UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO DE SISTEMAS

CARRERA:

INGENIERÍA DE SISTEMAS

TEMA:

"SEGURIDAD DE INFORMACIÓN EN IOT Y BIG DATA, UN MAPEO SISTEMÁTICO"

AUTOR:

Joseline Roxana Neira Melendrez

TUTOR:

Msg. Máximo Giovani Tandazo Espinoza

Abril 2021
GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **Joseline Roxana Neira Melendrez**, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

Joseline Neira

Nombre: Joseline Roxana Neira Melendrez
CI. 0930939939

Msc. Maximo Tandazo Espinoza
C.I. 0916028921
Firma.

Seguridad de Información en IoT y Big Data, un mapeo sistemático

Abstract. Se revisaron propuestas científicas para conocer la situación bibliográfica de estas áreas de investigación que convergen. El problema es la obtención y análisis de información sobre artículos científicos de primer nivel en tema de seguridad de información en IoT y Big Data que ayude en la orientación y situación en bibliotecas virtuales como ACM, Springer, IEEE Xplore y Web Of Science. El objetivo es realizar una revisión bibliográfica para conocer la situación de la seguridad de información en IoT y Big Data mediante un mapeo sistemático en los últimos 5 años. La metodología utilizada fue la investigación exploratoria y analítica para la obtención de los artículos científicos; además el mapeo sistemático propuesto por Petersen para la clasificación y obtención de resultados sobre el tema de búsqueda; la búsqueda se orienta a categorizar los hallazgos de divulgaciones científicas. Esta investigación resultó una identificación de artículos científicos disponibles en las bibliotecas virtuales sobre seguridad de información, IoT y Big Data; una clasificación de los artículos científicos sobre seguridad de información aplicados a IoT y Big Data mediante mapeo sistemático; un análisis de los resultados de la revisión sistemática. Se concluyó que la seguridad de la información es importante en muchas áreas científicas y empresariales, los entornos públicos generan gran cantidad de datos y estos datos deben ser procesados con las respectivas seguridades; de acuerdo a nuestros resultados ACM con el 49% de documentos relevantes, es una buena alternativa para búsqueda sobre Seguridad de información en IoT y Big Data, además ACM es una estructura especializada en tecnologías de información.

Scientific proposals were revised to understand the bibliographical status of these areas of research that converge. The problem is obtaining and analyzing information on top-level scientific articles on information security in IoT and Big Data that helps in the orientation and situation in virtual libraries such as ACM, Springer, IEEE Xplore and Web Of Science. The objective is to know the situation of information security in IoT and Big Data through a systematic mapping in the last 5 years. The methodology used was exploratory and analytical research to obtain scientific articles; in addition, the systematic mapping proposed by Petersen for the classification and obtaining of results on the search topic; the search is aimed at categorizing the findings of scientific disclosures. This research resulted in the identification of scientific articles available in virtual libraries on information security, internet of things and big data; classification of scientific articles by systematic mapping; and analysis and interpretation of the results of the systematic review using the critical criterion regarding the bibliographic reference. It was concluded that information security is important in many scientific and business areas, public environments generate a large amount of data and this data must be processed with the respective security; According to our results, ACM with 49% of relevant documents, is a good alternative for searching on Information Security in IoT and Big Data, in addition ACM is a structure specialized in information technologies.

Keywords: Information Security, IoT, Big Data, Systematic mapping.

1 Introducción

De acuerdo a [1] para el 2030 existirán 125 billones de dispositivos conectados a internet; de aquí nace Internet of Things (IoT) que tiene importante influencia en muchas áreas y organizaciones; es necesaria la seguridad y privacidad de toda la información porque son generados, procesados, revisados por personas y dispositivos[2].

Una buena característica de IoT es que los dispositivos generan, ceden, monitorean y procesan datos; los datos en cualquier formato se envían y se almacenan en la nube; Iot se utiliza en áreas como deporte, enseñanza, comercialización, infraestructura, servicios, salud[3], manufactura, edificios, ciudades inteligentes, redes de servicio eléctrico, redes de servicio de agua, infraestructura y residencia[4].

Los activos de información son valoradas en las organizaciones; Big Data analiza el impacto de estos grandes volúmenes de datos generados en redes sociales, sistemas de información, hardware, comercialización, enseñanza, ciudad inteligente, fabricación de productos, negocios digitales, entre otros[5].

La seguridad de información se basa en estándares o procedimientos[6]; algunos de esos estándares son: International Organization for Standardization (ISO) 27001, ISO 27032, National Institute of Standards and Technology (NIST), International Information System Security Certification Consortium (ISC), Control Objectives for Information and Related Technologies (COBIT), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Health Information Trust Alliance (HITRUST), North American Electric Reliability Corporation (NERC)[7].

El problema es la obtención y análisis de información sobre artículos científicos de primer nivel en tema de seguridad de información en IoT y Big Data que ayude en la orientación y situación en bibliotecas virtuales como ACM, Springer, IEEE Xplore y Web Of Science.

¿Por qué es necesario realizar un mapeo sistemático de seguridad de información en IoT y Big Data?

Para conocer parte de la situación bibliográfica de la seguridad de información sobre estos conceptos IoT y Big Data; conocer que estándares de seguridad se han aplicado a IoT y Big Data; conocer el impacto de este tema en las bibliotecas de primer nivel, países, áreas de aplicación, años de publicación, entre otros.

El objetivo es realizar una revisión bibliográfica para conocer la situación de la seguridad de información en IoT y Big Data mediante un mapeo sistemático en los últimos 5 años.

La metodología utilizada es la investigación exploratoria y analítica para la obtención de los artículos científicos; además el mapeo sistemático propuesto por Petersen[8] para la clasificación y obtención de resultados sobre el tema de búsqueda; la búsqueda se orienta a categorizar los hallazgos de divulgaciones científicas.

2 Materiales and Métodos

2.1 Materiales

En la sección materiales describimos conceptos sobre seguridad de información, IoT, Big Data y referencias en la utilización de IoT y Big Data.

Seguridad de información. Los lineamientos ayudan a obtener el costo y beneficios en procesos de seguridad; el modelo propuesto analiza las practicas, estándares y riesgos, también asiste en el impacto del hardware y software[6]. Los modelos de seguridad de información ayudan en auditoría del área informática; auditan las estrategias para minimizar los riesgos y aumentar las política de seguridad[7]. Se considera la Confidencialidad, Integridad y Disponibilidad son importantes en la ciberseguridad[9]. Entre los estándares de seguridad tenemos los siguientes: ISO 27000, GSM Association, Open Web Application Security Project, Publicly Available Specification[10].

IoT. Una arquitectura IoT de tres capas propuesta en [3] tiene las siguientes capas: sensores, red, servicios y aplicaciones; estas capas tienen estándares internacionales. En arquitecturas IoT de tres, cuatro y cinco capas; las capas más utilizadas son sensores o percepción, red, servicios o middleware, aplicación o negocios; algunas áreas que se aplica IoT es salud, servicios varios y dominios inteligentes[11].

Big Data. IoT genera datos de producto y servicios que Big data los analiza; para realizar el análisis la plataforma debe ser escalable, contar con almacenamiento distribuido, tener tolerancia a fallos y procesos eficientes[5]. Minimizar las amenazas a la privacidad personal, mitigar las intimidaciones a la seguridad pública y mantener los datos sensibles a los ataques son desafíos que la seguridad de la información tiene en Big Data; algunas estrategias para aumentar la seguridad son: encriptación de los datos, uso de clave, aplicar filtros, respaldos, dividir procesos, interfaces diferentes, aplicaciones más seguras, leyes para el uso de datos[12]. Otros recomiendan implementar leyes para gobiernos, ciudadanos y proveedores; técnicas de privacidad, anonimato en la entrega de datos públicos, mitigar el daño a los datos, planes de vigilancia física o medidas lógicas para proteger los servidores y medios de comunicación; es necesario implementar métodos de protección a la información de Big Data[13].

IoT y Big Data. En [14] se propuso una infraestructura donde IoT se usa para generación y transporte de datos, Big Data se usa para procesamiento de datos; aumentaron la confianza de datos en tres fases. El mapeo sistemático se utilizó en [15] para comparar arquitecturas Big Data que corrigen problemas de IoT; la clasificación y análisis de referencias resultó en 16 artículos en 7 clasificaciones: artículos, problemas, área, arquitectura, características de arquitectura, exploración y tecnología. Existe una relación entre IoT y Big Data, los procesos que se aplican en ambos son: análisis de datos, métodos de análisis, aplicaciones de para volúmenes de datos, tipos de arquitectura; las

áreas donde se utilizan IoT y Big Data son: tráfico, electricidad, servicios, abastecimientos, agricultura y redes; existe la oportunidades o aprovechamiento como: ciudades, salud, comercialización y logística[16].

2.2 Métodos

Alcance de esta investigación. Se utiliza la investigación exploratoria y analítica para la obtención de los artículos científicos; además el mapeo sistemático propuesto por Petersen[8] para la clasificación y obtención de resultados sobre el tema de búsqueda; la búsqueda se orienta a categorizar los hallazgos y frecuencia de divulgaciones científica.

Peterson define las siguientes fases:

- Plantear las preguntas de investigación
- Ejecutar la búsqueda bibliográfica
- Seleccionar los artículos científicos o conferencias
- Clasificar los artículos científicos o conferencias
- Analizar e interpretar los datos tabulados

Fase 1: Plantear las preguntas de investigación

Table 1. Preguntas con sus posibles respuestas.

	Pregunta	Datos a obtener
P1	¿Cuál es la cantidad de documentos potenciales desde enero 2016 a noviembre 2020 en la búsqueda propuesta?	Cantidad de documentos por biblioteca virtuales
P2	¿Cuál es la cantidad de documentos relevantes?	Cantidad de documentos por años y citaciones por documento
P3	¿Cuáles son los tipos de documentos localizados?	Tipos de documentos por biblioteca virtual
P4	¿En qué áreas de aplicación están los documentos localizados?	Áreas de aplicación

Fase 2: Ejecutar la búsqueda bibliográfica

Las bases de datos *Association for Computing Machinery (ACM), SPRINGER, IEEE XPLORE y Web Of Science (WOS)* fueron utilizadas para la búsqueda de artículos científicos; las palabras claves para la búsqueda son: information security, IoT, Big Data; la búsqueda bibliográfica es de artículos científicos desde enero-1-2016 hasta noviembre-21-2020; se exceptúan los libros o capítulos de libro que soliciten pago por ver.

Para la proximidad y selección de los documentos hacia la búsqueda, se examinaron los títulos y los resúmenes de cada documento, verificando su pertinencia después de la búsqueda general, luego se seleccionaron de acuerdo a: documentos duplicados, títulos no pertinentes.

Búsqueda final en ACM:

[Publication Title: information security in IoT and big data] AND [Publication Date: (01/01/2016 TO 11/30/2020)]; resultó 79552

Publisher only ACM: 35219
Journal: 2275
Types: 942
Selection: 26

Búsqueda final en IEEE Xplore:

("All Metadata":Information Security, IoT, Big Data)
Filters Applied: 2016 – 2020; resultó 461
Security of data: 81
"Document Title":Security IoT Big Data): 7

Búsqueda final en SPRINGER:

'Information AND Security, AND IoT, AND Internet AND of AND Things, AND Big AND Data' within 2016 – 2020; resultó 3664
Articles: 2285
Discipline Computer Science: 939
Subdiscipline Computer Science General: 309
Selection: 11

Búsqueda final en WOS:

Database: Web of Science Core Collection
TOPIC: (Information Security IoT Big Data) OR TITLE: (Information Security, IoT, Big Data); Timespan: Last 5 years. Indexes: SCI-EXPANDED, SSCI, A&HCI, ESCI; Resultó 167
Articles 139
Open access 55
TITLE: (Security IoT Big Data)
Timespan: Last 5 years. Indexes: SCI-EXPANDED, SSCI, A&HCI, ESCI.
Selection: 9

3 Resultados

En base a los objetivos específicos del anteproyecto se propusieron los siguientes resultados y dentro de cada resultado se desarrollan las preguntas de investigación:

- Identificación de artículos científicos disponibles en las bibliotecas virtuales sobre seguridad de información, IoT y Big Data.
- Clasificación de los artículos científicos sobre seguridad de información aplicados a IoT y Big Data mediante mapeo sistemático.
- Análisis de los resultados de la revisión sistemática mediante el criterio crítico.

3.1 Identificación de artículos científicos disponibles en las bibliotecas virtuales sobre seguridad de información, IoT y Big Data.

En este primer resultado damos la respuesta a la primera pregunta de investigación.

P1: ¿Cuál es la cantidad de documentos potenciales desde enero 2016 a noviembre 2020 en la búsqueda propuesta?
En la Tabla 2, en cada fila están los datos de cada biblioteca virtual consultada, la columna Documentos Potenciales son los totales de búsqueda desde 2016 al 2020 por cada biblioteca; después cada columna contiene el detalle por cada año.

Tabla 2. Documentos por biblioteca.

Biblioteca	Doc. Potenciales	2016	2017	2018	2019	2020
ACM	79,552	21,064	18,064	16,674	14,544	9,206
IEEE XPLORE	461	18	70	93	142	138
SPRINGER	3,664	578	922	381	618	1,165
WOS	167	6	10	25	66	60

3.2 Clasificación de los artículos científicos sobre seguridad de información aplicados a IoT y Big Data mediante mapeo sistemático.

En este segundo resultado damos la respuesta a la segunda, tercera y cuarta pregunta de investigación.

P2: ¿Cuál es la cantidad de documentos relevantes?
Después de los filtros y selecciones aplicadas en la sección métodos se obtuvieron las cantidades expresadas en Tabla 3; cada fila corresponde a los últimos 5 años; cada columna corresponde a cada biblioteca revisada; en total está la cantidad de documentos relevantes por cada biblioteca.

Tabla 3. Documentos por biblioteca.

Año	ACM	IEEE XPLORE	SPRINGER	WOS
2016	6	0	2	1
2017	8	3	2	1
2018	3	0	4	1
2019	5	3	1	4
2020	4	1	2	2
Total	26	7	11	9

La cantidad de citaciones promedio (Fig. 1) se determinó así: por cada biblioteca virtual se sumó la cantidad de citaciones que están en la bibliografía de cada documento, y esta suma se dividió para la cantidad de documentos relevantes.

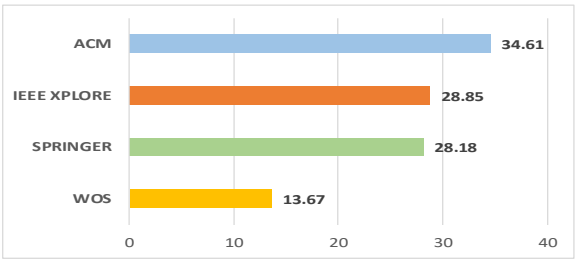

Fig. 1. Cantidad de citaciones promedio por biblioteca.

P3: ¿Cuáles son los tipos de documentos localizados?
Los diferentes tipos de documentos por biblioteca son presentados en Tabla 4; cada fila es el tipo de documento y cada columna es la biblioteca clasificada.

Tabla 4. Documentos por biblioteca.

Tipo de documento	ACM	IEEE XPLORE	SPRINGER	WOS
Conference	10	3		
Journal	16	3	8	6
Editorial material				2
Magazine		1		
Review			3	1

La tabla 5 presentamos las referencias clasificadas por tipo de documento y biblioteca; 3 son conferencia, 33 son artículos científicos.

Tabla 5. Referencias por biblioteca.

Tipo de documento	ACM	IEEE XPLORE	SPRINGER	WOS
Conference	[17], [18], [19], [20], [21], [22], [23], [24], [25], [26]	[27], [28],[29]		
Journal	[30],[31],[32],[33],[34],[35], [36],[37],[38],[39],[40],[41], [42], [43], [44], [45]	[46],[47], [48]	[49],[50],[51], [52], [53], [54], [55], [56]	[57], [58], [59], [60], [61], [62]
Editorial material				[63], [64]
Magazine		[65]		
Review			[66], [67],[68],	[69]

P4: ¿En qué áreas de aplicación están los documentos localizados?
Las distintas áreas donde se aplicó seguridad para IoT y Big Data están clasificadas en Tabla 6; cada fila es un área y cada columna es una biblioteca.

Tabla 6. Áreas de aplicación por biblioteca.

Áreas	ACM	IEEE XPLORE	SPRINGER	WOS
Security and privacy	15		5	
Security and Protection	2			
Cloud computing	1			
Computer Science		2	4	4
Chemistry Analytical				1
Energy		1		1
Information Storage and Retrieval	1			
Information systems	4			
Instrumentation				1
Networks	3	3	2	2
Tourism		1		

3.3 Análisis de los resultados de la revisión sistemática mediante el criterio crítico.

La mayor cantidad de ***documentos potenciales*** después de la búsqueda la tiene ACM que contiene 79552 documentos, recordemos que es "una plataforma especializada en tecnologías de información" por ello la gran cantidad de documentos; luego SPRINGER resultó con 3664 documentos, esta biblioteca cubre áreas como medicina, ingenierías y ciencias sociales; luego IEEE resultó con 461 documentos, esta es una biblioteca de información científico-tecnológico de las ingenierías; WOS resultó con 167, esta biblioteca cubre áreas como ciencias exactas y sociales. De acuerdo a la exploración realizada a estos temas potenciales, son demasiados generalizados o no se relacionan directamente con todas las palabras de búsqueda; muchos son temas aislados sobre Seguridad o IoT o Big Data, por esta razón hay gran cantidad de documentos.

La Fig. 2 expresa la cantidad de ***documentos relevantes*** por biblioteca, la información pertenece a la Tabla2 que son los documentos ya filtrados o seleccionados; aquí ACM tiene 26 documentos, SPRINGER tiene 11 documentos, WOS tiene 9 documentos, IEEE tiene 7 documentos; es decir ACM tiene el 49% de la información buscada sobre el tema (Fig. 3), IEEE tiene el 13% la menor cantidad de documentos. Además, ACM tiene 34.61 citaciones promedio por documento, y WOS tiene 13.67 citaciones promedio por documento. De acuerdo a estos resultados ACM es la mejor biblioteca con mayor información.

El principal ***tipo de documento localizado*** es Journal con 33 documentos en las 4 bibliotecas, es decir el 62.26% de documentos relevantes son temas muy específicos e investigaciones recientes, son escritos por expertos para expertos.

El siguiente es tipo es Conference con 13 documentos, es decir el 20.63% son documentos de encuentros científicos que compartieron o discutieron avances en el tema de búsqueda.

El siguiente es tipo Review con 4 documentos, es decir el 7.54% son estudios descriptivo y críticos desde una perspectiva seccional o conjuntiva, no son documentos originales, pero si contienen información sobre el tema específico.

El siguiente es tipo Editorial Material con 2 documentos, es decir el 3.77% son artículos de opiniones por personas o grupos.

El ultimo tipo es Magazine con 1 documento, es decir el 1.88% son publicaciones periódicas sobre el tema buscado.

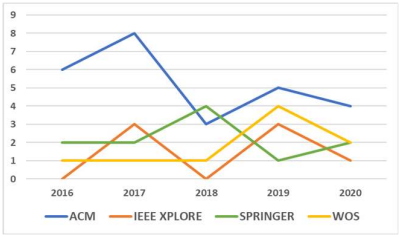

Fig. 2. Publicaciones por biblioteca

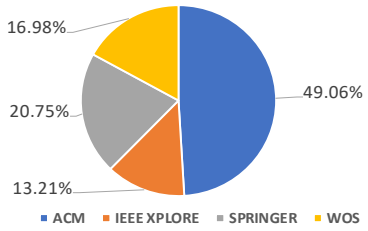

Fig. 3. Impacto de temas

La principal ***área de aplicación*** de los documentos relevantes es Seguridad y Privacidad con 20 documentos, es decir 37.74% trabajaron sobre tecnologías que aumentan la posibilidad de garantizar la protección y que los datos sean accedidos por sus propios dueños. En el área Ciencias de la Computación aplicaron 10 documentos, en área Redes aplicaron 10 documentos, es decir cada área tiene 18.87% para mejorar fundamentos teóricos o asegurar comunicaciones en IoT y Big Data.

4 Discusión

- Relación de los resultados: los artículos científicos disponibles en las bibliotecas virtuales sobre el tema de búsqueda fueron identificados desde localización macro a micro; estos artículos potenciales fueron clasificados y filtrados mediante mapeo sistemático; el análisis de los resultados demuestra las proporciones e impacto del tema en las bibliotecas virtuales.
- Generalizaciones de los resultados: hemos mostrado nuestros resultados en tablas y gráficos autodescriptivos para que el lector entienda en menor tiempo los objetivos del presente documento.
- Excepciones: en nuestra investigación no se consideró sinónimos como Privacidad, Volumen de Datos, Datos Grandes, Interconexión de Objetos; sólo nos limitamos a 4 bibliotecas virtuales ACM, IEEE Xplore, Springer y WOS; la Universidad Politécnica Salesiana también tiene acceso a SCOPUS y Science Direct.
- Sobre el tema de búsqueda existe información de más de 5 años, ACM tiene documentos potenciales desde 2010, IEEE tiene documentos desde 2011, Springer tiene documentos desde 2010, WOS tiene documentos desde el 2014.
- ACM ofrece información en línea sobre la cantidad de citaciones y número de veces que el documento sea bajado, además algunos documentos tienen anexado archivos de video, imágenes, pdf y archivos empaquetados; WOS ofrece la cantidad de veces que el documento ha sido citado y cantidad de veces bajadas.

- Como consecuencia teórica de nuestra propuesta esperamos que los resultados puedan ser un apoyo en la toma de decisión para abordar el tema de seguridad de información en entornos IoT y Big Data, y dar a conocer el impacto sobre estas bibliotecas revisadas.

5 Conclusiones

- Se concluyó que la seguridad de la información es importante en muchas áreas científicas y empresariales, los entornos públicos generan gran cantidad de datos y estos datos deben ser procesados con las respectivas seguridades; de acuerdo a nuestros resultados ACM con el 49% de documentos relevantes, es una buena alternativa para búsqueda sobre Seguridad de información en IoT y Big Data, además ACM es una estructura especializada en tecnologías de información.
- En IoT los dispositivos públicos o privados pueden contener datos sensibles, la seguridad trata de mitigar los ataques; en Big Data el nivel de seguridad es ajustado al valor de la información para proteger la privacidad.
- Estos temas tienen su convergencia en la recolección, almacenamiento y procesamiento de la información; es necesario aplicar seguridades a los datos en todas sus etapas.

Acknowledgment

Thanks to Universidad Politécnica Salesiana del Ecuador (Sede Guayaquil).

References

1. Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., Ming, H.: AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. 2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019. 305–310 (2019). https://doi.org/10.1109/CCWC.2019.8666450
2. Lv, Z., Qiao, L.: Analysis of healthcare big data. Futur. Gener. Comput. Syst. 109, 103–110 (2020). https://doi.org/10.1016/j.future.2020.03.039
3. Strielkina, A., Illiashenko, O., Zhydenko, M., Uzun, D.: Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. In: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). pp. 67–73. IEEE (2018)
4. Minoli, D., Sohraby, K., Occhiogrosso, B.: IoT Security (IoTSec) Mechanisms for e-Health and Ambient Assisted Living Applications. Proc. - 2017 IEEE 2nd Int. Conf. Connect. Heal. Appl. Syst. Eng. Technol. CHASE 2017. 13–18 (2017). https://doi.org/10.1109/CHASE.2017.53
5. Rahul, K., Banyal, R.K.: Data Life Cycle Management in Big Data Analytics. Procedia Comput. Sci. 173, 364–371 (2020). https://doi.org/10.1016/j.procs.2020.06.042
6. Rathod, P., Hamalainen, T.: A Novel Model for Cybersecurity Economics and Analysis. IEEE CIT 2017 - 17th IEEE Int. Conf. Comput. Inf. Technol. 274–279 (2017). https://doi.org/10.1109/CIT.2017.65

7. Sabillon, R., Serra-Ruiz, J., Cavaller, V., Cano, J.: A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). In: 2017 International Conference on Information Systems and Computer Science (INCISCOS). pp. 253–259. IEEE (2017)
8. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic Mapping Studies in Software Engineering. 1–10 (2007). https://doi.org/10.14236/ewic/EASE2008.8
9. Parekh, G., DeLatte, D., Herman, G.L., Oliva, L., Phatak, D., Scheponik, T., Sharman, A.T.: Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. IEEE Trans. Educ. 61, 11–20 (2018). https://doi.org/10.1109/TE.2017.2715174
10. Brass, I., Tanczer, L., Carr, M., Elsden, M., Blackstock, J.: Standardising a Moving Target: The Development and Evolution of IoT Security Standards. SSRN Electron. J. 2018, 1–9 (2018). https://doi.org/10.2139/ssrn.3437681
11. Lu, Y., Xu, L. Da: Internet of things (IoT) cybersecurity research: A review of current research topics. IEEE Internet Things J. 6, 2103–2115 (2019). https://doi.org/10.1109/JIOT.2018.2869847
12. Yang, M., Zhou, X., Zeng, J., Xu, J.: Challenges and solutions of information security issues in the age of big data. China Commun. 13, 193–202 (2016). https://doi.org/10.1109/CC.2016.7445514
13. Shamsi, J.A., Khojaye, M.A.: Understanding privacy violations in big data systems. IT Prof. 20, 73–81 (2018). https://doi.org/10.1109/MITP.2018.032501750
14. Pouryazdan, M., Fiandrino, C., Kantarci, B., Soyata, T., Kliazovich, D., Bouvry, P.: Intelligent Gaming for Mobile Crowd-Sensing Participants to Acquire Trustworthy Big Data in the Internet of Things. IEEE Access. 5, 22209–22223 (2017). https://doi.org/10.1109/ACCESS.2017.2762238
15. Cravero, A.: Big data architectures and the internet of things: A systematic mapping study. IEEE Lat. Am. Trans. 16, 1219–1226 (2018). https://doi.org/10.1109/TLA.2018.8362160
16. Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I.A.T., Siddiqa, A., Yaqoob, I.: Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. IEEE Access. 5, 5247–5261 (2017). https://doi.org/10.1109/ACCESS.2017.2689040
17. Khan, L.: Big IoT Data Stream Analytics with Issues in Privacy and Security. 22–22 (2018). https://doi.org/10.1145/3180445.3180455
18. Davoudian, A., Liu, M.: Big Data Systems: A Software Engineering Perspective. ACM Comput. Surv. 53, (2020). https://doi.org/10.1145/3408314
19. El Haourani, L., El Kalam, A.A., Ouahman, A.A.: Big Data security and privacy techniques. ACM Int. Conf. Proceeding Ser. (2020). https://doi.org/10.1145/3386723.3387841
20. Laassiri, J.: Data security and risks for IoT in intercommunicating objects. ACM Int. Conf. Proceeding Ser. Part F129474, 1–4 (2017). https://doi.org/10.1145/3090354.3090357
21. Hajiheydari, N., Talafidaryani, M., Khabiri, S.H.: IoT Big data value map: How to generate value from IoT data. ACM Int. Conf. Proceeding Ser. 98–103 (2019). https://doi.org/10.1145/3312714.3312728
22. Boulakbech, M., Messai, N., Sam, Y., Devogele, T., Hammoudeh, M.: IoT mashups : From IoT big data to IoT big service. ACM Int. Conf. Proceeding Ser. Part F130522, (2017). https://doi.org/10.1145/3102304.3102324
23. Das, S.K., Yamana, H.: Securing big data and IoT networks in smart cyber-physical environments. ACM Int. Conf. Proceeding Ser. Part F130526, 189–194 (2017). https://doi.org/10.1145/3128128.3128157
24. Shantha Mary Joshitta, R., Arockiam, L., Sheba Kezia Malarchelvi, P.D.: Security analysis of SAT_JO lightweight block cipher for data security in healthcare IoT. ACM Int. Conf. Proceeding

Ser. 111–116 (2019). https://doi.org/10.1145/3358505.3358527
25. Venkatraman, S., Overmars, A., Fahd, K., Parvin, S., Kaspi, S.: Security Challenges for Big Data and IoT. ACM Int. Conf. Proceeding Ser. (2020). https://doi.org/10.1145/3378904.3378907
26. Morales, G.D.F., Bifet, A., Khan, L., Gama, J., Fan, W.: IoT big data stream mining. Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min. 13-17-August-2016, 2119–2120 (2016). https://doi.org/10.1145/2939672.2945385
27. Saenko, I., Kotenko, I., Kushnerevich, A.: Parallel Processing of Big Heterogeneous Data for Security Monitoring of IoT Networks. Proc. - 2017 25th Euromicro Int. Conf. Parallel, Distrib. Network-Based Process. PDP 2017. 329–336 (2017). https://doi.org/10.1109/PDP.2017.45
28. Duncan, B., Whittington, M., Chang, V.: Enterprise security and privacy: Why adding IoT and big data makes it so much more difficult. Proc. 2017 Int. Conf. Eng. Technol. ICET 2017. 2018-January, 1–7 (2017). https://doi.org/10.1109/ICEngTechnol.2017.8308189
29. Toapanta, S.M.T., Romero, H.X.H., Saltos, N.S.M., Gallegos, L.E.M.: Prototype of a security model applied to IoT with big data for tourist management in the cities of Ecuador. Proc. 3rd World Conf. Smart Trends Syst. Secur. Sustain. WorldS4 2019. 147–152 (2019). https://doi.org/10.1109/WorldS4.2019.8904016
30. Chatterjee, U., Chakraborty, R.S., Mukhopadhyay, D.: A PUF-based secure communication protocol for IoT. ACM Trans. Embed. Comput. Syst. 16, (2017). https://doi.org/10.1145/3005715
31. Tiloca, M., Nikitin, K., Raza, S.: Axiom: DTLS-based secure IoT group communication. ACM Trans. Embed. Comput. Syst. 16, 1–29 (2017). https://doi.org/10.1145/3047413
32. Tabrizi, F.M., Pattabiraman, K.: Design-level and code-level security analysis of IoT devices. ACM Trans. Embed. Comput. Syst. 18, (2019). https://doi.org/10.1145/3310353
33. Shukla, S.K.: Editorial: Security of mobile devices. ACM Trans. Embed. Comput. Syst. 16, (2017). https://doi.org/10.1145/3129534
34. Li, J., Li, T., Liu, Z., Chen, X.: Secure deduplication system with active key update and its application in IoT. ACM Trans. Intell. Syst. Technol. 10, (2019). https://doi.org/10.1145/3356468
35. Siboni, S., Shabtai, A., Tippenhauer, N.O., Lee, J., Elovici, Y.: Advanced security testbed framework for wearable IoT devices. ACM Trans. Internet Technol. 16, (2016). https://doi.org/10.1145/2981546
36. Jiang, X., Lora, M., Chattopadhyay, S.: An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices. ACM Trans. Internet Technol. 20, (2020). https://doi.org/10.1145/3379542
37. Bertino, E., Choo, K.K.R., Georgakopolous, D., Nepal, S.: Internet of things (IoT): Smart and secure service delivery. ACM Trans. Internet Technol. 16, 1–7 (2016). https://doi.org/10.1145/3013520
38. Konstantinidis, A., Irakleous, P., Georgiou, Z., Zeinalipour-Yazti, D., Chrysanthis, P.K.: IoT data prefetching in indoor navigation SOAs. ACM Trans. Internet Technol. 19, (2018). https://doi.org/10.1145/3177777
39. Anagnostopoulos, N.A., Ahmad, S., Arul, T., Steinmetzer, D., Hollick, M., Katzenbeisser, S.: Low-cost Security for Next-generation IoT Networks. ACM Trans. Internet Technol. 20, (2020). https://doi.org/10.1145/3406280
40. Li, Y., Gai, K., Ming, Z., Zhao, H., Qiu, M.: Intercrossed access controls for secure financial services on multimedia big data in cloud systems. ACM Trans. Multimed. Comput. Commun. Appl. 12, 1–18 (2016). https://doi.org/10.1145/2978575
41. Ye, C., Ling, H., Xiong, Z., Zou, F., Liu, C., Xu, F.: Secure social multimedia big data sharing using scalable JFE in the TSHWT Domain. ACM Trans. Multimed. Comput. Commun. Appl. 12,

(2016). https://doi.org/10.1145/2978571
42. Berti-Equille, L., Ba, M.L.: Veracity of big data: Challenges of cross-modal truth discovery. J. Data Inf. Qual. 7, 10–12 (2016). https://doi.org/10.1145/2935753
43. Taherkordi, A., Eliassen, F., Horn, G.: From IoT big data to IoT Big Services. Proc. ACM Symp. Appl. Comput. Part F128005, 485–491 (2017). https://doi.org/10.1145/3019612.3019700
44. Saunier, L., Delic, K.: Big data: corporate security is a big data problem. Ubiquity. 2018, 1–11 (2018). https://doi.org/10.1145/3242149
45. Celik, Z.B., Fernandes, E., Pauley, E., Tan, G., McDaniel, P.: Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities. arXiv. 52, (2018)
46. Sollins, K.R.: IoT big data security and privacy versus innovation. IEEE Internet Things J. 6, 1628–1635 (2019). https://doi.org/10.1109/JIOT.2019.2898113
47. Li, F., Li, H., Wang, C., Ren, K., Bertino, E.: Guest editorial special issue on security and privacy protection for big data and IoT. IEEE Internet Things J. 6, 1446–1449 (2019). https://doi.org/10.1109/JIOT.2019.2908460
48. Li, F., Xie, R., Wang, Z., Guo, L., Ye, J., Ma, P., Song, W.: Online Distributed IoT Security Monitoring with Multidimensional Streaming Big Data. IEEE Internet Things J. 7, 4387–4394 (2020). https://doi.org/10.1109/JIOT.2019.2962788
49. Tu, L., Liu, S., Wang, Y., Zhang, C., Li, P.: An optimized cluster storage method for real-time big data in Internet of Things. J. Supercomput. 76, 5175–5191 (2020). https://doi.org/10.1007/s11227-019-02773-1
50. Zhou, Z., Tsang, K.F., Zhao, Z., Gaaloul, W.: Data intelligence on the Internet of Things. Pers. Ubiquitous Comput. 20, 277–281 (2016). https://doi.org/10.1007/s00779-016-0912-1
51. Zang, L., Yu, Y., Xue, L., Li, Y., Ding, Y., Tao, X.: Improved dynamic remote data auditing protocol for smart city security. Pers. Ubiquitous Comput. 21, 911–921 (2017). https://doi.org/10.1007/s00779-017-1052-y
52. Jesse, N.: Internet of Things and Big Data: the disruption of the value chain and the rise of new software ecosystems. AI Soc. 33, 229–239 (2018). https://doi.org/10.1007/s00146-018-0807-y
53. Sun, Y., Bie, R., Thomas, P., Cheng, X.: New advances in data, information, and knowledge in the Internet of Things. Pers. Ubiquitous Comput. 20, 653–655 (2016). https://doi.org/10.1007/s00779-016-0955-3
54. Choi, J., In, Y., Park, C., Seok, S., Seo, H., Kim, H.: Secure IoT framework and 2D architecture for End-To-End security. J. Supercomput. 74, 3521–3535 (2018). https://doi.org/10.1007/s11227-016-1684-0
55. Wu, J. xing, Li, J. hua, Ji, X. sheng: Security for cyberspace: challenges and opportunities. Front. Inf. Technol. Electron. Eng. 19, 1459–1461 (2018). https://doi.org/10.1631/FITEE.1840000
56. Velzen, J.T. van: Securing the Insecurable? Datenschutz und Datensicherheit-DuD. 613–616 (2017)
57. Stergiou, C., Psannis, K.E., Gupta, B.B., Ishibashi, Y.: Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT. Sustain. Comput. Informatics Syst. 19, 174–184 (2018). https://doi.org/10.1016/j.suscom.2018.06.003
58. Vardhan, Manu; Kumar, M.: Special Issue on Security and Privacy Issues in Cloud Computing, Big Data and IoT Technology: Current Progress and Future Directions Preface. Int. J. Inf. Secur. Priv. 13, (2019)
59. Sollins, K.R.: IoT Big Data Security and Privacy Versus Innovation. IEEE Internet Things J. 6, 1628–1635 (2019). https://doi.org/10.1109/JIOT.2019.2898113

60. Li, F., Xie, R., Wang, Z., Guo, L., Ye, J., Ma, P., Song, W.: Online Distributed IoT Security Monitoring With Multidimensional Streaming Big Data. IEEE Internet Things J. 7, 4387–4394 (2020). https://doi.org/10.1109/JIOT.2019.2962788
61. Li, F., Li, H., Wang, C., Ren, K., Bertino, E.: Guest Editorial Special Issue on Security and Privacy Protection for Big Data and IoT. IEEE Internet Things J. 6, 1446–1449 (2019). https://doi.org/10.1109/JIOT.2019.2908460
62. Amanullah, M.A., Habeeb, R.A.A., Nasaruddin, F.H., Gani, A., Ahmed, E., Nainar, A.S.M., Akim, N.M., Imran, M.: Deep learning and big data technologies for IoT security. Comput. Commun. 151, 495–517 (2020). https://doi.org/10.1016/j.comcom.2020.01.016
63. Shinzaki, Takashi; Morikawa, Ikuya; Yamaoka, Yuji; Sakemi, Y.: IoT Security for Utilization of Big Data: Mutual Authentication Technology and Anonymization Technology for Positional Data. FUJITSU Sci. Tech. J. 52, (2016)
64. Chin, W.-L., Li, W., Chen, H.-H.: Energy Big Data Security Threats in IoT-Based Smart Grid Communications. IEEE Commun. Mag. 55, 70–75 (2017). https://doi.org/10.1109/MCOM.2017.1700154
65. Chin, W.L., Li, W., Chen, H.H.: Energy Big Data Security Threats in IoT-Based Smart Grid Communications. IEEE Commun. Mag. 55, 70–75 (2017). https://doi.org/10.1109/MCOM.2017.1700154
66. Colombo, P., Ferrari, E.: Access control technologies for Big Data management systems: literature review and future trends. Cybersecurity. 2, (2019). https://doi.org/10.1186/s42400-018-0020-9
67. Sharma, A., Kaur, J., Singh, I.: Internet of Things (IoT) in Pharmaceutical Manufacturing, Warehousing, and Supply Chain Management. SN Comput. Sci. 1, 1–10 (2020). https://doi.org/10.1007/s42979-020-00248-2
68. Abi Sen, A.A., Eassa, F.A., Jambi, K., Yamin, M.: Preserving privacy in internet of things: a survey. Int. J. Inf. Technol. 10, 189–200 (2018). https://doi.org/10.1007/s41870-018-0113-4
69. Tariq, N., Asim, M., Al-Obeidat, F., Zubair Farooqi, M., Baker, T., Hammoudeh, M., Ghafir, I.: The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey. Sensors. 19, 1788 (2019). https://doi.org/10.3390/s19081788