Preparación de Artículos revista Vínculos: Ciencia, Tecnología y Sociedad
Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

Mecanismos de seguridad en el internet de las cosas

Security mechanisms on the internet of things

Miguel Ángel Leguizamón-Páez[1], Andrés Camilo Morales-Suárez[2], Shaythe Stewar Díaz-Ávila [3]

Para citar: A. C. Morales-Suárez, S. S. Díaz-Ávila, M. A. Leguizamón-Páez,. "Mecanismos de seguridad en el internet de las cosas". *Revista Vínculos: Ciencia, Tecnología y Sociedad*, vol. 16, no. 2, julio-diciembre de 2019, pp. XX-XX. DOI: 10.14483/2322939X.15758

Resumen

El presente artículo tiene como objetivo realizar un análisis de algunos métodos de seguridad que se emplean en el internet de las cosas (IoT, por sus siglas en inglés), teniendo en cuenta sus características, funcionamiento, beneficios y esquemas de vanguardia, así como las buenas prácticas de seguridad, generando estrategias de control y protección en tecnologías de *hardware* y *software*. Teniendo en cuenta que "en la actualidad cada ataque informático es un desafío en el campo de la seguridad de la información" [1], en el agitado entorno de las tecnologías, y con la incorporación de objetos cotidianos como casas, vehículos, electrodomésticos, entre otros, que se encuentran conectados a internet, la información que se maneja a través de estos se encuentra expuesta a ataques en diversas situaciones. Con la falta de controles y medidas para el manejo de la información y mecanismos de seguridad para la información en hogares, empresas, corporaciones y hasta entidades gubernamentales, en la mayoría de los casos se deben tomar acciones preventivas que asuman las características y

[1] Magíster en ciencias de la información y las comunicaciones, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia. Correo electrónico: maleguizamonp@correo.udistrital.edu.co, ORCID: https://orcid.org/0000-0003-0457-0126
[2] Tecnólogo en Sistematización de Datos, Universidad Distrital Francisco Jose de Caldas, Colombia, Bogotá. webmaxteril, Colombia. Correo electrónico: orion2264@hotmail.com, ORCID: https://orcid.org/0000-0003-2999
[3] Tecnólogo en Sistematización de Datos, Universidad Distrital Francisco Jose de Caldas, Colombia, Bogotá. ICETEX, Colombia. Correo electrónico: shaytherdiaz@hotmail.com, ORCID: https://orcid.org/0000-0002-4198-0397

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

funcionalidades de los mecanismos de seguridad de IoT que se presentarán en el artículo, sirviendo para analizar e identificar los problemas de seguridad en los dispositivos conectados a internet y algunos mecanismos de seguridad existentes que brinden mayor seguridad a la información en ambientes IoT.

Palabras clave: amenazas, arquitectura IoT, dispositivos IoT, internet de las cosas (IoT), mecanismos de seguridad, vulnerabilidades.

Abstract

The purpose of this article is to analyze some security methods used on the Internet of Things (IoT), taking into account their characteristics, operation, benefits and cutting-edge schemes, as well such as good security practices in IoT devices, generating control and protection strategies, in hardware and software technologies. Bearing in mind that "at the present time every computer attack is a challenge in the field of information security" [1], that is why in the hectic environment of technologies, and with the implementation of everyday objects such as houses, vehicles, appliances among others that are connected to the internet, allows the information that is handled through these are affected to attacks in various situations, and with the lack of controls and measures for the management of information and security mechanisms For information on homes, companies, corporations and even government entities in most cases, preventive actions must be taken that assume the characteristics and functionalities of the security mechanisms of (IoT) presented in the article in review mode bibliographic, will serve to analyze and identify security problems in devices connected to the Internet of things, and some security mechanisms that provide greater information security in IoT environments.

Keywords: threats, IoT architecture, IoT devices, internet of things (IoT), security mechanisms, vulnerabilities.

1. Introducción

El internet de las cosas (IoT) ha tomado mucha fuerza, convirtiéndose en una de las tecnologías más impactantes en los últimos años. Ofrece gran variedad de posibilidades dentro de la industria tecnológica por su capacidad de conectar objetos a la red de redes y poder acceder a estos en cualquier lugar, siempre que se cuente con conexión a internet.

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

A pesar de los grandes beneficios que ofrece la tecnología IoT, tiene debilidades, esto debido a que los fabricantes de dispositivos IoT centraron sus esfuerzos en desarrollar componentes para que objetos comunes se pudieran conectar a internet sin haber tenido en cuenta en su momento la seguridad. Lo anterior, llevó a que objetos conectados a internet queden expuestos, permitiendo que se usaran como medio para que los ciberdelincuentes realicen ataques informáticos, ocasionando que se afecten muchos sectores empresariales como fue el caso de "el proveedor de internet Dyn, en el año 2016, en su sistema de dominio de Internet (DNS), que afectó principalmente a la costa Este de Estados Unidos con una cantidad de tráfico registrada de aproximadamente 1,2 Terabytes por segundo" [1], [2]. Este tipo de ataque fue conocido como Botnet Mirai, un *malware* que afectó sitios web de empresas reconocidas como Amazon, PayPal, Spotify.

Algunas de las plataformas de *software* y *hardware* de dispositivos IoT no cuentan con las medidas de seguridad apropiadas, esto es porque muchos de sus fabricantes dejan de brindarle soporte o simplemente no cuentan con módulos de seguridad para protección de la información que circulan a través de estos dispositivos. Por ello, en este artículo se presenta un análisis de algunos mecanismos de seguridad para estos tipos de plataformas en los cuales se contemplan protocolos de ciberseguridad, modelos de arquitectura de comunicación y un análisis de cuáles son las vulnerabilidades y amenazas más comunes en ambientes IoT, además de cómo estos pueden ser mitigados con la implementación de mecanismos de seguridad IoT [2].

2. Contexto

El IoT es la tecnología que consiste en objetos con capacidad para conectarse a internet, interactuar entre sí y compartir información al estar conectados a la red de redes. Los dispositivos IoT generan grandes cantidades de información valiosa para las empresas, la cual utilizan para analizar y generar nuevas ideas, productos e investigaciones [3]. Sin embargo, por ser una tecnología que no se encuentra en una fase de madurez, tiende a sufrir vulnerabilidades, esto se ve reflejado al momento de su implementación en algunos sectores debido a la falta de seguridad en los dispositivos y la falta de conocimiento por parte del usuario, quienes tienden a dejar las claves de acceso por defecto en los dispositivos IoT, permitiendo a los cibercriminales realizar ataques a través de estos

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

dispositivos. Según estudios realizados por Symantec, los mayores ataques se realizan haciendo uso de los dispositivos IoT, aprovechando su fácil acceso y control de los dispositivos de forma remota con ataques *ransomware* [4].

3. Plataformas IoT

En la actualidad, existen diferentes ecosistemas IoT, cada uno presenta su propia particularidad dependiendo del sector en el que se implemente la solución, como son:

- La agricultura y ganadería. En este sector, la implementación de IoT permite la realización de actividades de siembra de forma automatizada y un monitoreo constante del suelo; además de esto, se implementan sistemas de riego automatizado, entre otro tipo de soluciones [2]-[5]. El implementar tecnologías IoT en el sector agrícola ha permitido la creación de métodos novedosos como son el control de humedad, análisis de PH, control de iluminación y sistemas de riego automatizado, aumentando la productividad de los productos como hortalizas y frutas de mejor calidad [6], [7]; también permite ser más amigable con el medio ambiente y aprovechar de forma más responsable y eficiente los recursos naturales como el agua [6]. Además de mejorar la productividad y ayudar al medio ambiente, el uso de esta tecnología ha permitido a las industrias agrícolas monitorear los cambios climáticos para poder evitar perdida de cultivos [8], ya que les ayuda a tomar decisiones de acuerdo con los datos que obtienen [9].

- Industria 4.0 o fábrica inteligente. Es un "modelo de organización y de control de la cadena de valor a través del ciclo de vida del producto por las tecnologías de la información" [10], es la automatización de fábricas utilizando componentes inteligentes, esto con el fin de obtener mayor producción; con ello, las empresas adquieren mayor ganancia y capacidad de adaptabilidad al cambio en el mercado. Permite realizar un monitoreo constante a los activos de la organización con el fin de poder dar soporte a los componentes que la conforman de forma oportuna y poder garantizar la calidad [5], [11].

- IoT en la salud, también conocido con Internet de las cosas médicas (IoMT). Consiste en la incorporación de dispositivos inalámbricos que permiten

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

monitorear a los pacientes, tener un seguimiento constante de los medicamentos que toman y la capacidad de ubicación cuando esté hospitalizado, todo esto con elementos de bajo costo que permiten la recopilación de datos de forma más oportuna y eficiente [5]. La incorporación del IoT en la medicina ha permitido a los médicos poder unir la telemática y la domótica, obteniendo así una atención más rápida en los pacientes dentro de centros hospitalarios a través de dispositivos que permiten monitorear a los pacientes con problemas cardiacos o respiratorios que se encuentran fuera o dentro de los centros de salud [12], [13]. Se tiene la capacidad de ofrecer soluciones de tratamientos en enfermedades de forma remota con el propósito de descongestionar centros y atender la gran demanda en cuanto atención hospitalaria en usuarios [14].

Los ambientes IoT, como los ya mencionados anteriormente, cuentan con una serie de plataformas que se dividen en *hardware* y *software* para su funcionamiento, los cuales se desarrollan en la Tabla 1 y la Tabla 2.

Hardware	**Descripción**
Arduino	En una plataforma de *hardware* libre, basado en una placa compuesta por microcontroladores, esta placa también cuenta con su propio entorno de *software* para desarrollo y es fácil de usar aplicable para proyectos multidisciplinares [15].
WaspMote	"Es una plataforma modular *open source* para construir redes de sensores inalámbricas de muy bajo consumo" [16].
Intel Galileo	"Es la primera placa arduino basada en la arquitectura de intel. Los encabezados se basan en el modelo arduino 1.0 pinout que se encuentran en las placas Arduino R3. Esto proporciona la capacidad de utilizar escudos compatibles, lo que permite extender la funcionalidad de la placa" [17].
RaspBerry PI	"Es un ordenador de placa reducida, que tiene el objetivo de estimular la enseñanza de informática en las escuelas, el software es de código abierto, y el hardware es libre, con un sistema operativo de una versión oficial adaptada de Debian" [18], [19].

Tabla 1. Plataformas *hardware*

Fuente: elaboración propia.

Software	**Descripción**
ThingSpeak	Es una plataforma *open source* que permite analizar información proveniente de dispositivos IoT. El usuario puede crear visualizaciones en tiempo real, enviar alertas; además de esto, ThingSpeak permite la integración de Matlab Analytics con el fin

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

	de poder realizar procesamiento de datos, visualizaciones y análisis [2].
Electric IMP	"La plataforma está diseñada específicamente para IoT con una arquitectura única de borde a empresa, con hardware, dispositivos y software en la nube totalmente integrados, comunicaciones, API, servicios en la nube" [20].
Amazon Web Services IoT	Ofrece servicios de *software* para dispositivos móviles, servicios de control y servicios de datos, también ofrece un SDK para dispositivos con AWS IoT que permite conectar el *hardware* del dispositivo con AWS IoT Core. "Además permite la comunicación bidireccional y segura entre elementos conectados a internet (sensores, accionadores, dispositivos integrados o inteligentes) y la nube de AWS a través de protocolos MQTT y HTTP" [21].
Google Cloud IoT	"Es un servicio totalmente gestionado con el que se puede conectar, gestionar e ingerir datos de millones de dispositivos repartidos por todo el mundo de forma segura y sencilla, esto permite que se puedan añadir datos de dispositivos distribuidos a un único sistema global que se integra fácilmente con los servicios analíticos de Google Cloud" [22]

Tabla 2. Plataformas *software*

Fuente: elaboración propia.

Cada uno de los ambientes IoT cuenta con diferentes tipos de soluciones, las cuales están conformadas por plataformas ya mencionadas; sin embargo, cada una de estas plataformas, así como ofrecen beneficios, tienen falencias en temas de seguridad porque se encuentran en fase temprana de desarrollo y algunas no cuentan con soporte por parte del fabrícate, teniendo en cuenta que constantemente se realizan cambios en las plataformas tanto en *hardware* como *software*. Así, estos dispositivos no son del todo seguros, lo cual no significa que no se puedan usar, es por ello que se presentarán algunos mecanismos de seguridad apropiados dependiendo del tipo de solución IoT que se desee implementar.

4. Amenazas y vulnerabilidades

4.1. Amenazas

Teniendo en cuenta el crecimiento de dispositivos IoT conectados a internet en tan poco tiempo, el flujo de información aumenta, ocasionando que el interés de los cibercriminales por atacar estos dispositivos también aumente, centrando sus esfuerzos

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

en afectar el mayor número de dispositivos para lograr su propósito. Lo anterior ocasiona que se manifiesten diversos tipos de amenazas y vulnerabilidades en los dispositivos IoT.

En este sentido, los ataques más comunes en el IoT son los de denegación de servicios distribuidos (DDos), espionaje, vigilancia y *ransomware* [23]. Los ataques DDos son las amenazas más comunes en entorno IoT y efectivas por su simpleza y efectividad, este tipo de métodos de ataque es utilizado en las empresas para verificar hasta qué punto los dispositivos mantienen su correcto funcionamiento [24], pero los cibercriminales lo emplean para lograr sus propósitos como son el robo de información, daños a dispositivos de red, entre otros, generando flujo de información desde diferentes puntos de conexión hacia un mismo punto. Este tipo de ataque también es efectivo al utilizar *bots*, que son considerados robots informáticos que se ejecutan de forma automática, permitiendo la manipulación de dispositivos infectados de forma remota [25].

Un ejemplo claro de ataques realizados a ecosistemas IoT es la utilización de recursos de *hardware* de forma inadvertida de los objetos conectados para temas de minado de bitcoins, ya que los ciberdelincuentes en la actualidad han encontrado atractiva esta nueva forma de conseguir dinero fácil [25].

Otra de las amenazas es el espionaje y la vigilancia, ya que los ciberataques realizados a los dispositivos IoT en ocasiones no son para generar daños, sino para poder tener acceso a la información de empresas, tomar control de dispositivos como cámaras con el propósito poder espiar, como fue el caso de una mujer holandesa [26] quien instaló cámaras en el interior de su casa con el fin de poder vigilar a su mascota; sin embargo, después de un tiempo se dio cuenta de que este dispositivo estaba siendo controlado por otra persona y que la habían estado espiando.

Los dispositivos IoT no cuentan con módulos fuertes en seguridad, cuando se implementan en objetos cotidianos sufren de amenazas, lo cual es aprovechado por los *hackers*. Otro tipo de ataque es el *ransomware*, considerado uno de los ataques más peligrosos que pueden existir en tanto que impide el acceso a la información del usuario; en pocas palabras, secuestran la información, pidiendo un rescate que debe realizarse con bitcoins o transferencia con tarjeta crédito. Este tipo de ataque tiene varias modalidades

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

en las que se puede infectar un dispositivo, uno es a través de un *malspam* o mensaje de correo, el cual puede incluir un archivo de Word, PDF o un link que redirecciona a la ruta en el que se encuentra el *malware*. En algunos de los casos, el *malspam* utiliza técnicas de ingeniería social para engañar al usuario con el fin de motivarlo a que abra y responda el correo con los archivos adjuntos o dar clic en links que contienen el *malware*. Muchas empresas han sido víctimas de este tipo de *malware* sin garantías de poder recuperar la información si pagan el valor exigido por el ciberatacante [27], [28].

Las amenazas ya mencionadas aprovechan las falencias que tienen los dispositivos IoT en cuanto a seguridad y son utilizados como medios para poder lanzar ataques que afectan o comprometen la infraestructura de red y, con ello, la información y componentes que dependan de esta para su buen funcionamiento en las organizaciones, hogares e incluso instituciones educativas. A pesar de ser una tecnología nueva, tiene debilidades frente a otro tipo de tecnologías que llevan bastante tiempo en el mercado, esto debido a que no se ha perfeccionado del todo.

4.2. Vulnerabilidades

Las vulnerabilidades que se presentan en entornos IoT son amplias y se pueden llegar a presentar o generar en entornos como son las interfaces web no seguras, las cuales no cuentan con un sistema de bloqueo de cuentas por intentos fallidos, permitiendo a los atacantes capturar información de las interfaces en un texto plano, lo mismo pasa con las autenticaciones que son débiles o que están expuestas en las redes internas. Lo anterior se ve evidenciado también en los servicios de red inseguros, ausencia de cifrado en las comunicaciones, interfaces *cloud* inseguras, interfaces móviles inseguras, configuraciones de seguridad insuficientes y seguridad física insuficiente [29]. Estas son las vulnerabilidades más comunes que se presentan en entornos IoT, los ataques realizados por los cibercriminales buscan explotarlas con el fin de tener el control dentro de la red [29].

Con los constantes ataques, vulnerabilidades y amenazas a las que están expuestos los entorno IoT, las empresas dedicadas a prestar servicios en la nube y fabricación de dispositivos IoT vieron la necesidad de usar e implementar métodos y estrategias de

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

seguridad que permitan proteger los dispositivos por los cuales circula la información y se almacenan; sin embargo, los métodos de seguridad normales no son efectivos en entornos IoT, teniendo en cuenta el uso de componentes inalámbricos que son controlados remotamente y que estos interactúan con otros objetos intercambiando información, ocasionando que sea un reto el poder generar mecanismos de seguridad, que es lo que se presentará en el siguiente apartado [30].

5. Mecanismos de seguridad en IoT

Primero, se realizará un énfasis en la diferencia que hay entre lo que es seguridad de la información y seguridad informática para poder entender mejor los mecanismos de seguridad que existen.

Muchas veces se confunde el concepto de seguridad de la información con seguridad informática [1], a pesar de que tienen cierta similitud son diferentes. La seguridad de la información trata de la protección de la información independientemente del medio en el que se encuentre, como son documentos físicos, medios magnéticos y conocimiento de las personas. La seguridad informática, por otro lado, concentra sus esfuerzos en proteger la infraestructura tecnológica y todos los componentes que hacen parte de ella, tanto de *software* como de *hardware*, es así que se diferencia una de la otra.

Tanto en la seguridad de la información como en la informática existen muchos métodos y estrategias considerados como mecanismos de seguridad, los cuales son herramientas o formas de control aplicados para detectar o prevenir ataques, un poco distintos a los que normalmente se usan en las organizaciones, ya que se está tratando con infraestructura inalámbrica en la cual se conectan objetos y no solamente móviles, portátiles y dispositivos de red. Estos mecanismos están enmarcados en los cuatro pilares de la seguridad de las comunicaciones, los cuales son la disponibilidad, autenticación, integridad y confidencialidad [31]. Para la implementación de seguridad dentro de estos pilares en entornos IoT, se tienen en cuenta varios protocolos de seguridad, los cuales están inmersos en modelos de arquitectura de comunicación.

5.1. Modelo de referencia de arquitetura IoT

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

Existen modelos de referencia en IoT propuestos por organizaciones que trabajan en la investigación y fabricación de componentes de tecnología IoT, como son el modelo IoTWF, Intel IoT, IoT simple, ITU, arquitectura de referencia Azure IoT, en el que se muestra cómo debería ser la conexión e interacciones de los componentes dentro de un entorno IoT. Cada uno de estos modelos de referencias trabaja ciertas capas con sus propias características, como es el caso del modelo de referencia IoTWF que trabaja siete capas (dispositivos físicos y controladores, conectividad, *Edge Computing*, almacenamiento de datos, abstracción de datos, aplicación, procesos y colaboración) [32]; este tipo de arquitectura permite una mayor interacción de los datos en la red, brindando un mejor tratamiento de estos antes de ser almacenados y en una de sus capas utiliza un sistema de filtrado usando *Edge Computing*, la cual permite mejorar el análisis de los datos transmitidos antes de ser almacenados en la base de datos.

El modelo de referencia de Intel IoT, a diferencia del IoTWF, trabaja seis capas con un componente transversal de seguridad, las seis capas que trabaja en esta arquitectura son *Business Layer*, *Application Layer*, *Control Layer*, *Management Layer*, *Data Layer* y *Analytics*, *Communications and Connectivity Layer*, *Security Layer*; con esta arquitectura se centran en que se garantice la seguridad e integración de objetos inteligentes de forma sencilla, haciendo uso de *hardware* y *software* en la nube que brindan seguridad [32].

Frente al modelo de referencia IoT simple, este es un modelo de cinco capas sensor o actuador, *gateway*, *network*, *management*/*analitycs* y Big Data/*datacenter*, al igual que en IoT Intel la seguridad es transversal, con un enfoque físico y lógico en el cual integran varios mecanismos de seguridad como autenticación, filtrado, encriptación y protección [33].

El modelo de referencia ITU tiene cuatro capas con dos componentes transversales, los cuales son gestión y seguridad. En la parte de gestión, cuenta con la gestión de dispositivos, desactivación y activación de forma remota, diagnóstico y actualizaciones de *software*, gestión de la topología de red, gestión del tráfico de red; en la seguridad, está concentrado en tres capas del modelo de referencia, los cuales son capa de aplicación que comprende la autenticación, autorización, integridad, privacidad, auditorias, antivirus; la capa de red se compone por la confidencialidad, autenticación y autorización, y la capa

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

de dispositivos la autorización, control de acceso, autenticación, confidencialidad y protección de datos.

El modelo de referencia de IBM tiene como propósito reducir las anomalías de distintas topologías, esta arquitectura está compuesta por tres capas las cuales son *Cloud*, *Edge* y *Devices*. La mayor interacción que se tiene con los dispositivos es a través de los dispositivos móviles para controlar, monitorear y analizar los datos, el único inconveniente con esta arquitectura es que solo es para trabajar con productos IBM [34].

En los modelos de referencia de arquitectura IoT ya mencionados, se puede observar cómo cada organización dedicada a ofrecer servicios de IoT plantea sus propios modelos IoT en el cual funcionan sus plataformas; sin embargo, no se cuenta con un modelo estándar, y en algunos modelos no se cuenta con los componentes de seguridad incorporados en la arquitectura. El tener diferentes arquitecturas de referencia y estar siendo implementadas en organizaciones implica tener mecanismos de seguridad específicos dependiendo del tipo de modelo de referencia que se esté utilizando, en estos casos es donde se tiene en cuenta lo que son los protocolos de comunicación, los cuales son utilizados en los entornos de IoT inalámbricos, alámbricos y de mensajería; al ver que estos protocolos también se utilizan en los entornos IoT, es indispensable saber qué mecanismos se pueden utilizar.

5.2. Métodos de seguridad en entornos IoT

Los modelos de referencia de arquitectura IoT propuestos por organizaciones se dedican a prestar servicios en este tipo de tecnología, incorporan dentro de sus modelos la seguridad como factor importante a la hora de su implementación; sin embargo, la seguridad ofrecida en alguno de estos modelos no es suficiente. Con el fin de poder reducir las vulnerabilidades a un nivel tolerable y mitigar los daños realizados por los ataques de cibercriminales en entornos IoT, organizaciones y universidades dedicadas al estudio de la seguridad han desarrollado métodos que pueden ser aplicados, teniendo en cuenta que son objetos cotidianos que se encuentran conectados a la red de redes, haciendo uso de protocolos de comunicación inalámbricos.

5.3. Certificados digitales IoT

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

Amazon AWS [35], a través de sus servicios, implementa métodos de seguridad y autenticación para aplicaciones IoT, aprovechando que todo el tráfico que pasa por su infraestructura se cifra por el *Transport Layer Security*, lo que permite la identificación de los dispositivos conectados por medio de certificados X509, teniendo en cuenta que es más seguro que sistemas de autenticación por nombre de usuario y contraseña o los *tokens* de portador; este tipo de certificado digital utiliza un sistema de cifrado asimétrico que le permite grabar las claves privadas de almacenamiento seguro de un dispositivo.

Microsoft, a través de la plataforma de Azure, al igual que AWS [36], soporta aplicaciones IoT, este servicio se conoce como Azure IoT Hub que permite conectar a internet de manera segura los objetos. Este tipo de servicio soporta el certificado digital X.509 para actividades de autenticación de los dispositivos conectados por medio de los protocolos HTTP, MQTT y/o AMQP, a diferencia de Amazon donde el usuario tiene que crear el certificado y asociarlo a un dispositivo, IoT Hub crea los certificados y los asocia a los objetos conectados a internet con un identificador junto con la clave privada, este tipo de certificado es validado y generado por una certificadora con el propósito de que estos dispositivos conectados se puedan autenticar en IoT Hub.

5.4. Criptografía en entornos IoT

La criptografía es uno de los métodos utilizado en los entornos IoT con los nuevos estudios para su aplicación sobre protocolos WSN (red de sensores inalámbricos), consiste en el despliegue de una red de sensores inalámbricos; este tipo de solución criptográfica se planteó para dos tipos de escenarios: la topología de estrella para que pueda trabajar con nodos de baja capacidad de procesamiento y sobre topología tipo Mesh, en el cual los nodos cuentan con capacidad de procesamiento mucho mayor. El objetivo de este tipo de encriptación es mantener el equilibrio entre la seguridad y los requerimientos de una red de sensores inalámbricos, donde se utiliza un árbol de nodos con función HASH, que es una función matemática usada para fines criptográficos, la cual permite una conversión de cadenas de longitud de datos en cadenas de *bits* de longitud fija [36], [37] en el que los nodos finales se encargan de enviar HASH de información a los nodos enrutadores. Luego de esto, la información es verificada para

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

asegurarse de que llegó completa, esta es trasmitida a cada nodo enrutador, aplicando la función HASH hasta llegar al nodo final del árbol [38].

5.5. *Blockchain* aplicado en entornos IoT

Uno de los métodos novedosos para la seguridad es el uso de tecnología *blockchain* en entornos IoT, el objetivo de este método de seguridad es el uso de contratos inteligentes para poder gestionar los recursos y así poder implementar mecanismos de seguridad utilizando una red *Ethereum*; este tipo de red permite realizar configuraciones de manera privada, dando la libertad elegir las direcciones que van a quedar dentro de la red y con esto poder crear cuentas para asignarlas a los dispositivos IoT.

Con el uso de contratos inteligentes en tecnología *blockchain* se permite el uso de mecanismos de seguridad de un modo más sencillo, ya que estos están inmersos en el contrato junto con registros de información y gestión de versiones, por lo que se almacena la mayor parte de la lógica del sistema [37].

Los métodos de seguridad ya mencionados son aplicables a los entornos IoT ofreciendo mayores posibilidades de proteger los objetos conectados; sin embargo, es importante aclarar que no hay un mecanismo de seguridad totalmente seguro, aunque ayudan a minimizar los riesgos a un nivel tolerable. Estos métodos, junto con los modelos de referencia propuestos, complementan una solución IoT para ser implementada en los diferentes sectores [37]-[39].

6. Conclusiones

La seguridad siempre ha sido un factor importante al momento de proteger la información, y con la llegada de la tecnología IoT se ha convertido en un reto el poder generar mecanismos que sean efectivos. Esto demuestra que, a pesar de los novedosos sistemas y mecanismos de seguridad, no son cien por ciento seguros, teniendo en cuenta que cada día los ciberdelincuentes encuentran una forma diferente de vulnerar la seguridad y conseguir atacar los entornos IoT. En conclusión, siempre será un reto el poder proteger la información y más aún el poder incorporar mecanismos de seguridad que se adapten o acoplen a los entornos IoT con el fin de poder proteger la información que circula en estos.

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

Referencias

[1] E. M. Garantivá, "Retos de Seguridad Informática y Seguridad de la Información" http://polux.unipiloto.edu.co:8080/00002246.pdf

[2] A. Segura Gavilán, "Seguridad en la internet de las cosas: propuesta de implantación segura de un sistema de seguridad con dispositivos IoT en una PYME" http://hdl.handle.net/10609/97447

[3] J. E. Salvatore *et al*., "Tecnologías de la información y las comunicaciones mediante IoT para la solución de problemas en el medio socio productivo". http://sedici.unlp.edu.ar/bitstream/handle/10915/67206/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

[4] Symantec, "ISTR Internet Security Threat Report". https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

[5] T. P. Valenzuela, "Investigación y análisis del ecosistema para el internet of the things en las áreas de smart cities, home automation, smart energy, connected vehicle, industria 4.0 y smart health", Tesis de grado, Universidad de Guayaquil, Guayaquil, 2019.

[6] F. J. Ruiz y K. Esquivel, "Internet de las cosas (IOT), una alternativa para el cuidado del agua (internet of things (IOT), an alternative for the care of water)". http://www.itcelaya.edu.mx/ojs/index.php/pistas/article/view/1815

[7] M. A. Mendoza y M. J. Suarez, "Paradigma IoT: desde su conceptualización hacia su aplicación en la agricultura", *Revista Espacios*, vol. 40, n.° 18, 2019.

[8] J. Hernández, J. Ramírez, J. Cruz y Á. Alarcón, "Monitoreo de variables agrometeorológicas en la fase de germinación de un cultivo de pimentón a través de IoT". https://revistas.utp.ac.pa/index.php/memoutp/article/view/2299/3187

[9] D. Hernández, B. Mazon y C. Escudero "Análisis de Datos Agropecuarios - Internet de las cosas (IoT)". https://www.researchgate.net/publication/327702411_Capitulo_3_Internet_de_las_cosas_IoT

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

[10] L. D. Candia, A. S. Rodríguez, N. Castro, P. Ambrosi y F. J. Díaz, "Mejoras en maquinaria industrial con IoT: hacia la industria 4.0", En: *XXIV Congreso Argentino de Ciencias de la Computación*, 2018.

[11] C. L. Cartagena y R. E. Quintanilla, "Plataforma IoT para el control y monitoreo de variables físicas con tecnología Open Hardware". http://hdl.handle.net/10972/3989

[12] G. T. Zárate y C. O. González, "El internet de la salud", *Universitaria*, vol. 2, n.° 9, pp. 34-35, 2018.

[13] L. J. Ramírez, A. F. Marín y A. Rodríguez, "Aplicación del Internet de las Cosas en la salud: caso en la Enfermedad Pulmonar Obstructiva Crónica", *Ciencia y Poder Aéreo*, vol. 13, n.° 1, pp. 82-92, 2018. https://doi.org/10.18667/cienciaypoderaereo.589

[14] M. Gonzáles, "Desarrollo de IoT, como solución para el tratamiento de enfermedades de manera remota", Tesis de maestría, Universidad de San Andrés, Buenos Aires, 2018.

[15] Arduino, "Arduino IoT". https://www.arduino.cc/en/Tutorial/HomePage

[16] L. Gracia, "Waspmote". https://unpocodejava.com/2012/08/21/que-es-waspmote

[17] Intel, "Introducción a las Placas Intel® Galileo". https://www.intel.la/content/www/xl/es/support/articles/000005912/boards-and-kits/intel-galileo-boards.html

[18] Wikipedia, "Raspberry Pi". https://es.wikipedia.org/wiki/Raspberry_Pi

[19] Fundación raspberry Pi, "Documentación de Raspberry Pi". https://www.raspberrypi.org/search/Que+es+RaspBerry+PI

[20] Electric Imp, Inc., "Plataforma Electric Imp". https://www.electricimp.com/platform/how-it-works/

[21] Amazon AWS, "Documentación de AWS IoT Core". https://docs.aws.amazon.com/es_es/iot/?id=docs_gateway

[22] Google Cloud, "Cloud IOT Core". https://cloud.google.com/iot-core/?&utm_source=google&utm_

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

[23] Wikipedia, "Ataque de denegación de servicio". https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

[24] J. E. Martínez y P. S. Atencio, "Creación de un ataque de ddos con inundación http-get con la metodología de la cadena cyber kill", *Iteckne*, vol. 16, n.° 1, pp. 41-47, 2019. https://doi.org/10.15332/iteckne.v16i1.2160

[25] A. Lohachab y B. Karambir, "Análisis crítico de DDoS: una amenaza de seguridad emergente sobre las redes IoT". https://link.springer.com/article/10.1007/s41650-018-0022-5

[26] Portal TIC, "La pesadilla del IoT: un hacker espía y habla a una mujer a través de la cámara de vigilancia de su casa". https://www.europapress.es/portaltic/ciberseguridad/noticia-pesadilla-iot-hacker-espia-habla-mujer-traves-camara-vigilancia-casa-20171006131138.html

[27] Malwarebytes Labs, "Ransomware". https://es.malwarebytes.com/ransomware/

[28] B. Dickson, "La amenaza del ransomware IoT es más grave de lo que piensas". https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/

[29] A. Calvo, "Seguridad en internet de las cosas: firmwares, vulnerabilidades y riesgos en la rapidez del desarrollo y consumo de internet of things". http://hdl.handle.net/10609/89625

[30] J. C. Najar, J. A. Bohada y W. Y. Rojas, "Vulnerabilities in the internet of things", *Revista Visión Electronica*, vol. 13, n.° 2, 2019.

[31] E. Zabalo, "Estudio del estado del arte en estándares y certificación en materia de seguridad cibernética aplicada a industria 4.0 e IOT", Tesis de grado, Universidad del país Vasco, 2019.

[32] A. Vélez, "Arquitecturas de referencia para IoT con transferencia segura de información", Tesis de grado, Universidad Nacional Abierta y a Distancia, Bogotá, 2019.

Fecha de envío: 13-10-2019
Fecha de recepción: 15-10-2019
Fecha de aceptación: 03-11-2019

[33] IOT Simple, "Modelo de Referencia IOT Simple". http://www.iotsimple.com/que-es-iot

[34] IBM® IBM Knowledge Center, "Arquitectura de referencia". https://www.ibm.com/support/knowledgecenter/es/SSPT3X_4.1.0/com.ibm.swg.im.infosphere.biginsights.install.doc/doc/inst_referArch.html

[35] Amazon AWS, "Certificados X.509". https://docs.aws.amazon.com/es_es/iot/latest/developerguide/x509-certs.html

[36] Amazon AWS, "AWS IoT Guía del desarrollador". https://docs.aws.amazon.com/es_es/iot/latest/developerguide/iot-dg.pdf

[37] L. Tudela, "Arquitectura blockchain para la securización de dispositivos iot mediante smart contracts", Tesis de grado, Universidad de Vigo, Pontevedra, 2019.

[38] L. Valencia y T. Guarda, "Seguridad de la Información en WSN aplicada a Redes de Medición Inteligentes basado en técnicas de criptografía", *RISTI*, vol. E17, p. 15, 2019.

[39] J. C. Najar y N. E. Suárez, "La seguridad de la información: un activo valioso de la organización", *Revista Vínculos: Ciencia, Tecnología y Sociedad*, vol. 12, n° 1, 2015. https://doi.org/10.14483/22484728.12345