Análisis de la Seguridad en Internet de las Cosas: Una Revisión Sistemática de Literatura

Security Analysis of the Internet of Things: A Systematic Literature Review

Juan Martínez, Jezreel Mejía, Mirna Muñoz
Centro de Investigación en Matemáticas Unidad Zacatecas
Av. Universidad no. 222, 98068
Zacatecas, México
{ juan.martinez, jmejia, mirna.munoz}@cimat.mx

Resumen — **Actualmente las personas dependen cada vez más de la comunicación a través de Internet para realizar sus actividades cotidianas. Como resultado de esto ha surgido el Internet de las cosas (IoT). Por tal motivo, se ha incrementado considerablemente el número de dispositivos conectados a Internet, alcanzando una cifra aproximada de 20 mil millones, y se espera que para 2020 llegue a 50 mil millones. Esto ha generado grandes retos para mantener la seguridad y privacidad de la información ya que la mayoría de los dispositivos móviles se centran en la conectividad y están incluyendo configuraciones por defecto donde la seguridad se ve gravemente afectada. Este artículo presenta los resultados obtenidos a través del método de revisión sistemática para establecer el estado actual de la seguridad en los dispositivos conectados a IoT. Como resultado de la revisión se detectaron las principales preocupaciones, amenazas, ataques, retos y algunas contramedidas.**

Palabras Clave - Internet de las cosas; IoT; Seguridad; Revisión Sistemática.

Abstract — **Nowadays people are increasingly dependent on the Internet to conduct their daily activities. As a result of this has emerged the Internet of Things (IoT). Therefore, it has significantly increased the devices connected to the Internet; reaching around of 20 billion connected devices, and is expected to reach 50 billion in 2020. This has created great challenges for maintaining security and privacy of information because most mobile devices focus on connectivity and are including default settings where security is severely affected. This paper presents the results obtained by the protocol of systematic review to establish the current state of security in IoT devices. As a result of the review the main concerns, threats, attacks, challenges, and some countermeasures were detected.**

Keywords – Internet of Things; IoT; security; systematic review.

I. INTRODUCCIÓN

Hoy en día el Internet se ha vuelto indispensable en la vida diaria de las personas, día a día se está incrementando su uso en prácticamente todos los ámbitos, conectando una amplia variedad de dispositivos, como: vestibles (wearables), electrodomésticos, automóviles, dispositivos médicos, una gran variedad de sensores (RFID, NFC, etc.), entre otros. Lo cual, originó que la cantidad de dispositivos conectados a Internet superara al número de habitantes en el mundo (entre 2008 y 2009), dando como resultado el término "Internet de las cosas" (IoT, por sus siglas en inglés) [1].

[1], [2] mencionan que para el año 2020 la cantidad de dispositivos conectados en total será de 50 mil millones, mientras que [3] argumentan que para el mismo año, habrá 25 mil millones de dispositivos sólo de IoT. Este gran incremento en el número de dispositivos conlleva un gran reto para la seguridad, ya que por lo general son productos novedosos que ofrecen una funcionalidad específica y muchos fabricantes descuidan las características de seguridad, debido a la competencia por llegar primero al mercado y que su producto sea fácil de usar [3].

Un estudio realizado por HP [4] revela que un 70% de los dispositivos de IoT no cifran sus comunicaciones, el 70% permiten a un atacante identificar la cuentas de usuario válidas, el 60% de los que tienen interfaz de usuario son vulnerables a distintos ataques como secuencias de comandos en sitios cruzados (XSS). Considerando que estos dispositivos recopilan una gran cantidad de información sensible para los usuarios, esto se vuelve un gran riesgo de seguridad [2].

El objetivo de este trabajo es realizar un análisis sobre el estado actual de la seguridad en IoT para mostrar qué problemas existen, cuáles ya se están abordando, cómo se está haciendo e identificar si hay algunos que se están dejando desatendidos.

Las siguientes secciones del documento están organizadas de la siguiente manera: en la sección 2 se presenta una breve contextualización acerca de IoT; la sección 3 describe el método de revisión sistemática desarrollado durante esta investigación; la sección 4 muestra los resultados del análisis de la revisión; y la sección 5 presenta las conclusiones.

II. CONTEXTUALIZACIÓN

El Internet de las cosas (IoT) se puede definir como una red altamente interconectada de entidades heterogéneas, tales como, etiquetas, sensores, dispositivos embebidos, dispositivos portátiles, etc., que interactúan y se comunican entre sí en tiempo real [5], [6]. IoT es un concepto que describe un futuro donde todos los objetos físicos estarán conectados a Internet y la interacción entre dispositivos es máquina a máquina (M2M), sin necesidad de intervención humana [7].

IoT revolucionará la manera en que las personas y las organizaciones interactúan con el mundo físico, la interacción con dispositivos domésticos, automóviles, plantas industriales, etc., sufrirá grandes modificaciones. También permitirá que muchos servicios como salud, educación y gestión de recursos, puedan ser mejorados para comodidad del cliente [8].

El rápido crecimiento de IoT está creando grandes oportunidades de negocios. Los productos y servicios asociados a IoT generarán ingresos superiores a los $300 mil millones de dólares para 2020 [7]. Verizon estima que actualmente el 10% de las empresas han adoptado IoT y que para 2025, las que lo hagan, serán 10% mas rentables que las que no [9].

III. REVISIÓN SISTEMÁTICA

Después de comprobarse la efectividad de la revisión sistemática en el área de la medicina, se decidió implementarla en la Ingeniería del Software y actualmente es usada para realizar investigaciones en una amplia gama de disciplinas (minería de datos, mejora de procesos, seguridad informática, aprendizaje virtual, etc.).

Una revisión sistemática de la literatura permite que permite identificar, evaluar, interpretar y sintetizar todas las investigaciones existentes y relevantes en un tema de interés particular.

Barbara Kitchenham, en el año 2004, fue la primer persona en presentar un método para realizar revisiones sistemáticas en el contexto de la Ingeniería del Software, el cual consta de 3 fases principales: planificación de la revisión, desarrollo de la revisión y reporte de resultados [10].

A. Planificación de la Revisión

La planificación es la primer fase de la revisión, aquí se desarrolla el protocolo que guiará la revisión, para esta investigación se consideraron las siguientes actividades: i) identificación de la necesidad de la revisión, ii) formulación las preguntas de investigación, iii) definición de la cadena de búsqueda y iv) selección de las fuentes de datos. Las cuales se describen brevemente a continuación:

1) Necesidad de la revisión: Con el acelerado crecimiento de IoT, cada día a más objetos se les agrega la funcionalidad de conectarse a Internet, y de acuerdo a Cisco esta tendencia continuará durante los próximos 20 años hasta conseguir que el 99% de los objetos se encuentren conectados [7]. Actualmente muchos fabricantes descuidan las medidas de seguridad que deben implementar en los dispositivos al competir por ser los primeros en sacarlos al mercado y que su configuración y uso sea lo más cómodo posible para el usuario.

2) Preguntas de investigación: (PI1) ¿Qué problemas de seguridad existen en IoT? y (PI2) ¿Qué aspectos se tienen que tomar en cuenta para mejorar la seguridad en IoT?

3) Cadena de búsqueda: Para resolver las preguntas de investigación se utilizaron las palabras clave: Internet de las cosas, IoT, seguridad y privacidad. Quedando "((security OR privacy) AND (Internet of things OR IoT))".

4) Fuentes de datos: Las fuentes seleccionadas fueron: ACM Digital Library, IEEE Xplore Digital Library, SpringerLink y ScienceDirect.

B. Desarrollo de la Revisión

El objetivo de esta segunda fase es identificar los estudios primarios y extraer la información de los mismos que sea relevante para la investigación. Para lo cual se incluyen las siguientes actividades: i) selección de los estudios primarios y ii) extracción de datos.

1) Selección de estudios primarios: Para seleccionar los estudios se definieron algunos criterios de inclusión y exclusión, además se siguió un procedimiento.

a) Criterios de inclusión: 1) estudios en idioma inglés o español, 2) estudios publicados del año 2011 a la fecha, 3) estudios que pertenezcan a la disciplina de seguridad en computación o redes, 4) estudios que contengan al menos dos palabras clave en el título y 5) Artículos que mencionen preocupaciones, amenazas, retos, ataques o contramedidas.

b) Criterios de exclusión: 1) estudios duplicados y (2) estudios que no contengan un análisis general de seguridad o privacidad de IoT.

c) Procedimiento: Para seleccionar los estudios primarios se realizaron los siguientes pasos: 1) adaptar la cadena de búsqueda al motor de la fuente seleccionada; 2) aplicar los criterios de inclusión 1, 2 y 3; 3) aplicar el criterio de inclusión 4; y 4) Leer resumen, introducción y conclusiones, y aplicar el criterio de inclusión 5 y los criterios de exclusión. En la Fig. 1 se muestra una visión general de la obtención de los 31 estudios primarios.

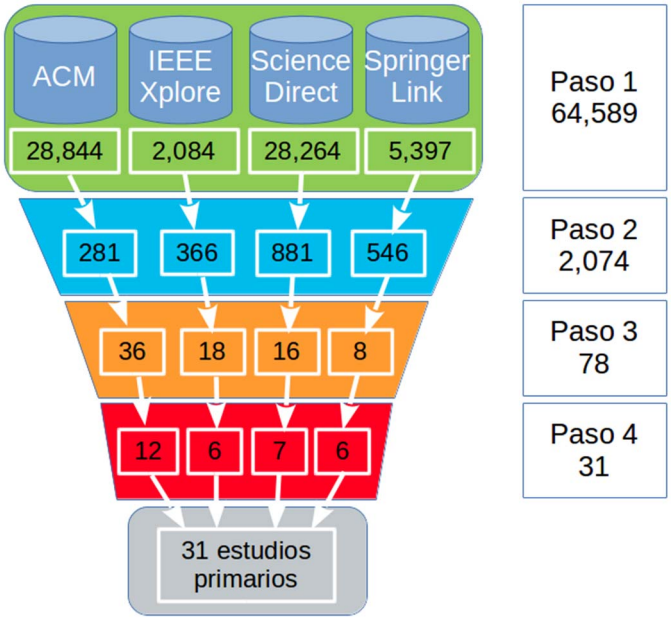

Figura 1. Filtrado de resultados.

El total de estudios primarios seleccionados se muestra en el Apéndice A.

2) Extracción de datos: Para la extracción de datos se diseñó una plantilla en una hoja de cálculo de Microsoft Excel donde se recopilaron los siguientes datos de cada estudio primario: Título, Autor, Año, Objetivo, Fuente y Contenido (Preocupaciones / Amenazas / Retos / Ataques / Contramedidas).

IV. Análisis de Resusltados

En esta sección se realiza una clasificación de los estudios primarios según su contenido para resolver las preguntas de investigación. Analizada la plantilla que sirvió para la extracción de datos de los estudios primarios se identificaron cinco áreas que se están investigando con respecto a la seguridad en IoT.

A. Estudios por Contenido

Como resultado del análisis, a continuación se enlistan en orden prioritario las áreas identificadas en los estudios primarios: 1) Retos, 2) Contramedidas, 3) Ataques, 4) Amenazas, y 5) Preocupaciones. En la Tabla 1 se muestran los datos cuantificados haciendo uso del identificador asignado a cada estudio en el Apéndice A.

TABLA I. Estudios por Tipo de Contenido

Contenido	Total	ID Estudio
Retos	22	S1, S2, S3, S4, S6, S7, S8, S9, S11, S14, S15, S16, S17, S18, S19, S20, S21, S22, S25, S26, S28, S31
Contramedidas	16	S1, S4, S5, S6, S8, S11, S12, S15, S19, S21, S22, S23, S25, S26, S27, S30
Ataques	15	S2, S4, S5, S6, S8, S10, S12, S15, S16, S17, S22, S24, S26, S27, S30
Amenazas	12	S2, S9, S10, S12, S13, S14, S17, S23, S24, S27, S29, S31
Preocupaciones	10	S2, S3, S10, S11, S17, S20, S25, S26, S30, S31

De cada una de las áreas revisadas anteriormente, se realizó una clasificación tomando en cuenta cuatro factores:

- Disponibilidad (que los dispositivos no dejen de funcionar o prestar el servicio).
- Seguridad física (barreras físicas y procedimientos de control para evitar que personas no autorizadas tengan contacto con los dispositivos).
- Control de acceso (mecanismos para evitar que personas no autorizadas accedan de manera lógica a los dispositivos).
- Comunicación (mecanismos para proteger la información mientras viaja entre emisor y receptor).

La identificación de las cinco áreas mostradas en la Tabla I y de los factores comunes a cada área descritos anteriormente permitió dar respuesta a las preguntas planteadas en la revisión sistemática.

1) PI1 ¿Qué problemas de seguridad existen en IoT?: Para dar respuesta a esta pregunta, se identificaron las áreas de preocupaciones, amenazas y ataques.

a) Preocupaciones: Una preocupación es un estado de inquietud o temor producido ante una situación difícil o un problema. Al analizar los estudios que contienen preocupaciones acerca de la seguridad en IoT se detectó que el aspecto que más preocupa a los investigadores es la comunicación (45.45%), y el de menor preocupación es el control de acceso (9.09%). La Fig. 2 muestra la clasificación completa.

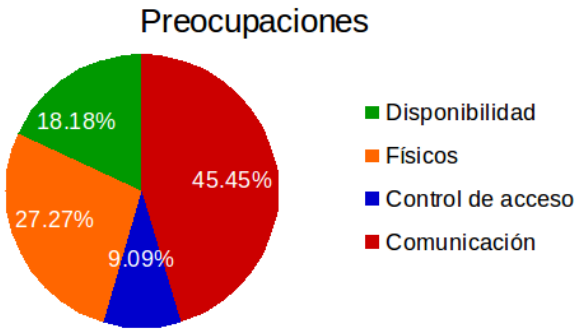

Figura 2. Clasificación de preocupaciones.

Dentro del área de la comunicación las principales preocupaciones son: comunicación inalámbrica, comunicación automática, ausencia de políticas de tráfico, fuga de información, recopilación excesiva de información, y difícil configuración.

b) Amenazas: Una amenaza es una cosa o persona que constituye una posible causa de riesgo o perjuicio para alguien o algo. Para identificar amenazas es necesario considerar las

características especiales de los dispositivos de IoT, ya que por lo general son dispositivos embebidos que no están pensados para que el usuario modifique las configuraciones o actualice el software. Como resultado del análisis se identificó que la mayor cantidad de amenazas se encuentran en el control de acceso (40.74%), mientras que las amenazas a la disponibilidad representan un porcentaje muy bajo (3.70%). La Fig. 3 muestra la clasificación completa.

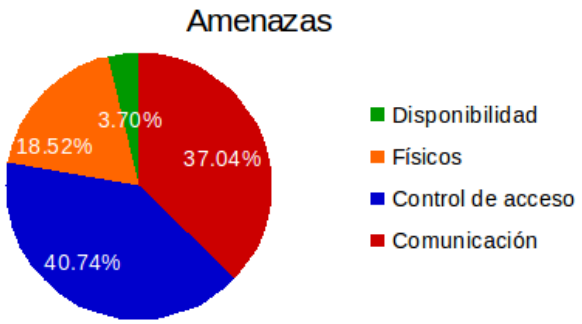

Figura 3. Clasificación de amenazas.

Las principales amenazas para el control de acceso son: métodos para obtener la clave secreta, puertas traseras, accesos no autorizados, insuficiente autenticación o autorización, interfaces inseguras, y mala configuración de seguridad.

c) Ataques: Un ataque es una acción violenta o impetuosa contra alguien o algo para hacerle daño o destruirlo. Al analizar los ataques se detectó que la mayor cantidad de éstos, están dirigidos a las comunicaciones (40.48%), mientras que los físicos son los que cuentan con el porcentaje mas bajo (11.90%). La Fig. 4 muestra la clasificación completa.

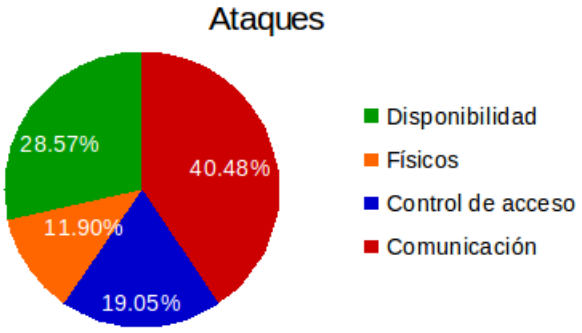

Figura 4. Clasificación de ataques.

Los principales ataques a las comunicaciones son: rastreo de paquetes, espionaje, interceptación, inyección de mensajes, divulgación no autorizada, ataques a la autenticación de datos, de agujero negro, modificación de ruta, ofuscación, y man-in-the-middle.

2) PI1 ¿Qué aspectos se tienen que tomar en cuenta para mejorar la seguridad en IoT?: Para dar respuesta a esta pregunta se identificaron las áreas de retos y contramedidas.

a) Retos: Un reto es un desafío o actividad que se debe realizar sobreponiéndose a diferentes tipos de dificultades. Los retos que enfrenta el IoT son grandes y cada día crecen ya que se van agregando nuevos dispositivos y se detectan nuevas vulnerabilidades. La mayor cantidad de retos son para el área de la comunicación (56%), identificando la menor cantidad de retos en el factor de disponibilidad (8%). La Fig. 5 muestra la clasificación completa.

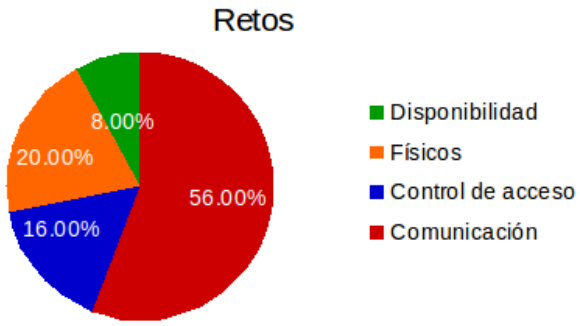

Figura 5. Clasificación de retos.

Los principales retos identificados para la comunicación fueron: estandarizar servicios de cifrado, estandarizar protocolos, establecer mecanismos anti-espionaje, asegurar las conexiones de extremo a extremo, garantizar la confidencialidad e integridad de los datos, implementar el protocolo DTLS (Datagram Transport Layer Security) y aprender políticas de seguridad.

b) Contramedidas: Las contramedidas son los mecanismos empleados para prevenir una amenaza o defenderse de un ataque. En temas de seguridad no se puede garantizar que alguna medida de protección sea 100% efectiva, debido a ello, se dedican muchas horas de investigación al rededor del mundo para tratar de proteger al mayor grado posible los sistemas de información y las redes de comunicaciones. En lo referente a IoT también se han desarrollado una cantidad considerable de contramedidas donde la mayoría son para proteger las comunicaciones (66.67%), y el menor porcentaje corresponde a la disponibilidad (6.06%). La Fig. 6 muestra la clasificación completa.

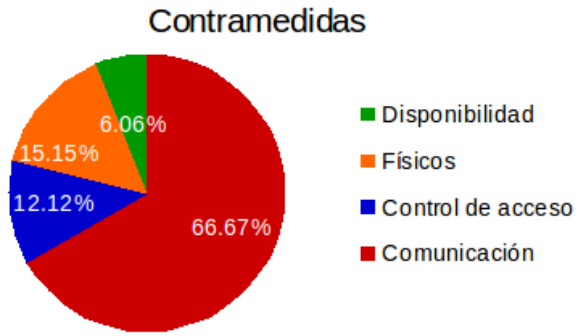

Figura 6. Clasificación de contramedidas.

Las principales acciones que se están realizando para proteger las comunicaciones son: protocolos de seguridad y algoritmos de cifrado ligeros, protocolos de enrutamiento, técnicas de enrutamiento, técnicas para preservar la privacidad, técnicas de minería de datos, esquemas de cifrado, extensión de

seguridad para DNS, códigos de autenticación de mensajes, tecnología de firma digital, estandarización de códigos.

B. *Resumen de Análisis por Factor*

Como resultado del análisis de los cuatro factores dentro de las cinco áreas, se presentan estos factores ordenados de acuerdo a los porcentajes totales obtenidos.

1) Comunicación: Ocupa el porcentaje mas alto en 4 de las 5 áreas. A pesar de que ocupa el mayor porcentaje en cuanto a amenazas, también se tiene contemplado como el principal reto y se está trabajando mucho en contramedidas.

2) Control de acceso: Tiene el mayor porcentaje en el área de amenazas, sin embargo al relacionar esas amenazas con la cantidad de ataques el porcentaje baja a menos de la mitad, aunque aún así, las contramedidas se quedan por debajo de los ataques.

3) Seguridad física: Tiene el segundo porcentaje mas alto en 3 de las 5 áreas. Sí es una gran preocupación pero el porcentaje de ataques no es muy alto y sí se tiene considerada una cantidad aceptable de contramedidas.

4) Disponibilidad: Aparece con el porcentaje mas bajo en 3 de las 5 áreas, pero ocupa el segundo lugar en ataques. Aunque el porcentaje de amenazas es poco, el de ataques es considerable y no existe una gran cantidad de contramedidas ni se considera como uno de los principales retos.

V. Conclusiones y trabajo futuro

En este trabajo se presentó una revisión sistemática de literatura para conocer el estado actual de la seguridad en IoT, centrándose en identificar áreas para categorizar factores de seguridad. La propuesta de áreas son: preocupaciones, amenazas, retos, ataques y contramedidas. Esta propuesta de áreas permitió una clasificación de cuatro factores comunes a éstas: disponibilidad, seguridad física, control de acceso y comunicación.

Como resultado de las áreas identificadas y de sus factores comunes, se identifico que el área de la comunicación es el factor que más se presenta dentro de las cinco áreas con un promedio de aparición de 49.13%. Dentro de este factor, las preocupaciones, amenazas, retos, ataques y contramedidas convergen hacia temas de cifrado, de los cuales se detectaron: 1) preocupaciones, amenazas y ataques (fuga de información, pérdida de confidencialidad, comunicaciones no protegidas, falta de cifrado de transporte, rastreo de paquetes, interceptación de mensajes, etc.) y 2) retos y contramedidas (estandarizar servicios de cifrado y descifrado, implementar protocolo DTLS, soporte para algoritmos de confidencialidad fuertes, asegurar conexiones de extremo a extremo, diseñar algoritmos de cifrado ligeros, esquemas de cifrado simétricos y asimétricos, etc.).

Por otro lado, en último lugar con un promedio de aparición de 12.9% en las áreas propuestas se encuentra el factor de disponibilidad. Abordándose temas comunes a las cinco áreas como son: denegación de servicio y denegación de servicio distribuida.

Como resultado de este trabajo de investigación puede observarse que el crecimiento de IoT va aumentando de forma muy acelerada y la seguridad debe ir a la par, ya que actualmente se están dejando temas de lado como lo es el factor de disponibilidad, siendo un aspecto fundamental en cualquier tipo de sistema.

Finalmente, cabe mencionar que a lo largo del análisis de los estudios primarios no se encontró una clasificación estandarizada para categorizar los aspectos de seguridad en IoT, por lo tanto, como resultado de este trabajo, se obtuvo y propuso una clasificación de cinco áreas y cuatro factores que permitan realizar dicho análisis y que servirán para añadir otros factores de seguridad que surjan a través del tiempo.

Como trabajo futuro, se llevarán a cabo análisis enfocados en cada una de las áreas propuestas de una manera mas especifica hacia aspectos de hardware y software en el IoT. Además, se pretende desarrollar un catálogo basado en estos resultados.

Agradecimientos

Esta investigación ha sido posible gracias al apoyo de CONACyT, a través de una beca de posgrado.

Referéncias Bibliográficas

[1] N. Figuerola, “Seguridad en Internet de las cosas Estado del Arte,” 2014.

[2] A. F. A. Rahman, M. Daud, and M. Z. Mohamad, “Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework,” *Proc. Int. Conf. Internet things Cloud Comput. - ICC ’16*, pp. 1–5, 2016.

[3] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, “Handling a trillion (unfixable) flaws on a billion devices,” *Proc. 14th ACM Work. Hot Top. Networks - HotNets-XIV*, pp. 1–7, 2015.

[4] Hewlett-Packard, “Internet of Things Research Study 2015 Report,” p. 6, 2015.

[5] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, “On perspective of security and privacy-preserving solutions in the internet of things,” *Comput. Networks*, vol. 102, pp. 83–95, 2016.

[6] C. Zhang and R. Green, “Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack over IoT Network,” in *Proceedings of the 18th Symposium on Communications & Networking*, 2015, pp. 8–15.

[7] S. Singh and N. Singh, “Internet of Things(IoT): Security Challenges, Business Opportunities & Reference Architecture for E-commerce,” in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 1577–1581.

[8] T. Xu, J. B. Wendt, and M. Potkonjak, “Security of IoT systems: Design challenges and opportunities,” in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2014, pp. 417–423.

[9] C. Tankard, “The security issues of the Internet of Things,” *Comput. Fraud Secur.*, vol. 2015, no. 9, pp. 11–14, 2015.

[10] B. Kitchenham, “Procedures for performing systematic reviews,” *Keele, UK, Keele Univ.*, vol. 33, no. TR/SE-0401, p. 28, 2004.

APÉNDICE A

[S1] S. Alam, M. M. R. Chowdhury, and J. Noll, "Interoperability of security-enabled Internet of Things," *Wirel. Pers. Commun.*, vol. 61, no. 3, pp. 567–586, 2011.

[S2] N. Cam-Winget, A.-R. Sadeghi, and Y. Jin, "Invited - Can IoT Be Secured: Emerging Challenges in Connecting the Unconnected," *Proc. 53rd Annu. Des. Autom. Conf.*, p. 122:1--122:6, 2016.

[S3] X. Caron, R. Bosua, S. B. Maynard, and A. Ahmad, "The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective," *Comput. Law Secur. Rev.*, vol. 32, no. 1, pp. 4–15, Feb. 2016.

[S4] Y. Ding, X. W. Zhou, Z. M. Cheng, and F. H. Lin, "A security differential game model for sensor networks in context of the internet of things," *Wirel. Pers. Commun.*, vol. 72, no. 1, pp. 375–388, 2013.

[S5] L. Galluccio, A. Leonardi, G. Morabito, and S. Palazzo, "Context Privacy in the Internet of Things," in *Trustworthy Internet*, Milano: Springer Milan, 2011, pp. 61–73.

[S6] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the IP-based Internet of Things," *Wirel. Pers. Commun.*, vol. 61, no. 3, pp. 527–542, 2011.

[S7] Y. H. Hwang, "IoT Security & Privacy: Threats and Challenges," in *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security - IoTPTS '15*, 2015, pp. 1–1.

[S8] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wirel. Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[S9] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A Standardization Perspective," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 265–275, Jun. 2014.

[S10] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things Security 'Hands-On,'" *IEEE Secur. Priv.*, vol. 14, no. 1, pp. 37–46, Jan. 2016.

[S11] C. Liu, "Securing networks in the internet of things era," *Comput. Fraud Secur.*, vol. 2015, no. 4, pp. 13–16, 2015.

[S12] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the internet of things," *Comput. Networks*, vol. 102, pp. 83–95, 2016.

[S13] J. Niu, Y. Jin, A. J. Lee, R. Sandhu, W. Xu, and X. Zhang, "Panel Security and Privacy in the Age of Internet of Things: Opportunities and Challenges," in *Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies - SACMAT '16*, 2016, pp. 49–50.

[S14] A. F. A. Rahman, M. Daud, and M. Z. Mohamad, "Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework," *Proc. Int. Conf. Internet things Cloud Comput. - ICC '16*, pp. 1–5, 2016.

[S15] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[S16] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," *Proc. 52nd Annu. Des. Autom. Conf. - DAC '15*, vol. 17, pp. 1–6, 2015.

[S17] R. Savola, H. Abie, and M. Sihvonen, "Towards Metrics-Driven Adaptive Security Management in E-Health IoT Applications," *Proc. 7th Int. Conf. Body Area Networks*, vol. 250241, no. SeTTIT, pp. 276–281, 2012.

[S18] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, 2015.

[S19] D. Singh, G. Tripathi, and A. Jara, "Secure layers based architecture for Internet of Things," *IEEE World Forum Internet Things, WF-IoT 2015 - Proc.*, pp. 321–326, 2015.

[S20] S. Singh and N. Singh, "Internet of Things(IoT): Security Challenges, Business Opportunities & Reference Architecture for E-commerce," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 1577–1581.

[S21] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno, "A decentralized approach for security and privacy challenges in the Internet of Things," *2014 IEEE World Forum Internet Things, WF-IoT 2014*, pp. 67–72, 2014.

[S22] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, and Y. Xiong, "Security and Privacy in the Internet of Vehicles," *2015 Int. Conf. Identification, Information, Knowl. Internet Things*, pp. 116–121, 2015.

[S23] C. Tankard, "The security issues of the Internet of Things," *Comput. Fraud Secur.*, vol. 2015, no. 9, pp. 11–14, 2015.

[S24] J. Veijalainen, D. Kozlov, and Y. Ali, "Security and Privacy Threats in IoT Architectures," *Proc. 7th Int. Conf. Body Area Networks*, no. International Conference on Body Area Networks, pp. 256–262, 2012.

[S25] R. H. Weber, "Internet of things: Privacy issues revisited," *Comput. Law Secur. Rev.*, vol. 31, no. 5, pp. 618–627, 2015.

[S26] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2014, pp. 417–423.

[S27] S. Yoon, H. Park, and H. S. Yoo, "Security Issues on Smarthome in IoT Environment," in *Computer Science and its Applications: Ubiquitous Information Technologies*, vol. 330, 2015, pp. 691–696.

[S28] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices," *Proc. 14th ACM Work. Hot Top. Networks - HotNets-XIV*, pp. 1–7, 2015.

[S29] C. T. Zenger, J. Zimmer, M. Pietersz, J. Posielek, and C. Paar, "Exploiting the Physical Environment for Securing the Internet of Things," in *NSPW '15 Proceedings of the 2015 New Security Paradigms Workshop*, 2015, pp. 44–58.

[S30] C. Zhang and R. Green, "Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack over IoT Network," in *Proceedings of the 18th Symposium on Communications & Networking*, 2015, pp. 8–15.

[S31] Z.-K. Zhang, M. C. Y. Cho, and S. Shieh, "Emerging Security Threats and Countermeasures in IoT," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security - ASIA CCS '15*, 2015, pp. 1–6.