Seguridad del Internet de las Cosas: STATE-OF-THE-ART REVIEW

Youssef Moises Abarca Reyes
yabarca@est.ups.edu.ec
Luis Alberto Galarza Aguilar
lgalarza@est.ups.edu.ec
Esteban Fernando Ordoñez Morales
eordonez@ups.edu.ec

***Resumen*—En este artículo presenta una visión general del estado del arte del uso del internet de las cosas (IoT), centrándonos principalmente en la seguridad del IoT. Se dará la definición del mismo, su origen así como se da a conocer los distintos beneficios y complicaciones que nos brinda tipo de tecnología como un sistema en general que puede controlar cualquier tipo de 'cosa' a través del uso del Internet. Se describirá sus principales características y como estas se han desarrollado al transcurrir el tiempo. A partir de esto se realizó una tabla que describirá una problemática en cuando a seguridad y el progreso que ha tenido en los últimos años para la solución del mismo. En sí, se dará a conocer los últimos avances que se han realizado y como estos han y van mejorando con el transcurso de los años.**

Abstract—In this paper presents an overview of the state of the art of using the Internet of Things (IoT), focusing primarily on the safety of IoT. Will the definition of it, its origin and discloses the various benefits and complications that gives us kind of technology as an overall system that can control any type of 'thing' through the use of the Internet. Its main characteristics will be described and how are you have developed as time passes. From this table that describe a problem and then to security and progress that has taken in recent years to solve the same place. As such, it will release the latest advances that have been made and how they and being improved over the years.

***Index Terms*—Internet, cosas, seguridad, IoT, IdC, revisión, sensores, software, review.**

I. Introducción

El Internet de las cosas (IoT) por sus siglas en inglés (Internet of Things) en si trata de comunicar los diferentes dispositivos y maquinas eléctricas y electrónicas que existen con el mundo exterior, es decir que a través de la utilización de sensores lograr que estos dispositivos lleguen a tener una mejor comprensión del mundo que los rodea. De esta forma, se logra de que las cosas tengan un cierto nivel de independencia para que puedan funcionar, uno de los ejemplos más comunes del Internet de las cosas es el sistema de fallas en un automóvil, cuando un automóvil tiene algún tipo de funcionamiento irregular este enciende una luz en el tablero indicando cuál es el problema. El Internet de las cosas tiene la finalidad de dar ciertas facilidades a la vida de las personas, automatizando las cosas para ahorrando una gran cantidad de tiempo.

Esta infraestructura incluye la evolución de Internet y de otras redes existentes implicadas. Se ofrece como objeto específico de identificación el sensor, y la capacidad de conexión como base para el desarrollo de servicio y aplicaciones de cooperación independientes. Estos se caracterizan por un alto grado de captura autónoma de datos, transferencia de eventos, conectividad de red e interoperabilidad [1]

Imaginemos una ciudad del futuro. Una ciudad «inteligente» en la que los teléfo nos móviles abren puertas, los sensores detectan fugas en las cañerías y las vallas publicitarias cambian sus anuncios de acuerdo con el perfil de consumidor de las personas que pasan por esa calle. Pequeños sensores permiten medir la temperatura de una habitación o el tráfico de taxis por las calles. Cámaras de seguridad velan por la seguridad en los edificios y paneles del metro indican el tiempo restante hasta la llegada del siguiente tren. [20]

A lo largo de los últimos años el Internet de las cosas ha tenido grandes avances, muchos dispositivos y aplicaciones actualmente guardan una gran cantidad de información en el Internet de los usuarios como pueden ser, su estado físico, su estado de cuenta bancaria e incluso el estado de seguridad de su casa. Uno de los principales inconvenientes del Internet de las cosas el factor seguridad, puesto ya que la mayoría de información se guarda en Internet, pueden existir personas que pueden estar en la capacidad y acceder a esta información y manipularla a su conveniencia, otros de los grandes inconvenientes es el fallo de los sensores que existen en estos (en las cosas), si estos llegaran a tener algún daño pueden proporcionar y guardar información errónea que puede resultar perjudicial o incluso molesta para el usuario.

II. Internet de las cosas

IoT es una tecnología que se ha desarrollado de forma muy avanza a lo largo de los últimos años. Nace de la unión unión del termino genérico M2M (maquina a maquina por sus siglas en ingles) y el Internet.

II-A. M2M

M2M se refiere a la interacción que existe entre una maquina y otra en la cual existe un cambio de información o una comunicación. Ésta interacción entre maquinas requiere diferentes opciones de conectividad: con cable e inalámbrica, banda ancha y datos en serie lentas. La mayoría de los dispositivos M2M normalmente permanecen apagados para ahorrar energía, es decir, la conectividad debe ser de bajo costo y bajo consumo de energía. [2]

II-B. Internet

Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación [3] que permite el intercambio de todo tipo de información entre sus usuarios.

Con la unión de estos dos conceptos fue creado el Internet de las cosas, el cual hoy en día es la base fundamental de muchas nuevas tecnologías como son:

- smart.Grid (redes inteligentes)
- smart.Home (Casa inteligente)
- smart.Building (Edificio inteligente)
- smart.City (Ciudad inteligente) [18]
- smart.****

II-C. Qué es el IoT?

La proliferación de un conjunto cada vez mayor de dispositivos capaces de conectarse directamente a Internet está dando lugar a un nuevo paradigma de computación ubicua. De hecho, la Internet- su despliegue y su uso- ha experimentado un crecimiento significativo en las últimas cuatro décadas, evolucionando desde una red de unos pocos cientos de hosts (en su forma ARPAnet) a una plataforma capaz de vincular miles de millones de entidades a nivel mundial. Inicialmente, la Internet conecta anfitriones institucionales y terminales acreditados a través de pasarelas especialmente desarrollados (routers). Más recientemente, la Internet se ha conectado servidores de todo tipo para los usuarios de todo tipo que buscan acceso a la información y aplicaciones. El crecimiento de Internet no muestra signos de desaceleración, y se está convirtiendo progresivamente el tejido de infraestructuras de elección de un nuevo paradigma para toda la computación ubicua incluyente y comunicaciones. La próxima evolución es conectar todas las "cosas" y objetos que tienen (o pronto tener) algun tipo de conexión inalámbrica incorporada (o de línea fija) conectividad a sistemas de control que apoyan la recolección de datos, análisis de datos y la toma de decisiones. "Las cosas" incluyen, pero no se limitan a, maquinaria, electrodomésticos, vehículos, personas, animales domésticos, ganado, animales, hábitats, los ocupantes individuales de hábitat, así como de las empresas. Interacciones se consiguen utilizando una plétora de posiblemente diferentes redes; dispositivos computarizados de diversas funciones, forman factores.[4]

El IoT es un tipo de evolución de la aplicación de Internet que se esfuerza por hacer que la información de una cosa (sea lo que sea) de forma segura disponible a escala global si / cuando dicha información es necesaria por un punto o puntos de agregación. Dado que la definición de la IoT es todavía en evolución, el material que sigue proporciona definiciones de conceptos ilustrativos, más que una definición bien redactado.[4] Pero se puede describir como una red de información de nueva generación que permite la comunicación (M2M) 2 y/o (H2M) [15] la comunicación de persona a máquina. Uno de los objetivos iniciales de la IoT es para permitir la conectividad de las distintas "cosas"; un próximo objetivo es ser capaz de que las "cosas" tengan un cierto grado de conciencia sobre su funcionamiento y su entorno (autosuficiencia).

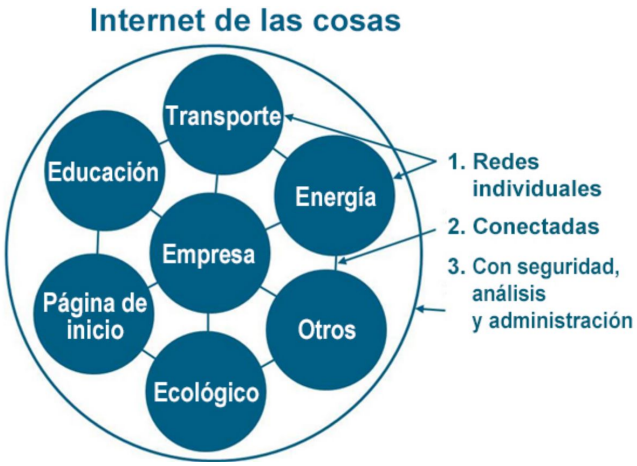


Figura 1. IdC se puede considerar la red de redes [14]

II-D. IoT como la red de redes

Actualmente, IoT está compuesta por una colección dispersa de redes diferentes y con distintos fines. Por ejemplo, los automóviles actuales tienen múltiples redes para controlar el funcionamiento del motor, las medidas de seguridad, los sistemas de comunicación y así sucesivamente. De forma similar, los edificios comerciales y residenciales tienen distintos sistemas de control para la calefacción, la ventilación y el aire acondicionado, la telefonía, la seguridad y la iluminación. A medida que IoT evoluciona, estas redes y muchas otras estarán conectadas con la incorporación de capacidades de seguridad, análisis y administración (ver Figura 1). Esta inclusión permitirá que IoT sea una herramienta aún más poderosa.[14]

Resulta interesante señalar que esta situación refleja lo que el sector de la tecnología experimentó en los primeros días de la red.

Antes de que podamos ver la importancia de IoT, es necesario comprender las diferencias que existen entre Internet y World Wide Web (o web). Por una parte el Internet su función principal es transportar información de un punto a otro, de manera veloz, confiable y segura. La web, por su parte, es una capa de aplicaciones que opera sobre la superficie de Internet y su función es proporcionar una interfaz que permite utilizar la información que fluye a través de Internet.

III. Apreciaciones en el Presente del IoT

El IoT alredor de los últimos años a tenido grandes avances, hoy en día muchas ciudades en el mundo implementan cada vez mas esta tecnología, para de esta manera ofrecer mejores servicios tanto en seguridad, eficiencia, ahorro entre otros.

A continuación se presenta una lista con las apreciaciones mas destacadas del IoT:

1. Con el auge en materia de conectividad, los hogares quieren volverse inteligentes y por eso demandan un mayor y mejor acceso a internet. Actualmente existen en

el mercado tecnologías como el WiFi 11AC que ayudan a los usuarios a tener una excelente conexión y a mejorar su calidad de vida.

2. Videovigilancia. Entre sus grandes beneficios, el Internet de las Cosas permite a las ciudades mejorar la calidad de servicios que ofrecen a los ciudadanos, en especial, en términos de seguridad. En el futuro, millones de objetos y sensores estarán conectados entre sí para comunicar datos que analicen, planeen, administren y tomen decisiones inteligentes de forma automática en las ciudades. Para empezar a responder a esta tendencia, las urbes están trabajando en la instalación de cámaras en las calles a través de avanzadas plataformas para reducir los delitos ciudadanos considerablemente, creando a su vez ciudades mucho más conectadas e inteligentes.
3. Controlar los hogares a distancia. Con la ayuda de sensores avanzados, las personas pueden automatizar el encendido y apagado de la luz en habitaciones y recibir alertas en el celular cuando hay movimiento en un lugar determinado de la casa.
4. Dispositivos para ahorrar energía. Ahorrar energía y cuidar el medio ambiente es una de las posibilidades que ofrece el Internet de las Cosas pues entre mayores posibilidades de conectividad haya, más fácil será hacer acciones que sean amables con el planeta. Hoy en día, por ejemplo, las ciudades pueden implementar sistemas de alumbrado inteligente que ahorran hasta un 80 % de energía debido a que solo se encienden ante la presencia de una persona, una bicicleta o un automóvil.
5. Movilidad. El Internet de las Cosas puede llegar a ser muy útil para que las ciudades mejoren su movilidad de forma considerable. Es así como, por ejemplo, los gobiernos tienen hoy la capacidad de instalar cámaras de tránsito inteligentes que hacen un conteo de cuántos carros transitan por determinadas calles haciendo posible descongestionar en forma inteligente y remota las calles especialmente en horas pico. [5]

III-A. Estimaciones del IoT en un Futuro próximo

En 2020, el número de objetos conectados a Internet será de más de 26.000 millones[16], [17] (excluyendo PCs, tablets y Smartphone), cerca de 30 veces los objetos conectados en 2009, según estudios realizados por la consultora Gartner [6]. Los números no dejan lugar a dudas sobre el interés, tanto a nivel académico como a nivel empresarial, de los temas relacionados con el IoT. Veamos ahora cifras sobre un tema de especial trascendencia e interés: la seguridad del IoT.

IV. Internet de las Cosas Empresas

Existe una alta competencia en lo que es fabricación de componentes para este tipo de tecnología, como lo son

- Sensores
- Baterías
- Transmisores
- Micro controladores
- Recolectores de energía
- Entre otros.

Por lo general este tipo de componentes son fabricados por empresas que ya han tenido una gran trayectoria ya sea por desarrollo investigativo y tecnológico. Empresas como:

- IO: O2 es la marca comercial de Telefónica UK Limited y es una empresa de comunicación digital líder, con la satisfacción del cliente más alta para cualquier proveedor de telefonía móvil según Ofcom . Con más de 23 millones de clientes, O2 corre redes 2G, 3G y 4G en el Reino Unido.www.o2.co.uk/news
- Cisco: En Cisco (NASDAQ: CSCO) clientes son lo primero y una parte integral de nuestro ADN está creando larga duración asociaciones de clientes y trabajar con ellos para identificar sus necesidades y ofrecer soluciones que apoyan su concepto. Cisco ha dado forma al futuro de Internet mediante la creación de un valor sin precedentes y una oportunidad para nuestros clientes, empleados, inversionistas y socios del ecosistema y se ha convertido en el líder mundial en la creación de redes. Obtenga más información visitando www.cisco.com
- Deutsche Telekom, una de las empresas de telecomunicaciones más grandes e innovadoras del mundo, ofrece una etiqueta totalmente blanco y abierta plataforma de hogar conectado. Puesto en marcha con éxito en Alemania a finales de 2013, que ya está disponible a nivel internacional, con un enfoque inicial en Europa. La plataforma se ha diseñado para mover la industria más allá de un control sencillo de los dispositivos conectados, para crear una base para nuevos servicios generadores de ingresos. Además, se ha construido para satisfacer las diversas necesidades de los numerosos jugadores de múltiples industrias diferentes, incl. las empresas de telecomunicaciones y servicios públicos, las aseguradoras y los minoristas, todos ellos con el objetivo de hacer la vida de nuestros clientes de los clientes 'más simple y más fácil, para ahorrar energía, obtener una mayor paz de la mente, y más. . Para obtener más información, visita: http://m2m.telekom.com/
- Google es una empresa multinacional estadounidense especializada en servicios y productos relacionados con Internet. Estos incluyen las tecnologías en línea de publicidad, la búsqueda, el cloud computing y software. La mayor parte de sus beneficios se derivan de AdWords. Google fue fundada por Larry Page y Sergey Brin, mientras estaban Ph.D. estudiantes de la Universidad de Stanford. Juntos poseen alrededor del 14 por ciento de sus acciones, pero controlan 56 de los derechos de voto de los accionistas a través supervoting valores. . Para obtener más información, visita: http://www.google.com
- Microsoft Reino Unido. Durante las últimas tres décadas, Microsoft ha transformado constantemente la forma en que las personas viven, trabajan, juegan y se conectan a través de una gran tecnología. Nos inspiran todos los días por la creencia genuina que podemos cambiar el mundo para mejor. Aquí en nuestro sitio web del Reino Unido encontrará más información sobre cómo estamos impulsando avances en la computación en nube, el desarrollo de nuevas formas para que las personas

interactúan con la tecnología en el hogar, visite MICROSOFT http://www.microsoft.com [10]
- Entre otras.

Se puede encontrar la definición de éstas y otras empresas de forma mas extendida en: http://iotinternetofthingsconference.com/companies/

V. La seguridad de IoT

El increíble desarrollo del IoT está cambiando por completo la tradicional percepción que se tenía de Internet, hacia una visión integrada de objetos "inteligentes" que interactúan entre sí. Tanto es así, que el número y diversidad de sensores y dispositivos desplegados está creciendo de forma realmente alarmante. Tal como se había apuntado, dentro de este nuevo paradigma, y especialmente en ámbitos en los que se manejan datos sensibles, la pérdida de información o acceso incontrolado puede afectar seriamente a la privacidad de sus usuarios, por lo que la seguridad se constituye como un factor clave en el desarrollo y despliegue de estos nuevos escenarios. Este es un tema preocupante, ya que en a día de hoy no se dispone de una guía clara de acción para la seguridad IoT.

Los expertos apuntan que una de las principales barreras para la implantación de IoT es precisamente la seguridad y la privacidad. El porqué es bien sencillo: por un lado, las restricciones que imponen los dispositivos y redes de la IoT impiden la aplicación directa de soluciones tradicionales de seguridad. En concreto, protocolos tradicionales de seguridad y criptografía requieren una gran cantidad de recursos de memoria y proceso, algo de lo que habitualmente carecen los dispositivos IoT.[19] Por tanto, la adaptación de soluciones de seguridad a este nuevo paradigma se presenta como un gran desafío. Además, cabe destacar que a diferencia de otros entornos más tradicionales, los dispositivos de IoT suelen trabajar en condiciones de mayor dificultad, en cuanto a los entornos que les rodean, entornos que muchas veces no están controlados e incluso son hostiles o propensos a ataques malintencionados [7].

V-A. Presente y futuro seguridad IoT

Grandes fabricantes como Intel han apostado fuertemente por mejorar la seguridad de IoT, convencidos de la potencia y crecimiento de este sector en auge. Así, Intel ha presentado muy recientemente tecnologías que ayudan a mejorar la protección de IoT, como por ejemplo su tecnología de protección de datos para transacciones, que tiene por objetivo asegurar las transacciones de objetos IoT (Intel Data Protection Technology for Transactions) o la pasarela de soluciones para el Internet de las Cosas (Intel Gateway Solutions for the IoT), que conecta de forma más segura los objetos IoT con Internet e incluso con soluciones en la nube [8]. Por su parte, la compañía Cisco dentro de sus iniciativas para fomentar el desarrollo del IoT, ha llevado a cabo este año el concurso "El Gran Desafío de Seguridad del Internet de las Cosas", donde recibió postulaciones provenientes de más de 33 países, entre start-ups, empresas y universidades, premiando las cuatro mejores soluciones con un premio total 300.000 dólares, repartidos en premios de 75.000 dólares, además de otorgarles un espacio de exposición en el próximo Foro Mundial del Internet de las Cosas [9].

VI. Problemas y retos identificados

Expertos de la Comisión Europea [11], a partir de diversos estudios realizados para identificar los potenciales riesgos en entornos altamente interconectados, señalan como problemas importantes a tener en cuenta, en cuanto a privacidad y protección de datos y seguridad de la información con respecto al IoT. Continuación destacamos los que hemos considerado de importancia:

- Evitar posibles fallos e interrupciones en el funcionamiento. Esto está muy relacionado con el modelo de arquitectura a utilizar en la prestación de los servicios basados en IoT: centralizado vs descentralizado.
- Es muy conveniente tener en cuenta las cuestiones de seguridad y privacidad en la fase de diseño, aunque normalmente esto no es así y estos aspectos se tienen en cuenta una vez en funcionamiento, algo que limita la efectividad de las medidas de seguridad y es menos eficiente en cuanto a los costes. Los objetos IoT no suelen disponer de recursos suficientes, memoria y procesamiento, como para implementar las protecciones necesarias de seguridad.
- El aumento de recopilación de datos puede plantear problemas de autenticación y confianza en los objetos.
- Reutilización de los datos / ampliación de la verdadera misión de los datos. Debido a la proliferación de cada vez más cantidad de datos en los entornos IoT, es posible que estos datos puedan llegar a utilizarse para otros propósitos para los que no fueron creados originalmente, algo que es necesario controlar.
- No siempre las personas son conscientes de las capturas de información o el tratamiento que se le está dando a esa información. El acceso y control de datos, el permiso para recopilarlos y la frecuencia óptima para su recolección, son aspectos necesarios a tener en cuenta.
- Pérdida / violación de la privacidad y protección de datos de los individuos.
- Realización de ataques maliciosos contra los dispositivos y sistemas IoT. Si no se utilizan los controles de seguridad adecuados esto se convierte en un problema grave que puede conducir a otros problemas como los anteriormente mencionados. Lo difícil aquí es identificar los controles más apropiados para los sistemas IoT, para los que todavía se desconoce su evolución futura.
- Lock-in del usuario, en cuanto a que los usuarios se queden "bloqueados" en un proveedor específico de servicios IoT y les sea sea difícil migrar a otros proveedores, algo provocado por la no homogenización.
- Ya existen algunos avances, como el diseño de un protocolo de autenticación para la comunicación entre dispositivos médicos a través de la tecnología RFID para garantizar la seguridad y privacidad de los datos de los pacientes, estudio donde investigadores de la Escuela Técnica Superior de Sistemas Informáticos de la Universidad Politécnica de Madrid participan han colaborado [12], [13].

- Pérdida del control por parte del usuario / dificultad en la toma de decisiones. Uno de los principales objetivos de la IoT es dar cierta autonomía a los objetos y permitirles tomar decisiones de forma automática. Es necesario saber acotarlo en los casos que pueda suponer un problema y controlarlo adecuadamente para que no suponga riesgos o afecte a sus usuarios.
- Legislación aplicable. Dado el carácter global de IoT, otro problema es que los individuos y empresas se enfrentan a una serie de leyes de protección de datos nacionales / regionales que ofrecen distintos niveles de protección. Es necesario prestar especial atención a las leyes aplicables dependiendo del lugar donde se encuentren los objetos del IoT. [13]

Con todo lo antes menciona, como se puede apreciar aunque el Internet de las cosas a tenido un crecimiento muy alto alrededor de los últimos años, aun no se han podido desarrollar protocolos de seguridad eficientes para el mismo, por su principal atributo o defecto del mismo, el Internet. Se ha desarrollado una cuadro (Cuadro I.) en la cual se da la problemática en cuando a seguridad y que tanto se a desarrollada ésta en estos últimos años.

VII. Conclusiones

1. El Internet de las cosas, mejorará la vida de las personas, ya que para muchos es considerado una utopía completamente salida de lugar, porque en realidad con el internet de las cosas se puedes lograr accesibilidad a una parte de la ciencia que antes ni si quiera se los imaginaba.
2. Pero aun así podemos decir también, hablando explícitamente de la seguridad en el Internet de las Cosas, que aunque parezca salido de contexto, este tema también tienes sus contras, dado que con la información necesario y los implementos necesarios, que pueda obtener una persona, pueden llegar a lograr el mismo objetivo al que queremos llegar nosotros, lograr acceder o manipular un objeto mediante el internet para su uso, lo que significa una gran desventaja en este tema.
3. Así también podemos decir que en base al problema anterior, que se refiere a la seguridad, algunas impresas como Intel, Cisco o Telefónica, están basados exclusivamente a encontrar la solución inmediata al problema. Dado que el internet de las cosas se viene en crecimiento bastante acelerado, dado que es uno de los mejores métodos de aplicación para lograr miles de objetivos en nuestra casa, carro, oficina, etc.
4. Algunos de los papers que hemos revisado son escasos en la solución oportuna en estos casos basados en la seguridad del Internet de las Cosas. Por lo tanto en nuestro paper hemos querido abrir las oportunidades necesarias para que se generen estudios más sistematizados y adecuados a la búsqueda de solución a este problema. Para así lograr mermar los riesgos potenciales que se generan en el gran universo del Internet de las Cosas o IoT.

Referencias

[1] H. Sundmaeker, P. Guillemin, P. Friess, y S. Woelffl E. Visión y retos para la realización de la Internet de las Cosas. Cluster de Proyectos de Investigación europeos en el Internet de las Cosas, European Commision, 2010.

[2] I. Davidson, “Machine-to-Machine (M2M) Gateway: Trusted and Connected Intelligence. ,” Networking Marketing Manager, EMEA, Freescale Semiconductor, Inc., pp. 2 , Oct. 2013.

[3] Real Academia Española, “Diccionario de la Real Academia Española (RAE). ,” Avance de la vigésima tercera edición.

[4] Minoli, Daniel. Building the Internet of Things with IPv6 and MIPv6 : The Evolving World of M2M Communications. Somerset, NJ, USA: John Wiley & Sons, 2013. ProQuest ebrary. Web. 14 July 2015.

[5] D-Link, “5 tecnologías que acercan a los latinoamericanos al Internet de las Cosas,” iT ahora, La Revista del Comprador Tecnologico, 19 Nov. 2014.

[6] R. Van der Meulen, “Gartner Says Personal Worlds and the Internet of Everything Are Colliding to Create New Markets. ,” Newsroom, 11 Nov. 2013.

[7] Notra, S .; Siddiqi, M .; Gharakheili, HH; Sivaraman, V .; Boreli, R. "Estudio experimental de la seguridad y la privacidad riesgos emergentes con electrodomésticos", Comunicaciones y Seguridad de Red (SNC), 2014 Conferencia IEEE sobre, En la página (s): 79-84

[8] Intel® IO Pasarelas, “Intel Gateway Solutions for the Internet of Things. ” Enlace: http://www.intel.com/content/www/us/en/internet-of-things/gateway-solutions.html

[9] F. Lamus, “Cisco anuncia los ganadores del “Gran Desafío de Internet de las Cosas”. ,” Newsroom, 16 Oct. 2014

[10] IoT Conferencia 2015, “IoT Companies – Internet of Things Companies. ,” INTERNET OF THINGS WORLD FORUM 2015, 2015.

[11] European Commission, “IoT Privacy, Data Protection, Information Security (European Commision). ,” 13 oct 2010.

[12] Picazo-Sanchez, P; Bagheri, N; Peris-Lopez, P; Tapiador, JE. Two RFID Standard-based Security Protocols for Healthcare Environments. JOURNAL OF MEDICAL SYSTEMS, 37 (5):10.1007/s10916-013-9962-3 OCT 2013

[13] CAIT (Centro de apoyo a la innovación Tecnológica), “Seguridad en el Internet. ,” Universidad Politécnica de Madrid, 2014

[14] D. Evans“Internet de las cosas: Cómo la próxima evolución de Internet lo cambia todo. ,” Cisco Internet Business Solutions Group (IBSG), Abr. 2011

[15] Jeremy Rifkin Enterprises, “La sociedad de coste marginal cero : el Internet de las cosas. ,” 1ra Edición, pp. 24-25. Sep. 2014.

[16] P. H. Diamandis, S. Kotler, “Abundancia: El futuro es mejor de lo que piensas. ,” Novoprint, pp. 88-90. 2013.

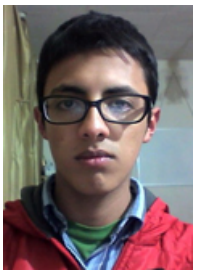
[17] A. Oppernheiner, “Crear o morir!: La esperanza de América Latina y las cinco claves de la innovación. ,” Internet de las Cosas, Debate, 2013.

[18] F. Telefónica, “Smart Cities: un primer paso hacia la Internet de las Cosas Fundación Telefónica. ,” 2011.1, 1

[19] D. Evans, “Internet de las cosas Cómo la próxima evolución de Internet lo cambia todo. ,” 2011

[20] C. Principal, “El Internet de las Cosas Fundación de la Innovación Bankinter. ,” accenture, pp. 3, 01 Enr. 2011

Biografía



Youssef Moises Abarca Reyes ,nació el 30 de Agosto de 1994, realizó sus estudios secundarios en el colegio Adolfo Valarezo de la ciudad de Loja, obtuvo el título de Bachillerato físico matemático. Cursa sus estudios superiores de Ingeniería Electrónica en la Universidad Politécnica Salesiana sede Cuenca donde desarrolla actividades extracurriculares en el proyecto de Vinculación con la Sociedad, realizando instalaciones eléctricas entre otras actividades en beneficio de la sociedad.

Problemática \ Avance	Bajo	Medio	Alto
Evitar posibles fallos e interrupciones en el funcionamiento.		✔	
Tener en cuenta las cuestiones de seguridad y privacidad en la fase de diseño.	✔		
El aumento de recopilación de datos puede plantear problemas de autenticación y confianza en los objetos.		✔	
Reutilización de los datos / ampliación de la verdadera misión de los datos.			✔
El acceso y control de datos.			✔
Pérdida / violación de la privacidad y protección de datos de los individuos		✔	
Realización de ataques maliciosos contra los dispositivos y sistemas IoT.		✔	
Lock-in del usuario.			✔
Pérdida del control por parte del usuario / dificultad en la toma de decisiones.		✔	
Legislación aplicable.			✔

Cuadro I
TABLA DE PROBLEMATICA DE SEGURIDAD Y COMO ÉSTE A AVANZADO.

Luis Alberto Galarza Aguilar, nació en Piñas - El Oro- Ecuador el 13 de Agosto de 1994, realizó sus estudios primarios en la Unidad de Educación Básica Sagrado Corazón de Jesús y sus estudios secundarios en el Instituto Tecnológico 8 de Noviembre y Colegio Nacional Técnico Leovigildo Loayza Loayza, obteniendo títulos de Bachiller en: Físico Matemático y Contabilidad y Auditoría, respectivamente. Ahora cursa sus estudios universitarios en la Universidad politécnica Salesiana en la carrera de Ingeniería Electrónica.