SEGURIDAD Y PREVENCIÓN EN EL INTERNET DE LAS COSAS

Ing. Flores Montaño Luis Alberto
Estudiante de Maestría en Informática SEPI
UPIICSA
Email: luisfloresmontano@hotmail.com
Mtro. Álvarez Sánchez Teodoro
Profesor de Maestría en Ciencias en Sistemas
Digitales CITEDI
Email: tass_63@hotmail.com
Dr. Álvarez Cedillo Jesús Antonio
Profesor de Maestría en Informática SEPI UPIICSA
Email: jaalvarez@ipn.mx

Resumen

El Internet de las cosas (en inglés IoT) es un paradigma moderno de una nueva era con dispositivos conectados a través de la internet. La amplia variedad de dispositivos y otros objetos conectados son conocidos como cosas. Un avance en este campo es realizar operaciones asistidas mediante un software para controlar las zonas de conexión. Para llevar a cabo esto se necesitan operaciones avanzadas con diversas capas de impedimento, por lo que se necesita mapear la capa de incorporación más fuerte incrustada con corta fuegos, autenticación / cifrado, protocolos de seguridad, detección de instrucciones y prevención de intrusión en los sistemas.

Este trabajo abarca la posibilidad de tener una seguridad en el internet de las cosas, mediante diversas medidas, esto último con la finalidad de frenar los ataques de los cibercriminales. Por lo que se propone un concepto de seguridad basado en tres capas para prevenir las actividades maliciosas; estas capas constan de la seguridad del dispositivo, seguridad de la comunicación y seguridad del servidor.

Palabras Clave: Internet de las cosas; Seguridad; ataques cibernéticos; seguridad de tres capas.

Abstract

The Internet of things is a modern paradigm of a new era with devices connected through the Internet. The wide variety of devices and other connected objects are known as things. An advance in this field is to perform assisted operations using software to control the connection zones. In order to accomplish this, advanced operations with various impediment layers are needed, so it is necessary to map the strongest incorporation layer embedded with fire breakers, authentication / encryption, security protocols, instruction detection and system intrusion prevention.

This work covers the possibility of having a security in the internet of things, through various measures, the latter with the purpose of curbing cybercriminal attacks. Therefore, a three-layer security concept is proposed to prevent malicious activities; These layers consist of device security, communication security and server security.

Keywords: Internet of things; Security; cyber attacks; Three layers security.

Texto alineado a la derecha

Introducción

Los cortafuegos (en inglés “firewalls”) no pueden ser implementados únicamente en este tipo de dispositivos. Los principales objetivos de los cibercriminales y ciberdelincuentes son los dispositivos informáticos integrados o embebidos. Las últimas lecciones y ocurrencias de piratería en Internet de las cosas han desafiado a expertos profesionales en la seguridad. Las salidas de seguridad de una computadora no podrían proporcionar una solución completa para que la seguridad idónea en los dispositivos del internet de las cosas. La significativa funcionalidad del internet de las cosas ha dado un alcance mucho más amplio para los ataques cibernéticos y ha conducido a eventos catastróficos, por lo que, la “duplicación” a estos dispositivos integrados es encontrada ampliamente por los cibercriminales, encontrando así una metodología o mecanismo de craqueo, que se puede aplicar a todos los dispositivos replicados y conllevar un gran estrago (Zheng,2015).

Diversas personas creen que la aplicación de algoritmos criptográficos proporciona una seguridad satisfactoria; sin embargo, esta última no garantiza una seguridad completa en estos dispositivos, por lo que se podría implementar protocolos criptográficos adicionales como un segundo tipo de enlace en internet de las cosas, esto con el propósito de complementar la seguridad de dichos dispositivos. Algo similar a la implementación de la tecnología para minimizar el riesgo de lo físico, implementado UVEEPROM o Flash de borrado (en inglés “flash eraser”) por lo que, es una medida adicional que puede ser segura en la seguridad de IoT. Sin embargo, la implementación de cualquier medida de seguridad no puede brindar más allá la seguridad más adecuada a IoT. Cabe mencionar que los cibercriminales tienen técnicas, las cuales han quebrantando las capas de seguridad ante los ataques.

II. Objetivo

Desarrollar estrategias para tener una seguridad en el internet de las cosas, mediante diversas medidas, con la finalidad de frenar los ataques de los cibercriminales.

III. Marco Teórico

En la industria, facturación y comercialización se han llegado a utilizar dispositivos IoT, con el propósito de monitorear y controlar operaciones cotidianas del equipo. Además, la asistencia médica se basa en el IoT conectado a dispositivos médicos para gestionar las funciones de un paciente de forma remota desde lugares lejanos, esto es implementado por la mayoría médicos que siguen experimentando el funcionamiento de dichos dispositivos, como se muestra en la figura 1.

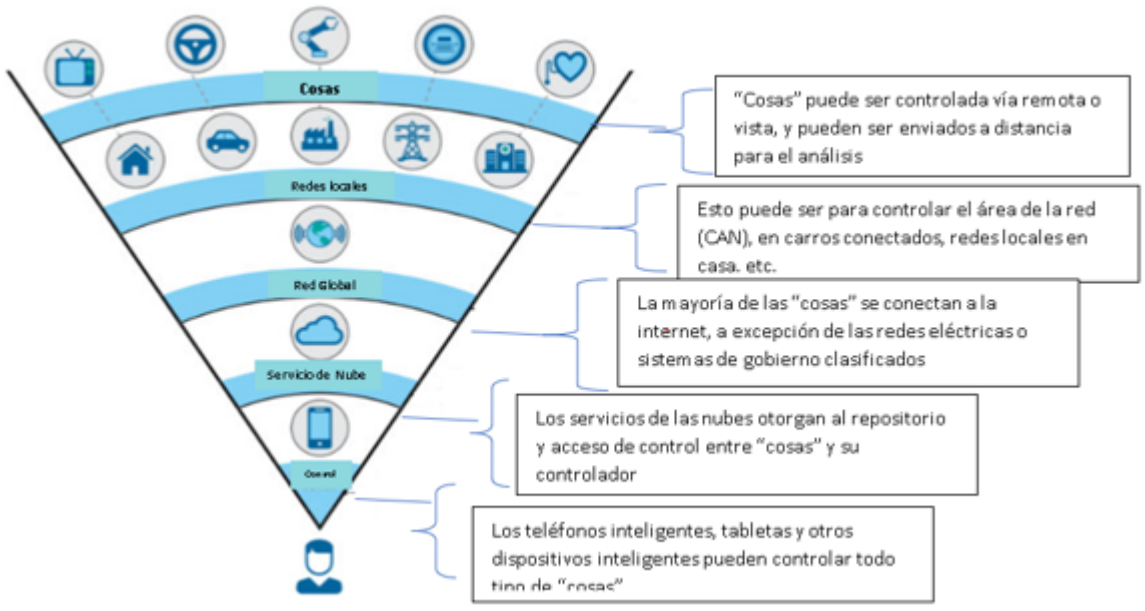

Figura 1. Arquitectura segura de IoT.

Por otro lado, la industria automotriz y de camiones está dando un valor significativo a los clientes mediante el suministro de los servicios de IoT a los vehículos comprados. Los dispositivos IoT utilizados en todos los sectores industriales son inalámbrico y utilizados de forma remota. Por lo que, en muchas ocasiones los cibercriminales quebrantan la conectividad con el usuario final de IoT y toman el control de dichos dispositivos. Esta situación puede conducir a una pérdida o fuga de datos para el propietario de los dispositivos que están interrelacionados.

El objetivo principal de esta investigación es proporcionar una solución adecuada con seguridad elevada para los dispositivos que participan en las operaciones de internet de las cosas, integrando la seguridad de datos, autenticación, seguridad y protección de la comunicación contra los ciberataques (Zheng,2015).

La idea del resultado deseado de la investigación es tomar posibles medidas de seguridad para los dispositivos y componentes involucrados en el internet de las cosas.

Todo esto a través de investigaciones previamente realizadas por otros autores, documentos y revistas internacionales sobre los ciberataques y adquisiciones para internet de las cosas, por lo tanto, se ha explorado soluciones contemporáneas sugeridas para los últimos ataques a los dispositivos IoT (Minoli,2017).

Por lo que, se sugiere una metodología de seguridad novedosa que distinga entre tres capas de seguridad para el internet de las cosas.

IoT conoce la superficie de un ataque lógico, este tipo de ataques han sido reconocidos con éxito en los dispositivos de arquitectura involucrada con una perspectiva más amplia ha dado medidas suficientes para la seguridad, ante los ataques hacia los dispositivos IoT, siendo vasto en los softwares complejos, así como de los sistemas operativos. La seguridad amplificada es esencial para proporcionar la protección contra los ataques. Esto ha sido efectivamente encontrado una solución viable en el "Logical TCB conducting", como se muestra en la figura 2.

Figura 2. Esquema de seguridad en IoT.

La sociedad "GSM" (Sistema global para las comunicaciones móviles) ha presentado soluciones para algunos críticos contra la implementación de seguridad de los dispositivos IoT. Ofreciendo respuesta a este problema de la lucha contra la clonación de dichos dispositivos con la autenticación de identidad "endoint". La identidad de "endpoint" se puede responder con llevar a cabo el "Trusted Computing Base", implementando "Trust Anchor", así como la implementación de "Tamper Resistant Trust Anchor" e implementando una API para usar el TCB asociado con el generador de números aleatorios científicamente comprobado (Amaral,2015).

El desafío contra el "Trust Anchor" se puede encontrar eficazmente con la consideración de la seguridad de la cadena de suministro, personalizar dispositivos de "endpoint" antes de la realización, exclusivamente la provisión para cada punto extremo. En anticipación a la cuestión de reducir la potencialidad de la personificación podría ser eficaz encontrado con la implementación de "endpoint" con seguridad

de la comunicación, Fabulous Forward Secrecy y utilizando un generador de números aleatorios y posteriormente la autorización de recolección de metadatos.

Tal es el caso de "Tata Consultancy", la cual ha hecho un diseño de IoT a prueba de manipulaciones e implementación en su reconocimiento. Mientras que se está implementando el dispositivo IoT preferido para la promulgación de dispositivos y despliegue implementado.

La solución adecuada a todo esto es el diseño teniendo términos del usuario y condiciones para estimar los posibles peligros y ataques pronosticados. Los dispositivos IoT pueden estar claramente protegidos con el posible apoyo continuo contra las amenazas y ataques, teniendo en cuenta las diferentes capas, como se muestra en la figura 3.

Figura 3. Dispositivos IoT que pueden estar protegido contra las amenazas y ataques, teniendo en cuenta las diferentes capas.

El Internet de las cosas es un objetivo de piratería para todos los ciberdelincuentes en general. Los vehículos de motor y sistemas de transporte que trabajan con Internet de las cosas son los objetivos principales para los ciberdelincuentes. Ya tienen que prestar atención sobre sus ataques y posibles daños a el segmento automovilístico (Mvelase,2011).

Por otro lado, la firma “Symantec” ha implementado un “código de protección incrustado” en los dispositivos IoT. Este código hace posible que los dispositivos funcionen contra la piratería tecnológica y no su vez el cubrimiento de la incursión (Cavoukian,2011).

IV. Materiales y métodos (Arquitectura y solución de seguridad propuestas)

Aprovechar la seguridad de IoT es el objetivo de esta investigación, para esto la solución de ajuste propuesta se divide en tres niveles, las cuales son: la implementación de seguridad a nivel del servidor, teniendo en cuenta que es el primer acoplamiento. El segundo nivel está implementando en el nivel de la seguridad en la capa de comunicación. Finalmente, el nivel de seguridad 3d el cual debe implementarse a nivel de dispositivo. El nivel de seguridad en los servidores virtuales estará en conjunción con la computación en los servidores (nube) (Gault,2017).

La implementación de IoT básicamente se realiza con los servidores. Cada uno de estos servidores son operados por usuarios remotos para controlar los dispositivos y gadgets. Por lo que la seguridad del servidor en la nube debe ser prioritaria, por lo que debe ser implementado en el nivel del servidor con formidable autenticación y autorización con encriptación digital estándar (Yale,2011).

El segundo nivel de seguridad se debe implementar en el nivel de comunicación. La comunicación efectiva entre los servidores y usuarios y la comunicación entre los servidores y dispositivos. La seguridad de implementación debe ser incorporado en la capa de comunicación en las operaciones de dispositivos IoT. Esta implementación se puede hacer con la incorporación de algoritmos de seguridad de red y medidas estrictas para ataques externos (Sirageldin,2012).

Y por último el tercer nivel de seguridad está en el dispositivo. Los cuales son dispositivos integrados con chips para almacenar el software, también deben implementarse con el antivirus y protección contra las vulnerabilidades y ataques externos. Los dispositivos son iguales y todos estos están conectados en múltiples los servidores. Si el cibercriminal ataca un solo dispositivo puede comprometer fácilmente a otros dispositivos. Por lo tanto, el nivel de seguridad del dispositivo es igual de importante en las operaciones de dispositivos IoT.

El sistema propuesto está enriquecido con tres capas de seguridad. La Implementación de operaciones de IoT de cualquier tipo de sistema. La implementación de seguridad propuesta que se desarrolla en tres capas para la seguridad de IoT, con el propósito de implementar una operación segura y a su vez monitorear las operaciones de los usuarios para el objetivo dispositivos. Posteriormente se describe la metodología del sistema propuesto (Sultana,2011).

V. Resultados

La implementación del internet de las cosas conlleva a una gran tarea de Implementaciones de seguridad estricta. El internet de las cosas es el objetivo principal para todos los ciberdelincuentes. Por lo que una vulnerabilidad significativa siempre quebrantara las comunicaciones para la finalidad del dispositivo conectado en el internet de las cosas. Los cibercriminales no sólo se concentran en el acceso físico de los dispositivos, estos siempre intentan romper las redes de comunicación y tomar el control de los dispositivos de forma remota, implementando de esta manera un mecanismo de hackeo o intrusión.

Por lo que se sugiere tres principios de seguridad en tres capas para evitar las posibles amenazas de seguridad y los ataques de los ciberdelincuentes, adicionalmente se hacen Implementaciones robustas y de almacenamiento a prueba de manipulaciones de claves criptográficas integradas con funciones criptográficas que están en la primera capa ya mencionada. Se debe establecer una comunicación estándar y segura entre el dispositivo y el operador de IoT.

El hardware utilizado en el proceso de IoT debe estar integrado con la seguridad mecanismo enfocado en la comunicación de red y establecido con protocolos de protección y técnicas de blindaje contra ataques tanto virtuales como físicos.

VI. Resultados y discusión

La Implementación de una arquitectura de seguridad para cada dispositivo con conectividad a los servidores de internet para posibles ataques de cibercriminales. La arquitectura de seguridad debe consistir en la fabricación de dispositivos con ciertas especificaciones, así como un sistema en específico para tener integración adecuada y transparencia sobre los dispositivos y servidores, como se muestra en la Figura 4.

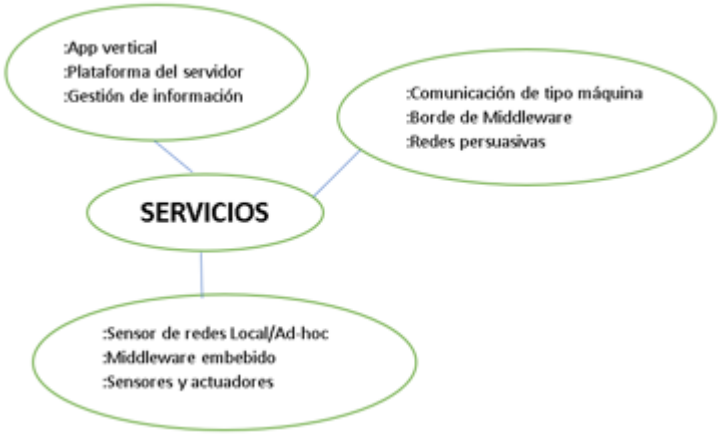

Figura 4. Tres capas de IoT.

La seguridad de tres capas debe implementarse en el nivel del dispositivo, nivel de comunicación y finalmente el nivel de servidor. Las actualizaciones y vulnerabilidades de seguridad contra los posibles ataques y desconocidos deben hacerse continuamente. La gestión siempre debe implementarse para construir prácticas de seguridad probadas, necesarias para la implementación de IoT para dispositivos específicos de administración. La transparencia debe mantenerse entre las operaciones de los desarrolladores de IoT, fabricantes de dispositivos IoT, proveedores de comunicación y empresas industriales y consumidores a nivel empresarial, como se muestra en la figura 5.

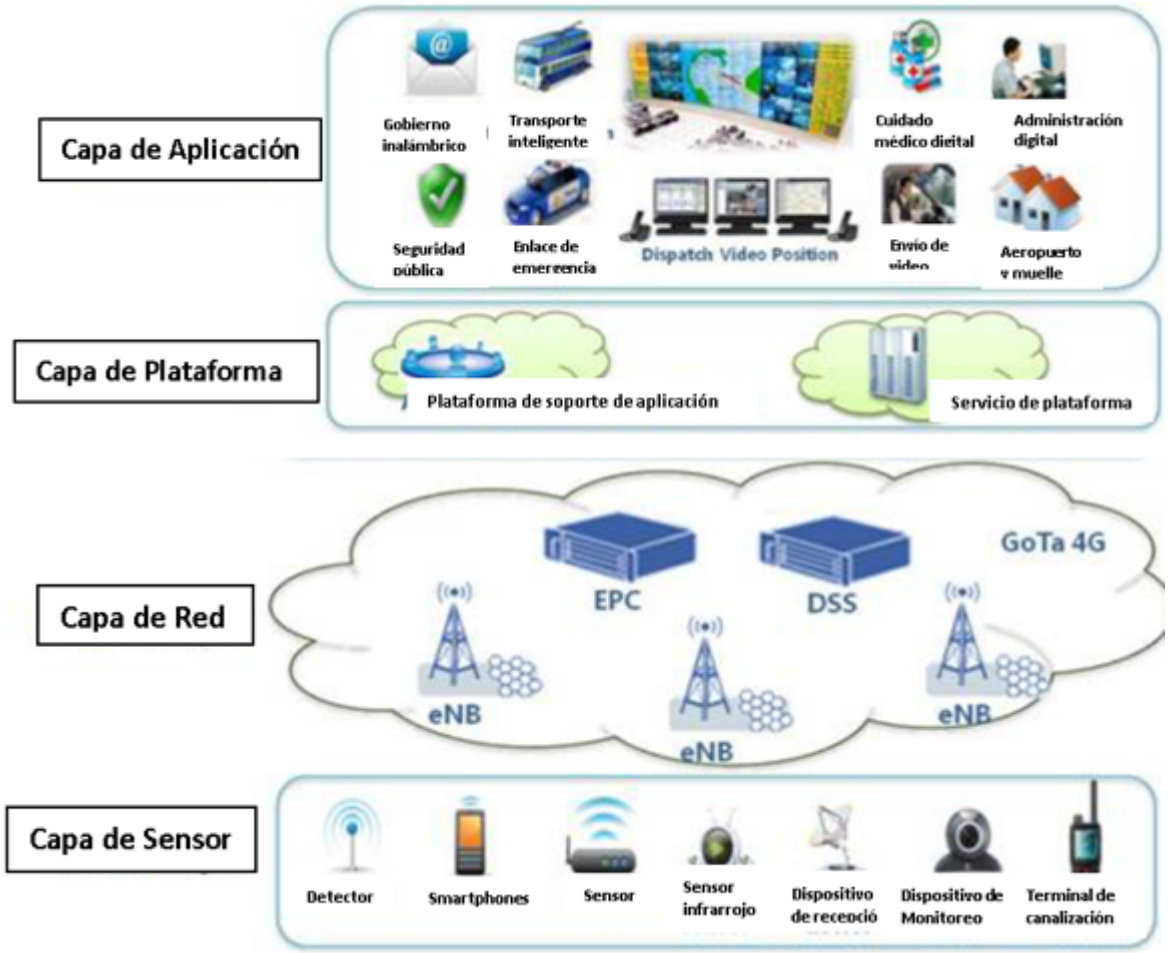

Figura 5. Integración de seguridad en los puntos en IoT.

Las recomendaciones que se consideran para una tener una seguridad más integra en los dispositivos IoT, son los siguientes:

- Es altamente recomendable incorporar la seguridad en la fase de diseño de IoT de un dispositivo en específico.
- Se recomienda encarecidamente promover actualizaciones de seguridad y gestión de vulnerabilidades para un dispositivo IoT propuesto. Se recomienda encarecidamente aplicar los datos TLS y DTLS. Cifrado de los datos transmitidos en la gestión de IoT.
- La autenticación y la gestión de claves es una solución obligatoria para seguir por los usuarios de IoT.
- La comunicación fuerte debe establecerse con el sistema y los dispositivos que se operan en el internet de las cosas independientemente del fabricante de los dispositivos.

V. Conclusiones

El internet de las cosas es el objetivo principal para los ciberdelincuentes. Esta investigación muestra la posibilidad de diversos ataques en diversos niveles del Internet de las Cosas operadas remotamente por los usuarios para controlar y monitorear. los dispositivos.

Así, el objetivo es sugerir las tres capas de implementación de seguridad para el mecanismo de funcionamiento de los dispositivos IoT. Por lo que la posibilidad implementación de seguridad de alto nivel ha sido sugerido a nivel de dispositivo, nivel de comunicación y nivel del sistema.

Además de esto es obligatorio el monitoreo de seguridad y actualización de implementaciones de seguridad de tiempo para prevenir ataques en los dispositivos IoT. Finalmente, se ha recomendado las posibles precauciones para implementar una seguridad satisfactoria en dispositivos IoT.

Referencias

1. Amaral, E. (**2015**) *"The Importance of a Standard Security Architecture for SOA - Based IoT Middleware",Communications Magazine.* IEEE

2. Cavoukian A. (**2008**) *"Privacy in the clouds,"*Springer Identity in the Information Society.

3. Gault M. (**2017**) *Rethinking security for the Internet of Things"* Guardtime Pinnacle Tower Rapenburgerstraat.

4. Minoli, K. (**2017**) *"loT Considerations Requirements and Architectures for Insurance Applications"* in book Internet of Things, CRC Press.

5. Mvelase P. (**2012**) *Çustom-made Cloud Enterprise Architecture for Small and Micro Enterprises,İnformation Retrieval & Knowledge Management (CAMP)* 589-601, Grid and Cloud Computing.

6. Sirageldin A. (**2012**)L. T. Jung, *Hybrid scheme for trust management in pervasive computing,"* 2012 International Conference on.

7. Sultana S. (**2008**) *Übicomp Secretary: A Web Service based Ubiquitous Computing Application,"Proceedings of the 2008/web* ACM symposium on Applied computing.

8. Yale University (**2011**) *Health Insurance Portability and Accountability Act (HIPAA) Policies, Updates and Reminders,.ºbtenido de: http://hipaa.yale.edu/guidance/policy.htm.* Yale University

9. Zheng, H. (**2015**) *"Toward Secure Large-Scale Machine-to-Machine Communications in 3GPP Networks", IEEE* Comm. Magazine Supplement,.