LAS CIBERMANEZAS EN LA IMPLEMENTACIÓN DEL INTERNET DE LAS COSAS MÉDICAS (IoMT)

Ing. Flores Montaño Luis Alberto
Estudiante de Maestría en Informática SEPI
UPIICSA

Lic.Aline Militzin Rojas Perea
Estudiante de Maestría en Doncencia ALIAT

Dr. Álvarez Cedillo Jesús Antonio
Profesor de Maestría en Informática SEPI UPIICSA

luisfloresmontano@hotmail.com
alinerojasp@hotmail.com
jaalvarez@ipn.mx

Boletín No. 70
1o. de enero de 2019

Resumen

En los últimos años, el Internet de las cosas ha ido en aumento, dispositivos conectados al internet los cuales usan controladores basados en microprocesadores con aplicaciones, teniendo así, dispositivos que van desde tostadoras hasta aviones, los cuales, se ha hecho notar su importancia en diversas áreas de la industria. Sin embargo, la industria de la salud ha sido más lenta en adoptar las tecnologías de Internet de las Cosas a comparación de otras industrias; el Internet de las Cosas Médicas (IoMT-por sus siglas en inglés- Internet of Medical Things), como es conocida, está preparada para transformar la forma en que mantenemos a las personas seguras y saludables, especialmente a medida que aumenta la demanda de soluciones para reducir los costos de la atención de la salud en los próximos años. El IoMT puede ayudar a monitorear, informar y notificar no solo a los cuidadores, sino también a los proveedores de atención médica con datos reales para identificar los problemas antes de que se vuelvan críticos o para permitir una intervención más temprana. Sin embargo, esta industria no solo ha sido lenta en adoptar la tecnología IoT, si no también lo ha sido en el tema de seguridad, puesto que muchas firmas dedicadas a la fabricación de dichos dispositivos han dado pocas o ninguna medida de seguridad para los dispositivos médicos. En esta investigación se darán a conocer algunos de los puntos importantes de cómo el IoMT, donde se consideran las las consecuencias de la falta de seguridad en dichos dispositivos.

1. Introducción

En el mundo de hoy, el Internet de las cosas (IoT) es omnipresente y tiene un gran potencial, sin embargo, hay que tener presente que dicha tecnología conlleva problemas de seguridad. Los dispositivos de IoT se utilizan en todas las industrias, incluyendo la de salud, la cual utiliza dispositivos son conocidos

como el Internet de las Cosas Medicas o IoMt (- por sus siglas en inglés Internet of Medical Things). Los cuales son inseguros y conllevan grandes riesgos que se deben tener en cuenta.

Existen diversos dispositivos para la salud involucrados como microscopios, refrigeradores que almacenan productos químicos, equipos de farmacia, bombas de infusión y camas inteligentes, que están conectados a la red del hospital en una arquitectura compleja de información, datos compartidos atraviesan la misma red, de modo que el equipo de tratamiento puede tener una visión compartida de los eventos. Cabe mencionar que este procedimiento no era posible con la tecnología de hace una década.

Además de la asistencia sanitaria, los dispositivos de IoMT también se utilizan para recopilar datos, monitorear sistemas y controlar el tejido que mantiene unidos el funcionamiento interno de muchas industrias. Las farmacias de los hospitales requieren el mismo nivel de controles que las refinerías, las instalaciones de generación de energía e incluso los almacenes con luces apagadas, donde los sensores evalúan los procesos con precisión y realizan ajustes casi en tiempo real.

Muchos de estos dispositivos se han agregado a las redes corporativas primarias debido al costo y la necesidad de monitorear los sistemas en todas las empresas. Sin embargo, estos últimos no fueron diseñados para hacer frente a los riesgos de la ciberseguridad presentes en la actualidad, ya que se ha brindado poca planificación a los parches de rutina.

Las organizaciones dedicadas al tratamiento para la salud tienen la necesidad de proteger datos confidenciales de los ataques cibernéticos, especialmente porque hay vidas en juego, pero las soluciones prácticas son difíciles de implementar. Por lo que, en esta investigación, se incluyen algunas medidas que se pueden aplicar a toda la IoT, pero más específicamente a la IoMT (Clyde,2018).

2. Contenido del artículo

Desde los sensores más pequeños hasta los sistemas completos de la sala de operaciones, Internet of Medical Things (IoT) ha ayudado a salvar vidas y a cambiar la práctica de la medicina (Zhu, 2012). Al capturar de forma remota los datos médicos, facilitar el suministro de medicamentos y habilitar las aplicaciones de salud digital, IoMT ofrece una mayor comodidad y funcionalidad a los pacientes y sus médicos, siendo más específicos en la importancia se describen a continuación:

- Garantizan el cumplimiento de las órdenes de los médicos. IoMT no pretende reemplazar a los proveedores de atención médica, sino que proporcionar los datos recopilados de los dispositivos para un mejor diagnóstico y planes de tratamiento, así como para reducir las ineficiencias y el desperdicio en el sistema de atención médica.
- Ayudan a monitorear el comportamiento y la actividad del paciente fuera de la clínica o consultorio, por lo que el proveedor tendrá datos reales para referirse al cumplimiento de las recomendaciones de terapia del paciente y lo que sucede después de que un paciente deja un centro médico.
- Crear productos farmacéuticos personalizados y determinar pautas de atención basadas en los sistemas biológicos únicos de un paciente en particular, IoMT abre la puerta a una atención médica más personalizada para cada individuo.

  A medida que aumente el número de dispositivos conectados, los sistemas de TI deberán determinar cómo manejar la carga de datos de forma segura. Para que las cosas de IoMT sean realmente transformadoras, las organizaciones de atención médica deberán descubrir cómo convertir todos los datos que se recopilan en información (Marr, 2018). Si bien el impulso de esta transformación está aumentando, se requerirá que los administradores del hospital, los fabricantes y los proveedores trabajen juntos para impulsar la metamorfosis cultural del cuidado de la salud.

  Como se mencionó anteriormente, desarrollar medidas de seguridad puede ayudar a las compañías de tecnología que producen productos de IoMT, componentes y software relacionado a mitigar esos riesgos. Antes de mencionar algunas medidas de seguridad para este tipo de dispositivos, se mencionará a detalle los riesgos que estos pueden producir.

1. Lesiones corporales. Si un dispositivo IoMT no funciona según lo planeado, las compañías de tecnología podrían ser responsables de las lesiones resultantes, o incluso de la muerte, de un

usuario o paciente. Por ejemplo, si un médico le receta una pastilla con un chip para tragar para verificar el cumplimiento de un paciente con un problema de memoria, y una falla evita que el transmisor envíe datos de cumplimiento al médico, es posible que el médico no reciba alertas de que el paciente no está tomando la medicación.

2. Errores y omisiones de tecnología. La tecnología IoMT puede dejar de funcionar debido a un error, omisión o acto negligente en el diseño de la tecnología. Si el comprador sufre pérdidas económicas o la interrupción de su negocio. Por lo que los gastos pueden ser catastróficos para un negocio de tecnología. Por ejemplo, si una aseguradora de salud ofrece un incentivo a los clientes que usan un rastreador de actividad física, y un error en el software de seguimiento exagera la cantidad de pasos, la compañía puede otorgar más descuentos de los que debería, conllevando pérdidas financieras.
3. 2. Los riesgos cibernéticos. Los ciberdelincuentes consideran que la información médica protegida es un objetivo atractivo para los ataques cibernéticos introduciéndose así, a los sistemas de información basados en IoT. Por lo que, si se llegaran a exponer esos datos, las empresas podrían enfrentar pérdidas financieras, interrupciones en los negocios o daños a la reputación por no proteger adecuadamente los datos que se encuentran en sus sistemas de información (Lee, 2015).

Por ejemplo, una compañía que fabrica monitores cardíacos portátiles puede tener lecturas médicas cargadas en una nube, por lo que los ingenieros serían los responsables de la seguridad de esta, sin embargo, si no configuran correctamente un parche de seguridad, podría crear una vulnerabilidad, dando paso a que los “hackers” obtengan el acceso a dicha información, y vendan los datos de salud confidenciales de un paciente con fines lucrativos y de daño a la salud de este.

Estas vulnerabilidades, que en gran medida no se han abordado en la atención médica, a su vez pueden plantear un daño potencial a los pacientes. Como lo comenta Scott Erven, director asociado de Protiviti, una firma de consultoría con sede en Menlo Park California

”No tenemos evidencia de que la vulnerabilidad en los dispositivos, o un problema de ciberseguridad en un dispositivo médico, haya causado un problema directo de seguridad del paciente. Pero debido a que estos dispositivos carecen de capacidad de captura de evidencia y de registro forense, me gusta decir que tenemos poca seguridad de que algo no ha sucedido ”.

Al igual que siguen surgiendo nuevas aplicaciones y dispositivos para IoMT, también están surgiendo nuevos riesgos para dicha tecnología. A pesar de estos riesgos, parece que la comunidad de la salud ha aceptado el hecho de que IoMT está llegando. Cabe mencionar que las empresas dedicadas al cuidado de la salud pueden ser consideradas responsables de lesiones corporales, pérdidas económicas a terceros y la falta de seguridad en los datos, mientras que; las empresas dedicadas a la tecnología pueden tomar medidas para ayudar a proteger contra alguno de los riesgos mencionados anteriormente. Las medidas a considerar para evitar los riesgos se mencionan a continuación:

Identificar todos los dispositivos IoT en la red, independientemente de la edad del dispositivo.

Realización de una evaluación de vulnerabilidad en cada dispositivo conectado para que los riesgos estén documentados y administrados. Todo riesgo debe tener un propietario de riesgo al que se le ha asignado la responsabilidad de mitigar ese riesgo. Estos riesgos deben revisarse trimestralmente, y cualquier cambio en el programa debe escalarse a la gerencia ejecutiva (Clyde,2018).

Evaluar e implementar sistemas adecuados de gestión de calidad y riesgo.

Construir en seguridad cibernética.

Evaluar las prácticas contractuales de la empresa.

Analizar las coberturas de responsabilidades del producto, civiles y cibernéticas, así como, los errores y las omisiones, y la cobertura de primera ayudar a proteger contra la responsabilidad potencial.

Otras acciones de seguridad básicas que los proveedores y fabricantes pueden tomar incluyen el cifrado y la realización de un arranque seguro. Esto quiere decir que cuando se enciende un dispositivo, se verifique que ninguna de sus configuraciones se haya modificado.

También es importante no solo hacer un inventario de todos los dispositivos y aplicaciones, sino también crear un ”diccionario de datos”.

Tener un inventario de aplicaciones no resuelve el problema, sin adicionalmente, tener y conocer un diccionario de datos. Es decir, se necesita saber y tener en un diccionario dónde residen todos los datos, dónde se origina, dónde se mueve, [y] cuáles son sus capacidades de transmisión.

3. Conclusiones

En este trabajo se vieron diversas ventajas que se tienen hoy en día con el uso de los dispositivos del internet de las cosas enfocadas a la industria de la salud, como es el caso de un diagnóstico adecuado no solo dentro de los hospitales si no también fuera de ellos y monitorear al paciente de una forma remota; sin embargo, como se vio durante esta investigación, todos estos avances tecnológicos conllevan una gran dedicación y una gran responsabilidad, en cuanto al control de estas.

Para llevar a cabo todo esto se necesita llevar una minuciosa inspección acerca de estos, en especial en lo relativo a seguridad, con la finalidad de no ser hackedos ni tener fugas de información para propósitos delictivos.

Posteriormente a tales riesgos, se observaron diversos métodos para ayudar a incrementar la seguridad y evitar la fuga de datos. Este tipo de métodos no solo son enfocados a las firmas dedicadas a la creación de estos dispositivos, si no también en los usuarios que los utilizan, como sería el caso del personal en los hospitales.

4. Referencias

1. Yu, L.; Lu, Y.; Zhu X (**2012**) *"Tecnologías civiles disruptivas, Seis Tecnologías con Potencial de Impacto en los intereses de Estados Unidos hasta el 2025"/Consejo Nacional de Inteligencia-NIC"; Washington D.C, Estados Unidos, 2008.*

2. Clyde H(**March 13, 2018**) *"The Risks of IoT in Medicine and Healthcare"/https://www.securitymagazine.com/articles/88811-exploring-the-wide-ranging-iot-risks-in-healthcare* Recuperado; September 28, 2018. from

3. O'Connor, Mary Catherine(**July 1, 2016,**) *"A Wearable That Listens for Troubling Coughs," /http://www.iotjournal.com/ articles/view?14687* Recuperado Nov 2016

4. López M., (**September 28, 2018**) *"Emerging Services as New Revenue Streams"/https://www.channelfutures.com/industry-perspectives/emerging-services-new-revenue-streams* Recuperado: September 30, 2018.

5. 5. Lee K.(**December 2015**) *"Healthcare IoT security issues: Risks and what to do about them"/https://internetofthingsagenda.techtarget.com/feature/Healthcare-IoT-security-issues-Risks-and-what-to-do-about-the* (September 25, 2018)

6. 6. Marr B. (**Jan 25, 2018**) *Why The Internet Of Medical Things (IoMT) Will Start To Transform Healthcare In 2018"/https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#2a90e34e4a3c*(September 26, 2018)