Revista de I+D TECNOLÓGICO
Portal de revistas: http://revistas.utp.ac.pa

El estado del arte: Salud inteligente y el internet de las cosas

State of art: Smart health and internet of things

Alberto Domínguez [1], Miguel Vargas-Lombardo [2*]
[1,2]*Facultad de Ingeniería de Sistemas Computacionales,* [1,2]*Universidad Tecnológica de Panamá, Panamá*
***Autor de correspondencia:** miguel.vargas@utp.ac.pa

RESUMEN– El Internet de las cosas (IoT) es la nueva tendencia de dispositivos en el mercado. Esta tecnología está siendo desarrollada por múltiples fabricantes de diversas partes del mundo para solucionar problemas específicos del día a día de las personas. Sin embargo, en la actualidad se están dando muchos casos de fallas de seguridad en dispositivos IoT, en este caso en hospitales. En este escrito también se describe el IoT como un complemento al sector salud haciendo referencia a las tecnologías creadas e implementadas por distintos fabricantes. Se presentan también los distintos métodos de seguridad que los fabricantes han implementado en sus soluciones y sus productos, desde diseños de topologías alámbricas e inalámbricas, hasta seguridad perimetral estricta de capa 2 y capa 3, las cuales trabajan en conjunto con la programación segura y recomendaciones para que el usuario final realice el uso adecuado del mismo. Al final del escrito se presenta la tecnología WBAN y los riesgos que conlleva junto con el IoT si no se asegura adecuadamente, ya que podría ser crítico y pondría en riesgo la vida de los pacientes. El objetivo es implementar en nuestro sistema IoT una capa extra de seguridad informática sin depender que el fabricante la haya embebido en su producto. Dicha capa dificulta que el atacante pueda manipular nuestros equipos a su conveniencia o que pueda explotar una falla conocida en un dispositivo que pueda perjudicar la vida, salud e integridad del paciente.

Palabras claves– *Fabricante, hospital, internet de las cosas, salud, seguridad informática, salud inteligente.*

ABSTRACT– The Internet of Things (IoT) is the new device trend in the market. This kind of technology is being developed by multiple manufacturers in various parts of the world to solve people's daily issues. However, there have been many cases of security failures in IoT devices, mainly at hospitals. This document describes IoT as a compliment in health area by referring created and implemented technologies by different manufacturers. Also, there are shown different security methods that manufacturers have implemented in their solutions and their products, from wired and wireless topologies designs to strict layer 2 and layer 3 security perimeters, which work together with secure programming and final user's recommendations to give a correct use of each device. At the end of this document WBAN technology is presented including the risks attached with IoT if it is not correctly secured because it could be critical and would endanger the lives of the patients. The main objective is to implement in our IoT system an extra security layer without depending on manufacturer embedded operating system on their product. This layer represents a challenge to the hackers and would be more difficult to gain access and manipulate our devices for their benefit or finding a vulnerability that can be exploited to harm the patient's life, health and integrity.

Keywords– *Manufacturer, hospital, internet of things, health, network security, smart health.*

1. Introducción

En el siguiente escrito se presenta una tecnología que, a pesar de ser tan exitosa, puede llegar a ser un completo fracaso si no se implementa Seguridad Informática, el Internet de las cosas (IoT) dirigido hacia la salud del ser humano implementado en hospitales de primer mundo.

Las compañías cada día son más competitivas e innovadoras por lo que exigen personal capacitado y certificado que aporten al desarrollo económico del país. En este caso el IoT específicamente en la salud, abre una puerta para especialistas en seguridad informática el cual debe conocer a cabalidad el entorno tecnológico en el que se encuentra el hospital y las tecnologías que brinda el mercado.

Adicional a esto, también se muestran los beneficios de implementar IoT en los hospitales, fabricantes, dispositivos y políticas en concepto de seguridad de la información que cumplan con los principios de confidencialidad, integridad y disponibilidad de las aplicaciones y servicios con la finalidad de facilitar el día a día del personal médico y la atención a los pacientes.

Si no se toman las medidas necesarias para proteger estos dispositivos de ataques informáticos según las necesidades del paciente, se podría causar hasta la

Citación: M. Vargas y A. Domínguez, "El estado del arte: Salud inteligente y el internet de las cosas", *Revista de I+D Tecnológico*, vol. 14, n.° 1, pp. 14-17, Junio, 2018.
Tipo de artículo: Revisión. **Recibido:** 20 de junio de 2017. **Recibido con correcciones:** 1 de diciembre de 2017. **Aceptado:** 11 de abril de 2018.

muerte, por ejemplo, una sobredosis de insulina para un paciente diabético ocurre cuando los niveles de glucosa en la sangre se encuentran por debajo de 70 mg / dL, si al paciente se le suministra insulina por medio de un dispositivo IoT que se encuentra bajo ataque podría causar una hipoglucemia bajo síntomas como desmayos, debilidad, convulsiones, problemas respiratorios entre otras.

2. Salud inteligente

El IoT crea un gran impacto en cada negocio y la salud es un negocio, por lo tanto, es importante que en un área tan importante como lo es la salud, el desarrollo y programación de estos dispositivos sea perfecto con actualizaciones periódicas ya que existen muchos factores que podrían poner la vida del paciente en peligro.

Los recientes avances en el área de la salud a diario crean una cantidad enorme de oportunidades en innovación dirigido a clínicas y hospitales en especial a dispositivos móviles. Además de describir los riesgos que conlleva esta tecnología, veamos los avances que esta tecnología presenta tanto para personal médico como para los pacientes. En un ambiente crítico como el de un hospital es necesario que el personal reciba notificaciones emitidas lo más pronto posible a través de la red al dispositivo o dispositivos que correspondan.

2.1 Desarrollo en los hospitales

Llaman la atención los mecanismos y métodos que pueden ser creados para hacer la vida de los médicos y pacientes mucho más fácil, desde realizar diagnósticos simples hasta el momento crítico en que se presenta una urgencia [1].

Esta tecnología a pesar de ser adquirida por los hospitales, aún se encuentra en etapas de desarrollo, pero presenta las siguientes ventajas:

- ✓ Simplicidad de uso: con una interfaz gráfica y amigable tanto para el paciente como para el personal médico se pueden asegurar respuestas oportunas, rápidas y efectivas.
- ✓ Ahorro energético: el *software* tiene la capacidad de mostrar en tiempo real la temperatura ambiente, gestión de encendido y apagado de luces en el hospital utilizando un sistema de domótica.
- ✓ Seguridad y control: Las alarmas generadas se almacenan en una base de datos MySQL y funciona de forma redundante ya que en caso de errores en la comunicación, la información se almacena localmente en cada dispositivo hasta que vuelvan a detectar que la base de datos se encuentra en línea.
- ✓ Optimizar procedimientos: muchas de las soluciones aparte de notificar a médicos y enfermeras, también tienen la facilidad de informar a personal de sanidad alguna necesidad de los pacientes sin importar su ubicación lo que ayuda a optimizar el trabajo de la enfermería.
- ✓ Implantación: El sistema hospitalario debe estar integrado en donde se puedan exportar registros y alarmas desde el cuarto donde se encuentra paciente hasta el personal médico y sanitario como se muestra en la figura 1.

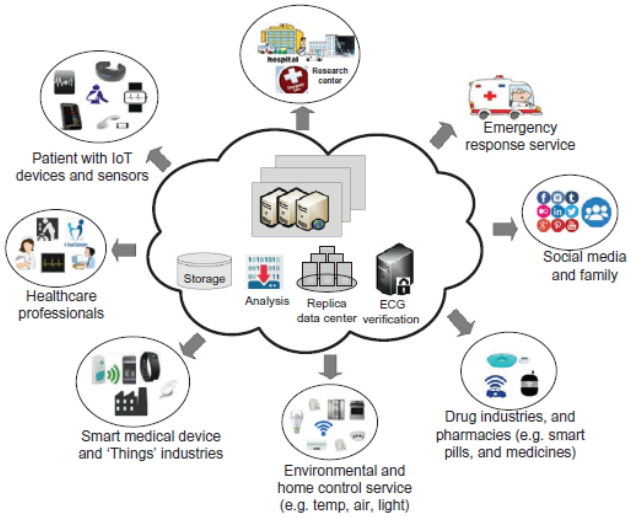

Figura 1. Ambiente integrado en soluciones IoT para hospitales [2].

2.2 Componentes

Como todos sabemos, las personas que se mantienen en constante movimiento en un hospital son los del departamento de enfermería. Este personal es el que debe estar mayormente familiarizado con cada uno de los componentes del hospital para que el paciente se sienta lo más cómodo posible [3].

- ✓ Dispositivos de radiofrecuencia: El IoT integrado con la tecnología de identificación por radio frecuencia (RFID), desmantela una nueva perspectiva para cada dispositivo involucrado por medio de un sistema inteligente del cual se obtiene información precisa.
- ✓ Terminales de habitación: Para que un paciente se encuentre en un ambiente cómodo, estas

terminales cuentan con la capacidad de funcionamiento autóctono capaz de realizar llamadas VoIP que garanticen el contacto con el personal médico o sanitario.

- ✓ Mecanismos de información: con estos dispositivos dedicados para personal médico es posible consultar tareas pendientes, codificar tareas y alarmas atendidas lo que brinda seguridad a los datos internos del hospital por medio de cifrado [4].

2.3 Empresas involucradas

Organizaciones encargadas del cuidado de la salud se encargan de evaluar estas soluciones para ser implementadas en los mejores hospitales a nivel mundial. Como resultado, las empresas desarrolladoras de estos productos tienen la oportunidad de explotar por medio del conocimiento tecnologías que permitan establecer soluciones colaborativas que brinden:

- ✓ Recursos compartidos.
- ✓ Mejor cuidado del paciente.
- ✓ Ahorro de tiempo.
- ✓ Capacitación del personal médico.
- ✓ Comunicación y colaboración [5].

2.3.1 Polycom

Gracias al poder de la colaboración, compañías como Polycom son capaces de desarrollar tecnologías lo suficientemente aptas y adecuadas que se adapten a las necesidades de los hospitales.

Los productos que brinda Polycom para la comunicación dirigida hacia el cuidado de la salud como se muestra en la figura 2, aprovechan su uso para el aprendizaje de estudiantes que cursan carreras de medicina y sus especialidades por medio de operaciones y distintas atenciones a los pacientes.

Figura 2. Colaboración telemédica multipunto de Polycom [3].

Estos equipos no brindan únicamente facilidad al personal médico, sino que también hacen que el paciente sienta confianza y comodidad al ser atendido. En consecuencia, Polycom ha facilitado las interconexiones por medio de su tecnología entre hospitales, centros médicos educativos y asociaciones para que sus integrantes puedan presenciar en tiempo real y les permita discutir sobre las dificultades y desafíos para buscar la solución más efectiva según el diagnóstico del paciente [6].

2.3.2 Avaya

Avaya es otra de las compañías que se ha encargado de innovar el mercado tecnológico pensando un poco más allá y con esto se refieren a implementar seguridad desde políticas hasta cifrado de tráfico con su línea **Surge** para hospitales.

Con una arquitectura desarrollada por Avaya llamada SDN (Software Defined Network) es capaz de administrar más de 150,000 dispositivos capaces de ser administrados por un controlador central encargado de todo el entorno y los dispositivos que forman parte de este.

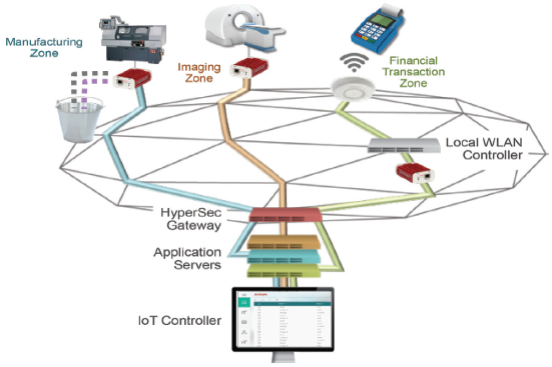

Figura 3. Componentes de Solución Avaya SDN [7].

Avaya ha implementado en sus dispositivos programación segura que se componen de segmentos aislados de la red interna puedan ser identificados por el controlador como se muestra en la figura 3, el tráfico viaja de forma cifrada dentro de la red y cada dispositivo tiene los recursos suficientes para ejecutar sus funciones en tiempo real.

Un estudio de The Global Analysis Benchmark Research de IBM comprobó que del 85% de los incidentes que involucran ataques criminales y maliciosos, el 25% de estos ataques fueron causados por personal interno y un 27% han sido por vulnerabilidades o por mal uso de los dispositivos, esto demuestra que la seguridad hay que implementarla a nivel de usuario y

las empresas responsables diseñar productos que brinden seguridad y privacidad [7].

3. WBAN

WBAN (Wireless Body Area Network) es una nueva tendencia en el mundo de IoT en la salud compuesto de sensores que ayudan a recolectar información sobre el estado de salud del paciente por medio de distintas pruebas a través de sensores.

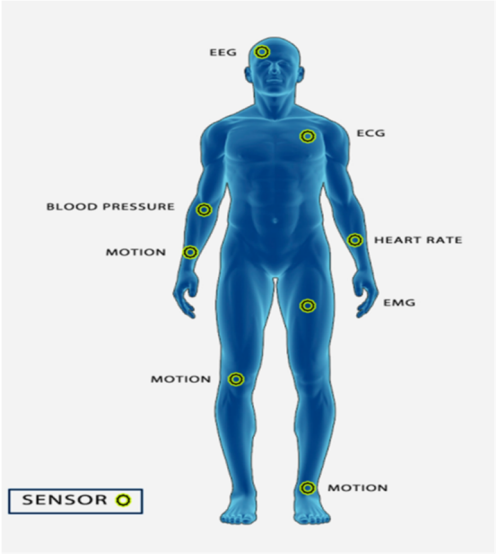

Figura 4. Sensores WBAN.

Como todo sistema informático y redes implementadas, los sistemas WBAN también requieren de medidas de seguridad para proteger los datos de los pacientes garantizando la confidencialidad, integridad y privacidad de los registros de salud en todo momento.

Esta tecnología brinda un mecanismo seguro de recaudación de información del paciente en donde la información solo puede ser recibida, procesada y enviada por personas y equipos autorizados por medio de mecanismos de cifrado a través del intercambio de llaves. Si un atacante tiene acceso a esta información y la modifica, podría atentar contra la vida del paciente ya que podría cambiar su diagnóstico e incluso la medicación a recetar [8].

4. Conclusiones y recomendaciones

El mundo de la tecnología es un mundo maravilloso en donde áreas como el IoT y la Seguridad Informática se llevan muy bien de la mano cuando se implementan juntas sobre todo si es para un beneficio que salva vidas. Como administrador de redes es recomendable realizar actualizaciones a los dispositivos cuando se realice el lanzamiento, en caso de tener habilitadas funciones que no serán utilizadas entonces deben desactivarse, deben deshabilitarse accesos remotos y segmentar la red por medio de VLANs para que la calidad de la comunicación sea perfecta debido a que los dispositivos que la conforman implementan cifrado lo que hace que la cantidad de tráfico incremente considerablemente.

5. Referencias

[1] P. Yang, O. Amft, Y. Gao, and L. Xu, “Special Issue on The Internet of Things (IoT): Informatics Methods for IoT-enabled Health Care,” J. Biomed. Inform., vol. 63, no. 2016, pp. 404–405, 2016.

[2] M. S. Hossain and G. Muhammad, “Cloud-assisted Industrial Internet of Things (IIoT) - Enabled framework for health monitoring,” Comput. Networks, vol. 101, pp. 192–202, 2015.

[3] S. D. Shapiro, “Transformational Healthcare Models,” Inflamm. Bowel Dis., vol. 22, no. 8, pp. 1984–1985, 2016.

[4] A. Santos, J. Macedo, A. Costa, and M. J. Nicolau, “Internet of Things and Smart Objects for M-health Monitoring and Control,” Procedia Technol., vol. 16, pp. 1351–1360, 2014.

[5] B. A. Kalbag and G. Silverman, “Enriching Business Processes through Internet of Everything,” Cisco Syst. Inc., no. June, pp. 1–15, 2014.

[6] Polycom, “New Healthcare Vision Collaborative video solutions improving care and reducing cost,” California, U.S., 2014.

[7] Avaya, “Avaya Surge IoT Solution Solution Brief,” California, U.S,2017. https://www.avaya.com/en/documents/avaya_surge_iot_solution_dn7829.pdf

[8] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications,” Egypt. Informatics J., 2016.