SEGURIDAD EN LAS CAPAS DE LOS DISPOSITIVOS DEL 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

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

En la última década, el Internet de las cosas (en inglés IoT) ha sido un tema relevante en la investigación, ya que son dispositivos que contienen elementos centrales del mundo moderno, estos son usados en lugares como hospitales, ciudades, organizaciones y edificios, otorgándole a las instalaciones ser más “inteligentes”. Por lo general, los dispositivos IoT tienen cuatro componentes principales los cuales son: detección, procesamiento de información, aplicaciones y servicios, acceso heterogéneo y componentes adicionales, como es el caso de seguridad y privacidad. En esta investigación se presenta las IoT en el punto de la seguridad teniendo una perspectiva de capas que comprenden estos dispositivos. Adicionalmente se centra en una visión general de la perspectiva de seguridad de IoT.

Palabras Clave: Internet de las cosas, seguridad, privacidad, confidencialidad, criptografía Algoritmos, Ataques de Seguridad.

Abstract

In the last decade, the Internet of things (in English IoT) has been a relevant topic in research, since they are devices that contain central elements of the modern world, these are used in places such as hospitals, cities, organizations and buildings, giving the facilities to be more “intelligent”. In general, IoT devices have four main components which are: detection, information processing, applications and services, heterogeneous

access and additional components, such as security and privacy. In this investigation, IoT is presented at the point of security, having a perspective of layers comprising these devices. Additionally it focuses on an overview of the IoT security perspective.

Keywords: Internet of things, security, privacy, confidentiality, cryptography Algorithms, Security Attacks.

I. Introducción

El internet de las cosas (en inglés Internet of Things-IoT) permite que varios dispositivos interactúen entre sí a través de la Internet. Esto garantiza que los dispositivos sean inteligentes y envíen la información a un sistema centralizado, que posteriormente monitoreará y tomará acciones de acuerdo con la tarea que esté realizando el usuario (Ponemon,2012).

Un dispositivo IoT se puede utilizar en diversas actividades, tal es el caso de asistencia sanitaria, transporte, entretenimiento, redes eléctricas y edificios inteligentes. Por lo que se espera que los dispositivos IoT actúen como un catalizador para las futuras innovaciones tecnológicas y esperando que su uso aumente exponencialmente en los próximos años (Mell,2009).

Por otro lado, la perspectiva de seguridad de los dispositivos IoT se enfrenta cada día con grandes retos. Por ejemplo: (1). Los dispositivos IoT se extiende al ïnternet.ª través del web convencional, la red de sensores y la red móvil, entre otras, (2) cada çosa.º dispositivo IoT se conecta a la ïnternet", y (3) estos dispositivos se comunican también entre ellos (Itani,2009).

Por lo que, con la seguridad y privacidad actual, surgen problemas en estos puntos; por lo tanto, se debe prestar más atención a investigar temas de confidencialidad, integridad y autenticidad con los datos recolectados por dichos dispositivos (Behl,2012).

II. Objetivo

Desarrollar los puntos de la seguridad en dispositivos IoT teniendo una perspectiva de capas que comprenden dichos dispositivos.

III. Marco Teórico (Capas principales de IoT)

En general, el internet de las cosas se puede dividir en cuatro niveles principales: Capa de percepción, capa de red, capa física y capa de aplicación (Yau,2011).

1. Capa de percepción:

Este es el primer de las capas y también es conocida como capa de reconocimiento; esta capa se encarga de recopilar todo tipo de información a través del equipo físico (como sensores) e identifica el entorno, la información incluye propiedades del entorno como la condición ambiental; y equipamiento físico como es el caso del lector RFID, todo tipo de sensores, GPS y otros. equipos. El componente clave en esta capa son los sensores para que "capturan" y "representan" la información del mundo físico en el mundo digital.

2. Capa de red:

La capa de segundo nivel es la capa de red, esta es responsable de la transmisión confiable de información de capa perceptiva, procesamiento inicial de la información, clasificación y polimerización. En esta capa la transmisión de información se basa en varias redes básicas, las cuales son la internet, red de comunicación móvil, red inalámbrica, redes satelitales, infraestructura de red y protocolos de comunicación, estos últimos son esenciales para el intercambio de información entre dispositivos.

3. Capa física:

La capa de tercer nivel es la capa física, esta establece una plataforma de soporte confiable para la capa de aplicación, la cual tiene todo tipo de computo inteligente que se organiza a través de la red y la nube. Por lo que juega un rol de combinar la capa de aplicación y la capa de red.

4. Capa de aplicación:

La capa de aplicación es el nivel superior y terminal, esta proporciona los servicios personalizados, según las necesidades de los usuarios. Los usuarios pueden acceder al Internet de las cosas a través de la interfaz de la capa de aplicación, como es el caso del uso de una computadora personal y equipo móvil.

En la figura 1 se muestra las distintas capas que se tiene, así como los dispositivos con los que se conforma cada una de las capas.

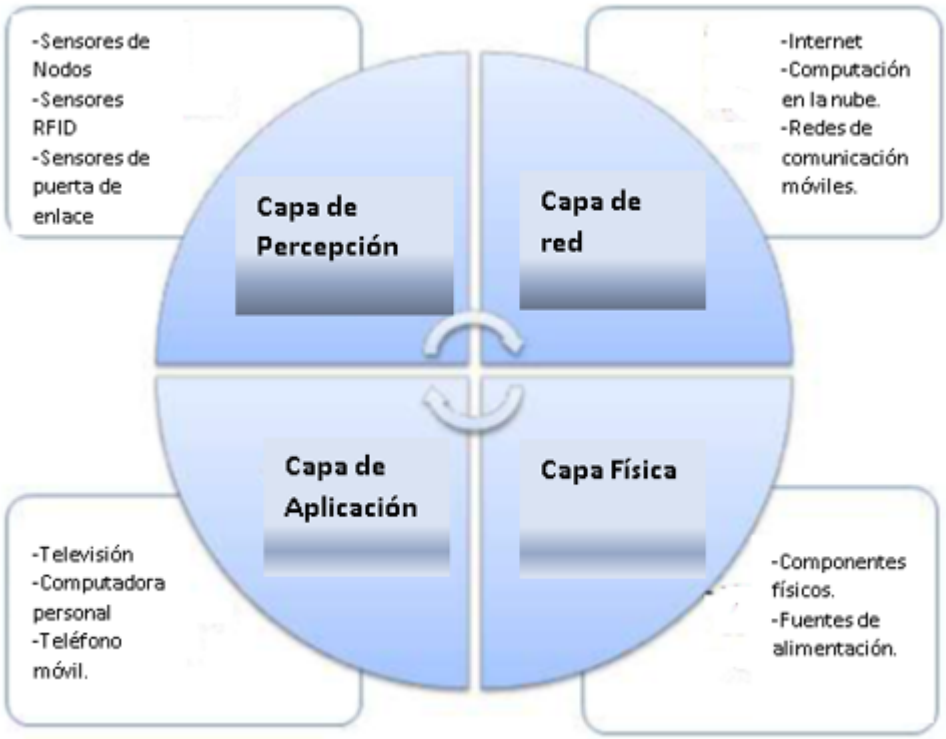

Figura 1. Capas IoT con sus respectivas capas.

IV. Materiales y métodos (Seguridad en IoT):

A. Características de seguridad:

1. Capa perceptual:

Por lo general, los nodos perceptivos tienen menos capacidad de almacenamiento y potencia en la computadora, ya que son simples y con menos poder. Por lo tanto, no es capaz de aplicar saltos de frecuencia en la comunicación y en la utilización de algoritmos de cifrado de clave pública para protección de seguridad, ya que es muy difícil configurar la seguridad o en su defecto un sistema de protección. Mientras tanto los ataques externos de la red como la denegación de servicios también conllevan problemas en cuanto a la seguridad. Por lo que los datos aún necesitan la Protección de la confidencialidad, integridad, autenticidad.

2. Capa de red:

Aunque la red central tiene completa capacidad de protección en cuanto a la seguridad, pero el ataque del hombre en el medio y la falsificación. Todavía existe el ataque, a lo largo de esto, la congestión puede ser causada enorme número de envío de datos. Por lo tanto, el mecanismo de seguridad en este nivel es muy importante para el IoT.

3. Capa de soporte:

Hacer el procesamiento masivo de datos y la decisión inteligente del comportamiento de la red, se realiza en esta capa, el procesamiento inteligente es limitado para información maliciosa, por lo que es un desafío mejorar la capacidad de reconocer la información maliciosa.

4. Capa de aplicación:

En este nivel se aplican diferentes medidas de seguridad para diferentes entornos de aplicación, la principal característica de esta capa de aplicación es el intercambio de datos que pueden dañar la privacidad de estos, el control de acceso y divulgación de información.

B. Requisitos de seguridad:

1. Capa perceptual:

En primer lugar, el nodo es necesario para la autenticación y evitar accesos ilegales a nodos; en segundo lugar, para proteger la confidencialidad de transmisión de información entre los nodos con datos. El cifrado es una necesidad absoluta y un procesamiento importante en avanzar; en cuanto más fuertes sean las medidas de seguridad, más es el consumo de recursos, para solucionar este problema. La tecnología de cifrado se vuelve más importante, donde se incluye un algoritmo criptográfico ligero y protocolos criptográficos. Al mismo tiempo la integridad y autenticidad de los datos del sensor se están convirtiendo en la principal investigación.

2. Capa de red:

En esta capa existen mecanismos de seguridad de comunicación, estos son difíciles de aplicar. La autenticación de identidad es un tipo de mecanismo para prevenir a nodos ilegales, por lo que es una premisa para el mecanismo de seguridad, la confidencialidad y la integralidad ya que son de igual importancia. Además, un ataque distribuido de denegación de servicio (en inglés DDoS) es un método

contra un ataque en la red y es particularmente grave en el internet de las cosas, para prevenir el ataque DDoS para el nodo vulnerable es otro problema para resolver en esta capa.

3. Capa de soporte:

La capa de soporte necesita mucha seguridad de la aplicación en cuanto a la arquitectura como en la nube y multipartidismo seguro. Cálculo, casi todo el algoritmo de cifrado fuerte y protocolo de cifrado, mayor seguridad del sistema la tecnología y antivirus.

4. Capa de aplicación:

Para resolver el problema de seguridad de la capa de aplicación, se necesitan dos cosas. Una de ellas es la autenticación y el acuerdo de claves, a través de la red heterogénea, la otra es la del usuario, utilizando la protección de la privacidad. Por otro lado, la educación y gestión son aspectos muy importantes para la seguridad de la información, especialmente la gestión de contraseñas. En resumen, la tecnología de seguridad en el internet de las cosas, son aspectos importantes y están llenos de desafíos. Adicionalmente, las leyes y regulaciones en manos de las autoridades también son de suma relevancia. En la figura 2, se muestran las capas de IoT, con soluciones para aumentar la seguridad.

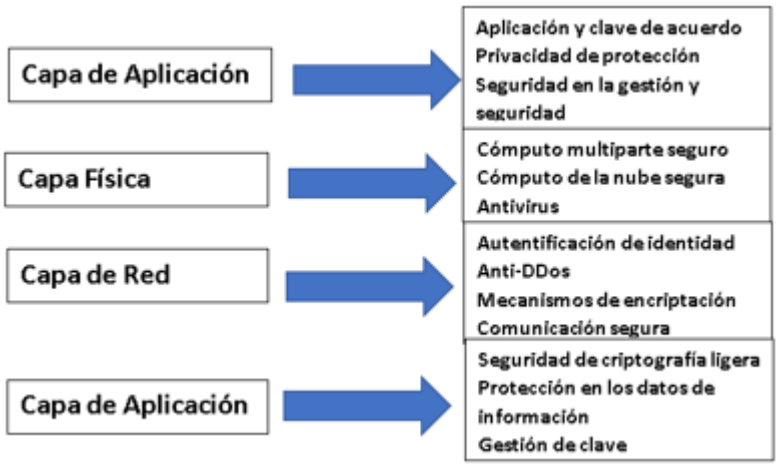

Figura 2. Capas de IoT implementando el aumento en la seguridad.

V. Resultados (Tecnología utilizada con fines de seguridad en IoT)

A. Mecanismo de cifrado:

En la capa de red de IoT y en la capa de aplicación, están conectados de cerca por lo que se deben de elegir entre usar “by-hop” y el cifrado de “extremo a extremo”, si se adopta la encriptación “by-hop”, solo se puede cifrar los enlaces que necesitan ser protegidos, ya que en la capa de red solo se puede aplicar a todos los negocios, lo que hace diferente a las aplicaciones implementadas de forma segura. De este modo, el mecanismo de seguridad es transparente para el negocio o aplicaciones, lo que le da una convivencia al usuario final. Mientras tanto, esto trae las características del rol completo de “by-hop”, tales como baja latencia, alta eficiencia, bajo costo, entre otras.

Sin embargo, debido a la operación de descifrado en el nodo de transmisión, utilizando el cifrado "by-hop" cada nodo puede obtener el mensaje de texto plano, por lo que este cifrado necesita una alta credibilidad de los nodos de transmisión.

B. Seguridad de la comunicación:

En primera los protocolos de comunicación hay algunas soluciones establecidas, estas soluciones pueden proporcionar integridad, autenticidad y confidencialidad para la comunicación, un ejemplo de esto es el TLS / SSL o IPSec. TLS / SSL, están diseñados para cifrar el enlace en la capa de transporte, y por otro lado, IPSec, están diseñados para proteger la seguridad de la capa de red, y a su vez proporcionan integridad, autenticidad y confidencialidad en cada capa.

No obstante, han surgido las necesidades de privacidad; lamentablemente esto último no es de uso común. Por lo que, mecanismos de seguridad de comunicación también son raramente aplicados hoy en día. Ya que los dispositivos IoT son pequeños y su poder de procesamiento, también lo es, esto conlleva a que la seguridad de la comunicación sea menudo débil. Mientras tanto, las redes principales son siempre las actuales o de la siguiente generación de la internet, por lo que la mayoría de la información es transmitida a través de esta.

Tabla 1. Propósitos de los algoritmos criptográficos.

Algoritmos	Propósito
Advanced encryption standard (AES)	Confidencialidad
Rivest shamir adelman (RSA)/ Criptografía de curva elíptica (ECC)	Firmas digitales
Diffie-hellman(DH)	Clave de acuerdo
SHA-1/SHA.256	Integridad

C. Protección de datos del sensor:

La integridad y autenticidad de los datos del sensor se está convirtiendo en el enfoque de investigación, así como la confidencialidad de los datos del sensor; sin embargo, esta última se da en un nivel menor de peligrosidad ya que sólo ocurre cuando un atacante puede colocar su propio sensor físicamente cerca del otro, por lo que podría percibir los mismos valores. por lo tanto, la necesidad de confidencialidad es relativamente baja. El otro objetivo principal de investigación en sensores es la privacidad, ya que esta es un problema importante. Por lo que se debe de adoptar mecanismos para proteger la privacidad de humanos y objetos en un entorno de dispositivos físicos.

La mayoría de las veces las personas a menudo no son conscientes de estos sensores en su entorno, por lo que es necesario establecer regulaciones para preservar la privacidad de las personas.

D. Algoritmos criptográficos:

Hasta ahora hay un conjunto de algoritmos criptográficos aplicados a la seguridad de protocolos en el internet como se muestra en la tabla 1. Por lo general, el cifrado simétrico es un algoritmo se utiliza para cifrar datos con fines de confidencialidad, como el cifrado de bloque estándar de cifrado avanzado (en inglés AES); el algoritmo asimétrico que utiliza a menudo firmas digitales y transporte de claves, como el "Remache Shamir Adelman" (en inglés RSA); el algoritmo de claves simétricas como es el caso de "Diffie-Hellman" (en inglés DH) y el SHA- 1 de los algoritmos de hash seguros SHA-256 que son aplicados a la integridad. Otro algoritmo asimétrico significativo es conocido como la "curva

elíptica criptográfico" (en inglés ECC), ECC puede proporcionar la seguridad mediante el uso de una clave de longitud más corta (Addo,2013).

Al implementar estos algoritmos criptográficos disponibles, tienen recursos necesarios, como la velocidad del procesador y memoria. Entonces, ¿cómo aplicar estas técnicas criptográficas a los dispositivos IoT, ya que no está claro, como hacer una mejor implementación para asegurar el avance en la investigación que los algoritmos puedan ser exitosos, implementandolos y usando memoria limitada y baja velocidad del procesador del dispositivo IoT? (Zhao,2012).

VI. Conclusiones

En los últimos años, este dominio emergente para los dispositivos IoT han estado atrayendo el interés significativo, y continuará en los próximos años. A pesar de la constante innovación, esta temática sigue confrontando nuevas dificultades y severos retos.

Por lo que, en esta investigación, se revisó concisamente la seguridad en el IoT, y las características de seguridad analizadas y los requisitos de cuatro capas, incluida la capa perceptiva, la capa de red, capa de soporte y capa de aplicación. Posteriormente se plantea la investigación del estado, desde la perspectiva de los mecanismos de cifrado, seguridad de las comunicaciones, protección de datos de sensores, y algoritmos de cifrado. Así como el planteamiento de los retos y en general, el desarrollo de los dispositivos IoT, lo cual conlleva los problemas en el aspecto de la seguridad, más serios, en los que son el punto esencial y el objetivo principal de la investigación en estos dispositivos.

VII. Referencias

1. Addo I.D. (**2013**) *"Toward Collective Intelligence for Fighting Obesity,"*COMPSAC.

2. Babar S. (**2011**) *"Proposed Embedded Security Framework for Internet of Things (IoT),"(Wireless VITAE), 2011 2nd International Conference.*Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology

3. Behl A. (**2012**) *.An Analysis of Cloud Computing Security Issues,Ïnformation and Communication Technologies (WICT).*

4. Holt R.C. (**2000**) *.A Reference Architecture for Web Servers,"Seventh Working Conference.* Reverse Engineering, 2000. Proceedings

5. Itani W. (**2009**) *"Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures,Çonference on Dependable, Autonomic and Secure Computing.* DASC Proceedings of the 2009 Eighth IEEE International

6. Mell P.(**año**) T. Grance, *.A NIST definition of Cloud Computing,"*National Institute of Standards and Technology, NIST.

7. Ponemon Institute, Microsoft (**Achieving Data Privacy in the Cloud: United States,"**) *Achieving Data Privacy in the Cloud: United States,/revista/web* Microsoft-Trustworthy Computing: Cloud Privacy.

8. Yau S. (**2011**) *.An Adaptive Approach to Optimizing Tradeoff between Service Performance and Security in Service-based Systems,Ïnternational Journal of Web Services Research.*

9. Zhao G. (**2012**) *"Privacy Enhancing Framework on PaaS,"2012 International Conference on.* Cloud and Service Computing (CSC)