UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO DE SISTEMAS

CARRERA:

INGENIERÍA DE SISTEMAS

TEMA:

“MAPEO SISTEMÁTICO: LA SEGURIDAD DE LA INFORMACIÓN EN DISPOSITIVOS IOT PARA EL SECTOR BANCARIO”

AUTOR:

Emely Shirley Vásquez Castro

TUTOR:

Msg. Máximo Giovani Tandazo Espinoza

Noviembre 2021

GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **EMELY SHIRLEY VÁSQUEZ CASTRO**, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

Firma del autor
Emely Shirley Vásquez Castro
CI. 0921874939

Firma del tutor
Msc. Máximo Giovani Tandazo Espinoza
CI. 0916028921

Mapeo Sistemático: La seguridad de la información en dispositivos IoT para el sector bancario

Máximo Giovani Tandazo Espinoza[1][0000-0002-8844-9384] and Emely Shirley Vásquez Castro [1][0000-0002-6323-7772]

[1] Carrera de Ingeniería de Sistemas, Universidad Politécnica Salesiana, Guayaquil, Ecuador
mtandazo@ups.edu.ec, evasquezc2@est.ups.edu.ec

Abstract. Esta investigación trata de ser un aporte para el área académica, científica y profesional sobre IoT en un dominio que es posiblemente sensible. El objetivo es conocer las diferentes medidas de seguridad de la información adoptadas o creadas en dispositivos IoT para el sector bancario. La metodología que se aplicó es el mapeo sistemático que es utilizado en la exploración médica e ingeniería, genera un informe de investigación estructurado con resultados clasificados o categorizados; es útil con resúmenes visuales o mapas, además con representaciones generales. Esta investigación resultó en un aporte el conocimiento sobre capas, categorías de seguridades y protocolos utilizados en arquitecturas IoT. Se concluyó que los dispositivos como primera línea de captación de datos aplican seguridad, pero no todas las arquitecturas especifican la seguridad de información en sus diferentes capas; el mapeo sistemático resultó en 32 publicaciones clasificadas, aquí el 44% de las arquitecturas se realizaron en modelos de 3 capas, las capas más utilizadas son Dispositivos en 14%, Red en 17%, y Aplicación en 11%; la categoría en seguridad de información más utilizada es Blockchain en 23% y Encriptación 14%.

Palabras claves: IoT, Banking domain, Information security, Systematic mapping.

1 Introducción

Las instituciones financieras utilizan de forma estratégica las Tecnologías de Información (*TI*) para brindar y gestionar los servicios bancarios escalables; el procesamiento de información es un factor de impulso en las finanzas a través de arquitecturas o plataformas informáticas; las *TI* se aprovechan para promover la bancarización de las actividades económicas y generar más movimiento de dinero; los bancos gestionan sus propias infraestructuras tecnológicas o la comparten para conexión y procesamiento de datos entre sucursales, cajeros automáticos, puntos de atención, entre otros; las infraestructuras bancarias reciben, envían, almacenan y procesan los datos entre los diferentes tipos de servicios para clientes, proveedores, accionistas y empleados administrativos[1].

Internet de las Cosas (*IoT*) es una parte de *TI*, *IoT* se basa en dispositivos o sensores que capturan datos de servicios, bienes o personas; los datos capturados se envían a Internet para su procesamiento y disponibilidad; las empresas utilizan *IoT* para optimizar las operaciones, funcionalidades del cliente y precios de servicios/productos; los bancos quieren obtener el valor de las finanzas en las empresas construidas sobre activos intangibles; existen dos oportunidades de *IoT* para los bancos: a) utilidad de los datos obtenidos por los sensores para incluir a los clientes y valorar la solvencia; b) relación estratégica con empresas en la fabricación de sensores para generar servicios de pago; además los principales componentes de una *IoT* son sensores, conectividad, procesamiento de datos e interfaz de usuario[2].

IoT es un ambiente que contiene nodos para capturar datos del mundo real y enviarlos a través de internet a almacenamiento en la nube o centros de datos, las aplicaciones informáticas están diseñadas para servicios a clientes o terceros; la digitalización de servicios bancarios exige plantear infraestructura tecnológica para obtener más clientes, estos servicios deben ser operativos, escalables y seguros en los datos que gestionan; la Fig. 1 muestra los principales componentes de una *IoT* bancaria que brinda servicios para clientes[1].

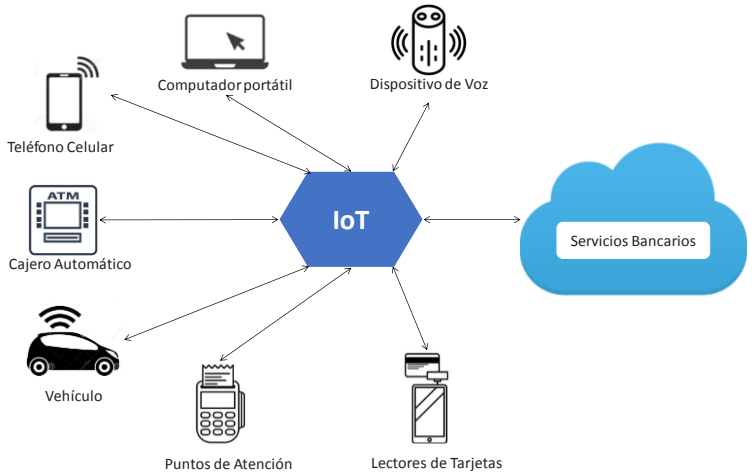

Fig. 1. IoT en domino bancario.

Las redes *IoT* permiten comunicación instantánea de la economía digital, la confiabilidad/seguridad es un desafío o preocupación; por lo general, los dispositivos *IoT* son de características limitadas en recursos y procesamiento[3].

De acuerdo a [1], existen tres tipos de seguridad en *IoT*: Seguridad de Información, Seguridad Física y Seguridad Administrativa; esta investigación se centra en la "Seguridad de Información".

Algunos de los problemas de seguridad en IoT son: accesos no autorizados, no aplicar seguridad en el diseño del dispositivo, los usuarios no actualizan las versiones, falta de confianza en las redes, inconvenientes en el cifrado, mal uso de puertos, falta

de auditorías. El impacto de la seguridad se refleja en la confidencialidad, integridad y disponibilidad de la información[4].

Los principales requisitos de una IoT son la confianza y la seguridad; los fabricantes y empresas de servicios tienen la responsabilidad en la protección de red IoT; pocas personas se inquietan por el nivel de seguridad al conectarse a esta clase de red, entre más económicos son los elementos de la red es menor el nivel de seguridad[5].

Algunas seguridades aplicadas en IoT generales son: framework, autenticación, encriptación[6], machine learning[7], reconocimiento facial[8], protocolos[9], entre otros.

Esta investigación trata de categorizar las seguridades de información aplicadas a dispositivos IoT en el dominio bancario, estos datos se encuentran en los artículos científicos de las bibliotecas virtuales.

El objetivo es conocer las diferentes medidas de seguridad de la información adoptadas o creadas en dispositivos IoT para el sector bancario mediante un mapeo sistemático.

2 Materiales y Métodos

2.1 Materiales

Otros conceptos de IoT: Infraestructura para obtener servicios a través de conexiones de dispositivos tecnológicos; dispositivos interconectados que capturan y comparten datos para un posterior análisis[10]. Tiene impacto en la sociedad, cada vez son más las cosas/dispositivos que transmiten datos previamente capturados[11].

IoT en el dominio bancario: El hardware portátil permite realizar consumos y pagos, el Barclays Bank con matriz en Londres tiene una solución en este tipo de hardware; el Idea Bank tiene vehículos con dispositivos IoT con cajeros automáticos para acercarse a los clientes, los depósitos aumentaron tres veces en relación a los cajeros estacionarios; los dispositivos IoT utilizan blockchain para aumentar la seguridad y privacidad de los datos, los bancos garantizan la inmutabilidad de los datos en esta red; los dispositivos que capturan imágenes y datos ayudan a entender las interacciones del cliente en las financieras, las expresiones faciales del cliente son utilizadas para evaluar la experiencia del cliente o seguimiento de amenazas; Chase Bank creó una plataforma IoT para servicio a clientes al llegar a un cajero automático, Barclays Bank utiliza IoT para asistencia de pasajeros discapacitados; Capital One con matriz en Estados Unidos utiliza Amazon Alexa para pagar las facturas de los clientes, Starling con matriz en Reino Unido utiliza Google Home para verificar saldos y elaborar pagos a través de la voz; Ant Financial captura los datos generados por una IoT y los analiza con IA para verificación de documentos en seguros de clientes, este análisis es en tiempo real; ICICI Bank utiliza un sistema de vigilancia basado en IoT e IA para comunicar el paso de intrusos mediante la captura de datos y el análisis; el monitoreo de un bien material a través de IoT permite el arrendamiento y establecer un modelo financiero[1]. El presupuesto de bancos que destinan a inversión en IoT es $117.4 millones; por lo general los bancos son las primeras instituciones en adoptar nuevas

tecnologías, el potencial de IoT en la banca es muy alto y genera nuevos servicios a los clientes basados en su comportamiento o patrones en las transacciones[2].

Trabajos de mapeo sistemático sobre IoT en varios dominios: El objetivo de [10] es conocer los componentes en la gestión de datos generados en IoT en dominio Big Data y optimizar los procesos en la producción agrícola; formularon 7 preguntas de investigación, se encontraron 400 trabajos de IoT y Big Data y los trabajos filtrados son 14; en las categorizaciones de procesos encontraron bodegaje, distribuciones y producción de fruta; entre los componentes de arquitecturas encontrados están sensores, conexiones, almacenamiento, procesos, análisis y visualizar.

La calidad de redes IoT fue revisada en [11], aquí se plantearon 6 preguntas de investigación, la exploración fue en 4 bibliotecas, en la primera búsqueda obtuvieron 29964 publicaciones y después de las filtraciones obtuvieron 478 publicaciones; la clasificación resultó en publicaciones de: calidad, rendimiento, seguridad, privacidad y pruebas; además IoT se utiliza en salud, ciudades, hogar, industria, energía, vestuario, edificios, logística, militar, transporte, aprendizaje, entre otros.

El objetivo de [12] es la revisión de niveles de servicios en aplicaciones informáticas IoT, entre las actividades se categorizaron las publicaciones, identificación en la falta de investigaciones en este dominio, se especificaron 8 preguntas de investigación, se revisaron 5 librerías digitales, encontraron 3269 publicaciones y con la clasificación obtuvieron 328 publicaciones; los tipos de investigaciones encontradas son soluciones, evaluaciones, validaciones, propuestas conceptuales; las contribuciones encontradas son framework, métodos, métricas y herramientas.

La clasificación de los desafíos en IoT de [13] resultó en lo siguiente: oportunidad en 27 publicaciones, comunicaciones en 22 publicaciones, interoperabilidad en 11 publicaciones, seguridad en 9 publicaciones, privacidad en 12 publicaciones, y desarrollo en 11 publicaciones.

Para revisar el modelado de procesos en IoT, en el artículo [14] se analizaron 600 documentos, en la clasificación obtuvieron 36 modelados diferentes; el estándar BPMN es utilizado en 73.33% de los casos, otros modelados utilizados son UMLAD, BPEL, Petri Nets y EPC.

La calidad de servicios para Cloud Computing en entorno IoT es revisada y categorizada en [15], después de analizar 509 documentos se obtuvo 59 documentos relevantes; en la clasificación se determinó contribuciones sobre servicios en 15%, lenguajes para servicios en 18%, framework en 22%, aplicación de modelos en 22%, y determinación de parámetros en 16%.

En la revisión de plataformas asistidas por el ambiente en entorno IoT [16], entre 7 bibliotecas virtuales se obtuvieron 711 documentos y después del filtrado se obtuvo 35 documentos; en la categorización las plataformas más utilizadas son framework en 34%, además obtuvieron 15 requerimientos para la implementación de estas plataformas.

2.2 Métodos

El mapeo sistemático ***MS*** es una metodología utilizada en la exploración médica e ingeniería, genera un informe de investigación estructurado con resultados clasifica-

dos o categorizados; es útil con resúmenes visuales o mapas, además con representaciones generales[17]. *MS* también es llamado cartografía sistemática, el *MS* entrega un panorama general sobre una investigación específica a través de filtros, clasificación, resultados cuantitativos, cualitativos de acuerdo a categorías; la búsqueda se orienta a literaturas para conocer el alcance sobre un tema y lugares de publicación; cabe recalcar que el *MS* es diferente a una revisión sistemática en los objetivos, enfoques y análisis; la fortaleza de un *MS* es estructurar un área de investigación[18].

Se aplica el MS a la *seguridad de la información en dispositivos IoT para el dominio bancario* en espera de conocer las medidas de seguridad que se utilizan en IoT; la Fig. 2 muestra los pasos para implementar la metodología, los pasos principales son las preguntas de investigación, realizar la búsqueda de documentos, discriminación de documentos, verificación de palabras claves, y extracción de datos; cada paso genera un resultado que se presenta en el lado derecho del gráfico.

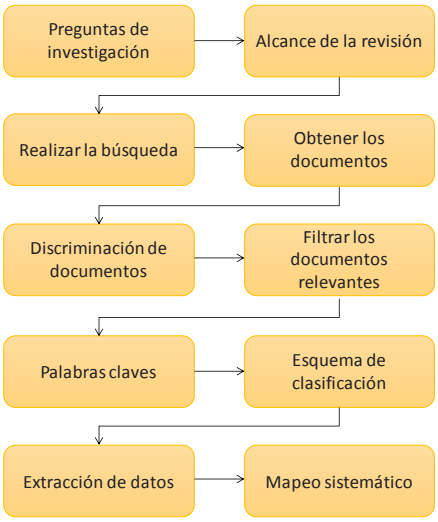

Fig. 2. Procesos del Mapeo Sistemático.

La búsqueda se plantea en bibliotecas virtuales que la Universidad Politécnica Salesiana tiene acceso:

Table 1. Bibliotecas de consulta.

Biblioteca	URL
ACM	https://bibliotecas.ups.edu.ec:3396/
Scopus	https://bibliotecas.ups.edu.ec:2226/search/form.uri?display=basic#basic
Science Direct	https://bibliotecas.ups.edu.ec:2230/
Springer	https://bibliotecas.ups.edu.ec:3401/

Las palabras claves para la exploración en las bibliotecas son: Security IoT Bank, Security IoT Finance, IoT Bank, IoT Finance.

Paso 1: Preguntas de investigación:

1. ¿Cuántas capas se utilizan en arquitecturas IoT y cuáles son las más utilizadas?
2. ¿Qué categorías se utilizan en seguridad de información?
3. ¿Cuáles son los protocolos más utilizados para seguridad de información?
4. ¿Cuáles son las características de las publicaciones?

Paso 2: Realizar la búsqueda

El siguiente paso es identificar las publicaciones en las bases de datos científicas ya establecidas anteriormente; la tabla 2 presenta las cadenas de búsqueda con los filtros aplicados y la cantidad de publicaciones obtenidas desde año 2017; los filtros se aplicaron de acuerdo a los parámetros permitidos por la plataforma científica; los primeros resultados generales son conferencias, revistas, capítulos de libros, libros, talleres, entre otros.

Table 2. Búsqueda en bibliotecas.

Biblioteca	Cadena de búsqueda	Resultados
ACM	All: security iot bank] AND [Publication Date: (01/01/2017 TO 04/30/2021)	40,969
	Filtro: Research article	31,825
	Filtro: Journal	4,334
	Reproducibles: Artifacts Evaluated & Functional	82
Scopus	TITLE-ABS-KEY (iot AND bank) AND PUBYEAR > 2016 AND PUBYEAR < 2021	236
	AND (LIMIT-TO (SUBJAREA , "COMP"))	177
	AND (LIMIT-TO (OA , "all"))	25
Science Direct	IoT Bank	2,968
	Years 2017..2021	2,149
	Computer Science	944
Springer	'IoT AND bank' within 2017 - 2021	2,068
	Discipline: Computer Science	888
	Sub Discipline: Information Systems Applications (incl. Internet)	216

Paso 3: Discriminación de documentos

De la búsqueda inicial se obtuvo un conjunto 46,241publicaciones, éstas son generales no necesariamente coinciden en los términos de búsqueda principal “IoT Bank”; son resultados que tienen una coincidencia con al menos una palabra de la búsqueda, por esto es necesario continuar con el filtro de acuerdo a la facilidad de cada base de datos; después de los filtros se obtuvieron 1,267 publicaciones.

Paso 4: Palabras claves

A estas 1,267 publicaciones se aplica la exclusión de título y resumen, al no encontrar las palabras claves en la revisión de título y resúmenes, se utilizan solo dos clases[12]: Relevante (R) en caso que título y el resumen están claros o de acuerdo a "IoT Bank"; No relevante (NR) en caso que el título y el resumen no esté claro o no esté de acuerdo al objetivo de esta investigación.
Dentro de esta revisión de los títulos, resúmenes y texto completo se aplicaron los criterios de inclusión y exclusión[18]; la lectura completa de una publicación fue necesaria en casos mínimos; entre las publicaciones existen propuestas de solución, investigación de verificación, publicaciones conceptuales, publicaciones de evaluación, y publicaciones de experiencia; los criterios aplicados son los siguientes:

Criterios de inclusión:

- Las publicaciones presentan algún resultado como arquitectura, método, modelo conceptual, marco, herramientas, caso de estudio, entre otros;
- Las publicaciones son del área IoT, banca, finanzas o comercio;
- Las publicaciones están entre enero 2017 a Abril 2020;
- Publicaciones de acceso abierto;
- Publicaciones en idioma inglés;

Criterios de exclusión:

- Publicaciones de mapeo sistemático o revisiones bibliográficas;
- Publicaciones duplicadas entre las bibliotecas de consulta;
- Publicaciones que solo presentan resúmenes de conferencias;
- Publicaciones que presenten estados del arte o revisiones;

Los criterios de inclusión se aplicaron en una primera instancia en la revisión del título, resumen y palabras claves para obtener aportes en *seguridad IoT en el área bancaria*; los criterios de exclusión se aplicaron en la segunda instancia en la revisión de resumen, conclusiones e introducción para asegurar publicaciones relevantes en el área de búsqueda; se obtuvieron 32 artículos representados en la Tabla 3 y Fig. 3.

Table 3. Artículos obtenidos.

Biblioteca	Cantidad	Investigaciones
ACM	10	[19], [20], [21], [22], [23], [24], [25], [26], [27], [28]
Scopus	5	[29], [30], [31], [32], [33]
Science Direct	5	[34], [35], [36], [37], [38]
Springer	12	[39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50]

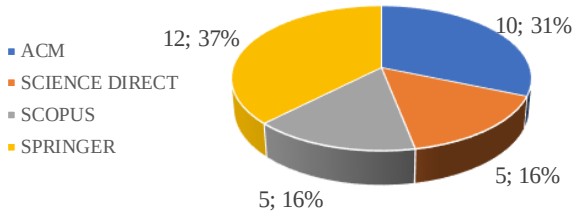

Fig. 3. Publicaciones seleccionadas.

Paso 5: Extracción de datos

En este paso se extraen los datos de los artículos seleccionados para mapear y clasificar las publicaciones que permitan contestar las preguntas de investigación; las publicaciones se organizaron en una hoja de cálculo con los siguientes datos: identificación, título, autores, año de publicación, país de los autores, área de investigación, propuesta, evaluación, caso de estudio, tipo de seguridad, protocolo; una hoja de cálculo similar fue utilizada por [17] y [18]; se realizó una extracción manual y dinámica para luego analizar los datos, aplicar frecuencias y clasificar categorías. El diagrama de burbujas representado en la Fig. 4 informa las frecuencias de protocolos y capas utilizadas en los artículos revisados; el volumen de una burbuja representa la cantidad de artículos en la categoría protocolo o capa; el gráfico de burbujas presenta un mejor entendimiento que las tablas de frecuencia, además genera una descripción general y proporciona un mapa.

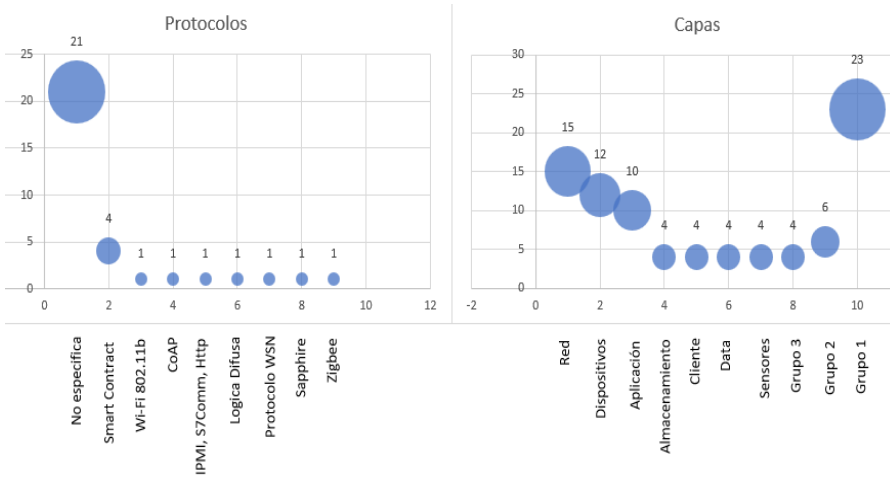

Fig. 4. Mapa sistemático.

3 Resultados

En esta fase se obtuvieron los resultados que son las respuestas a las preguntas de investigación, estas preguntas se realizaron en el paso 1; además se hace un análisis de los datos.

3.1 ¿Cuántas capas se utilizan en arquitecturas IoT y cuáles son las más utilizadas?

Entre las 32 publicaciones seleccionadas, las arquitecturas utilizaron diferentes cantidades de capas o niveles; el 9% utilizaron arquitecturas de 2 Capas (3 publicaciones); el 44% utilizaron arquitecturas de 3 Capas (14 publicaciones); el 28% utilizaron arquitecturas de 4 Capas (9 publicaciones); otro 9% utilizaron arquitecturas de 5 Capas (3 publicaciones); y otro 10% no especificaron ninguna capa (3 publicaciones); aquí la mayoría de arquitecturas utiliza el modelo de 3 capas; la Fig. 5 muestra la utilización de capas.

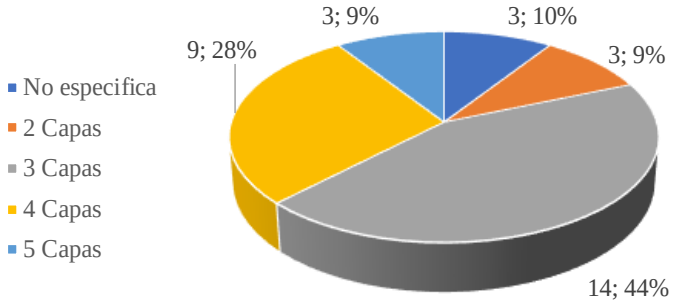

Fig. 5. Cantidad de capas en arquitecturas.

Las capas más nombradas o utilizadas son: La capa Red fue nombrada en 17% (15 veces). La capa Dispositivos fue nombrada 14% (12 veces). La capa Aplicación fue nombrada 11% (10 veces). Las capas Almacenamiento, Cliente, Data y Sensores fueron nombradas 5% cada una (4 veces cada capa). En el grupo 3 están las capas 4 fueron nombradas 5% (3 veces cada capa): Servicios, Servidor, User y se incluyen las no especificadas. En el grupo 2 están las 6 capas que fueron nombradas 7% (2 veces cada capa): Alta, Baja, Blockchain, Intermedia, Nube, Software. En el grupo 1 están las 23 capas que fueron nombradas 27% (una sola vez cada capa): Activadores, Administración, Analysis, Back End, Batch, Cadena, Cloud, Computing , Concenso, Data capture, Data Management, Exposition, Extension, Framework, Gateway, Hardware, Identificación, Middleware, Plataforma, Proveedor, Speed, Transferencia, Report. La Fig. 6 muestra a la capa Red más utilizada en 17%.

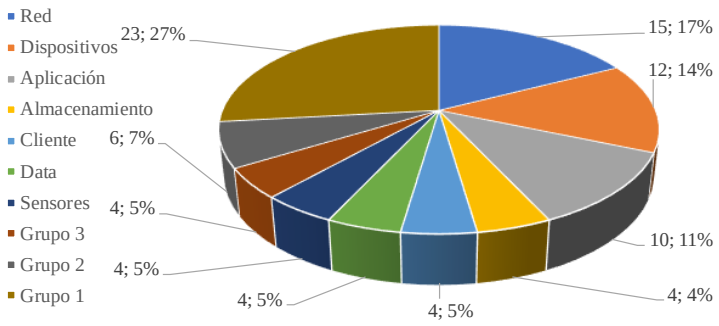

Fig. 6. Capas utilizadas

3.2 ¿Qué categorías se utilizan en seguridad de información?

En las categorías de seguridad de la información, la más utilizada es Blockchain en 23% de las publicaciones (7 publicaciones), la categoría Encriptación es utilizada en 14% de las publicaciones (4 publicaciones), la categoría Biométrico es utilizada en 7% de las publicaciones (2 publicaciones); las categorías Bluetooth, Gateway, Framework, QR Code, Cluster y Filtro fueron utilizadas en 3% de las publicaciones cada una (6 publicaciones). Además, 11 publicaciones no especificaron la seguridad utilizada en la arquitectura IoT. La Fig. 7 muestra Blockchain como más utilizada para seguridad.

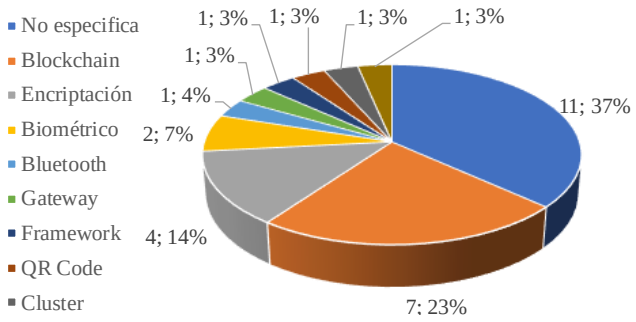

Fig. 7. Categorías en seguridad de información.

3.3 ¿Cuáles son los protocolos más utilizados para seguridad de información?

Entre los protocolos de seguridad utilizados están: Smart Contract en 13% de las publicaciones (4 publicaciones); los protocolos Wi-Fi 802.11b, CoAP, IPMI, S7Comm, Http, KAMSTRUP, SNMP, SSH, Logica Difusa, WSN, Sapphire y Zigbee se utilizan en 3% de las publicaciones cada una (7 publicaciones). Además, el 66% de las publi-

caciones (21 publicaciones) no especificaron el protocolo utilizado en la arquitectura IoT. La Fig. 8 muestra Smart Contract como protocolo más utilizado en las publicaciones revisadas.

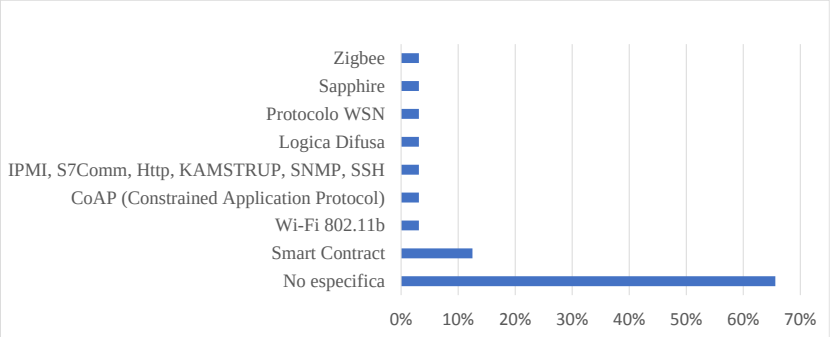

Fig. 8. Protocolos utilizados en seguridades.

3.4 ¿Cuáles son las características de los artículos obtenidos?

Las publicaciones IoT apuntan a varias áreas (Fig. 9), la mayor área es Security and Privacy en 31% (10 publicaciones); Data en 28% (9 publicaciones); Network en 25% (8 publicaciones); Applied computing en 6% (2 publicaciones); Software en 6% (2 publicaciones); Computer systems organization en 3% (1 publicación).

Los tipos de investigaciones (Fig. 10) resultaron en Journal article en 78% (25 publicaciones), Book en 16% (5 publicaciones), y Conference en 6% (2 publicaciones).

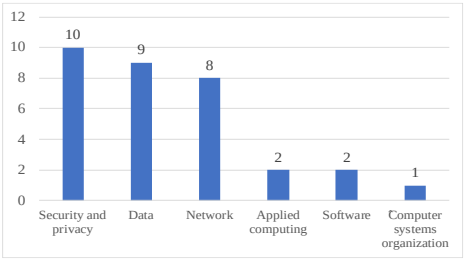

Fig. 9. Áreas de investigaciones.

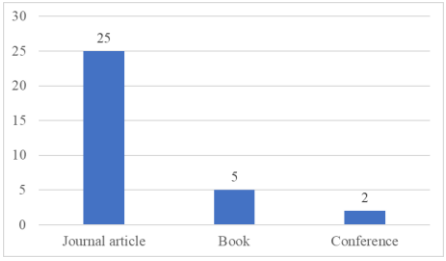

Fig. 10. Tipos de investigaciones.

USA tiene 7 publicaciones científicas de IoT en banca o finanzas; Italia tiene 4 publicaciones; China y Corea tienen 3 publicaciones cada país; Arabia Saudita, Canadá, Marruecos y Pakistán tienen 2 publicaciones cada país; los siguientes países tienen una publicación cada uno: Australia, Dubái, Emiratos Árabes, España, Francia, Hong Kong, India, Irán, Israel, Noruega, Qatar, Reino Unido, Romania, Taiwán y Varsovia.

En 2017 resultó 19% de documentos (6 publicaciones); en 2018 resultó 41% (13 publicaciones); en 2019 resultó 16% (5 publicaciones); en 2020 resultó 16% (5 publicaciones); al 2021 resultaron 9% (3 publicaciones); en la Fig. 12 se resalta el año 2018 con mayores publicaciones de IoT en banca o finanzas.

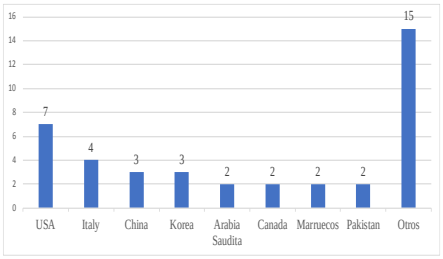

Fig. 11. Países de producción en investigaciones.

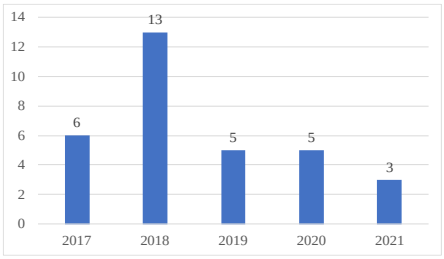

Fig. 12. Producción por años.

4 Discusión

- Las capas utilizadas en arquitecturas IoT fueron especificadas en 90%; las categorías utilizadas en seguridades de información fueron especificadas en 63%; los protocolos utilizados para seguridad fueron especificados sólo en 34%; la biblioteca Springer y el país USA son los mayores publicadores sobre IoT en el dominio bancario.
- Por lo general, la seguridad en la interoperabilidad de los dispositivos es aplicada por estándares generales que son entregados por los fabricantes; las investigaciones detalladas sobre seguridades o desafíos en IoT son documentos más extensos en tiempos, recursos y esfuerzo.
- La cantidad de publicaciones de IoT en el dominio bancario es muy bajo, en relación al avance del sector bancario en las Tecnologías de Información y Comunicación; existen pocos trabajos de mapeo sistemático sobre IoT en el dominio bancario o financiero; no se trató los tiempos y costos en implementación de seguridades en redes IoT.
- Esta investigación puede servir a otros científicos para conocer sobre seguridades en arquitecturas IoT en el dominio bancario, además proponer modelos IoT en base a las 32 referencias seleccionadas.

5 Conclusiones

Se concluyó que los dispositivos como primera línea de captación de datos aplican seguridad, pero no todas las arquitecturas especifican la seguridad de información en sus diferentes capas; el mapeo sistemático resultó en 32 publicaciones clasificadas, aquí el 44% de las arquitecturas se realizaron en modelos de 3 capas, las capas más

utilizadas son Dispositivos en 14%, Red en 17%, y Aplicación en 11%; la categoría en seguridad de información más utilizada es Blockchain en 23% y Encriptación 14%.

El área de mayor publicación es Seguridad y Privacidad en 31% y son documentos de tipo Journal, las arquitecturas IoT en el dominio bancario tienen un buen enfoque aunque en menor cantidad en relación a otros dominios como salud, educación, ciudades entre otros.

Agradecimientos

Gracias a Universidad Politécnica Salesiana del Ecuador (Sede Guayaquil), al grupo de investigación de la sede Guayaquil "Computing, Security and Information Technology for a Globalized World" (CSITGW) creado de acuerdo con resolución 142-06-2017-07-19.

References

1. Ramalingam, H., Venkatesan, V.P.: Conceptual analysis of Internet of Things use cases in Banking domain. IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON. 2019-Octob, 2034–2039 (2019). https://doi.org/10.1109/TENCON.2019.8929473
2. Lande, R.S., Meshram, S.A., Deshmukh, P.P.: Smart banking using IoT. Proc. 2018 3rd IEEE Int. Conf. Res. Intell. Comput. Eng. RICE 2018. 2018-Janua, (2018). https://doi.org/10.1109/RICE.2018.8627903
3. Ugwuanyi, E.E., Ghosh, S., Iqbal, M., Dagiuklas, T.: Reliable resource provisioning using bankers' deadlock avoidance algorithm in MEC for industrial IoT. IEEE Access. 6, 43327–43335 (2018). https://doi.org/10.1109/ACCESS.2018.2857726
4. Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., Ghani, N.: Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Commun. Surv. Tutorials. 21, 2702–2733 (2019). https://doi.org/10.1109/COMST.2019.2910750
5. Rizvi, S., Kurtz, A., Pfeffer, J., Rizvi, M.: Securing the Internet of Things (IoT): A Security Taxonomy for IoT. Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018. 163–168 (2018). https://doi.org/10.1109/TrustCom/BigDataSE.2018.00034
6. Hameed, A., Alomary, A.: Security issues in IoT: A survey. 2019 Int. Conf. Innov. Intell. Informatics, Comput. Technol. 3ICT 2019. (2019). https://doi.org/10.1109/3ICT.2019.8910320
7. Hussain, F., Hussain, R., Hassan, S.A., Hossain, E.: Machine learning in iot security: Current solutions and future challenges. arXiv. 22, 1686–1721 (2019)
8. Balla, P.B., Jadhao, K.T.: IoT Based Facial Recognition Security System. 2018 Int. Conf. Smart City Emerg. Technol. ICSCET 2018. (2018). https://doi.org/10.1109/ICSCET.2018.8537344
9. Mahendra, S., Sathiyanarayanan, M., Vasu, R.B.: Smart security system for businesses using internet of things (iot). Proc. 2nd Int. Conf. Green Comput. Internet Things, ICGCIoT 2018. 424–429 (2018). https://doi.org/10.1109/ICGCIoT.2018.8753101

10. Cravero, A., Lagos, D., Espinosa, R.: Big data / IoT use in wine production: A systematic mapping study. IEEE Lat. Am. Trans. 16, 1476–1484 (2018). https://doi.org/10.1109/TLA.2018.8408444
11. Ahmed, B.S., Bures, M., Frajtak, K., Cerny, T.: Aspects of Quality in Internet of Things (IoT) Solutions: A Systematic Mapping Study. IEEE Access. 7, 13758–13780 (2019). https://doi.org/10.1109/ACCESS.2019.2893493
12. Mubeen, S., Asadollah, S.A., Papadopoulos, A.V., Ashjaei, M., Pei-Breivold, H., Behnam, M.: Management of Service Level Agreements for Cloud Services in IoT: A Systematic Mapping Study. IEEE Access. 6, 30184–30207 (2018). https://doi.org/10.1109/ACCESS.2017.2744677
13. Lepekhin, A., Borremans, A., Ilin, I., Jantunen, S.: A systematic mapping study on internet of things challenges. Proc. - 2019 IEEE/ACM 1st Int. Work. Softw. Eng. Res. Pract. Internet Things, SERP4IoT 2019. 9–16 (2019). https://doi.org/10.1109/SERP4IoT.2019.00009
14. Torres, V., Serral, E., Valderas, P., Pelechano, V., Grefen, P.: Modeling of IoT devices in Business Processes: A Systematic Mapping Study. Proc. - 2020 IEEE 22nd Conf. Bus. Informatics, CBI 2020. 1, 221–230 (2020). https://doi.org/10.1109/CBI49978.2020.00031
15. Girs, S., Sentilles, S., Asadollah, S.A., Ashjaei, M., Mubeen, S.: A Systematic Literature Study on Definition and Modeling of Service-Level Agreements for Cloud Services in IoT. IEEE Access. 8, 134498–134513 (2020). https://doi.org/10.1109/ACCESS.2020.3011483
16. Duarte, P., Coutinho, E.F., Boudy, J., Hariz, M., Viana, W.: Using IoT in AAL Platforms for Older Adults: A Systematic Mapping. Proc. - 2020 IEEE 44th Annu. Comput. Software, Appl. Conf. COMPSAC 2020. 705–710 (2020). https://doi.org/10.1109/COMPSAC48688.2020.0-177
17. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic Mapping Studies in Software Engineering. Presented at the June 1 (2008)
18. Petersen, K., Vakkalanka, S., Kuzniarz, L.: Guidelines for conducting systematic mapping studies in software engineering: An update. Inf. Softw. Technol. 64, 1–18 (2015). https://doi.org/10.1016/j.infsof.2015.03.007
19. Lee, Y.J., Kim, K.S., Lee, H.J.: Demo abstract: Smart piggy bank: In-home banking system for children. Proc. - 2017 IEEE/ACM 2nd Int. Conf. Internet-of-Things Des. Implementation, IoTDI 2017 (part CPS Week). 293–294 (2017). https://doi.org/10.1145/3054977.3057318
20. 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 F1305, (2017). https://doi.org/10.1145/3102304.3102324
21. Zhang, P., Shi, X., Khan, S.U.: Can quantitative finance benefit from IoT? SmartIoT 2017 - Proc. Work. Smart Internet Things. 0–5 (2017). https://doi.org/10.1145/3132479.3132491
22. Kim, B.Y., Choi, S.S., Jang, J.W.: Data managing and service exchanging on IoT service platform based on blockchain with smart contract and spatial data processing. ACM Int. Conf. Proceeding Ser. 59–63 (2018). https://doi.org/10.1145/3209914.3209916

23. Giura, P., Jim, T.: Sapphire: Using network gateways for IoT security. ACM Int. Conf. Proceeding Ser. (2018). https://doi.org/10.1145/3277593.3277611
24. Taherkordi, A., Herrmann, P.: Pervasive Smart Contracts for Blockchains in IoT Systems. In: Proceedings of the 2018 International Conference on Blockchain Technology and Application - ICBTA 2018. pp. 6–11. ACM Press, New York, New York, USA (2018)
25. Ammar, Z., AlSharif, A.: Deployment of IoT-based honeynet model. ACM Int. Conf. Proceeding Ser. 134–139 (2018). https://doi.org/10.1145/3301551.3301586
26. Jaimunk, J.: Privacy-preserving cloud-IoT architecture. Proc. - 2019 IEEE/ACM 6th Int. Conf. Mob. Softw. Eng. Syst. MOBILESoft 2019. 146–147 (2019). https://doi.org/10.1109/MOBILESoft.2019.00029
27. Baba-Cheikh, Z., El-Boussaidi, G., Gascon-Samson, J., Mili, H., Guéhéneuc, Y.G.: A preliminary study of open-source IoT development frameworks. Proc. - 2020 IEEE/ACM 42nd Int. Conf. Softw. Eng. Work. ICSEW 2020. 679–686 (2020). https://doi.org/10.1145/3387940.3392198
28. Luckner, M., Grzenda, M., Kunicki, R., Legierski, J.: IoT Architecture for Urban Data-Centric Services and Applications. ACM Trans. Internet Technol. 20, (2020). https://doi.org/10.1145/3396850
29. Ammirato, S., Sofo, F., Felicetti, A.M., Raso, C.: Bank Branches as Smart Environments: Introducing a Cognitive Protection System to Manage Security and Safety. In: IFIP Advances in Information and Communication Technology. pp. 61–73 (2018)
30. Nita, S., Mihailescu, M., Pau, V.: Security and Cryptographic Challenges for Authentication Based on Biometrics Data. Cryptography. 2, 39 (2018). https://doi.org/10.3390/cryptography2040039
31. Fu, M.-H.: Integrated Technologies of Blockchain and Biometrics Based on Wireless Sensor Network for Library Management. Inf. Technol. Libr. 39, (2020). https://doi.org/10.6017/ital.v39i3.11883
32. Kumar, R.A., Adilakshmi, G., Venkata Hanuman, G.: Face Recognition using Raspberry Pi-3 in IOT. Int. J. Eng. Adv. Technol. 8, 2477–2481 (2019). https://doi.org/10.35940/ijeat.F8557.088619
33. Lee, J., Choi, S., Kim, D., Choi, Y., Sun, W.: A Novel Hardware Security Architecture for IoT Device: PD-CRP (PUF Database and Challenge–Response Pair) Bloom Filter on Memristor-Based PUF. Appl. Sci. 10, 6692 (2020). https://doi.org/10.3390/app10196692
34. Khanboubi, F., Boulmakoul, A., Tabaa, M.: Impact of digital trends using IoT on banking processes. Procedia Comput. Sci. 151, 77–84 (2019). https://doi.org/10.1016/j.procs.2019.04.014
35. Zhao, J.: Corporate Financial Risk Prediction Based on Embedded System and Deep Learning. Microprocess. Microsyst. (2020). https://doi.org/10.1016/j.micpro.2020.103405
36. Khan, M.A., Salah, K.: IoT security: Review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. 82, 395–411 (2018). https://doi.org/10.1016/j.future.2017.11.022
37. Sánchez-Arias, G., González García, C., Pelayo G-Bustelo, B.C.: Midgar: Study of

communications security among Smart Objects using a platform of heterogeneous devices for the Internet of Things. Futur. Gener. Comput. Syst. 74, 444–466 (2017). https://doi.org/10.1016/j.future.2017.01.033

38. Cuomo, S., Di Somma, V., Sica, F.: Analysis of a data-flow in a financial IoT system. In: Procedia Computer Science. pp. 508–512 (2017)
39. Zhuang, Y., Man Leung, A.C., Hughes, J.: Matching in proximity authentication and mobile payment ecosystem: What are we missing? Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 10155 LNCS, 163–172 (2017). https://doi.org/10.1007/978-3-319-62024-4_12
40. Boumlik, A., Bahaj, M.: Big Data and IoT: A Prime Opportunity for Banking Industry. In: Lecture Notes in Networks and Systems. pp. 396–407 (2018)
41. Liao, D., Li, H., Wang, W., Wang, X., Zhang, M., Chen, X.: Achieving IoT data security based blockchain. Peer-to-Peer Netw. Appl. (2021). https://doi.org/10.1007/s12083-020-01042-w
42. Bujari, A., Furini, M., Mandreoli, F., Martoglia, R., Montangero, M., Ronzani, D.: Standards, Security and Business Models: Key Challenges for the IoT Scenario. Mob. Networks Appl. 23, 147–154 (2018). https://doi.org/10.1007/s11036-017-0835-8
43. Cohen, A., Cohen, A., Gurewitz, O.: Secured Data Gathering Protocol for IoT Networks. Springer International Publishing (2018)
44. Li, D., Cai, Z., Deng, L., Yao, X., Wang, H.H.: Information security model of block chain based on intrusion sensing in the IoT environment. Cluster Comput. 22, 451–468 (2019). https://doi.org/10.1007/s10586-018-2516-1
45. Mousavi, S.K., Ghaffari, A., Besharat, S., Afshari, H.: Security of internet of things based on cryptographic algorithms: a survey. Wirel. Networks. 27, 1515–1555 (2021). https://doi.org/10.1007/s11276-020-02535-5
46. Odiete, O., Lomotey, R.K., Deters, R.: Using Blockchain to Support Data and Service Management in IoV/IoT. In: Advances in Intelligent Systems and Computing. pp. 344–362. Springer International Publishing (2018)
47. Alshehri, M.D., Hussain, F.K.: A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). Computing. 101, 791–818 (2019). https://doi.org/10.1007/s00607-018-0685-7
48. Rizvi, S.S.H., Zubair, M., Ahmad, J., Hashmani, M., Khan, M.W.: Wireless Communication as a Reshaping Tool for Internet of Things (IoT) and Internet of Underwater Things (IoUT) Business in Pakistan: A Technical and Financial Review. Wirel. Pers. Commun. 116, 1087–1105 (2021). https://doi.org/10.1007/s11277-019-06937-3
49. Touati, F., Tariq, H., Crescini, D., Mnaouer, A. Ben: Development of Prototype for IoT and IoE Scalable Infrastructures, Architectures and Platforms. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 202–216. Springer International Publishing (2018)
50. Turban, E., Outland, J., King, D., Lee, J.K., Liang, T.-P., Turban, D.C.: Mobile Commerce and the Internet of Things. Presented at the (2018)