Análisis de Seguridad para la Autenticación y Privacidad en Entornos IoT

David Bello-Bustamante[1], Carlos Alberto Ochoa Rivera[2], Alessandra Reyes-Flores[2]
[1,2]Facultad de Estadística e Informática, Maestría en Sistemas Interactivos Centrados en el Usuario, Universidad Veracruzana, Av. Xalapa s/n, Obrero Campesina, 91020 Xalapa-Enríquez, Ver., México
[1]zS18016332@estudiantes.uv.mx, [2]{cochoa, itreyes}@uv.mx
***Área de participación**: Sistemas Computacionales*

Resumen

El Internet de las Cosas (*Internet of Things*, IoT), es una tecnología encargada de mantener dispositivos interconectados que a su vez pueden compartir información, datos y comunicarse entre sí para cumplir un objetivo en común. Al ser una tecnología reciente se espera que el número de dispositivos conectados aumente de manera significante, convirtiéndose en parte importante de la vida cotidiana de una persona, pero que podría exponer información personal de ésta. Por lo tanto, es de gran importancia considerar la seguridad de los nodos que serán los encargados de mantener la conexión entre los dispositivos que se encuentren conectados en un entorno IoT. En este documento se realiza un análisis de trabajos relacionados en cuanto a la seguridad en IoT con la finalidad de obtener características principales de la autenticación y privacidad, estas servirán para propuestas futuras de seguridad que apoyen a los desarrolladores a crear entornos IoT seguros.

***Palabras clave**: IoT, Seguridad, Autenticación, Privacidad.*

Abstract

The Internet of Things (IoT), is a technology responsible for maintaining interconnected devices, in turn they can share information, data and communicate with each other to meet a common goal. Being a recent technology, the number of connected devices is expected to increase significantly, becoming an important part of a person's daily life, but which could expose their personal information. Therefore, it is of great importance to consider the security of the nodes that will be responsible for maintaining the connection between the devices that are connected in an IoT environment. In this document, an analysis of related works regarding security in IoT is carried out with the purpose of obtaining main authentication and privacy features, these will serve for future security proposals that support developers to create secure IoT environments.

***Key words**: IoT, Security, Authentication, Privacy.*

Introducción

El Internet de las Cosas (*Internet of Things*, IoT), es una tecnología que permite conectar tanto como personas, como objetos o dispositivos, que a su vez estos permiten el intercambio de bienes y servicios en las redes. Weber [2010], define a IoT como una arquitectura técnica global emergente basada en Internet que facilita el intercambio de bienes y servicios en las redes de la cadena de suministro global, en donde se tienen que establecer medidas de seguridad que garanticen la resistencia a ataques, la autenticación de datos, el control de acceso y la privacidad del cliente.

IoT ha crecido con gran rapidez, de tal forma que se espera un aumento de las interconexiones de los dispositivos y, por lo tanto, una gran cantidad de información que será compartida de manera inalámbrica en su mayoría. Al ser una tecnología reciente y al depender, en su mayoría, de una conexión inalámbrica, surgen diversos

problemas de seguridad, por ejemplo, el uso de servicios de red inseguros, la falta de mecanismos de actualización seguros, insuficiente protección a la privacidad, entre otros. Es importante garantizar que la información que se comparten entre los dispositivos no se vea comprometida y, en caso de ser comprometida, poder mitigar lo más pronto posible la invasión a la seguridad y privacidad de estos.

La tecnología de IoT presenta nuevos retos, como el tratar de mantener una conexión segura entre los dispositivos que comparten información en sí, muchos desarrolladores de esta nueva tecnología se preocupan principalmente por la funcionalidad, conectividad y diseño de los dispositivos, dejando de lado la seguridad de estos. Un entorno de IoT maneja distintas aplicaciones de acuerdo con las necesidades de donde este aplicado, sin embargo, si las personas que se encuentran interactuando dentro del entorno, como lo podrían ser desarrolladores, colaboradores y empleados, no toman medidas de seguridad y no protegen la información, la confidencialidad de los datos que se comparten se podría decir que se encuentra en riesgo.

Los principales criterios de inclusión ocupados para la selección de los documentos para el análisis fueron: revistas, conferencias y artículos formales de fuentes confiables, documentos relacionados con la seguridad y el análisis de técnicas para la autenticación y privacidad en IoT, así como de amenazas y vulnerabilidades. Por otra parte, los criterios de exclusión fueron: documentos e investigaciones anteriores al año 2010, literatura que solo estaba disponible en forma de resúmenes o presentaciones de diapositivas, y documentos que no tengan contribución alguna o no hablen de trabajos a futuro. Los estudios de revisión sistemática se identificaron utilizando la siguiente cadena de búsqueda: ((“Security” OR “Privacy”) AND (“IoT” OR “Internet of Things”) AND “Authentication”), buscando principalmente en las siguientes bases de datos: IEEExplore, Springer Link y Google Academic. Tomando en cuenta los criterios de inclusión y exclusión, la búsqueda se acotó en ocho documentos que son tomados en cuenta en el actual trabajo.

En este artículo se presenta una investigación sobre proyectos de seguridad enfocados en prevalecer la autenticación y privacidad de usuarios dentro de un entorno IoT, así como, se hace un análisis de lo que estos trabajos han considerado importante para la implementación de un entorno IoT seguro. De acuerdo con el análisis realizado en los trabajos de investigación se obtendrán las características relevantes de la autenticación y de la privacidad de cada uno de estos, que servirán para propuestas futuras de seguridad y que apoyen a los desarrolladores a crear entornos IoT seguros. Se pretende que las propuestas futuras tomen en cuenta las características obtenidas del análisis y se agreguen otras más teniendo presente aspectos de usabilidad que apoyen al buen uso del entorno evitando así fallas en la seguridad de este, como lo podrían ser las malas practicas por parte del usuario que dejan al entorno vulnerable ante posibles ataques.

En la sección dos se hace una breve explicación de lo que es IoT. Se adentra al tema principal que es la seguridad y privacidad en IoT en la sección tres, donde también se habla acerca de los principales servicios y mecanismos de seguridad que se toman en cuenta en IoT. Posteriormente, en la sección cuatro se habla de las amenazas y vulnerabilidad que afectan a la autenticación y privacidad en IoT. En la sección cinco se realiza el análisis de los trabajos que se enfocan apoyar a la autenticación y privacidad de IoT. En la sección seis se realiza la discusión del análisis realizado de los trabajos seleccionados. Por último, en la sección siete la conclusión del presente trabajo.

Internet de las cosas (IoT)

El Internet de las Cosas (*Internet of Things*, IoT), es una tecnología que se encarga de mantener dispositivos interconectados, que a su vez comparten información, datos y se comunican entre sí para cumplir un objetivo en común. Cendón [2019], menciona en su publicación que en 2009 fue cuando Kevin Ashton, profesor del MIT en aquel entonces, usó la expresión *Internet of Things* de manera pública, aunque el propio Ashton ha comentado que la expresión se ha venido manejando desde 1999, más no se había hecho pública.

IoT en las últimas décadas ha avanzado de tal forma que cada vez es más común conectarse a Internet con mayor facilidad y con dispositivos relativamente de bajo costo, por ejemplo, teléfonos, electrodomésticos, relojes, automóviles, entre otros. IoT se aplica en distintas áreas, ya que depende de la creatividad e ingenio de los desarrolladores para ajustar productos y servicios en las diversas áreas de aplicación [Alcaraz, 2014]:

- En el hogar: para el control y automatización de los sistemas del hogar, la monitorización del estado de la casa y electrodomésticos inteligentes.
- En ciudades: control y monitorización del tráfico.
- En los automóviles: para facilitar el mantenimiento de sus productos y aumentar la información que los usuarios reciben de sus automóviles.
- En la salud: para el control y tratamientos más eficientes y para el cuidado de personas mayores.
- En el medio ambiente: para la recolección de información sobre ciertos indicadores ambientales, como lo podría ser la calidad del aire, suelo o agua.

Jing y cols. [2014], en su trabajo señalan que las aplicaciones IoT brindan comodidad a las personas, pero qué si estas aplicaciones no garantizan la seguridad de la privacidad personal, entonces la información privada corre el riesgo de filtrase en cualquier momento. Por lo tanto, la seguridad en IoT no debe ser ignorada.

Seguridad en IoT

La seguridad, en redes, consiste en prevenir y tratar de proteger lo mejor posible la intrusión no autorizada de personas o mecanismos maliciosos que expongan la privacidad de los datos que se manejan en una red. Por otra parte, la seguridad en redes inalámbricas supone una mayor complejidad para mantener la seguridad dentro de ésta, ya que no dependen de una infraestructura de cables como una red tradicional, sino de un enlace que utiliza ondas electromagnéticas (radio e infrarrojo), por lo que la información que se comparte dentro de la red puede ser interceptada con más facilidad dejándola vulnerable a ataques mal intencionados.

Zhao y col. [2013], definen los problemas de seguridad de IoT como los mismos que se presentan en las WSN (*Wireless Sensor Network*), en las redes de comunicaciones móviles e Internet, pero en IoT se presentan otros problemas más particulares, de los cuales los más a resaltar son: el problema de la protección de la privacidad, la autenticación de la red, los problemas de control de acceso, el almacenamiento y la gestión de la información.

De cierta forma, estar conectados en la actualidad en una red inalámbrica y preservar la privacidad es unos de los retos que se generan con el uso de IoT, mientras más personas usen diferentes servicios de Internet, es más difícil mantener la confidencialidad de su información personal, por lo cual, es importante asegurar a los usuarios que al utilizar esta tecnología su información no se verá afectada y su privacidad se mantendrá protegida.

Alcaraz [2014], alude que la privacidad y la seguridad en IoT podrían ser los aspectos más desafiantes al implementar esta tecnología, ya que un usuario al estar conectado en un entorno IoT muchas veces ignora como y quien se encuentra recolectando información de su dispositivo sin su consentimiento, donde esta información podría considerarse sensible, tal como conversaciones, el estado bancario, geoposicionamiento, etc.

Sánchez y cols. [2013], señalan que por lo general los intrusos escanean protocolos y puertos conocidos de los dispositivos conectados a una red para así intentar acceder a páginas de administración de estos, en caso de no tener éxito, usan escaneos más sofisticados que imitarán el comportamiento de un usuario autorizado dentro del entorno, de esta forma extrayendo información personal de los usuarios que se comparte dentro del entorno.

Existen requisitos de seguridad y privacidad que deben ser considerados al crear entornos de IoT que ayudarán a la disminución de riesgos o a la mitigación de estos [Weber, 2010]:

- Resiliencia a los ataques: el entorno tiene que estar preparado para posibles fallas dentro de este, así como de tenerlas detectadas.
- Autenticación de datos: la información que se maneja dentro del entorno exige ser autenticada y verificar que viene de una fuente legítima.
- Control de acceso: se requiere implementar un control de acceso que garantice que solo personas con permisos puedan hacer uso de los servicios que se comparten dentro del entorno.

Servicios de seguridad en IoT

La mayoría de los servicios de IoT son proporcionados mediante WSN, en estas redes los dispositivos que se interconectan son llamados nodos o motas, el cometido de estos dispositivos es recopilar la información del entorno y transmitirla a una estación base donde se almacenan y se analizan los datos [Rodríguez y cols., 2014]. De acuerdo con las características de los nodos sensores y del entorno a donde se implemente, se requiere tomar precauciones y consideraciones para garantizar la confidencialidad, integridad y disponibilidad de los datos que se comparten dentro del entorno IoT.

Para poder garantizar atenuación o mitigación de ataques y vulnerabilidades se necesita disponer de un nivel de seguridad y privacidad de acorde a los servicios que se prestan dentro del entorno IoT y de la información que se comparte. Sanchez y cols. [2015], menciona que este nivel de seguridad y privacidad se realiza mediante servicios de seguridad obtenidos mediante un conjunto de mecanismos y contramedidas capaces de contrarrestar los ataques o amenazas sobre los elementos que se deben proteger. A continuación, en la Tabla 1 se mencionan los servicios de seguridad que son ocupados dentro de un entorno IoT.

Tabla 1. Servicios de Seguridad ocupados en un entorno IoT [Sanchez y cols., 2015].

Servicio de seguridad	Características
Autenticación	Para identificar la entidad comunicante y la fuente de datos.
Control de Acceso	Para prevenir el uso no autorizado de los recursos.
Confidencialidad de los Datos	Para protegerlos contra la revelación no autorizada.
Integridad de los Datos	Para garantizar que no han sido alterados o destruidos de una manera no autorizada.
No Repudio	Para dar prueba del origen de los datos o de entrega de estos
Disponibilidad	Para garantizar la continuidad de la accesibilidad y utilización por las entidades autorizadas.
Privacidad	Para controlar la información que posee un usuario y limitar la cantidad de personas autorizadas para obtenerla.

Los servicios de seguridad se proporcionan mediante mecanismos que apoyan a la seguridad de estos, se pueden ocupar solos o combinados. Ruiz y cols. [2016], resaltan que cualquier persona maliciosa puede llegar a manipular los dispositivos encargados de compartir la información dentro del entorno, de tal forma de comprometer el canal de comunicación entre estos, pero con el uso de algunos mecanismos de seguridad se podrían llegar a evitar o mitigar estas vulnerabilidades. Los mecanismos que más resaltan al momento de crear un entorno IoT son: el cifrado, el uso de firmas digitales, mecanismos para el control de acceso y de integración de datos, el intercambio de autenticación, entre otros [Sanchez y cols., 2015].

Amenazas y vulnerabilidades en IoT

La seguridad de la información es un aspecto importante el cual está dando de qué hablar dentro de IoT, ya que el número de dispositivos conectados a Internet es cada vez mayor, lo que supone un crecimiento en la exposición de los datos en la red, Evans [2011]. Existen distintas amenazas y vulnerabilidades dentro de IoT que ponen en riesgo la seguridad del entorno dado que un atacante aprovecha estas vulnerabilidades y amenazas para adentrase en este. Las amenazas y vulnerabilidades atacan directamente a los servicios de seguridad IoT con la intención principal de exponer la privacidad de los datos que se manejan dentro del entorno.

Perera [2018], divide las amenazas y vulnerabilidades en ocho grupos en función de la finalidad para la cual se utiliza cada una de ellas, como este trabajo está enfocado en cubrir la autenticación y privacidad de usuarios solo serán tomadas en cuenta las amenazas y vulnerabilidades que puedan comprometer a estos dos atributos de seguridad dentro de un entorno IoT como lo muestra la Tabla 2.

Tabla 2. Amenazas y vulnerabilidades que afectan a la autenticación y privacidad en un entorno IoT, [Perera, 2018].

Grupo	Función del ataque	Características	Ataques
1	Abusos/Ataques negativos	Amenazas y vulnerabilidades que se adentran en el sistema para controlarlo.	• Malware • *Exploit* • Denegación de Servicio (DDoS) • Suplantación de dispositivos • Modificación de la información
2	Interceptores/ Secuestradores de comunicaciones	Amenazas y vulnerabilidades que se utilizan para recolectar información de los dispositivos mientras es transferida a través del entorno.	• *Man-in-the-Middle* • Secuestro del protocolo de comunicación • Intercepción de la información • Analizadores de la red • Reproducción de mensajes
3	Empleados maliciosos	Amenazas y vulnerabilidades que surgen tras exponerse datos sensibles intencionalmente.	• Filtrado de información privada

De esta manera quedan tres grupos donde si se llevan a cabo estas amenazas y vulnerabilidades se vería afectada la autenticación y la privacidad de los usuarios dentro de un entorno IoT.

Análisis de trabajos enfocados en la autenticación y privacidad de IoT

Se ha identificado que los servicios de seguridad se apoyan unos a otros, es decir, la autenticación permite un mejor control de acceso y la privacidad ayuda a la confidencialidad de los datos, por lo tanto, se ha realizado un análisis de trabajos de investigación en los que se han enfocado en apoyar a algunos servicios. Particularmente, en análisis se realizó sobre proyectos enfocados en autenticación y privacidad.

Existen diversos trabajos que ayudan a facilitar la obtención de datos para apoyar a la seguridad en cuanto a privacidad y autenticación dentro de un entorno IoT. En la Tabla 3 se muestra una comparativa de características de los trabajos analizados.

Tabla 3. Tabla de características destacadas en trabajos relacionados en seguridad de IoT.

	Tipo de trabajo	Sugerencias relevantes	Fases/ Capas/ Requerimientos/ Componentes	Características de autenticación	Características de Privacidad	Caso de estudio
Ning y cols. [2012]	Arquitectura de Seguridad	U2IoT (*Unit IoT and Ubiquitous IoT*), IPM (*Information, Physical and Management*)	Seguridad de la información, seguridad física, seguridad de la administración	Control de acceso inteligente: el uso de la autenticación heterogénea. Autenticación jerárquica: establecer la autenticación jerárquica mutua.	Transparencia: permitir al usuario saber qué entidad contiene sus datos. Trazabilidad: permitir al usuario conocer la información del servicio al que está conectado.	Arquitectura de seguridad basada en la red IPM
Geovanny y col. [2015]	Esquema de seguridad para entorno IoT seguro	Niveles de seguridad que ayudan a la construcción de la seguridad desde niveles más bajos a más altos	Concienciación sobre la seguridad, Seguridad física y de red, Prácticas de codificación segura, Gestión de identidad y acceso, Monitoreo de la Integridad,	Uso de la Autenticación Multifactor (MFA) para accesos remotos, Listas de Control de Acceso (*Access Control Lists*, ACL) de red.	Uso de IDS/IPS (Sistema de Detección y Prevención de Intrusos). Realización de pruebas para detectar vulnerabilidades.	Establecimiento de mecanismos de seguridad a considerar con la innovación tecnológica de IoT.

			Políticas de seguridad			
Pal y cols. [2017]	Arquitectura de control de acceso	Control de acceso seguro para IoT	Dispositivo de usuario, Cosas (sensores), Sistema de Gestión Central, Registro de Datos en Repositorio	Almacenamiento de atributos de usuario que otorgan acceso a roles y capacidades para el uso de servicios.	Reduce el incremento de información al asignar un rol	Propuesta de una arquitectura de control de acceso basado en roles
Kim y cols. [2016]	Arquitectura de red segura para IoT	Medidas de seguridad para la autenticación de entidades	Autorización y autenticación frecuentes, conectividad intermitente, entre otros requisitos de seguridad	Autenticación mutua automatizada: poder autenticarse sin la intervención del usuario. Uso de Seguridad en la Capa de Transporte (*Trasport Layer Security,* TLS)	Uso del protocolo DTLS (*Datagram Transport Layer Security*) para proteger la privacidad en las comunicaciones y prevenir la intercepción y manipulación	Arquitectura de seguridad basada en entidades de autorización locales
Liu y cols. [2012]	Método de autenticación y control de acceso	Protocolo de autenticación y esquema de control de acceso	Análisis de seguridad para pruebas del protocolo propuesto	Uso de Control de Acceso Basado en Roles (*Role-Based Access Control*, RBAC)	Comunicación solida en la capa de aplicación con el establecimiento de claves seguras simples y eficientes.	Autenticación y control de acceso para IoT
Khan y cols. [2018]	Técnica de autenticación para IoT	Autenticación basada en el protocolo Oauth 2.0	Autenticar y controlar de manera eficiente el acceso de los usuarios autorizados que intentan utilizar los recursos de una red IoT	Uso del protocolo Oauth 2.0 para la autorización usuarios.	Uso de tokens para autenticarse y obtener acceso a los recursos solicitados.	Técnica de autenticación basada en el protocolo Oauth 2.0 para IoT
[Imam y col., 2017]	Marco de seguridad para IoT	Uso de un enfoque híbrido utilizando diferentes marcos	IoT, Nivel de dispositivo, Nivel de red y Nivel de Sistema	Identificar y probar identidad, verificar que la información introducida es correcta	Monitorear el tráfico y alertar al sistema cuando haya tráfico sospechoso.	Marco de seguridad que toma en cuenta tres niveles, de dispositivo, de red y de sistema
[Rachid y cols., 2015]	Arquitectura de privacidad en IoT	Seguridad de dispositivos, de comunicación y de los usuarios	Capa de detección, de red y de aplicación	N/A	Información del usuario accesible solo para entidades autorizadas	Arquitectura de privacidad sensible al contexto de IoT

El criterio principal por el cual fueron tomados en cuenta los artículos mencionados en la tabla anterior es la seguridad, ya que todos estos tratan de mantener la privacidad y la autenticación de la información que se comparte en IoT. Como se observa, los artículos proponen en su mayoría arquitecturas de seguridad que se enfocan en el control de acceso con el uso de distintos protocolos. Aunque estos trabajos presentan soluciones para apoyar a la seguridad, en específico a la autenticación y privacidad de los servicios y usuarios de IoT, como menciona Abdukhalilov [2017], existen aún problemas por solucionar, donde se deben desarrollar e implementar soluciones adecuadas que garanticen el control de acceso y la privacidad de los usuarios y las cosas, la autenticación entre los dispositivos y que cumplan con ciertas políticas de seguridad y confidencialidad.

 ISSN 2007-8102

Discusión

En las arquitecturas propuestas por Nings y cols. [2012], Pal y cols. [2017], y Kim y cols. [2016], su principal objetivo es mantener un control de acceso y autenticación en cuanto a la jerarquía de roles que se pueden manejar dentro del entorno IoT. Nings y cols. [2012], se apoyan de un modelo basado en la unidad y ubicuidad (U2IoT) asegurando de esta forma la información y la administración (IPM) del entorno IoT. Por otro lado, Pal y cols. [2017], se centran en la autenticación de los dispositivos, tanto de usuario como de los sensores que son ocupados dentro del entorno, así asignando servicios específicos dependiendo del tipo de rol que se maneje. La arquitectura propuesta por Kim y cols. [2016], se enfoca en la autorización y autenticación sin la intervención del usuario, aplicando protocolos como DTLS en la capa de transporte, asegurando así los servicios proporcionados dentro del entorno. Por último, la arquitectura propuesta por Rachid y cols. [2015], se centra en la seguridad de los dispositivos, de la comunicación y de los usuarios, propone otros dos niveles de seguridad en las capas y los servicios de la arquitectura.

El esquema de seguridad propuesto por Gevanny y col. [2015], propone el uso de diversos mecanismos y protocolos en las distintas capas de seguridad que se manejan en IoT, otro punto a resaltar de este trabajo es que manejan una ACL de red, que ayuda a mantener un registro de los usuarios que se autentican en el entorno y con el uso de IDS/IPS detectar y prevenir la intrusión de usuarios o dispositivos maliciosos. Lui y cols. [2012], proponen un método de autenticación y control de acceso partiendo de un análisis de seguridad, usando el protocolo RBAC que apoya a la seguridad en la capa de aplicación estableciendo claves que se comparten entre los dispositivos dentro del entorno. Por último, Khan y cols. [2018], proponen una técnica de autenticación basada en el protocolo Oauth 2.0 que ocupa tokens para la autorización de usuarios, de esta forma asegurando la privacidad de la información que se maneja, ya que a partir de ello los usuarios pueden hacer uso de los servicios prestados por IoT. Imam y col. [2017], propone un marco de seguridad para IoT, en el cual ocupa varios marcos obteniendo como resultado uno híbrido, no menciona mecanismos de autenticación y privacidad, pero hace referencia a principios de estos, por ejemplo, verificar y probar la identidad del usuario, monitorear el tráfico y alertar al sistema de posible tráfico sospechoso.

Con base en el análisis comparativo de las diferentes características que integran los artículos mencionados en la Tabla 3, los trabajos cumplen con la principal función que es mantener la privacidad y la autenticación en IoT, de manera global, la seguridad. Por otra parte, estos trabajos se preocupan por el diseño e implementación de un entorno tomando en cuenta los dispositivos que serán ocupados, la información que tiene que ser confidencial y monitoreando la integridad de este, así como del diseño e implementación creando prácticas o pruebas que ayuden a verificar que estos trabajos si cumplen con la protección del sistema y/o entorno. Cabe mencionar que estos trabajos solo se preocupan por mantener la seguridad en cuanto a fallas que puedan presentar los dispositivos y a la posible intrusión de usuarios, pero dejan de lado los problemas que se pudiesen presentar por las malas practicas de los usuarios que ya se encuentran dentro del entorno IoT, dejando vulnerable a este ante posibles ataques que afecten el entorno seguro.

Conclusiones

En el presente trabajo se mencionan algunas áreas de aplicación importantes de IoT se describen los aspectos relevantes de seguridad dentro de esta tecnología, mencionando los servicios de seguridad que apoyan a mantener la seguridad dentro de los entornos IoT. También se realizó una explicación de las amenazas y vulnerabilidades que afectan a la autenticación y privacidad en un entorno IoT. Por último, se identificaron trabajos de investigación enfocados en prevalecer la seguridad de los sistemas o entornos IoT, de estos trabajos se obtuvieron las características de autenticación y privacidad más relevantes. Posteriormente se realizó un análisis de los trabajos de investigación que apoyan a la seguridad en IoT, tomando en cuenta como principales servicios a la autenticación de dispositivos y usuarios, y a la privacidad de la información.

El análisis realizado servirá para crear a futuro propuestas de seguridad centradas en el usuario, en las cuales se tomarán en cuenta las observaciones realizadas en este trabajo y se agregarán otras más que apoyen a los desarrolladores a generar entornos más seguros para los usuarios y que los datos que se manejan dentro del entorno no se vean afectados por usuarios maliciosos u otras entidades externas. Se pretende que las propuestas futuras apoyen al entorno IoT a estar preparado para posibles fallas de los usuarios que hacen uso de este. Estas fallas pudiesen ser desde malas prácticas, hasta de filtración de información confidencial por parte de ellos, así como de los problemas de seguridad mencionados.

Referencias

1. Weber, R. H. (2010). Internet of Things–New security and privacy challenges. Computer law and security review, 26(1), 23-30.
2. Whitten A. and Tygar J. D., 1998. Usability of Security: A Case Study, Carnegie Mellon School of Computer Science Technical Report, December 1998. (Available at http://reportsarchive. adm.cs.cmu.edu/anon/1998/abstracts/ 98-155.html)
3. Sanchez Alarcon, J. A., Lopez Santidrian, L., and Martínez Ortega, J. F. (2015). Solución para garantizar la privacidad en el internet de las cosas. El profesional de la información, 24(1), 62-70.
4. Barrera, G. M. (2018). Estilo arquitectónico para aplicaciones IoT (No. 664). Universidad del CEMA.
5. Rodríguez Molina, J., Martínez Ortega, J. F., Rubio Cifuentes, G., and Hernández Díaz, V. (2014). A proposal for an Internet of things-based monitoring system composed by low capability, open source and open hardware devices.
6. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., and Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20(8), 2481-2501.
7. Liu, J., Xiao, Y., and Chen, C. P. (2012, June). Authentication and access control in the internet of things. In 2012 32nd International Conference on Distributed Computing Systems Workshops (pp. 588-592). IEEE.
8. Perera Bartual, Ó. (2018). Análisis y parametrización de la seguridad en sistemas IoT (Doctoral dissertation).
9. Evans, D. (2011). Internet de las cosas. Cómo la próxima evolución de Internet lo cambia todo. Cisco Internet Bussiness Solutions Group-IBSG, 11(1), 4-11.
10. Perez, N. B., Bustos, M. A., Berón, M., and Rangel Henriques, P. (2018). Análisis sistemático de la seguridad en internet of things. In XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste).
11. Ning, H., and Liu, H. (2012). Cyber-physical-social based security architecture for future internet of things. Advances in Internet of Things, 2(01), 1.
12. Rodríguez, C., and Geovanny, F. (2015). El Internet de las cosas y las consideraciones de seguridad (Master's thesis, Quito/PUCE/2015).
13. Pal, S., Hitchens, M., and Varadharajan, V. (2017, October). Towards a Secure Access Control Architecture for the Internet of Things. In 2017 IEEE 42nd Conference on Local Computer Networks (LCN) (pp. 219-222). IEEE.
14. Kim, H., Wasicek, A., Mehne, B., & Lee, E. A. (2016, August). A secure network architecture for the internet of things based on local authorization entities. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 114-122). IEEE.
15. Khan, J., ping Li, J., Ali, I., Parveen, S., ahmad Khan, G., Khalil, M., ... & Shahid, M. (2018, December). An Authentication Technique Based on Oauth 2.0 Protocol for Internet of Things (IoT) Network. In 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP) (pp. 160-165). IEEE.
16. Cendón, B. (2019). La historia del Internet de las Cosas (IoT). Retrieved from http://www.bcendon.com/el-origen-del-iot/
17. Alcaraz, M. (2014). Internet de las Cosas. Universidad Católica Nuestra Señora de la Asunción, 2-3.
18. Ruiz, M., Alvarez, E., Serrano, A., & Garcia, E. (2016). The convergence between wireless sensor networks and the Internet of Things; challenges and perspectives: A survey. IEEE Latin America Transactions, 14(10), 4249-4254.
19. Abdukhalilov, S. G. (2017, November). Problems of security networks internet things. In 2017 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-7). IEEE.
20. Imam, A. H., & Azer, M. A. (2017, December). Internet of Things security framework. In 2017 13th International Computer Engineering Conference (ICENCO) (pp. 378-382). IEEE.
21. J. P. Nzabahimana, "Analysis of security and privacy challenges in Internet of Things," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kiev, 2018, pp. 175-178.
22. Rachid, S., Challal, Y., & Nadjia, B. (2015, November). Internet of things context-aware privacy architecture. In 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA) (pp. 1-2). IEEE.
23. M. Williams, J. R. C. Nurse and S. Creese, "Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things," 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, 2017, pp. 181-18109.
24. M. El-hajj, M. Chamoun, A. Fadlallah and A. Serhrouchni, "Analysis of authentication techniques in Internet of Things (IoT)," *2017 1st Cyber Security in Networking Conference (CSNet)*, Rio de Janeiro, 2017, pp. 1-3.
25. G. Chu, N. Apthorpe and N. Feamster, "Security and Privacy Analyses of Internet of Things Children's Toys," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 978-985, Feb. 2019.