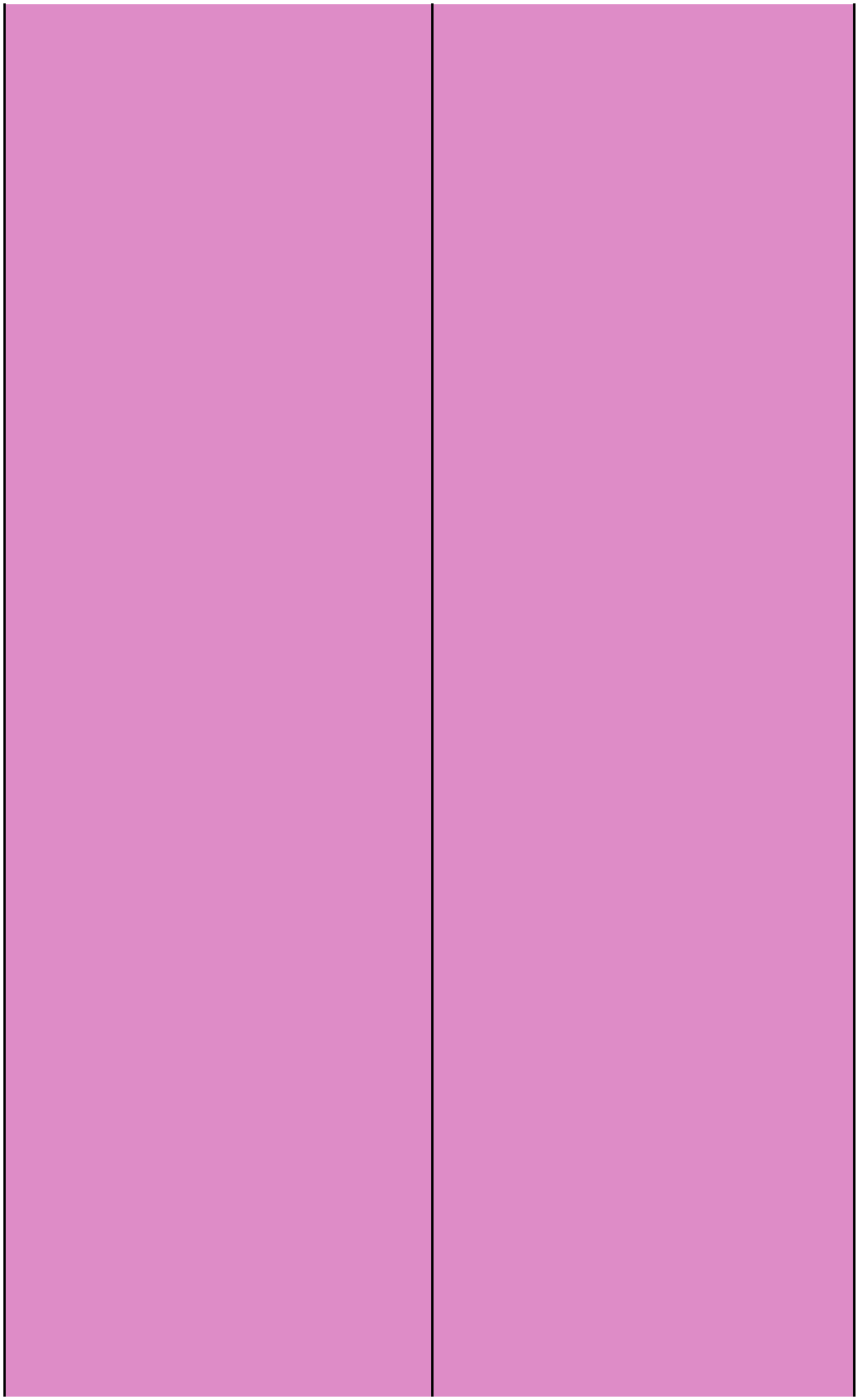
Protocol and registration	Eligibility criteria

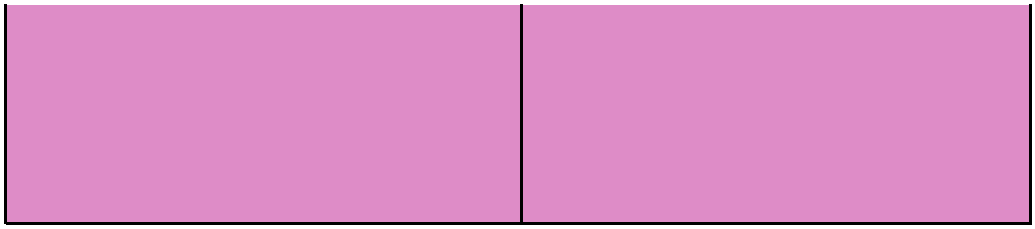


Primero se realizó una búsqueda de la bases de datos con más influencias en búsqueda de artículos, por medio de las cuales se encontraron los artículos de utilidad que sirvieron para realizar el estado del arte, teniendo en cuenta cuales eran los artículos más viables para la revisión de este tipo de	

literatura. Segundo, se crearon diferentes algoritmos de búsqueda para poder observar el que fuera más específico tomando como guía la pregunta problema. Tercero se realizó el filtro #2 el cual se basó en la pregunta problematizada y el tema. Después de esto se seleccionados los algoritmos de búsqueda más específicos respecto al tema, y de cada una se hizo una revisión rápida para saber los artículos que tenían la opciones de descargarlos y tiene más criterios para ser seleccionados, en este proceso se realizó un filtro 3 donde solo quedaron 10 artículos, en los cuales cada uno de estos fue de gran ayuda para la realización de estado del arte, además se encuentro variedad entre encuestas, casos de uso, investigación, entre otros.	El criterio de búsqueda que se tuvo fue entre los años 2012 -2017 y todos los artículos, desde filtro 1 están es un estado de publicación activa.







/Topic

METHODS

Search	Study selection
	Este artículo se seleccionó porque nos muestra dos escenarios claves en la nueva C-IoT que apenas está emergiendo y puede ser decisivo para la transformación el sistema celular de quinta generación, además de la principal conectividad de estos dispositivos es a través de la señal celular de largo alcance. Teniendo en cuenta este contexto, el C-IoT puede ser llamado el celular de las cosas, aunque a un se atiene al termino C-IoT, y esto con llevar a aumentar el número de dispositivos móviles, el cual tendrá como consecuencia la congestión de red, y la ventaja que tiene estos dispositivos C-IoT es que funcionan fácilmente a frecuencias más bajas utilizando el espectro de banda estrecha. En otras palabras la demanda de dispositivos C-IoT está aumentando exponencialmente y debe estudiarse con lupa.
	En este artículo es el primero en mostrar el control de acceso en entornos IoT, y presenta de manera integral los modelos, protocolos y soluciones de framework en IoT y para realizar una implementación de IoT se debe llevar a cabo un excelente análisis de requisitos de seguridad y privacidad para los dominios de aplicaciones IoT.

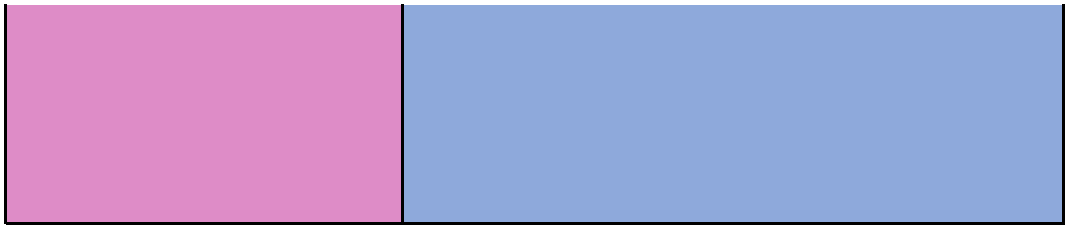
	Este artículo fue seleccionado porque tiene como fin realizar un análisis completo de IoT, incluyendo los diferentes tipos de tecnología para IoT, brindando al final una contribución importante a IoT.	

	Este artículo se seleccionó porque muestra diferentes entornos inteligentes basados en IoT, además muestra un estado del arte, taxonomía y desafíos de investigación abierta que ayuda para la solución de la pregunta problema.	
	Este artículo se escogió porque explora a través de las preguntas: ¿Qué deben hacer las empresas para tener éxito en la implementación a nuevos modelos de negocio o complementarlos?. Además ¿Cuál es el papel de la estandarización en la capacidad de las empresas para crear y apropiarse de valor en el contexto de la IoT? y estas se resuelven por medio de ilustraciones empíricas en el marco conceptual propuesto.	
La búsqueda electrónica fue		

realizada en la base de datos de Scopus, por medio de las siguientes Keywords: Internet of Things, Innovation, Development, Techological Development, Deployment, Telematics, Engineering, cada una de estas Keywords fueron tomadas basando en la pregunta problema para obtener un resultado acertado en la revisión de los artículos.	
	Este artículo fue seleccionado porque, si bien IoT tiene muchas esperanzas para diferentes sectores y hay muchos problemas de seguridad y desafíos descubiertos, por lo tanto, se necesitan nuevas soluciones para asegurar la red inteligente. Esto requiere un enfoque evolutivo adaptando y poniendo controles y políticas de seguridad en el lugar para los nuevos casos de usos, que se estudian a profundidad en este artículo.
	Este artículo se seleccionó porque muestra diferentes perspectivas de IoT, que sirve para tener un mejor punto de vista desde diferentes puntos de vistas de IoT.

	Este artículo se seleccionó porque muestra el contexto actual de las causas de innovación tecnológica frente IoT por medio de una serie de cuestiones de integración de la infraestructura urbana digital y física: el papel de "Big Data".
	Este artículo se seleccionó porque proporciona una revisión de la literatura pertinente sobre los factores que pueden afectar el camino de una innovación. Además de

	proporcionar un estudio de caso de estudio de IoT de China y muestra un desarrollo de un marco que vincula los impactos, indicadores de desempeño y determinantes relacionados con el sector de IoT en China.
	Este artículo fue seleccionado porque se mostrara a detalle sobre los servicios del proyecto VITAL basado en IoT que se implementan, y se describe casos de uso específicos en los que la plataforma VITAL, el cual desempeña un rol importante.



Data collection process	Data items
Revisión de la literatura.	Internet celular de las Cosas (C-IoT), quinta generación (5G), Edge Computing (EC), procedimiento RACH, dispositivos que generan datos con frecuencia (DFD) y dispositivos que generan datos con menos frecuencia (DNFD), NarrowBand (NB-IoT), Proyecto de Asociación de Tercera Generación (3GPP), Mecanismo de restricción de acceso extendido (EAB).
Basado en encuestas integrales de cuestión de control de acceso en el Internet de las Cosas.	Cuestiones de control de acceso, modelos, protocolos y soluciones de framework, seguridad, privacidad, confianza, tecnologías, aplicaciones, plataformas de nube, arquitectura, consumo de energía y cuestiones de seguridad, la calidad del servicio y las implicaciones de minería de datos todos en el contexto de IoT, Modelo de referencia OM-AM.

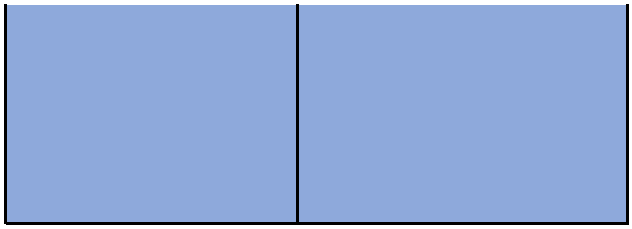
Basado en encuestas de propósito general de IoT, encuestas orientadas a datos, encuestas de IoT vs cloud computing y encuestas de IoT vs. Y documentos que tratan de aplicaciones IoT.	Internet de las Cosas (IoT), grandes datos, ontología, semántica, minería de datos con grandes datos, servicios para grandes datos, Internet social de las cosas (S-IoT), computación en la nube.

	Entornos inteligentes basados en IoT.
	Modelos de negocio, Internet de las Cosas, normalización, interoperabilidad, ilustraciones empíricas.

	IoT, red inteligente, seguridad, intimidad, desafíos, privacidad.
	Internet de las Cosas, seguridad, privacidad, confianza.

	Grandes volúmenes de datos, la infraestructura digital , Internet de las Cosas, mantenimiento urbano.

Revisión de la literatura: Caso de estudio	Internet de la Industria de las cosas (IIoT), China.
Basado en encuesta	Cloud of Things (CoT) , IoT, ciudades inteligentes, VITAL.



RESULTS
Study characteristics
C-IoT es una de las tecnologías más prometedoras en los sistemas celulares de quinta generación.
Procedimiento RACH rápido y ahorra energía.
Los dispositivos C-IoT funcionan con frecuencia más bajas utilizando el espectro de banda estrecha.
Es un desafío para los operadores habilitar más dispositivos C-IoT bajo una única estación base (BS) y recibir suficientes recursos para satisfacer las necesidades de la aplicación.
El mercado estará inundado de miles de millones de dispositivos que costaran mucho menos, pues la demanda será mayor.
Los dispositivos C-IoT son pequeños y se pueden desplegar en cualquier tipo de terreno, además de que se despliegan es una ubicación fija y requiere que funcionen durante años con una batería limitada.
El mecanismo RACH desempeña un rol importante en el consumo energía y se utiliza para asociar un dispositivo a estación base (BS) de servicio.
Los dispositivos C-IoT transmiten una pequeña cantidad de datos y luego se van a "dormir" cuando han terminado el proceso.
La cobertura se dirige a los sistemas de banda estrecha, la densidad se soluciona utilizando un procedimiento RACH eficiente que permite un millón de dispositivos bajo una sola BS y la tactilidad se logra empleando la EC en la BS, cubrir las necesidades de las diferentes aplicaciones. NB-IoT permiten la comunicación bidireccional en un contexto fiable y seguro utilizando una conexión celular con ancho de banda estrecho.
El método 3GPP es cuando cada dispositivo intenta conectarse a la BS con una probabilidad fija.
Cualquier sistema de control de acceso eficaz debe satisfacer las principales propiedades de seguridad de la confidencialidad, integridad y disponibilidad.
Sistema completo de control de acceso cubre las siguientes tres funciones: Autenticación, autorización y rendición de cuentas.
La autorización comprende las siguientes fases: definición de una política de seguridad (conjunto de reglas), selección de un modelo de control de acceso para encapsular la política definida, implementación del modelo y aplicación de las reglas de acceso.
La capa de protocolos de red de 7 capas de OSI, optamos por el framework OM-AM de cuatro capas acuñado.
Modelo OM-AM significa Objetivo, Modelo, Arquitectura y Mecanismo.
Las capas objetivo y modelo (OM) articulan lo que los objetivos de seguridad y lo que debe lograrse, mientras que la arquitectura y las capas de mecanismo (AM) tratan cómo satisfacer estos requisitos.
Objetivo: Capa que sirve para un fondo referencial en el que se basan todas las medidas de control de accesos que defina las reglas según las cuales el control de acceso deber ser regulado.
Modelo de autorización: Su función es superar la brecha entre las políticas de alto nivel y los mecanismos de bajo nivel definiendo medios de cómo debe aplicarse las normas de autorización para proteger los recursos.
Arquitectura: En esta capa se describe las entidades, flujos de trabajo y las interacciones entre ellas.

Mecanismos: Esta capa define las funciones de bajo nivel para aplicar políticas y definir como se evalúan las solicitudes de acceso en relación con dichas políticas.
En Internet tanto los principales productores de datos como los consumidores son seres humanos. En cambio en IoT, los actores principales se convierten en cosas, lo que significa que las cosas son la mayoría de los productores de datos y los consumidores.
En un sistema típico de procesamiento de datos de sensores, las técnicas, incluida la agregación de datos, la comprensión de datos , el modelado y la consulta en línea, deben realizarse en el sitio o en la red para reducir el costo de la comunicación.
Linked Data es un método para publicar datos estructurados e interconectar tales datos para hacerlo más útil con el propósito de extraer triples de marco de descripción de recursos (RDF) de flujos de datos no estructurados.
IoT puede beneficiarse de las capacidades y recursos prácticamente ilimitados de las nubes para compensar sus limitaciones tecnológicas.
Las nubes se pueden beneficiar de IoT, extendiendo su alcance para hacer frente a las cosas del mundo real de una manera más distribuida y dinámica, y para la entrega de nuevos servicios en un gran número de escenarios de la vida real.
Descubrimiento de conocimiento en bases de datos (KDD) y tecnologías de minería de datos deben ser rediseñadas para IoT con el fin de hacer frente a gran cantidad de datos.
La tecnología RFID se considera una tecnología fundamental para IoT. Otra tecnología básica, que contribuye al desarrollo de IoT, son las redes de sensores inalámbricos (WSN).
Las encuestas de propósito general de IoT coinciden en un conjunto de cuestiones de investigación abierta para IoT, como la normalización, la calidad, la seguridad o la movilización.
El significado de IoT no es solo una gran cantidad de dispositivos interconectados, es que los datos generados a partir de estos dispositivos se analizan a partir de nuevas técnicas de datos para proporciona nuevas perspectivas sobre el entorno que nos rodea.
En términos generales, este paradigma tecnológico puede implementarse de acuerdo con tres modelos de servicio: software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS) . Infraestructura como servicio (IaaS) proporciona hardware de TI a las organizaciones. Estos recursos cumplen con los requisitos de los usuarios finales en términos de memoria, informática y almacenamiento; Plataforma como servicio (PaaS) ofrece una plataforma de desarrollo donde los usuarios finales pueden construir sus propias aplicaciones en la nube. Normalmente, los contratos PaaS se complementan con IaaS para crear soluciones en la nube para las empresas; Software como Service (SaaS) ofrece software o aplicaciones a través de Internet. Los usuarios finales no necesitan instalar y ejecutar la aplicación en sus equipos locales.
Un entorno inteligente es aquel que es capaz de obtener conocimiento y aplicarlo para adaptarse a las necesidades de sus habitantes para mejorar su experiencia de este entorno.
La previsión de un crecimiento tan significativo muestra que IoT se convertirá en el tejido de las sociedades modernas para realizar la visión de entorno inteligente.
El trabajo entornos inteligentes basado en IoT generalmente se pueden clasificar en las siguientes áreas: ciudades inteligentes, hogares inteligentes, redes inteligentes edificios inteligentes, transporte inteligente, salud inteligente e industria inteligente.

La arquitectura facilita el co-desarrollo, la apertura y la convergencia de IoT de varias tecnologías que son esenciales para la realización de ciudades inteligentes.
Los servicios basados en la Web usan protocolo sin estado y no se hacen para sesiones a largo plazo.
Las principales tecnologías de Internet inalámbrica son WiFi, 3G, 4G y satélite. El WiFi se utiliza principalmente en hogares inteligentes, ciudades inteligentes, transporte inteligente, industrias inteligentes y entornos de edificios inteligentes; mientras que 3G y 4G se utilizan principalmente en ciudades inteligentes y entornos de red inteligente. Las satélites se utilizan en transporte inteligente, ciudades inteligentes y entornos de red inteligente.
Los objetivos clave del entorno inteligente basado en IoT son la reducción de costos, la mejora de la utilización, el mantenimiento proactivo y la mínima interacción del usuario.
Las principales redes inalámbricas son redes inalámbricas de área local (WLAN), redes inalámbricas de área personal (WPAN), redes de área extensa (WAN), redes de área metropolitana (MAN) y redes inalámbricas de área regional (WRAN). Estas redes tienen diferentes características en términos de tamaño, transferencia de datos y accesibilidad soportada.
Los estándares inalámbricos de área local más utilizados en entornos inteligentes basado en IoT son IEEE 802.11, IEEE 802.15.1 e IEEE 802.15.4. IEEE 802.11 se utiliza en hogares inteligentes, edificios inteligentes y ciudades inteligentes. IEEE 802.15.1 y IEEE 802.15.4 tienen una cobertura relativamente más corta que IEEE 802.11, y se utilizan principalmente en sensores y otros objetos desplegados en los entornos inteligentes.
La integración de IoT con entornos inteligentes puede recolectar una variedad de datos de diferentes fuentes y aplicar técnicas de datos y minería para tomar decisiones inteligentes.
IoT involucra tanto la innovación como el alcance de múltiples industrias y áreas de aplicaciones.
Según los autores se sugiere que la creación de calor en el comercio electrónico podrían ser el resultado de como las empresas hacen negocios, es decir, mediante la introducción de nuevas estructuras de transacciones, el contenido de las transacciones y los participantes de estas.
"Un modelo de negocio representa el contenido, la estructura y la gobernanza de las transacciones diseñadas para crear valor a través de la explotación de oportunidades de negocio".
Las oportunidades de negocio de IoT pueden cambiar el diseño de las estructuras de las transacciones, ya que IoT podría crear nuevas formas de valor al unir las fuentes de creación de valor de los mercados físicos y virtuales.
El monitoreo en productos inteligentes conectados puede facilitar modelos basados en el rendimiento.
IoT permite el control remoto de productos inteligentes conectados.
La escalabilidad de las estructuras de transacciones emergentes también puede crear valor, permitiendo que las transacciones fluyan de manera autónoma dentro del sistema y generando datos que pueden ser valioso para sistemas.
El control remoto es una fuente de creación de valor que puede transformar el contenido de las transacciones en los modelos de negocio, ya que la conectividad y la inteligencia en los productos cambian fundamentalmente que objetos pueden ser controlados de forma remota.

Combinando el monitoreo y el control, el contenido también puede ser transformado por la capacidad de optimización. El valor creado por la capacidad de optimización de productos inteligentes conectados podría depender de la capacidad de las empresas para asociarse y resolver problemas de compatibilidad e interoperabilidad entre productos.
El valor de IoT puede co-crearse cada vez más en interacción con los consumidores, el papel de las comunidades de usuarios o desarrolladores puede aumentar, y definiciones tales como "productor" y "consumidor" pueden transformarse en nuevas formas por los consumidores el papel de un pro consumidor en mayor medida.
La red inteligente es el protocolo y el hardware que integra las TIC en el sistema eléctrico para aumentar la eficiencia del sistema y la rentabilidad.
El modelo Instituto Nacional de Estándares y Tecnología (NIST) consta de siete dominios lógicos: Generación a granel, Distribución de energía, transmisión de potencia, operaciones, mercado, proveedores de servicios y clientes. Este modelo a su vez distingue tres tipos de clientes: HAN (Red de Área de Hogar), BAN (Red de Área de Construcción) e IAN (Red de Área Industrial).El modelo Instituto Nacional de Estándares y Tecnología (NIST) consta de siete dominios lógicos: Generación a granel, Distribución de energía, transmisión de potencia, operaciones, mercado, proveedores de servicios y clientes. Este modelo a su vez distingue tres tipos de clientes: HAN (Red de Área de Hogar), BAN (Red de Área de Construcción) e IAN (Red de Área Industrial).
Entre la distribución y el dominio del cliente se basa Infraestructura de Medición Avanzada (AMI), que gestiona e interactúa con el medidor inteligentes y los clientes a través de una comunicación bidireccional.
Un ecosistema IoT representa una colección de dispositivos inteligentes que interactúan de forma colaborativa para cumplir una meta común.
IoT se considera que desempeña un papel importante a fin de construir un seguro, estable y fiable de nueva generación de la plataforma de red inteligente.
Se abordan tres tipos de dominios de privacidad y desafíos de seguridad: dominio del cliente, dominio de la información y la comunicación, y el dominio de red.
Analizar los requisitos de seguridad y privacidad en sistemas complejos como en las redes inteligentes es un factor crucial para prevenir fallas o eventos que pueden influir o comprometer la confidencialidad, integridad y disponibilidad de los diferentes sistemas TIC involucrados en el soporte de varios procesos en el sistema de red inteligente.
IoT es una red global que puede conectar objetos reales y virtuales de una manera única, haciendo uso de los datos captados por los sensores, de los dispositivos de comunicación y localización.
Las 24 horas del día, 7 días a la semana, se presenciara un aumento en los aparatos y los objetos inteligentes que interferirán poderosamente en nuestras vidas, hábitat en el que vivimos y en constante expansión de sus capacidades sensoriales y de acción.
IoT es definitivamente un factor importante de innovación y crecimiento económico.
La importancia de las medidas de seguridad se incrementa mucho en la IoT, así como la responsabilidad de los involucrados en su formulación y aplicación.
En IoT, el elemento que va a ser identificado será el dispositivo, y no el individuo.
Cada persona debe asegurarse de estar protegida por soluciones técnicas eficientes, re-interpretadas y actualizadas. Después de este primer paso de sensibilización, la investigación debe concentrarse más adelante en las acciones técnicas, económicas, legales, sociales y éticas para evitar que el IoT se convierta en un temible e intruso Gran Hermano.

Cuando se habla del problema de seguridad se debe tener en cuenta todos los elementos involucrados: el dispositivo de IoT, la nube, la aplicación móvil, las interfaces de red, el software, uso del cifrado, uso de la autenticación y seguridad física.
El uso de "Big Data" está empezando a ser objeto de estudios también en la ciudad para una mejor comprensión de la dinámica y gestión de la infraestructura urbana y es la escala del territorio y de sus infraestructura que aparece en el momento adecuado para hacer productivo las innovaciones de la relación entre el medio ambiente construido y grandes volúmenes de datos.
El escenario de la evolución tecnológica: Sensores, grandes volúmenes de datos e Internet de las cosas.
La necesidad de formas innovadoras de adquisición y procesamiento de la información en términos de múltiples conexiones y expansión de la capacidad de conocimiento, la toma de decisiones y la reacción se abre un campo adicional de la innovación, se refiere al concepto de la Internet de los objetos (IO).
La IO se caracteriza por tres componentes principales: 1) los objetos digitales con sensores integrados. 2) los sistemas hub o computadora con que recogen los datos generados y utilizarlos. 3) una red de comunicación para conectar los objetos y el almacenamiento de datos, para permitir la interacción entre todos los elementos involucrados.
Sin duda, teniendo en cuenta los servicios a escala urbana, el papel de los gobiernos de las ciudades es crucial para la aplicación de la IO.
Las ciudades y sus servicios representan una plataforma ideal para el desarrollo y la investigación de la IO, así como un caso de prueba con la participación de otras partes interesadas, tales como gestores de redes públicas y privadas, además de la infraestructura, los fabricantes de sistemas hardware y software de control e información, asociaciones profesionales .
La implementación de un proceso de respuesta adaptativa en tiempo real automatizado requiere la disponibilidad de dos elementos: un sistema capaz de controlar el construido en forma capilar y continua y un patrón de respuesta a las condiciones detectadas, capaz de procesar los activos de información a gran volumen, alta velocidad y alta variedad.
La lógica de este tipo de modelos se podría desarrollar en relación con el principio básico de la "detección y respuesta", que se redujo en relación a dos factores: la dimensión temporal y la gradualidad de la aplicación de automatismos.
China tiene la industria de IoT más desarrollada y la infraestructura relacionada.
IoT es la red de objetos físicos o "cosas" incrustados con electrónica, software y sensores, que están provistos de identificadores únicos y poseen la capacidad de transferir datos a través de la Web con un mínimo o ninguna intervención humana.
China ha demostrado una tendencia de mejora en las actividades innovadoras relacionadas con la IoT en comparación con generaciones anteriores de tecnologías. Las empresas chinas han creado algunos productos y servicios innovadores relacionados con IoT.
Las demandas de una nueva tecnología como la IoT son altas cuando la trayectoria de la tecnología alternativa existente es poco atractiva. Por otro lado, es probable que las empresas tecnológicas en una trayectoria atractiva queden atrapadas en un sistema heredado.
El desarrollo económico es clave, por eso se han desarrollado diversas iniciativas de IoT para impulsar los objetivos relacionados con la modernización económica.
La mayoría de los proyectos IoT implican dispositivos conectados con sensores simples y pasivos para administrar, monitorear y optimizar sistemas y procesos.

China quiere aumentar la probabilidad de establecer estándares globales en los productos IoT en comparación con los otros intentos anteriores, las empresas chinas poseen más patentes relacionadas con la IoT que cualquier otro país del mundo.
Diversos sectores como el transporte, el comercio minorista, la energía, la logística, los servicios públicos, la fabricación pueden beneficiarse del despliegue del IOT en el procesamiento de información en tiempo real para aumentar la eficiencia, reducir los costos y administrar las infraestructuras.
La combinación de IoT y análisis de datos grandes permitirá a las empresas de la industria manufacturera beneficiarse de la detección de bajo costo, la recopilación de datos en tiempo real y más eficiente análisis avanzado de datos.
China es el país de mayor éxito en lograr una rápida difusión de las telecomunicaciones.
Las plataformas más representativas IoT son : GSN (Global Sensor Networks) , LSM (Linked Sensor Middleware), Sensor- Cloud, Open IoT, Xively.
La computación en la nube atrae la atención tanto de la academia como de la industria en todo el mundo, porque es capaz de transformar modelos de provisión de servicios sobre las industrias de la tecnología de la información completamente actual.
Las ventajas y beneficios prometidos por el modelo de Sensing as a Service son las siguientes: compartir y reutilizar datos de sensores, la reducción del coste de adquisición de datos debido a naturaleza compartida y recopilar datos previamente no disponibles entre otros.
Los dispositivos IoT pueden conectarse a Internet, sus datos pueden anotarse utilizando una ontología de sensores , se puede codificar en formatos web estándar y pueden estar disponibles en Cloud, estableciendo así CoT.
El concepto de ciudad inteligente considerado desde el punto de vista de las administraciones y proveedores de la red se traduce en una infraestructura de red que es la siguiente: (1) altamente interconectada: superando la heterogeneidad de los dispositivos y las plataformas IoT , es posible proporcionar conectividad ubicua; 2) rentable: el despliegue y la organización de la red deben ser lo más automáticos posible y deben ser independientes de la intervención humana; (3) eficiente de la energía: capaz de realizar una utilización eficiente de los recursos, con el fin de satisfacer los principales requisitos de las aplicaciones verdes; Y (4) confiable: que la conectividad, la ubicuidad de la red debe ser garantizada sobre todo en el caso de condiciones excepcionales y adversas.
En el contexto de VITAL, un factor muy importante está representado por la virtualización de interfaces que en combinación con herramientas de contexto cruzado que permiten el acceso y gestión de objetos heterogéneos soportados por diferentes plataformas y gestionados por diferentes actores administrativos definimos la plataforma VITAL como una arquitectura CoT.
El acceso a datos y servicios de los objetos heterogéneos involucrados en VITAL se basan en la implementación de las Interfaces de Acceso Universal Virtualizadas (VUAIs) que hace posible considerar un único acceso virtual haciendo que la plataforma de arquitectura sea incrédulo.
La capa VUAI se basa en una supuesta meta-arquitectura y capa de migración e incluye varios conectores para comunicar e interconectar diferentes plataformas IoT y Nubes.

El principal reto de VITAL es integrar en una plataforma incrédula una multitud de datos heterogéneos y funcionalidades producidas y ofrecidas por diferentes sensores y sistemas de IoT gestionados por organizaciones y entidades dispares (independientes).
Las ontologías VITAL pueden agruparse en cuatro áreas principales: sensores y mediciones de sensores, ciudades inteligentes, sistemas y servicios IOT, sistemas VITAL y servicios.

DISCUSSION	
Summary of evidence	**Limitations**
Se evaluó el desempeño de dos mecanismos RACH y se presentaron los siguientes resultados: RACH rápido reduce el número de colisiones y también el tiempo de asociación en comparación con 3GPP EAB. El tiempo ahorrado usando RACH rápido aumenta exponencialmente en comparación con 3GPP EAB a medida que aumenta la densidad de la red.	
En esta encuesta se estableció, una taxonomía de aplicaciones de dominio de IoT, también se proporcionó un análisis OM-AM del proceso de autorización en IoT, al igual que los pros y contras de las soluciones de control de acceso existentes desde una perspectiva de IoT y su usabilidad en las aplicaciones de dominio IoT ya definidas. Además se evaluó la literatura relacionada ya definida en términos cuantitativos y cualitativos basado en los principales requisitos de seguridad de IoT. Entre otras cosas, también se identificaron los principales desafíos de aplicar mecanismos de control de acceso a IoT. También se muestra las ventajas y desventajas de adoptar una gestión de control de acceso distribuida o centralizada de IoT.	El paradigma IoT todavía tiene que afrontar desafíos arduos relacionados con la aplicación de mecanismos de seguridad y control de acceso en entornos restringidos. También se argumenta que los protocolos de Internet comúnmente utilizados no pueden aplicarse en todo los casos a entornos restringidos.

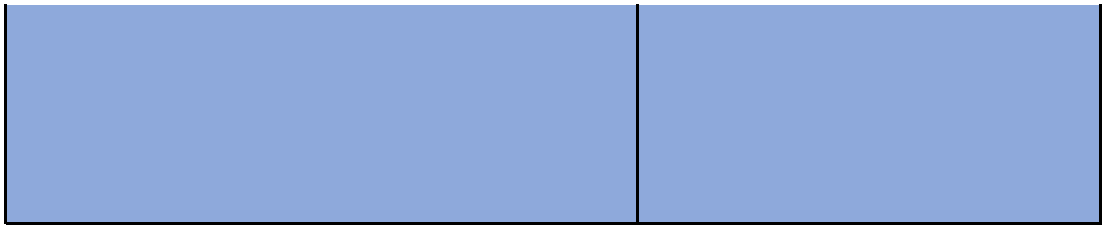
En este trabajo se llevó a cabo la revisión de las encuestas disponibles con el fin de proporcionar servicios inteligentes bien integrados y orientados al contexto para el IoT. Además, se propone un estado de la técnica de IoT total desde la perspectiva contextual que permite la integración de IoT y las redes sociales en el emergente Internet social de las cosas (SIoT). Finalmente se describe la diversidad de servicios para IoT.	Estos artículos no cubren específicamente las técnicas de procesamiento y gestión de datos, que son fundamentales para abarcar plenamente el IoT. Se ha señalado que es mucho más fácil crear datos que analizarlos, por esta razón el nuevo modelado conceptual, así como los nuevos paradigmas de técnicas de minería de datos, será crucial para proporcional valor y significado a los datos inicialmente vacíos.

SSe presenta una discusión sobre los entornos inteligentes basado en IoT de última generación para ayudar a los lectores a comprender los esfuerzos recientes en esta dirección. También se diseña una taxonomía temática considerando los facilitadores de comunicación, los tipos de red, las tecnologías, los estándares inalámbricos de área local, los objetivos y las características. Además, se presenta el estudio de casos reportados y se discute las oportunidades sin precedentes generadas por la integración de IoT con entornos inteligentes y desafíos de la investigación abierta como direcciones de investigación futuras. Y finalmente se concluye con el despliegue de IoT puede ser una de las futuras plataformas para permitir que los objetos del mundo físico se comuniquen entre si al garantizar una alta funcionalidad, eficiencia energética, interactividad rica y una capacidad de respuesta nítida de forma dinámica.	
La aplicación de este marco en ilustraciones empíricas puede contribuir a una mejor comprensión de las implicaciones potenciales que los productos inteligentes conectados pueden tener sobre los modelos de negocio, las fuentes de creación de valor y el rendimiento de la empresa. Además, se ha ilustrado múltiple ilustraciones relativas a cuestiones relacionadas con normas, como la interoperabilidad y compatibilidad de productos, basándose en estos se puede argumentar que la normalización es un campo relevante en la investigación	La literatura IoT que discute las implicaciones en el rendimiento de la empresa, la competencia o las fuentes de creación de valor es actualmente muy escasa. Una debilidad en la capacidad para interpretar IoT y su impacto en el rendimiento de la empresa podría ser la falta de perspectivas holísticas y marcos desarrollados para este fin. Es necesaria realizar una investigación adicional para ampliar la comprensión del impacto de IoT potencial en las empresas y los

futura de modelos de negocio en el contexto IoT.	factores de comprensión que pueden restringir la difusión de IoT.
Las ideas y recomendaciones esbozadas en todos los trabajos de investigación revisados pueden ayudar a los servicios públicos a estar en una posición fuerte para prevenir estas amenazas potenciales, aunque será imposible neutralizar completamente la probabilidad de intrusiones cibernéticas destructivas. Los requisitos de privacidad y seguridad en las redes inteligentes basadas en IoT solo se investigan más, a fin de construir normas bien definidas y más seguras para la comunicación y protección. En este artículo se cree firmemente que con una legislación adecuada, consideraciones socio-éticas y mecanismos avanzados de seguridad cibernética , se puede construir una red inteligente segura y confiable para reducir costos para los clientes, reducir las emisiones de CO2 y reducir el calentamiento global y un mejor ambiente para las generaciones futuras.	La adopción de la tecnología IoT para el despliegue y la gestión de la red inteligente todavía está en una etapa temprana y muchos desafíos siguen sin resolverse con respecto a las implicaciones de privacidad y seguridad.
En los últimos años, los tipos de ataques que han sido reportados a través del IoT han sido tan diversos, desde la explotación de las vulnerabilidades de las aplicaciones Web hasta los ataques hombre-en-medio o los ataques con contraseña. Otra debilidad importante que no es suficientemente explorada en la teoría, cuando el tráfico de un empleado remoto vuelve a entrar a través de la red empresarial, los tipos de ataques disponibles deberían constituir una gran preocupación para los administradores de seguridad	Desafortunadamente IoT todavía está en su "infancia", es necesario que las directrices reglamentarias y las mejores prácticas de la industria sean resueltas y superar las barreras técnicas. También se debe reconocer que no existe una legislación específica relacionada con IoT, por lo que para cualquiera nueva conexión o tecnología, se aplican las normas de privacidad y protección de datos vigentes. Mientras los grandes datos aumentan también se alimentan

administradores de seguridad.	datos aumentan también se alimentan grandes preocupaciones sobre la seguridad.
Entre las perspectivas de investigación que se pueden destacar en el desarrollo de algunas áreas temáticas y en profundidad puntos de vista: 1) Una revisión del mismo concepto de infraestructura, teniendo en cuenta las nuevas claves interpretativas y aplicable a los modelos operacionales del capital fijo y conceptos económicos, con la definición de nuevas categorías de entidades inmateriales y materiales y sus relaciones. 2) La investigación de posibles nuevos modelos y procesos de gestión del conocimiento y flujos de personas, materiales, energía, entre otros sobre la base de procedimientos que se definen en relación con los procesos lineales y para la toma de decisiones. 3) Evaluación de las posibles nuevas formas de resistencia urbana obtenida a través de una visión general del sistema de servicios de infraestructura. 4) La interpretación de los edificios y partes de los mismos que los nodos de una red de información y terminales dentro de un flujo bidireccional de información en comparación con la ciudad. 5) Revisión de los enfoques tradicionales para la evaluación del riesgo y gestión aplicada a la infraestructura.	No parece adecuado para sacar conclusiones ya que los escenarios de posibles aplicaciones son múltiples y todos los precursores de las innovaciones y modificaciones de los paradigmas y las prácticas tradicionales que caracterizan el diseño y la gestión de la infraestructura urbana.
Respecto a la demanda se puede argumentar que la trayectoria de China asociada con tecnología no-IoT es menos potente. En cuanto al progreso técnico, que puede definirse en términos de un desplazamiento de la curva de las posibilidades de producción y /o del aumento del número de bienes producibles, en comparación con los países industrializados, es probable la adopción del IoT para llevar a un progreso técnico más significativo en China. En general, el IoT es probable que produzca un efecto dramático en países en desarrollo como China, que actualmente están utilizando tecnologías relativamente primitivas en la mayoría de las	A pesar de limitaciones y contratiempos asociados con la medida de política del gobierno, la industria China ha crecido rápidamente, el mercado chino de IoT es el resultado de una serie de fuerzas contradictorias y conflictivas. No

tecnologías relativamente primitivas en la mayoría de las áreas. Por lo tanto, China tiene más incentivos y oportunidades para adoptar el IoT. En cuanto a las instituciones formales, las políticas proactivas del gobierno y otras intervenciones con el fin de crear un ambiente IoT adecuado han desempeñado un papel clave en la evolución del IoT. Actualmente, China está en condiciones de invertir más que la mayoría de las demás economías. Los factores relacionados con las instituciones, la demanda y la oferta ofrecen condiciones favorables para la creación y difusión de productos y servicios relacionados con la IOT. Sin embargo, la política de innovación no se traduce necesariamente en innovaciones de IoT de alta calidad.	contradictorias y conflictivas. No obstante, algunos cambios pueden obstaculizar el uso de IoT, el mal uso y el abuso de los datos personales y la información se informó a ser problemas clave para los consumidores chinos que reciben créditos de las grandes empresas de datos.
En este trabajo se previó en la computación en nube un puente valido de la IoT, Internet de las personas a través de Internet de Servicios. Esta nueva perspectiva permite la realización de una integración horizontal de varias plataformas, mediante la implementación de un nivel de virtualización especifico, la plataforma VITAL, en el contexto del proyecto, garantiza la interoperabilidad semántica de diferentes y diferentes plataformas IoT. Las VUAIs implementan una meta-arquitectura y capa de migración, con diferentes conectores y controladores para permitir la comunicación entre las distintas plataformas. De esta forma, la plataforma basada en VITAL CoT puede ser considerada como una solución muy prometedora para los problemas de fragmentación en el contexto de las ciudades inteligentes.	Se presentas varias plataformas IoT que pueden ser consideradas de manera eficiente en el contexto de la ciudad inteligente, pero para superar la brecha entre las plataformas IoT, es necesario considerar una convergencia de estas plataformas y ecosistemas. Existen diferentes desafíos relacionados con el CoT en ciudades inteligentes, tanto desde el punto de vista técnico como desde el punto de vista de la privacidad.



Conclusions
En este artículo, se enumeraron los desafíos que deben ser abordados para que C-IoT sea factible y se discuten dos soluciones de transformación clave para los desafíos, describiendo el papel de EC en C-IoT y sus beneficios en varias implementaciones. Por lo tanto, los mecanismos propuestos permiten la conexión de millones de dispositivos C-IoT en ambientes densos.
El trabajo futuro consiste en implementar un marco de control de acceso que preserva la privacidad basado en el modelo de referencia OM-AM presentado para concebir un marco de control de acceso adecuado para IoT.

En este trabajo, se presenta una revisión sistemática de las diversas encuestas de IoT. El gran volumen de encuestas citadas hace más fácil obtener una imagen general del estado actual de la técnica en el IoT. En este artículo por primera vez examina el estado del arte IoT desde las perspectivas del contexto que incluye SIoT.

En este artículo se proporciona una revisión de los esfuerzos de investigación realizados para integrar IoT con entorno inteligentes.
Al aplicar el marco propuesto, las ilustraciones empíricas podrían ser categorizadas por los componentes de la construcción del modelo de negocio.

Este documento representa una encuesta exhaustiva de las contribuciones más recientes sobre aspectos de seguridad y privacidad de las aplicaciones IoT en redes inteligentes e identifica algunos de los desafíos y vulnerabilidades restantes relacionados con la seguridad y privacidad.

Una de las direcciones más importantes en la evolución de IoT es el mercado de seguridad. Los dispositivos que componen el IoT amplio realizan diferentes funciones, exponen superficies de amenazas diversas y por supuesto requieren estrategias de seguridad que son específicas para cada categoría de dispositivo.

Ya que no se sacan conclusiones, es más apropiado identificar posibles áreas de investigación y experimentación, que, por la naturaleza multi e interdisciplinar que distingue los temas, requerirá, entre muchas habilidades interesadas, diseño, gestión de artefactos y procesos.

Los factores relacionados con la demanda, el suministro y las instituciones han interactuado de una manera única que ha

determinado la trayectoria de IoT en China. Esta investigación pone de relieve los roles complementarios de las empresas locales y extranjeras en la creación y el despliegue de innovaciones relacionadas con IoT en China.
En este trabajo se consideró las plataformas IoT como una solución viable para hacer ciudades inteligentes. La proliferación de las TIC representa nuevas oportunidades para el desarrollo de nuevos servicios, contribuyendo a hacer ciudades más sostenibles. Las diversas plataformas de IoT han dado lugar a ecosistemas diferentes y heterogéneos de IoT que introducen un grado significativo de fragmentación.