TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 17. No. 2, mayo-agosto, 2018, p.42- 51 ISSN 1729-3804

SERVICIOS DE AUTENTICACIÓN Y AUTORIZACIÓN ORIENTADOS A INTERNET DE LAS COSAS

Maureen Valentina Parra Mondragón[1], Edward Paul Guillén[2]

[1,2]Universidad Militar Nueva Granada, Cra 11 101-80 Bogotá D.C
[1,2]e-mail: u1401167@unimilitar.edu.co, edward.guillen@unimilitar.edu.co

RESUMEN

El crecimiento de la cantidad de dispositivos con la capacidad de conectarse a internet y comunicarse por medio de la red ha generado la concepción del sistema llamado IoT (Internet of Things). Este sistema ha despertado interés en la sociedad y sus implementaciones cada vez aumentan más en número, por esta razón es necesario que este nuevo entorno esté asegurado y que las identidades de los dispositivos involucrados estén protegidas. En este documento se explican las partes que conforman al internet de las cosas y los tipos de ataques cibernéticos que podrían recibir cada una de ellas. Como consecuencia a esto, se muestra como los certificados digitales son una de las herramientas que podrían ser utilizadas para la autenticación de los dispositivos que forman parte de un sistema IoT y así mismo, se encuentran diferentes arquitecturas de seguridad implementadas con certificados digitales por empresas desarrolladoras como AWS (Amazon Web Services) y Microsoft. Finalmente, se encontrará una propuesta de arquitectura de seguridad en un entorno IoT con certificados digitales basados en una estructura On Premise que incluye un servidor local y servicios de la nube.

PALABRAS CLAVES: Internet de las cosas, seguridad, certificados digitales, llave pública y privada, Computación en la nube.

AUTENTICATION AND AUTORIZATION SERVICES TO THE INTERNET OF THINGS

ABSTRACT

The growth of the total number of devices with the ability to connect to Internet and communicate through the network has conceived a system called IoT (Internet of Things). This system has aroused interest in society and its implementations are increasing in number, for this reason it is necessary to secure communication on this new environment and to protect identities of involved devices. Digital certificates are one of the tools to be used to authenticate devices member parts of IoT systems. This document explains main parts that make up the internet of things and the types of cyber attacks that each of them could receive. As a consequence of this, different security architectures implemented with digital certificates are shown by development companies such as AWS (Amazon Web Services) and Microsoft. Finally, a security architecture proposal will be found in an IoT environment with digital certificates based on On Premise structure that includes a local server and cloud services.

KEY WORDS: Internet of Things, security, digital certificates, private and public key, Cloud Computing.

1. INTRODUCCIÓN

El IoT (Internet of Things) provee conexión a diferentes dispositivos tecnológicos que permiten que sean utilizados en diferentes circunstancias. Ésta nueva tecnología está revolucionando el mundo y la manera de vivir de las personas. Gubbi [1] afirma que para el 2020 habrá billones de dispositivos conectados a la red, por este motivo IoT está tomando un papel muy importante en la sociedad, pues dará la posibilidad de controlar

ambientes como el hogar, el cuidado de la salud, el transporte, entre otros. IoT en la salud conlleva a una recolección de datos automática, al rastreo de los dispositivos y a la autenticación de los mismos, para prevenir la alteración de los datos y evitar hechos como la formulación de medicamentos o aplicación de tratamientos erróneos al paciente. IoT en el transporte se ha implementado en algunas aerolíneas permitiendo a los usuarios realizar el check-in desde el celular para el registro, además en algunos sistemas existen sensores que actúan como identificadores para la solicitud del equipaje, este sensor debe ser protegido de los atacantes. IoT en el hogar permite también al usuario monitorizar todos los elementos conectados a internet, la contraseña que poseen estos dispositivos debe ser confidencial para evitar el daño del hogar por robo o intrusión de datos, por esto se debe tener una seguridad confiable y capaz de predecir o alertar cualquier acción sospechosa [2]. En todos estos ambientes en donde se puede y se ha aplicado la tecnología de IoT es necesaria la protección de la identidad de los dispositivos para asegurar el sistema.

Según la compañía Symantec, los ataques en sistemas IoT aumentaron un 600% desde el año 2016 al 2017, estos ataques tienen origen principalmente en Japón, China, Rusia, India, Estados Unidos y Brasil. Estos daños en la red pueden hacer que la conexión entre dispositivos se rompa y así mismo, hacer que se pierdan datos necesarios para el funcionamiento correcto del sistema [3].

En este estudio también se encontró que los usuarios utilizan la misma contraseña y nombre de usuario durante mucho tiempo y además de esto con un bajo nivel de seguridad. En este sentido, los usuarios son más vulnerables a un ataque de robo de información, lo cual se puede ver evidenciado en las tablas 1 y 2 [3].

Tabla 1: Nombres de usuario mas utilizados para ataques a sistemas IoT.

Nombre de Usuario 2017	Porcentaje del 2017	Nombre de Usuario 2017	Porcentaje del 2016
root	40	root	33,5
admin	17,3	admin	14,1
enable	10,3	DUP root	6
shell	10,2	DUP admin	2,1
guest	1,5	ubnt	1,3
support	1,4	test	1,1
user	1,1	oracle	1,1
ubnt	0,9	postgres	0,7
DUP root	0,6		0,7
supervisor	0,5	123321	0,6

Tabla 2: Contraseñas mas utilizados para ataques a sistemas IoT.

Contraseña 2017	Porcentaje del 2017	Contraseña 2016	Porcentaje del 2016
system	10,3	admin	9,5
sh	10,2	root	5,8
123456	9,1	12345	5
admin	3,7	123456	3,7
1234	3,1	password	3,2
password	2,5	1234	2,4
12345	2,5	ubnt	1,7
	2,3	admin123	1
root	2,1	abc123	0,9

support	1,2	pass	0,7

En la siguiente sección se nombran y explican diferentes ataques que se han realizado a los sistemas IoT, además de esto se profundiza en el ataque DoS (Denial Of Service) el cual ha sido muy utilizado recientemente por los atacantes. Seguido de esto se encontrará como los certificados digitales ayudan a la protección de un sistema conectado a internet y disminuyen la probabilidad de ataque o daño al sistema al que el intruso quiera dañar o robar información y finalmente las conclusiones de la investigación.

2. ESTADO DEL ARTE

Internet of Things (o internet de las cosas), se define como la interconexión en red de los objetos que usamos de forma cotidiana y que son capaces de conectarse a través de internet [4]. Gracias a los avances tecnológicos se estima que IoT ofrecerá nuevas oportunidades para crear aplicaciones que mejorarán la calidad de nuestras vidas [1].

Internet de las cosas fue una visión al futuro desde el principio de la era tecnológica, incluso desde el primer momento en que se estableció la primera comunicación entre computadoras o red de ordenadores llamada ARPANET [5]. Años después, en 1990 John Romkey crea el primer dispositivo que puede mantener una conexión a internet, una tostadora que se podía apagar y encender por medio de internet. Posteriormente, en 1997 se da la primera descripción de sensores. El término de IoT es expresado por primera vez en 1999 por Kevin Ashton en MIT (Massachusetts Institute of Technology) y al mismo tiempo inventaba un sistema de identificación de objetos por medio de Radio Frequency Identification (RFID) [6].

Para el 2005, publicaciones de organizaciones reconocidas comenzaron a citar artículos y documentos que hacían referencia a IoT y tres años después, empresas de desarrollo incentivan el uso del protocolo IP para IoT. Como consecuencia de estos avances, en 2011 se lanza IPV6 lo que provoca que empresas importantes como CISCO, ERICSON E IBM inicien a tomar iniciativas de capacitación en este nuevo tema [6]. La Unión Internacional de Telecomunicaciones (UIT) definía el IoT como promesa y lo definiría en la recomendación UIT-T Y.2060, como "una infraestructura global para la sociedad de la información. De esta forma permite servicios avanzados interconectando cosas físicas y virtuales, basada en tecnologías de la información y comunicación interoperables existentes y en evolución" [7].

Después de estas fechas, el desarrollo de IoT es expuesto por invenciones tales como el primer refrigerador con conexión a internet propuesto por LG. Refrigerador capaz de indicar al usuario el estado de la comida, entre otras más invenciones [6].

A partir de estos desarrollos se comienza a introducir el concepto de IoT, el nuevo modelo que, según investigaciones [1], revolucionará el entorno de las personas, volviéndola más digital. Este concepto lo han definido como el nuevo modelo de internet, o la revolución del mismo, que mezcla diferentes tecnologías y aspectos, por esto IoT también es considerado como la red de redes [8] ya que es capaz de integrar diferentes elementos ayudando a facilitar la vida de las personas.

Está descrito [1] que para la visualización completa de IOT eficiente, segura y escalable, el mercado debe estar obligatoriamente orientado a la computación y almacenamiento de recursos, es ahí donde IoT se integra con la computación en la nube. La computación en la nube es el nuevo modelo que ofrece servicios por medio de centro de datos de nueva generación fundamentados en tecnología de almacenamiento virtualizado [10]. La cantidad de dispositivos y de información que en un futuro podría manejar IoT solo podría ser administrada y almacenada por la computación en la nube, aquí es donde se encuentra la necesidad de que estos sistemas se integren [9].

En la actualidad, donde millones de dispositivos se conectan a internet y a plataformas que prestan el servicio de computación en la nube, es necesaria una red confiable y segura para que no se vean alterados los datos o la información que viaja por la misma. Por esta razón se crearon varios métodos para asegurar el tráfico de la red. En IoT son datos muy pequeños los que viajan, pero alguna alteración maliciosa en estos puede generar muchos problemas presentándose problemas en el sistema.

Cualquier parte de IoT puede verse afectada por un ataque ya sea el hardware, el software o el en la capa de enlace. La unión de estos tres elementos conforma un sistema IoT [11]:

- Hardware: se entiende como la parte física de un entorno IoT. Los objetos partícipes en esta red pueden ser sensores que se comunican entre ellos y así mismo intercambian información sobre el

entorno en el que se encuentran y el estado de este, recolectando datos como: la humedad, el movimiento, la temperatura, entre otros. Se han realizado estudios para mejorar la eficiencia energética en un sistema IoT ya que este aspecto ha sido un problema al aumentar la cantidad de sensores en la red. A pesar de esto un sistema conectado a internet presenta una gran interoperabilidad con otras tecnologías como los celulares, las tabletas y los computadores [11].

- Software: Es una herramienta usada por el hardware para el soporte y manejo de la cantidad de datos que generan los diferentes dispositivos conectados a la red. El crecimiento y la adopción de IoT en infraestructura, es decir en hardware, hará que sea necesario que exista un soporte en software para la comunicación, intercambio y tratamiento de información recogida por los objetos inteligentes [11].

- Capa de Enlace: Representa el canal de comunicación entre el software y el hardware por el que se transmite la información. Para que IoT funcione correctamente y se pueda garantizar una gran calidad de servicio es necesario que cada una de las partes se encuentren en buen estado y seguras. Cada una de las partes poseen tecnologías seguras para que la comunicación entre estas sea confiable. Además, IoT es capaz de realizar la toma de decisiones en la capa de aplicación, capa de red y capa de percepción según el servicio solicitado [11].

Existen diferentes ataques que pueden afectar a todo un sistema IoT aun si solamente se aplica a una de las tres partes que lo conforman, como, por ejemplo:

Ataques en la capa física o hardware

Los dispositivos conectados a la red que intercambian datos por medio de esta pueden ser vulnerados por medio de los siguientes ataques, algunos son:

- Jamming: es un ataque que se aplica a los dispositivos finales de la red y consiste en crear interferencia en la comunicación mediante señales de radio. Al atacar a un dispositivo específico el atacante impide que se realice la transmisión de datos y posteriormente además impide que los datos se retransmitan repetidamente. Este ataque es capaz de tumbar una red de comunicaciones completa [11].

- Tampering: este tipo de ataque puede generar diferentes daños, una forma de aplicarlo es introducir un malware para obtener información de la red redireccionándola afuera de la misma para conocer su contenido como las claves de cifrado. Al obtener todas las características de un dispositivo por medio de un software malicioso este se puede duplicar en todos los sentidos: hardware, software y todos sus aspectos con el objetivo de dañar las funcionalidades de los demás dispositivos conectados a la red [11].

Ataques a la capa de enlace

Los usuarios son vulnerables al robo de información personal en el intercambio de información entre dos o varios dispositivos. Algunos ataques que se presentan en la capa de enlace de comunicación y en la red son:

- Denegación de servicio: el atacante busca saturar la red inundando a los puertos de una gran cantidad de tráfico generando que el servidor no pueda contestar y se detenga su servicio. DoS (Denial of Service) hace que la red está ocupada lo que implica que los dispositivos conectados a la misma no se puedan comunicar y esto es un problema en un contexto IoT [12].

- Sniffing: es un ataque que se realiza mediante un programa que permite capturar el tráfico que viaja por la red. Al seleccionar un paquete se puede extraer información importante del usuario como el enrutamiento y topología de la red, direcciones ip de origen y destino, entre otros aspectos [12].

Ataques en la capa de aplicación o software

Existen ataques que se aplican a la interfaz de la red y así mismo a la interfaz de usuario de IoT, uno de los más implementados es:

- Ataque Clon: se presenta cuando una entidad maliciosa copia entidades ya creadas y utiliza estas características para influenciar en el sistema como realizando cambios en la red o haciendo que se duplique la información. Además de esto, este ataque es capaz de cambiar los mensajes que se quieran publicar en un entorno IoT. Al obtener características de otros nodos conectados a la red se cree que está permitidos en dicha red y por esto es tan difícil detectar un ataque clon. [13].

Estadísticas de ataque DDoS (Distibuted Denial of Service)

Los ataques a la red afectan directamente a un entorno IoT afectando la comunicación entre dispositivos o demás aspectos ya mencionados. La compañía VeriSign experta en redes y comunicaciones elaboró un reporte que muestra que el número de ataques DDoS (Distributed Denial of Service) disminuyeron del primer al segundo cuarto del año 2017 [14].

El tamaño del paquete del ataque también ha ido disminuyendo a medida que se encuentran más formas de mitigar el ataque. Según los datos tomados desde el tercer cuarto del año 2015 hasta el segundo del 2017, se reportan tamaños de paquete pasando de ataque de 10 Gbps a 1Gbps [14].

Existen diferentes estrategias para aplicar el ataque de DDoS que utilizan los atacantes para inundar la red de su objetivo. VeriSign reportó que DDoS multi-vector o multisistema fue el más mitigado en el tercer trimestre del 2017 acarreando el 74% del total. Mirai Bonet es una de las estrategias más difíciles de mitigar pues utilizan protocolos difíciles de detectar lo que hace que se necesite un monitoreo frecuente de la red [14].

En el segundo trimestre del 2017 se obtuvo la siguiente información con respecto a las estrategias utilizadas para aplicar DDoS [14]:

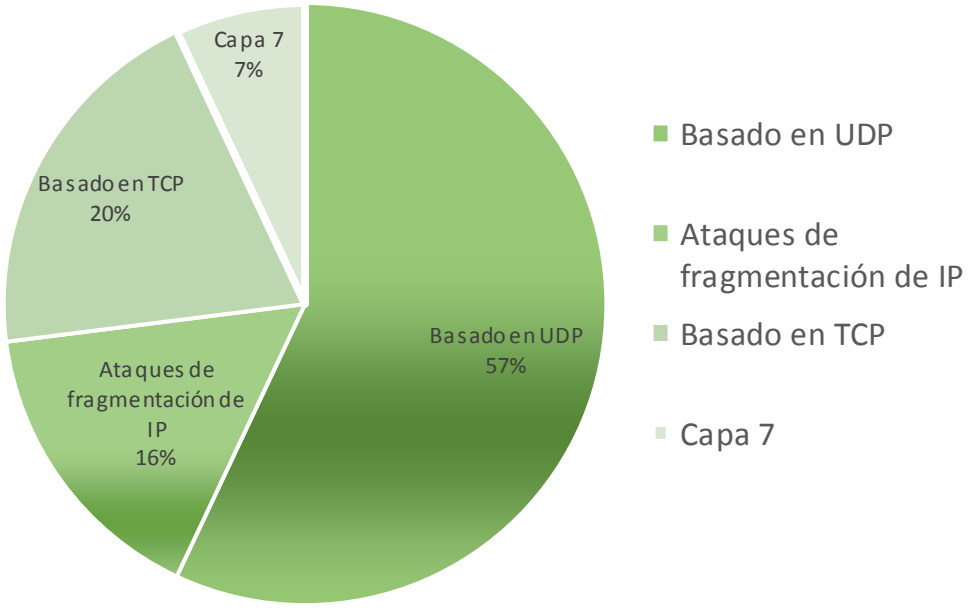

Figura 1: Tipos de ataques de DDoS en el segundo trimestre del 2017

En la Figura 1 [14], se puede observar que el tipo de ataque DDoS más utilizado para dañar los sistemas es el que está basado en UDP. Los ataques DDoS basados en UDP consisten en saturar al sistema atacado con paquetes que contienen datagramas UDP, al recibir muchas solicitudes de orígenes que no puede encontrar el sistema atacado se agobia y no es capaz de responder a todos sus clientes [l5].

Estos ataques afectaron a varios sectores de la industria como por ejemplo el sector financiero, las plataformas de cloud computing, el sector público, sector de entretenimiento, telecomunicaciones y comercio en línea. El sector financiero fue el más afectado en la mayoría de los trimestres analizados. En el tercer trimestre del 2016 este sector recibió ataques que superaron 200 Gbps de tamaño, pero para el cuarto trimestre del mismo año el sector más afectado fueron las plataformas de cloud computing sobrepasando ataques de 100 Gbps de tamaño [15].

3. LOS CERTIFICADOS DIGITALES COMO OPCIÓN PARA LA SEGURIDAD EN IoT

Como consecuencia a estas estadísticas se sugirió un sistema de seguridad por medio de certificados digitales. Este sistema es uno de los mecanismos utilizados para mitigar el riesgo asociado con la información almacenada e intercambiada entre dispositivos conectados en red. Mediante estos certificados digitales se busca garantizar identidad y autenticación para cualquier acceso a los datos confidenciales. La identidad provee confianza a los usuarios porque permite asegurar que las entidades en los extremos son quienes dicen ser. La verificación de identidad es un elemento fundamental para la seguridad efectiva del dispositivo en red.

Los certificados digitales son un mecanismo que provee seguridad por medio de la autenticación de una identidad única. Además de esto, los certificados digitales también permiten una transmisión de datos segura y una comunicación confiable. Este mecanismo también está implementado para mantener la integridad de la llave pública o PKI (Public Key Infraestructure) y unir la información del propietario a la llave pública de una manera segura [16].

La infraestructura existente de PKI (Public Key Infraestructure o Infraestructura de la llave pública) es capaz de acomodarse para prestar una seguridad adecuada a IoT, pues es considerada una de las mejores opciones para los dispositivos conectados a la red. Los certificados PKI son evidencia de que la identidad de las organizaciones, los dominios y los dispositivos se estableció correctamente porque los certificados vinculan criptográficamente las claves públicas a dichas identidades [17].

Este es el componente de autenticación que IoT necesita para su seguridad. En estas áreas de seguridad, PKI sobresale como una solución probada. Varios grupos de la industria promocionan la flexibilidad y la de aplicaciones de PKI como una opción líder para la seguridad de la información y la comunicación [17].

4. CERTIFICADOS DIGITALES PROPUESTOS PARA LA SEGURIDAD EN IoT

Existen diferentes empresas desarrolladoras de nuevas tecnologías como programas, dispositivos, almacenamiento en la nube, sistemas IoT, entre otras. Amazon y Microsoft son compañías que han creado sistemas para la implementación de IoT y así mismo buscan métodos para la seguridad de estos dispositivos. Una opción para la seguridad del sistema es la implementación de los certificados digitales en los objetos conectados a la red que intercambian información. Como consecuencia a esto, las estructuras de seguridad implementadas con este método por Amazon y Microsoft se podrán observar a continuación.

Certificados digitales de AWS (Amazon Web Services) que soportan IoT

AWS tiene soporte de seguridad y autenticación para aplicaciones de IOT ya que todo el tráfico que sale y entra a este servicio está cifrado por TLS (Transport Layer Security). Se puede observar en la Figura 2 [18], que cada dispositivo conectado debe tener una identificación para lograr la comunicación con el gestor de mensajes, por ello todas las credenciales o identificación deben estar aseguradas. La seguridad en AWS IoT se divide en cuatro métodos, uno de ellos es la identificación por medio de los certificados X.509. Los usuarios que elijan los certificados para asegurar su identidad deben administrarlos ya que se encargarán de asignar una identidad única a cada dispositivo y configurar los permisos de cada certificado para el mismo. Al realizar la conexión, el dispositivo necesariamente debe identificarse con el certificado, además de esto, el agente de mensajes autenticará cada dispositivo que se quiera conectar y autorizará todos los permisos que éste necesite que se le habiliten para cualquier acción y así AWS IoT podrá enviar mensajes de un dispositivo a otro si es necesario [19].

Los certificados proveen un sistema de autenticación muy fuerte, este método permite que se puedan usar claves privadas y que estas queden almacenadas en el dispositivo generando que los archivos criptográficos se queden guardados en un dispositivo específico. Por esto es necesario que el certificado sea asignado a solamente un dispositivo y que este dispositivo esté en la capacidad de soportar la sustitución de los certificados para evitar tiempos inactivos y mantener la comunicación estable y segura [19].

En el momento de autenticar el certificado X.509 de un cliente, AWS IOT solicita y verifica el estado del mismo para posteriormente validarlo en un registro de certificados. Todo esto también para que el dispositivo se comunique y autentique con el servidor correcto, estas autenticaciones están presentes también en las conexiones MQTT (Message Queuing Telemetry Transport) [19].

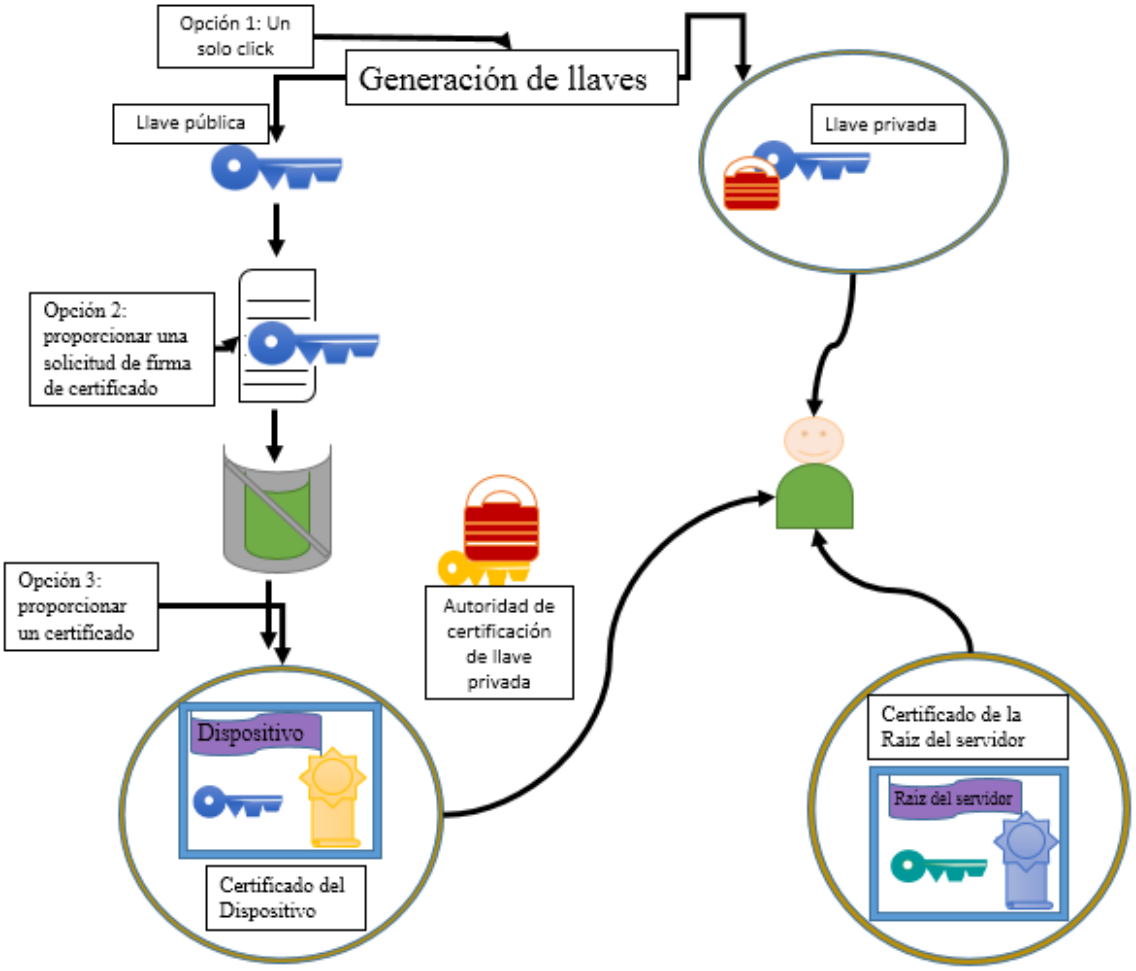

Figura 2: Infraestructura de asignación de un certificado digital a un dispositivo en AWS (Amazon Web Services).

Certificados digitales de AZURE que soportan IoT

Azure, es la plataforma que presta servicios de la nube de Microsoft y permite el desarrollo de aplicaciones y demás servicios a sus usuarios. Azure IoT Hub es el servicio que se encarga de conectar de manera segura los dispositivos relacionados con el internet de las cosas de los usuarios en Microsoft. Este servicio soporta los certificados X.509 para realizar la autenticación de los dispositivos activos en IoT Hub que están conectados por medio de protocolos como HTTP (Hypertext Transfer Protocol ó protocolo de transferencia de hipertexto), MQTT (Message Queue Telemetry Transport ó transporte de telemetría de mensaje de cola) ó AMQP (Advanced Message Queuing Protocol ó Protocolo avanzado de cola de mensajes) [20].

En la Figura 3 [21], se muestra que la autenticación realizada por medio de certificados en Azure IoT Hub incluye certificados que pueden estar enlazados con el dispositivo el cual utiliza para identificarse. Un certificado generado por el fabricante e introducido al dispositivo junto con la clave privada. Un certificado validado y generado por una autoridad de certificación usado para la identificación y autenticación en IoT Hub [21].

En la Figura 3 expuesta por [21], se puede observar cómo se registra un dispositivo en IoT Hub, esta plataforma provee soporte de registro el cual se realiza por medio de una codificación, en el que se especifica qué dispositivo se va a registrar, la identificación del dispositivo, el mecanismo de autenticación que se va a registrar (certificado X.509) y la huella digital (valor único asignado a un certificado digital).

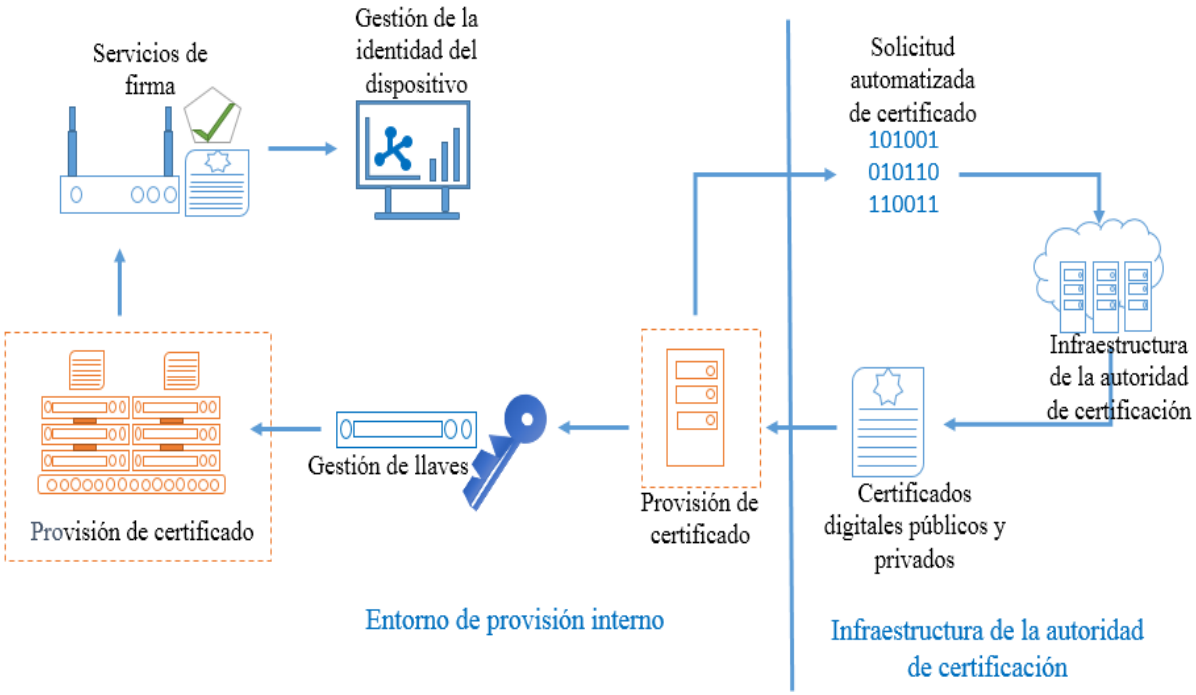

Figura 3: Infraestructura de asignación de un certificado digital a un dispositivo en AZURE.

Certificados digitales en una infraestructura propuesta de IoT con cloud on-premises

Una arquitectura "on premise" es una de las infraestructuras que reúne servicios propios de computación en la nube y que también contiene recursos fuera de la nube como los servidores locales [22]. En la arquitectura propuesta por los autores en la Figura 4 se implementa un sensor conectado a la red y a un servidor local para recibir la autenticación y poder intercambiar datos entre las partes. Cuando el sensor recibe la identificación por parte del servidor local tendrá acceso a los servicios de la plataforma de la computación de la nube elegida. Con esta propuesta se busca implementar un entorno IoT y lograr que el servidor por medio del directorio activo realice el proceso de identificación al sensor.

Una infraestructura de cloud on-premises tiene ventajas sobre infraestructuras que son netamente cloud, las principales son:

1. La elasticidad que posee con respecto al aumento o aprovechamiento de capacidades físicas o virtuales de alguna característica del sistema, como, por ejemplo, el almacenamiento de información [23].
2. El ahorro de recursos energéticos al no necesitar encender los nodos físicos para terminar de realizar cierta actividad, como, por ejemplo, terminar de montar una máquina virtual ya que este proceso se puede realizar directamente con recursos en la nube [23].
3. Es una infraestructura confiable y eficaz en escenarios que no cuentan con muchos recursos computacionales [23].
4. La flexibilidad para la administración de datos almacenados en los equipos, es decir, no es necesario estar en el nodo físico para poder ver y editar la información [23].

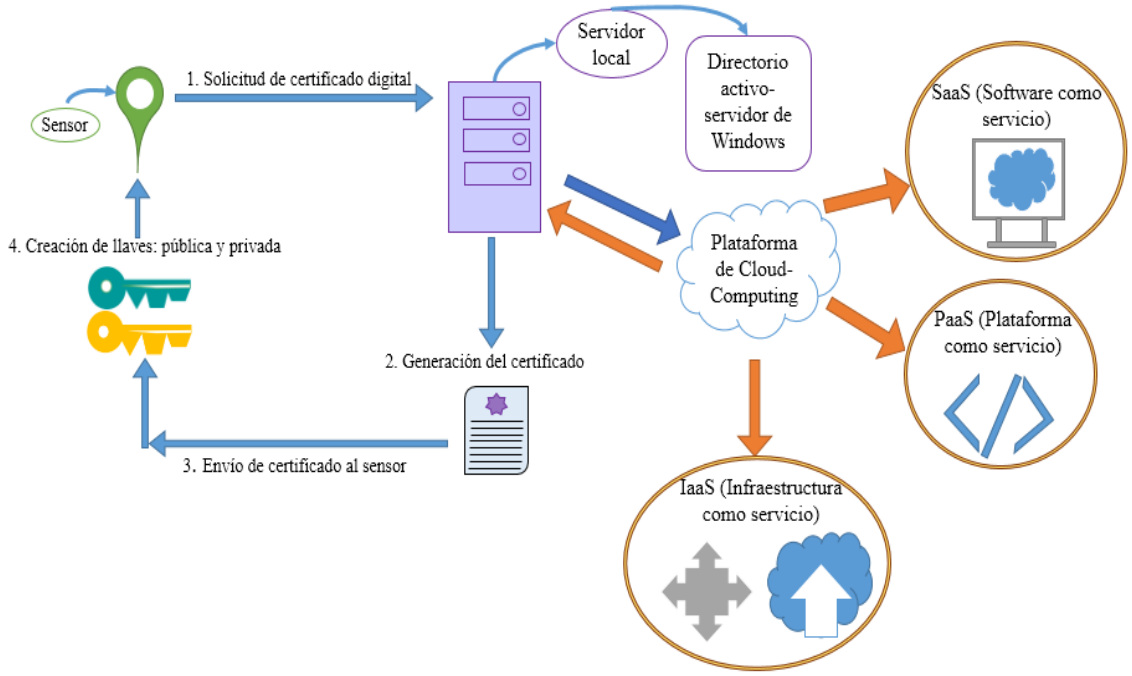

Figura 4: Infraestructura propuesta de asignación de un certificado digital a un dispositivo IoT.

5. CONCLUSIONES

La seguridad en un sistema IoT es un enigma para muchas organizaciones aún, pues esta tecnología ha crecido tanto que es necesaria un sistema de seguridad confiable para los usuarios, ya que se deben evitar daños que afecten la integridad del ambiente. Los ataques en IoT pueden llegar a destruir el sistema poniendo en peligro la vida de las personas, por esto es necesario la protección de la identidad de todo lo que está involucrado en este nuevo ambiente.

Los certificados digitales y la llave pública son dos elementos que, efectivamente, ayudan a la protección de la identidad de un dispositivo en un sistema. En IoT estas herramientas serán la base para construir un sistema de seguridad que se acople y soporte más a este nuevo ambiente que se está implementando en la sociedad. En este momento los certificados digitales no son suficientemente seguros como para considerarlos la principal seguridad para un ambiente IoT, pues estos elementos requieren de modificaciones en su estructura y administración para hacerlos más adecuados a esta nueva tecnología.

Las plataformas de computación en la nube dan el soporte necesario para la implementación de un sistema IoT, además uno de los métodos de seguridad que ofrecen está basada en los certificados digitales, los cuales no serán obsoletos para asegurar un ambiente IoT. Más bien los certificados digitales presentarán una evolución para ser más confiables en el nuevo entorno que se implementará con más fuerza en un futuro con base a las nuevas arquitecturas propuestas.

Con la arquitectura de cloud on-premises propuesta se espera conseguir la recolección de los datos recogidos por el sensor después de que este se haya autenticado mediante un certificado digital. El certificado digital y las llaves: pública y privada, se generarán en el servidor local, pero autenticarán servicios en la nube como el almacenamiento de la información recolectada. En el servidor local se encontrará el directorio activo que proporcionará permisos a los equipos y usuarios como, por ejemplo, la autenticación del sensor como un equipo y del usuario asignando permisos al sensor sobre su configuración en el directorio activo.

RECONOCIMIENTOS

Este trabajo fue posible en parte gracias a la Universidad Militar Nueva Granada, con la financiación del proyecto INV-ING-2646.

REFERENCIAS

[1] GUBBI, Jayavardhana, et al. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, 2013, vol. 29, no 7, p. 1645-1660.

[2] NAWIR, Mukrimah, et al. Internet of Things (IoT): Taxonomy of security attacks. En *Electronic Design (ICED), 2016 3rd International Conference on*. IEEE, 2016. p. 321-326.

[3] SYMANTEC. ISTR Internet Security Threat Report [en línea]. Mountain View, CA. [ref. 18 de julio del 2018]. Disponible en Web: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.

[4] XIA, Feng, et al. Internet of things. *International Journal of Communication Systems*, 2012, vol. 25, no 9, p. 1101-1102.

[5] LEINER, Barry M., et al. A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, 2009, vol. 39, no 5, p. 22-31.

[6] SURESH, P., et al. A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. En *Science Engineering and Management Research (ICSEMR), 2014 International Conference on*. IEEE, 2014. p. 1-8.

[7] ITU. *Internet of Things Global Standards Initiative*. Recomendación UIT-T Y.2060. Geneva. Switzerland. 2012.

[8] EVANS, Dave. The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, 2011, vol. 1, no 2011, p. 1-11.

[9] CHOWDARY, E. Deepak; YAKOBU, D. Cloud of Things (CoT) integration challenges. En *Computational Intelligence and Computing Research (ICCIC), 2016 IEEE International Conference on*. IEEE, 2016. p. 1-5.

[10] CACERES, Ramon; FRIDAY, Adrian. Ubicomp systems at 20: Progress, opportunities, and challenges. *IEEE Pervasive Computing*, 2012, vol. 11, no 1, p. 14-21.

[11] BILLURE, Rajendra; TAYUR, Varun M.; MAHESH, V. Internet of Things-a study on the security challenges. En *Advance Computing Conference (IACC), 2015 IEEE International*. IEEE, 2015. p. 247-252.

[12] KAMBLE, Arvind; MALEMATH, Virendra S.; PATIL, Deepika. Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. En *Emerging Trends & Innovation in ICT (ICEI), 2017 International Conference on*. IEEE, 2017. p. 33-39.

[13] ANTHONIRAJ, J.; RAZAK, T. Abdul. Clone Attack Detection Protocols in Wireless Sensor Networks: A Survey. *International Journal of Computer Applications*, 2014, vol. 98, no 5.

[14] VERISIGN. Verisign Distributed Denial of Service Trends Report [en línea]. Reston, VA. [ref. 20 de julio del 2018]. Disponible en Web: http://www.axians.co.uk/gods-and-monsters/assets/VRSN_DDoS_TR_Q2-17_Axians_201709-WebFinal.pdf

[15] IMPERVA CAPSULA. Udp Flood What is a UDP Flood Attack [en línea]. [ref. 20 de julio del 2018]. Disponible en Web: https://www.incapsula.com/ddos/attack-glossary/udp-flood.html.

[16] CHOUDHURY, Suranjan; BHATNAGAR, Kartik; HAQUE, Wasim. Public key infrastructure implementation and design. John Wiley & Sons, Inc., 2002.

[17] SCHUKAT, Michael; CORTIJO, Pablo. Public key infrastructures and digital certificates for the Internet of things. En *Signals and Systems Conference (ISSC), 2015 26th Irish*. IEEE, 2015. p. 1-5

[18] Amazon Web Services. Understanding the AWS IoT Security Model [en linea]. [ref. 15 de agosto del 2018]. Disponible en Web: https://aws.amazon.com/es/blogs/iot/understanding-the-aws-iot-security-model/

[19] Amazon Web Services. AWS IoT Developer Guide [en línea]. Seattle, WA. [ref. 16 de agosto del 2018]. Disponible en Web: http://docs.aws.amazon.com/es_es/iot/latest/developerguide/iot-dg.pdf#iot-security-identity

[20] Microsoft, Control access to IoT Hub, Microsoft [en linea]. Redmond, WA. [ref. 17 de agosto del 2018]. Disponible en Web: https://opbuildstorageprod.blob.core.windows.net/output-pdf-files/en-us/Azure.azure-documents/live/iot-hub.pdf

[21] DIGICERT, Internet of Things PKI Security for Smart Systems and Networked Devices [en linea]. Lehi, UT. [ref. 19 de agosto del 2018]. Disponible en Web: https://www.digicert.com/internet-of-things/provisioning-deployment.htm

[22] Amazon Web Services. Tipos de cloud computing [en linea]. [ref. 20 de agosto del 2018]. Disponible en Web: https://aws.amazon.com/es/types-of-cloud-computing/

[23] CALATRAVA, Amanda, et al. Towards Migratable Elastic Virtual Clusters on Hybrid Clouds. En Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on. IEEE, 2015. p. 1013-1016.