IoT, METODOLOGÍA Y PROBLEMAS ACTUALES EN EL MUNDO DE LAS TELECOMUNICACIONES

Rodrigo Lita Zamora
UPIICSA
lita1e@hotmail.com

Daniel Eduardo Gatica Flores
UPIICSA
daniel_eduardo02@hotmail.com

Abstract

The IoT has been the method of communication between objects that most played in this last decade. It has allowed the telecommunications industry to grow because of the need for networks where these objects are going to be connected to each other in order to be manipulated remotely as this paradigm suggests. Objects as basic as appliances such as the complex that can be the car, at present, are connected to the network allowing its control from remote places having easy access when required and needed. The objects handle different modes of use and connection between them since to link will not be equal to each other and with this the telecommunications play an important role with the nodes. Likewise, the paradigm has faced great challenges due to questions about its security in the application of this method of interconnection between them. We will visualize the impact of the IoT during the last decade to know how it will have an impact in the future.

Introducción

El internet de las cosas o IoT (Internet of Things) refiere a la conexión del mundo en la red donde cada objeto esta interconectado entre sí, a su vez, es un mundo de noticias y una tendencia de mercadotecnia. El IoT es un paradigma de la década pasada que llego para quedarse y evolucionar juntos con los objetos que se conecta a través de este, ha ganado fama entre las más modernas tecnologías de telecomunicaciones.

En el mundo de las telecomunicaciones, el IoT sirve gracias a un sensor de redes inalámbricas (WSN) junto con una identificación de radio frecuencia (RFID). Las redes inalámbricas son parte esencial e integral de los sistemas IoT, pero no todo es felicidad en estos campos conjuntos ya que las redes inalámbricas presentan restricciones importantes en el manejo de los dispositivos como lo es el hecho de que la comunicación por ondas de radio consumen más energía que la comunicación por cable o simplemente las redes usadas en los sistemas IoT fueron diseñadas para otros fines como la multimedia o telefonía.

Indudablemente, la fortaleza del IoT se basa en las ideas de los campos de aplicación en donde este puede atacar para ayudar a que nuestro día a día sea más eficiente y eficaz. Campos de aplicación como las tareas domesticas, la "e-health", la enseñanza mejorada, la domótica, los negocios, la automatización, la logística entre otras son ejemplos de los escenarios en donde el IoT está atacando en la actualidad y seguirá fortaleciendo.

Tiempo atrás se decía que el IoT estaría presente en todo lugar de la vida cotidiana y con el paso del tiempo se ha demostrado que esto es verdad. La comunidad científica ha tenido debates acerca de una definición concisa de lo que es el IoT, principalmente por definir cómo es que los objetos se clasifican teniendo distintas visiones para el mismo paradigma.

Metodologías

Algunos autores definen al IoT como "Internet orientado" mientras que otros lo definen como "Objetos orientados" pero el hecho de que las palabras internet y cosas estén escritas juntas nos da la idea que el internet de las cosas refiere a "Una red mundial de objetos interconectados de acceso único, basada en los estándares de los protocolos de comunicación". (INFSO, 2008)

El IoT maneja ciertas metodologías y arquitectura haciendo que sea funcional este paradigma, una de las herramientas esenciales para esto son los protocolos pero en especifico los de la comunicación teniendo estos un problema al no proporcionar la abstracción necesaria para algunas aplicaciones debido a que los sistemas IoT requieren comunicaciones multi hop o de extremo a extremo.

Algunos protocolos de alto nivel satisfacen las necesidades de la naturaleza y duración de los sistemas IoT. Un ejemplo de estos protocolos es el HTTP que lleva un diseño de solicitud y respuesta, el usuario solicita un archivo y el servidor responde a lo solicitado.

Con el crecimiento del IoT los dispositivos interconectados son llamados sensores en el internet, que a su vez generan un cierto tipo de información para ciertos propósitos que usaran otros sensores. Estos sensores tienen una clasificación siendo sensores fijos y sensores móviles. Cada sensor fijo en la red tiene una serie de nodos para llegar a otro sensor fijo mientras que los sensores móviles no cuentan con algún nodo fijo (fig. 1).

Teniendo la clasificación de los sensores, estos siguen cuatro categorías de enlace, las cuales se determinan en: Fijo a Fijo, Fijo a Móvil, Móvil a Fijo, Móvil a Móvil. Estas conexiones se dan gracias a la existencia de nodo de solitud y un nodo de respuesta quienes tendrán la función de hacer la conexión entre objetos.

En la comunicación fijo a fijo, cuando el primer nodo encuentra al segundo en una posición tratara de crear la ruta más corta para el envió de la información entre los nodos siendo el primer nodo el solicitante y el segundo el de respuesta.

En el modo de comunicación fijo a móvil; el primer sensor que es fijo enviara una búsqueda del sensor móvil para su localización, una vez encontrado el sensor se procederá a mandar la información por medio del nodo más corto encontrado. De igual manera el primer sensor será el solicitante y el segundo el de respuesta.

Cuando se habla de un modo de comunicación móvil a fijo; el sensor móvil enviara la información al sensor fijo más cercano al área de donde este se encuentre, teniendo como el solicitante al móvil y el de respuesta al fijo.

Por último, una comunicación de sensor móvil a móvil será por medio de sensores fijos intermedios. Primero el sensor móvil enviara la información al sensor fijo más cercano y este a su vez la repetirá a otros sensores fijos para que llegue al sensor móvil de destino que se encuentre en el área del sensor fijo con la información repetida.

Sharad Saxena define que las conexiones entre estos sensores se dan por la cantidad de nodos existentes con los objetos. Teniendo como "O" a los objetos que se clasifican en objetos móviles (O_m) y los fijos (O_f), y a su vez a los nodos "E" teniéndolos como fijos (E_f) y dinámicos (E_d). Con esta definición podemos denotar entonces:

$O = O_f \cup O_m$ y $E = E_f \cup E_d$ (Saxena, 2017)

Retos del IoT, cuestiones de seguridad y privacidad.

Los proyectos más reconocidos en la materia del IoT son la automatización y control de tu hogar mediante tu teléfono celular a distancia o la revisión de este mediante los mismos instrumentos que llevas contigo a cualquier lugar. Este tipo de proyectos además de novedosos han hecho incertidumbre sobre si el sistema será seguro o no.

Para tener una perspectiva acerca del diseño de estos sistemas de seguridad y su implementación tomaremos como ejemplo el proyecto de la "implementación de sistemas de seguridad a una residencia por medio del IoT" de unos estudiantes de Guatemala miembros del IEEE. Ellos plantean sus sistemas de seguridad mediante cámaras de seguridad que tomaran evidencias y serán mandadas a un controlador a través de la red, sensores de movimiento que alertaran la presencia de algún individuo en el área determinada, controladores por medio de Raspberry Pi lo Arduino para que el usuario pueda tomar acciones con los resultados de las cámaras y los sensores mismos que serán controlados también desde un módulo de comunicación.

Estos son los sistemas de seguridad que plantean para la automatización de una casa mediante el IoT ya que las funciones del hogar estarán manejadas mediante servomotores y microcontroladores que están esparcidos en el hogar, ellos concluyen que el hogar será seguro ya que, además, se realizo una pagina web en donde se hace el control total del hogar teniendo confianza en su seguridad.

Pero eso no lo es todo sobre la incertidumbre en la seguridad, otro de los aspectos es un posible ataque hacker a ellos entorpeciendo sus sistemas haciendo que estas medidas de seguridad sean inseguras y teniendo desconfianza de ellas. Por eso mismo, encontramos un sistema de seguridad encargado de ellos que se denomina el "Self-Healing Group Key Distribution" (SGKD) que es un protocolo de seguridad añadido a las redes inalámbricas no confiables, el problema de este protocolo es que en este las claves de sesiones pueden ser recuperadas mediante los paquetes de mensajes recibidos con anterioridad a través de un host que los solicite. Por ello se planteó el protocolo AP-SGKD que tiene mas seguridad y confianza al usar acceso mediante dobles cadenas y múltiples puntos de acceso para garantizar la propiedad de la cuenta del individuo.

Antonio Alcón, Lourdes López, José Martínez presentan un modelo en donde se soluciona y garantiza la seguridad del IoT a través de las telecomunicaciones para la confianza de las personas en este paradigma. Ellos mencionan que los niveles de seguridad y privacidad sobre los elementos que deben de protegerse deben de estar sometidos a lo que mencione el marco legal en el que está orientado el servicio.

Así mismo se dan las acciones que se debe de hacer en un sistema de IoT para sus seguridad dentro de el, las acciones son las siguientes:

- Autenticación, el usuario deberá de demostrar que es el mediante un sistema con protocolo AP-SGKD
- Control de acceso por medio de los sensores.
- Integridad de los datos para cerciorar que no han sido manipulados.
- No repudio con el fin de demostrar el origen de los datos.
- Confidencialidad de los datos para su protección ante una revelación no autorizada, en este punto se puede hacer uso del protocolo AP-SGKD

Conclusiones

Como vemos el IoT tiene mucho potencial para ayudarnos en nuestra vida cotidiana en varios aspectos. Además que este puede proporcionarnos control en una gran variedad de aspectos gracias a la facilidad de comunicación que este tiene con el mundo y su versatilidad. Sin embargo sabemos que tiene debilidades que necesariamente se tiene que tratar como es el caso de la seguridad. Por lo que podemos concluir que:

- Es necesario que el AP-SGKD se encuentre en todos los dispositivos ya que es un protocolo que se encarga de proteger nuestros datos y al dispositivos.

- Incluir sensores para el control del dispositivo y confidencialidad de los datos con el apoyo del AP-SGKD.
- Incluir diversas medidas de seguridad extras como firmas digitales, cifrado, autentificación, diversos mecanismos de control, etc.

Recursos electrónicos

1. Atzori, L., Iera, A., Morabito, G. (2010, Junio 1). The Internet of Things: A survey. Recuperado el 10 de septiembre de 2018, de www.elsevier.com/ locate/comnet
2. Biljana, L. Risteska, S., Trivodaliev, K. (2016, Octubre 1). A review of Internet of Things for smart home: Challenges and solutions. Recuperado el 10 de septiembre de 2018, de www.elsevier.com/locate/jclepro
3. Friedow, C., Volker, M., Hewelt, M. (Revisado en 2018. Septiembre 10). Integrating IoT Devices into Business Processes. Recuperado el 10 de septiembre de 2018, de www.elsevier.com/ locate/comnet
4. Fuentes, O., Pérez, J. (2017) Implementación de un Sistema de Seguridad Independiente y Automatización de una Residencia por medio del Internet de las Cosas. Recuperado el 10 de septiembre de 2018, de www.elsevier.com/ locate/comnet
5. Guo, H. et. al. (2018, Julio17). Self-healing group key distribution protocol in wireless sensor networks for secure IoT communications. Recuperado el 10 de septiembre de 2018, de www.elsevier.com/locate/fgcs
6. Mijares, M., Bonillo, P. (2017) Modelo Teórico para la Especificación y Gestión de Procesos de Negocio sobre el Internet de las Cosas (IoT), sustentados en Big Data. Recuperado el 11 de Septiembre de 2018, de www.elsevier.com/
7. Otsuka, T., Torri, Y., Ito, T. (2018). An Innovative Outdoor IoT System Architecture for Service Oriented Things. Recuperado el 11 de septiembre de 2018, de https://doi.org/10.1007/978-3-319-70019-9_19
8. Sánchez, J., Santidrian, L., Martínez, J. (2015). Solución para garantizar la privacidad en internet de las cosas. Recuperado el 11 de septiembre de 2018, de http://orcid.org/0000-0002-3673-2735
9. Saxena, S. (2017). Abstracting Communication Methodology in IoT Sensors to Eliminate Redundancy and Cycles. Recuperado el 12 de septiembre de 2018, de www.elsevier.com/
10. Serpanos, D., Wolf, M. (2017). Internet-of-Things (IoT) Systems Architectures, Algorithms, Methodologies. Recuperado el 12 de septiembre de 2018, de https://doi.org/10.1007/978-3-319-69715-4
11. Sosa, C. et. al. (2018. Agosto 27). Methodology for the model-driven development of service oriented IoT applications. Recuperado el 13 de septiembre de 2018, de www.elsevier.com/locate/sysarc