IoT Best Practices and their Components: A Systematic Literature Review

C.M. Medina O., J.C. Blandón A., C.M. Zapata J., and J. I. Ríos P.

***Abstract*—Internet of Things (IoT) is a technology that consists of interconnected entities (intelligent physical objects, services and software systems) via the Internet, which serve automatically and in a coordinated way in data management to achieve greater efficiency and productivity in industrial processes and contribute to improve the quality of people life. As the use of devices grows, so do the challenges for creating secure, operable, scalable and cost-effective IoT systems. The specialized literature shows interest in the application of best practices for the construction of IoT systems and so improving the compatibility of hardware and software systems, communication problems, security and privacy. This paper searchs in indexed journals in order to identify best practices and their current components to create IoT systems. The study applies a systematic literature review method implemented in six phases (planning, primary search, preliminary selection, selection, data extraction and analysis) that allows information to be extracted consistently. We obtain 97 papers applying the method to carry out the analysis. The results show there are different proposals that use some mechanism of knowledge representation for the creation or improvement IoT systems. The paper is a theoretical basis for creating better IoT systems in organizations and reducing costs.**

***Index Terms*—Artificial Intelligence, Internet of Things, IoT Best Practices, IoT Components, Systematic Literature Review.**

I. Introducción

La tecnología *IoT (Internet of Things)* es uno de los pilares clave de la cuarta revolución industrial, pues tiene potencial en innovaciones y beneficios para toda la población. Sus aplicaciones se reflejan en ingeniería, agricultura, medicina e incluso en áreas donde no está suficientemente clara la manera de abordar su implementación [1]. Aly *et al.* [2] mencionan que la tecnología *IoT* se define como una infraestructura global que permite utilizar servicios avanzados mediante la interconexión de elementos físicos y virtuales basados en tecnologías de comunicación e información existentes, interoperables y en evolución.

Actualmente, la academia y el sector empresarial muestran un enorme interés en la creación de sistemas *IoT* con el fin de simplificar y mejorar la eficiencia de los procesos, buscando una mejor calidad de vida para las personas. Esto hace que exista en el mercado una gran oferta de dispositivos electrónicos, así como plataformas de Internet en las que se desarrollan sistemas *IoT*. Esa variedad también se convierte en un problema, porque se construyen muchos sistemas pero de manera heterogénea, es decir, cada sistema tiene sus propias especificaciones lógicas, modelos de ensamblaje, formas de comunicación y sus propias implementaciones, lo que limita la colaboración entre distintos sistemas *IoT*. Otros problemas que aparecen desde la planificación son: i) malas estimaciones de riesgos en los procesos que se modelan; ii) sistemas no escalables por diseños defectuosos; y iii) poca existencia de metodologías y estándares de naturaleza *IoT*, lo que conlleva a malas prácticas y genera problemas económicos y legales [3].

Zambonelli [4] identifica que las características generales de los sistemas de *IoT* se clasifican en los siguientes grupos: cosas, infraestructuras de *software*, servicios y aplicaciones, las cuales necesitan multitud de métodos para lograr una adecuada implementación [5]. También, a esos métodos no se les da la relevancia, pero es necesario cambiar ese paradigma para mejorar la comunicación entre los diferentes componentes, con el fin de realizar una implementación adecuada para solucionar problemas en la industria [6].

Bellman y Oorschot [7] proponen una definición de mejores prácticas con la intención de reducir la ambigüedad en el término: algo que implica una acción con una serie de pasos conocidos y probados que nace de cierto grado de consenso o de uso común dentro de un grupo de expertos técnicos o investigadores en un campo dado y se considera mejor que otros medios para lograr el mismo objetivo. Mencionan también que las mejores prácticas contienen técnicas existentes probadas y repetibles a futuro por los interesados. Este estudio selecciona las mejores prácticas actuales de *IoT* teniendo en cuenta estos criterios.

Gyrard *et al.* [8] reconocen la importancia de aplicar mejores prácticas al implementar soluciones basadas en *IoT*. Benkhelifa *et al.* [9] afirman que, dada la naturaleza heterogénea de los dispositivos y protocolos, la seguridad en la *IoT* es una prioridad de investigación. Además es necesario incluir defensas de segunda línea porque las prácticas actuales son insuficientes. Beltramen [10] menciona que muchas de las personas que realizan trabajos *IoT* no tienen un conocimiento profundo en la materia y es necesario reducir la brecha entre los autodidactas y expertos para que se creen sistemas *IoT* que soporten los futuros desafíos tecnológicos.

El objetivo de esta Revisión Sistemática de Literatura (RSL) es identificar las mejores prácticas y principales componentes de *hardware* y *software* empleados en la creación de sistemas *IoT*. Se utiliza un método donde se definen las preguntas de investigación, luego se busca la información en bases

C.M. Medina is Master student at the Universidad Tecnológica de Pereira, e-mail:pepe@utp.edu.co

J. C. Blandón A. is Full Professor at the Universidad Católica de Pereira, Colombia, e-mail:juanc.blandon@ucp.edu.co

C. M. Zapata J. is Full Professor at Computer and Decision Departament, Faculty of Mines, Universidad Nacional de Colombia Sede Medellín, e-mail:cmzapata@unal.edu.co

J.I. Ríos P. is Full Professor at the Universidad Tecnológica de Pereira, e-mail:jirios@utp.edu.co

de datos especializadas, después se selecciona y extrae la información importante para luego realizar un análisis de la información [11]. El artículo se estructura como se menciona a continuación: en la sección 2, se analizan los trabajos previos relacionados. En la sección 3 se describe el método utilizado para realizar el estudio y se detallan los pasos siguientes. En la sección 4, se presentan los resultados del estudio. En la sección 5, se realiza la discusión sobre los hallazgos del estudio. Finalmente en la sección 6 se presentan las conclusiones obtenidas al final de la revisión.

II. Trabajos Relacionados

Existen estudios que analizan las mejores prácticas, los componentes de software y hardware y los métodos actuales usados para implementar sistemas *IoT*. A continuación, se describen algunas investigaciones relevantes encontradas en la revisión de literatura.

Bellman y Oorschot [7] profundizan en el concepto de mejores prácticas concluyendo, luego de una revisión de literatura, que falta mucha comprensión sobre lo que realmente significa este concepto. El estudio categoriza las mejores prácticas a partir de un conjunto de 1014 mejores prácticas de seguridad en *IoT* tomadas de fuentes industriales, gubernamentales y académicas, y describe cómo se aplican durante el ciclo de vida de los dispositivos.

Kamaludeen *et al.* [12] identifican a partir de una revisión de literatura algunas prácticas para el desarrollo de aplicaciones para hogares inteligentes basados en *IoT* que no cubren todas las fases involucradas en las etapas de desarrollo. Los investigadores proponen una guía de mejores prácticas para ayudar a los desarrolladores de software a configurar el hardware, a elegir el lenguaje de programación correcto y a ahorrar tiempo en la búsqueda de prácticas adecuadas para la implementación del sistema.

Merzouk *et al.* [13] desarrollan un estudio que compara las capacidades, principales características y comportamientos de los métodos usados para implementar sistemas *IoT*. Los autores analizan primero métodos de Ingeniería de Software aplicados a *IoT*, para luego compararlos con métodos diseñados específicamente para sistemas *IoT*. El estudio concluye que se necesita un nuevo método para administrar la naturaleza real de *IoT*.

Fortino *et al.* [14] realizan una revisión de literatura para identificar los métodos, marcos de trabajo, plataformas y herramientas usadas actualmente para el desarrollo de sistemas *IoT*. La investigación incluye la revisión de setenta productos relevantes a través de un enfoque comparativo y práctico, basado en características generales de la ingeniería *SoS (System of Systems)* revisadas a la luz de los principales sistemas *IoT*.

Los estudios presentados utilizan métodos de revisión sistemática de literatura para alcanzar los objetivos de la investigación. Algunos de ellos carecen de una descripción detallada de los pasos que desarrollan para aplicar el método [12]–[14]. Esta investigación se basa en el seguimiento riguroso del método de Kitchenham [11] para Ingeniería de Software, que plantea fases bien estructuradas que comprenden planificación, ejecución y reporte o documentación. Este tipo de métodos permite recopilar la información basada en la evidencia disponible sobre un tema o fenómeno y responder a ciertas preguntas de investigación. Además, estas técnicas son un diseño de investigación observacional y retrospectivo que sintetiza los resultados de múltiples investigaciones primarias.

III. Método

Una revisión sistemática de literatura busca desarrollar un análisis objetivo sobre un tema en particular por medio de un método confiable, preciso y verificable. Mediante una serie de pasos ordenados se identifica, evalúa e interpreta toda la literatura disponible alrededor de una o varias preguntas de investigación [15]. En este trabajo se utiliza el método de Kitchenham [11], el cual tiene las fases que se presentan en la Tabla I.

TABLA I
Método RSL

Fase	Actividad
Planeación	Definir las preguntas de investigación.
Búsqueda primaria	Especificar el tipo de búsqueda.
	Seleccionar las fuentes de información.
	Definir las cadenas de búsqueda.
Selección preliminar	Eliminar documentos irrelevantes.
	Eliminar documentos duplicados.
Selección	Definir criterios de inclusión.
	Definir criterios de exclusión.
Extracción de datos	Definir criterios de calidad.
	Extraer datos de cada documento.
Análisis	Analizar la información recolectada.
	Dar respuesta a las preguntas de investigación.

En este artículo se extrae información relevante relacionada con las mejores prácticas en *IoT* y sus principales componentes de *hardware* y *software* desde material científico; posteriormente se analiza la información encontrada. En los siguientes apartados, se describen detalladamente las actividades mencionadas en la Tabla I.

A. Planeación

En esta fase se definen las preguntas de investigación que son la base del estudio.

A1. Definir las Preguntas de Investigación: Kitchenham y Charters [15] mencionan un método para la construcción de las preguntas de investigación teniendo en cuenta tres aspectos: i) población; ii) intervención; y iii) resultados. Basados en las recomendaciones, se plantean las preguntas de investigación utilizadas para este artículo.

a) ¿Cuáles son las mejores prácticas empleadas en la actualidad para el desarrollo de sistemas *IoT*?
b) ¿Cuáles son los principales componentes de *hardware* y *software* empleados en la actualidad para el desarrollo de sistemas *IoT*?
c) ¿Qué métodos se usan para la creación de sistemas *IoT*?

B. Búsqueda Primaria

Kitchenham *et al.* [11] proponen que para la búsqueda primaria se realicen tres actividades. La primera consiste en especificar el tipo de búsqueda. La segunda se relaciona

con seleccionar las fuentes de extracción de información. La tercera es definir las cadenas de búsqueda (*strings*) para utilizar en las bases de datos especializadas.

B1. Especificar el Tipo de Búsqueda: Existen dos tipos de búsqueda, manual y automatizada. La manual consiste en ingresar diferentes cadenas de búsqueda en diferentes bases de datos y luego elegir qué documentos son relevantes. En la automatizada primero se definen unas cadenas de búsqueda, luego se lanzan a las distintas bases de datos y se tienen en cuenta inicialmente todos los resultados independiente de su relevancia. En este artículo se lleva a cabo un tipo de búsqueda automatizada.

B2. Seleccionar las Fuentes de Información: Las bases de datos utilizadas para la revisión son indexadas, confiables y especializadas en diferentes tipos de sistemas. Para seleccionarlas se tiene en cuenta el ranking de Journals en Ingeniería de *Google Scholar* basado en el índice H5 [16] y el ranking de *Scimago* [17]. Luego se revisa en qué Bases de Datos se encuentran esos *Journals* y se toman las más representativas. Finalmente, se consideran algunos referentes bibliográficos [18]–[20].

B3. Definir las Cadenas de Búsqueda: Según las preguntas de investigación se definen tres cadenas de búsqueda (*strings*) y sus respectivas formas de representación que son las siguientes:
Cadena 1 (C1): *IoT current best practices*.
Cadena 2 (C2): *IoT hardware and software main components*.
Cadena 3 (C3): *IoT development method*.

C. Selección Preliminar

Luego se procede a realizar la búsqueda en cada una de las bases de datos seleccionadas utilizando las cadenas de búsqueda C1, C2 y C3. En la Tabla II se presenta el número de artículos encontrados en la primera búsqueda.

TABLA II
RESULTADO BÚSQUEDA INICIAL

Base de Datos	C1	C2	C3	Total
IEEE Xplore Digital Library	221	39	18	278
Scopus	49	59	27	135
Science Direct	28	62	53	143
Springer	71	42	23	136
Web of Science	105	89	90	284
ACM	45	31	50	126
Ebsco	66	35	17	118
Total	585	357	278	1220

Con los documentos resultantes se realiza una selección preliminar de los candidatos, es decir, se eliminan los documentos que se consideran irrelevantes y los duplicados, tal como se describe a continuación.

C1. Eliminar Documentos Irrelevantes: Para determinar la relevancia de cada artículo, se realizan dos fases de análisis y filtrado. En la primera se realiza una ronda de eliminación donde se considera la relevancia de acuerdo con el título, resumen (*abstract*), palabras clave (*keywords*), introducción y conclusiones. Si después del filtrado no es clara la relevancia del documento, se aplica la segunda fase, la cual consiste en revisar la totalidad del artículo.

Después de aplicar las dos fases de filtrado, se descarta el número de artículos que se detalla en la Tabla III .

TABLA III
DOCUMENTOS IRRELEVANTES

Base de Datos	C1	C2	C3	Total
IEEE Xplore Digital Library	121	23	11	155
Scopus	9	24	13	46
Science Direct	19	40	31	90
Springer	56	21	14	91
Web of Science	46	35	58	139
ACM	31	18	36	85
Ebsco	36	12	5	53
Total	318	173	168	659

La Tabla IV presenta el número de artículos que aprueban la etapa de análisis y filtrado preliminar, lo que significa que se tendrán en cuenta para las etapas posteriores de la revisión.

TABLA IV
DOCUMENTOS RESULTANTES

Base de Datos	C1	C2	C3	Total
IEEE Xplore Digital Library	69	14	7	90
Scopus	14	8	11	33
Science Direct	9	17	16	42
Springer	8	5	6	19
Web of Science	22	20	15	57
ACM	8	8	9	25
Ebsco	6	14	4	24
Total	136	86	68	290

C2. Eliminar Documentos Duplicados: Una posibilidad latente es el hecho de encontrar documentos repetidos en distintas bases de datos. Teniendo en cuenta esto, se eliminan los documentos repetidos para evitar redundancia, confusión y reprocesos en el momento de analizar los artículos. La Tabla V presenta los valores actualizados después de eliminar los artículos repetidos.

TABLA V
DOCUMENTOS RESULTANTES SIN DUPLICADOS

Base de Datos	C1	C2	C3	Total
IEEE Xplore Digital Library	31	2	0	33
Scopus	26	27	3	56
Science Direct	0	5	6	11
Springer	7	16	3	26
Web of Science	37	34	17	88
ACM	6	5	5	16
Ebsco	24	9	8	41
Total	131	98	42	271

D. Selección

En esta fase se definen los criterios de inclusión y exclusión, lo que permite un filtrado sistemático a los documentos seleccionados. El objetivo es decidir la relevancia de los artículos para responder a las preguntas de investigación.

D1. Definir Criterios de Inclusión: Se refiere a los requisitos para seleccionar un documento. Los criterios de inclusión utilizados son: i) el documento tiene relación directa con la temática mejores prácticas, principales componentes o métodos de desarrollo en *IoT*; ii) el idioma del documento se presenta en inglés o español; iii) el documento o estudio es un artículo de revista académica, artículo en conferencia, publicación de un taller o capítulo de un libro; iv) el formato del texto está completo y se accede a su total contenido; y v) la fecha de publicación está dentro del periodo de publicación 2017 y 2022.

D2. Definir Criterios de Exclusión: Se definen como los criterios por los cuales se descarta un documento. Los criterios de exclusión usados son: i) el documento no tiene relación directa con la temática mejores prácticas, principales componentes o métodos de desarrollo en *IoT*; ii) documento con idioma diferente a inglés o español; iii) el documento o estudio es un *White paper*, libro, publicación no científica o un resumen; iv) no se encuentra el formato en texto completo, o está incompleto; y v) la fecha de publicación no está dentro del periodo de publicación 2017-2022.

Después de aplicar los criterios de inclusión y exclusión se obtienen como resultado los artículos a los cuales se les realiza un respectivo análisis para responder a las preguntas de investigación. En la Tabla VI se presenta la información correspondiente a los artículos resultantes desde cada base de datos especializada.

TABLA VI
DOCUMENTOS RESULTANTES

Base de Datos	C1	C2	C3	Total
IEEE Xplore Digital Library	17	5	8	30
Scopus	8	3	2	13
Science Direct	5	1	2	8
Springer	3	1	2	6
Web of Science	10	6	2	18
ACM	4	3	3	10
Ebsco	2	7	3	12
Total	49	26	22	97

E. Extracción de Datos

Se procede a la revisión de cada uno de los documentos relevantes por medio de los criterios de calidad y el formulario de extracción de datos que permite documentar el proceso.

E1. Definir Criterios de Calidad: Los criterios de calidad se definen teniendo como base las cadenas de búsqueda (*strings*). Así, se crean preguntas para cada una de ellas y se evalúan los documentos. Las preguntas se formularon en la Tabla VII.

Se utilizan las preguntas para comprobar que los artículos resultantes realmente ayudan a responder las preguntas de investigación que se formulan para el estudio y se documenta para facilitar las fases posteriores.

E2. Extraer Datos de cada Documento: En esta actividad se diseña un formulario de extracción de datos para registrar con precisión la información de la literatura, especialmente los estudios primarios. Al final se organiza la información de acuerdo con los términos de búsqueda utilizados y la influencia de cada documento para ayudar a resolver las preguntas de investigacion. En la Tabla VIII se presenta el formulario de extracción de datos que se utiliza en este trabajo.

TABLA VII
CRITERIOS DE CALIDAD

Cadena	Pregunta
C1: *IoT current best practices*	¿El autor menciona que se trata de una buena práctica en *IoT*? ¿La actividad propuesta tiene elementos de mejores prácticas según Bellman y Oorschot [7]?
C2: *IoT hardware and software main components*	¿Se mencionan los componentes *software* y/o *hardware* empleados?
C3: *IoT development method*	¿El autor propone, complementa o modifica un método para implementar sistemas *IoT*?

TABLA VIII
FORMULARIO DE EXTRACCIÓN DE DATOS

Información	Descripción
Título del documento	Título original conservando su idioma.
Autores	Se especifica el nombre de todos los autores independientemente de la cantidad.
Fuente de información	Base de datos en la cual se encuentra el documento.
Año de Publicación	Año de publicación disponible en la revista y/o Base de Datos.
Tipo de Documento	Se especifica qué tipo de documento es, por ejemplo: artículo en conferencia, artículo de revista académica, etc.
Prácticas *IoT*	Se especifica las prácticas detectadas en el documento.
Componentes de *hardware*	Se especifica los componentes de *hardware* encontrados en el documento.
Componentes de *software*	Se especifica los componentes de *software* encontrados en el documento.
Métodos	Se especifica los métodos *IoT* usados o mencionados en el documento.

Después se analiza la información que se recolecta en el formulario de extracción de datos y con ello se da respuesta a las preguntas de investigación.

IV. RESULTADOS

En esta sección se presentan los resultados de la revisión sistemática de literatura y, con ello, se busca desarrollar la fase de análisis planteada en el método de Kitchenham [11]. Para lograrlo, se describen las mejores prácticas, componentes y métodos encontrados en la literatura para el desarrollo de sistemas *IoT*.

A. Mejores Prácticas para Sistemas IoT

A continuación se presentan mejores prácticas en *IoT* según las características descritas por Bellman y Oorschot [7] y que se relacionan con aspectos de seguridad, ciudades y hogares inteligentes, calidad de datos, redes y plataformas en la nube.

A1. Seguridad: Dingman *et al.* [21] estudian un grupo de 131 mejores prácticas en *IoT*, las cuales se tomaron desde seis fuentes de información como: *Federal Trade Commission (FTC), the National Highway Traffic Safety Administration (NHTSA), the Federal Bureau of Investigation (FBI), the Online Trust Alliance (OTA), the National Institute of Standards & Technologies (NIST)*, y *the Open Web Application*

Security Project (OWASP). El estudio arrojó como resultado 56 recomendaciones de mejores prácticas que se aplican en las áreas de desarrollo, funcionamiento de los dispositivos, políticas de los dispositivos, vulnerabilidades, funcionamiento del sistema, privacidad, análisis de amenazas, autenticación y prácticas de organización. Estas recomendaciones se evaluaron con base en tres incidentes a gran escala relacionados con la seguridad de dispositivos *IoT*.

Debido al aumento en los últimos años del número de dispositivos y usuarios conectados con sistemas *IoT* mediante Internet, las políticas de privacidad y seguridad de datos se afectan con los avances en *IoT* [22]. Los investigadores vienen centrando su atención en estudiar las mejores prácticas de seguridad relacionadas con el acceso y manipulación de los datos que se generan en diferentes fuentes de sistemas *IoT*. Tres grandes áreas se abordan para la aplicación de las mejores prácticas: dispositivos, conectividad y seguridad en la nube [23].

Los dispositivos *IoT* son diversos y se hace necesario categorizarlos para tener un mejor control de la información que generan y de la manera como se accede a ellos. Javed *et al.* [24] sugieren clasificarlos como dispositivos de transmisión, de recepción y de transmisión y recepción. Además, brindan sugerencias para analizar la capacidad de almacenamiento y el procesamiento seguro de los datos dentro del dispositivo, todo esto como parte de un conjunto de mejores prácticas durante la etapa de diseño y desarrollo de sistemas *IoT*. La aplicación de mejores prácticas en la configuración e instalación de los dispositivos *IoT* como: *hubs* [25], *Raspberry Pi* [26], *Arduino* [12], sensores inalámbricos [27] y cámaras *IP* [28], aumenta el nivel de seguridad y permite reducir las vulnerabilidades de los sistemas. Estas prácticas se basan en el análisis del funcionamiento [21], [29], [30], conectividad [21], [29]–[33] y las políticas de acceso a los dispositivos [21], [29]–[33].

Los sistemas *IoT* se basan en redes que conectan billones de dispositivos que recolectan y envían grandes cantidades de información. Para mitigar los problemas de seguridad asociados con la conectividad, se proponen algunas mejores prácticas basadas en la arquitectura e implementación de las redes. Entre algunos aspectos relevantes de la interconexión de dispositivos para la definición de las mejores prácticas están: la selección de la conectividad inalámbrica adecuada [2], [23], [25], [32], [34]–[37], la gestión de la energía [2], [24], [31], [34]–[38], la potencia [23], [29], [31], [34], [38], la gestión del ancho de banda [2], [24], [28], [31], [35]–[37], [39], la instalación y configuración de los dispositivos [24], [25], [28], [29], [31], [37], la autenticación [21], [23]–[25], [28], [29], [31]–[38], la defensa contra ataques [21], [23]–[25], [28], [29], [31]–[34], [36]–[39], la detección de intrusos [32], [34], [37], la restricción del acceso físico [23], [24], [28], [38], la transmisión y privacidad de los datos [2], [21], [23]–[25], [31], [33]–[39] y la capacitación de los usuarios [21], [32], [33].

El envío, procesamiento y almacenamiento de datos por medio de servicios en la nube es una tendencia en los sistemas *IoT*. Las empresas implementan los componentes *IoT* haciendo uso de tecnología de punta a bajo costo [40]. Esto implica la creación de sistemas en diferentes escenarios que suponen nuevos retos de seguridad. Algunas de las mejores prácticas para la seguridad de servicios en la nube incluyen: la implementación de servicios web siguiendo las recomendaciones del *W3C (World Wide Web Consortium)* [8], [29], [41] , la utilización de *SenML (Sensor Measurement Lists)* [8], [41] para la representación de datos de sensores, la implementación de la autenticación basada en *JSON (JWT, JavaScript Object Notation Web Token)* [41], el uso del esquema *XACML (eXtensible Access Control Markup Language)* [23], [30], [42], para la seguridad física en los centros de datos, la utilización de *SSL/TLS (Secure Sockets Layer*, basado en *Transport Layer Security)* [3], [23], [34] para el cifrado de los datos enviados a la nube, el uso de un sistema híbrido de detección de intrusos (*IDS*) [7], [9], [23], [33], [34], [36], [37], [39], [43], [44] y el empleo de *IPsec* (protocolos para comunicaciones *IP* que implementan la autenticación y el cifrado a nivel de red para cada paquete *IP*) [3], [9], [23], [31], [34], [37], [38], [45].

A2. Ciudades y Hogares Inteligentes: Los hogares inteligentes son las aplicaciones de sistemas *IoT* más comunes, que permiten el monitoreo y control posiblemente de forma remota de diferentes aspectos en el hogar [46], [47]. Las mejores prácticas para la implementación de dispositivos *IoT* en hogares inteligentes incluyen aspectos de seguridad [12], [29], [46]–[51], protección [29], [48], conectividad [12], [48], [49], consumo de energía [48], [50], administración, control y costo de los componentes de comunicación [12], [48].

Una de las áreas de aplicación de *IoT* más importantes y de mayor progreso es el concepto de ciudad inteligente [1], la cual se entiende como un centro urbano que mediante una gestión óptima de los recursos, proporciona una alta calidad de vida a sus habitantes de una manera sostenible y eficiente [52]. Para mitigar los problemas técnicos, socioeconómicos y ambientales, algunas de las mejores prácticas para lograr ciudades sostenibles involucran la distribución geográfica adecuada de los recursos y servicios [53]–[55], el mejoramiento de la conectividad en la última milla [53], [55], [56], la promoción del respeto por el medio ambiente [48], [52], [53], [56], la promoción y sensibilización acerca del uso de fuentes alternativas de energía [53], [56], la promoción de la agricultura urbana [53], [56], el desarrollo de normas y reglamentos más estrictos sobre el cambio climático [53], [55], la reducción de la huella de carbono [53], [55], la imposición de impuestos de sostenibilidad a los visitantes [53], el desarrollo de políticas urbanas basadas en el análisis de datos [53], [55], [56] y la regulación de los roles en la cadena de valor de los sistemas *IoT* [54].

A3. Calidad de los Datos: En el entorno *IoT* se generan grandes volúmenes de datos recolectados de diferentes fuentes de información. La calidad de los datos repercute de manera directa en el funcionamiento de los sistemas *IoT*. Pérez-Castillo *et al.* [57] presentan un conjunto de mejores prácticas para la gestión de la calidad de los datos (*DQ, Data Quality*) en entornos inteligentes de productos conectados (*SCP, smart, connected product*), teniendo en cuenta las normas ISO/IEC 25012 e ISO 8000-62. Las recomendaciones van desde recolección de los datos hasta la gestión del ciclo de vida del sistema.

A4. Redes: Las Redes de Sensores Inalámbricos (*WSN, Wireless Sensor Networks*) se utilizan en los sistemas *IoT* para recolectar datos de los componentes interconectados [58], [59]. En el análisis del comportamiento de estas redes es necesario establecer métricas que ayuden a caracterizar el desempeño del sistema. Entonces, se plantean mejores prácticas para la medición de parámetros críticos teniendo en cuenta la literatura analizada sobre métricas desde el año 2010, la categorización de las métricas y la construcción de un modelo de sistema abstracto para redes *WSN* [27].

Otra opción es conectar los dispositivos *IoT* mediante redes de área amplia de baja potencia (*LPWAN, Low power wide area network*) [40], [60]–[63], lo que permite obtener amplia cobertura y bajo consumo de energía. Para definir mejores prácticas en las técnicas de implementación de redes *LPWAN*, Wang *et al.* [60] comparan las principales características de tres técnicas: *LoRaWAN*, *NB-IoT* y *Sigfox* [3], [35], [40], [61], [64]; también, proponen un índice llamado *LP-INDEX* basado en seis aspectos a considerar en la implementación de aplicaciones *IoT*: latencia, capacidad de datos, energía y costo, cobertura y seguridad.

A5. Plataformas en la Nube: Las mejores prácticas para el procesamiento de datos en sistemas *IoT* apoyados en servicios en la nube incluyen: i) el almacenamiento sólo de datos críticos para ahorro de energía y ancho de banda [65]; ii) el uso de protocolos de aplicación como *MQTT (Message Queueing Telemetry Transport)* [64], *REST (Representational State Transfer)* [37], *CoAP (Constrained Application Protocol)* [64], *XMMP (Extensible Messaging and Presence Protocol)* [51] y *Web Socket* [62]; iii) la implementación en lenguajes de programación como *Embedded C*, *NodeJS*, *Java* y *Python* [66]; iv) el uso de entornos de desarrollo para aplicaciones web y *Android e IOS* [62], [66]; v) la utilización de entornos de aprendizaje de realidad virtual (*VRLE, Virtual Reality Learning Environment*) [67]. El resumen del análisis de las mejores prácticas se muestra en la Tabla IX.

TABLA IX
MEJORES PRÁCTICAS EN *IoT*

Práctica	Referencias	Propósito	Proceso
Utilizar protocolos de normas vigentes	[2], [21], [23], [31], [34]–[39], [41], [47]–[50], [53], [56]	Seguridad	I
Proteger mensajes sensibles implementando cifrado	[21], [23], [28], [31], [32], [34], [36]–[38], [47], [48]	Seguridad	I
Impedir el acceso no autorizado a los dispositivos	[21], [23], [24], [28], [30], [32]–[34], [36]–[38], [47], [49], [50], [53]	Seguridad	A, D, I
Minimizar la recopilación de datos	[21], [23], [36], [46], [65]	Seguridad	A, D, I
Deshabilitar servicios y puertos innecesarios en dispositivos	[21], [32], [34], [36], [37], [39]	Seguridad	A, D, I
Elegir el lenguaje de programación adecuado	[1], [12], [38], [39]	Desarrollo	A, D, I
Restringir el acceso físico a los dispositivos	[28], [37], [38], [48], [57]	Seguridad	A, D, I
Capacitación para concientizar sobre la seguridad en *IoT*	[28], [32], [33], [67]	Seguridad	A
Implementación de la red de dispositivos mediante la segmentación y segregación de la red	[1], [32], [34]–[36], [57], [65]	Redes	A, D, I
Implementación de parches de seguridad tanto a nivel de *OS/firmware* como de aplicaciones	[32], [37], [38]	Seguridad	I
Utilizar una única clave criptográfica por dispositivo	[21], [23]–[25], [37], [38], [60]	Seguridad	A, D, I
Utilizar técnicas de análisis de *big data* para recopilar, gestionar y analizar grandes volúmenes de datos	[1], [28], [30], [37], [39], [40], [46], [50], [53], [58], [67], [68]	Calidad de datos, seguridad	I
Mejorar el consumo de energía de los dispositivos	[1], [2], [24], [27], [29], [31], [32], [34], [35], [38], [40], [52]–[54], [56], [60], [65], [69], [70]	Dispositivos	I
Utilizar los servicios de cloud computing para almacenar y procesar datos	[2], [22], [23], [35], [37], [40], [48], [50], [53], [56], [67], [70], [71]	Gestión de datos	A, D, I

(A = Análisis, D = Diseño, I = Implementación)

B. Componentes de Software y Hardware para el Desarrollo de Sistemas IoT

Los componentes utilizados para desarrollar soluciones *IoT* evolucionan de acuerdo con el contexto de su uso. Allí existen trabajos enfocados principalmente a la agricultura [64], [72], [73], ciudades inteligentes [52]–[56], [60] y salud [23], [45], [68], [71]. También suelen evolucionar de acuerdo con la arquitectura de las redes de conexión, la definición de nuevos estándares y normas, así como con la implementación de nuevos paradigmas de computación. En esta sección se presentan las características de los componentes de *software* y *hardware IoT* usados en la actualidad.

Los teléfonos inteligentes (*smartphones*) son dispositivos equipados con múltiples sensores que permiten a los usuarios conectarse a sistemas *IoT* desde los rincones más remotos del mundo [22]. Las dos principales plataformas de *software* usadas en estos dispositivos son *Android* y *IOS* [48]. Existen también implementaciones del sistema operativo *GNU/Linux* tanto para la administración y configuración de sensores como para la configuración de servidores de procesamiento de datos [1], [26], [32], [70]. Diversas implementaciones de sistemas *IoT* utilizan *MySQL* como gestor de almacenamiento y administración de los datos [28], [38], [58]. Algunos proyectos utilizan un componente de *software* llamado sensor virtual (*virtual sensor*) que permite procesar la información disponible como lo haría un sensor físico [64], [74] .

Para el diseño de dispositivos *IoT*, Pereira *et al.* [35] proponen agruparlos en tres categorías: i) pasivos (sin batería ni radio); ii) semi-pasivos (con batería sin radio); y iii) activos (con batería y radio). Además, estudian diferentes tecnologías y su implementación para afrontar los retos de consumo de energía y comunicación de los dispositivos: (a) comunicación por retrodispersión; (b) transferencia de energía inalámbrica (*Wireless Power Transfer, WPT*); (c) recolección de energía (*Energy Harvesting, EH*); (d) dispositivos sin circuitos; (e) transferencia inalámbrica simultánea de información y energía (*SWIPT*); y (f) radio despertador.

Según Fortino *et al.* [14] las plataformas *IoT* permiten conectar diferentes dispositivos para administrar y procesar los datos que se reciben, para luego activar ciertas acciones como respuesta a la información obtenida. Los autores realizan un estudio para determinar las principales características de estas plataformas, llegando a la conclusión que son: la interoperabilidad, la autonomía, la escalabilidad y la inteligencia. Encontraron que para la conectividad de los componentes se utilizan *Gateways* [23] a menudo enriquecidos con adaptadores de *software plug-and-play*, adoptando diversas tecnologías de comunicación como *WiFi* [40], [45], [61], [75], *Bluetooth* [40], [51], [64], *NFC (Near-Field Communication)* [37], [40], [64], [73], *ZigBee* [40], [47], [76] y *LoRa* [36], [45], [61], [75], [77]. También, se utilizan protocolos de capa de aplicación como *REST(Representational State Transfer* [37], *MQTT (Message Queueing Telemetry Transport)* [51], [78], [79] y *CoAP (Constrained Application Protocol)* [64]. En cuanto a los formatos de intercambio de datos, se mencionan *XML*

(Extensible Markup Language) [51], *JSON (JavaScript Object Notation)* [80], *RDF (Resource Description Framework)* [29] y *CSV (Comma Separated Values)* [8], los cuales a su vez constituyen estándares. La mayoría de las plataformas *IoT* se diseñaron originalmente para implementarlas en la nube con capacidad para procesar un gran número de datos apoyadas en plataformas externas de análisis de datos como *AppEngine* [14] y *Hadoop MapReduce* [14]. De las herramientas para desarrollar sistemas *IoT*, concluyen que las más utilizadas son *APIs* (*Application Programming Interface*), *middlewares* (software intermedio que permite la comunicación entre las aplicaciones y los dispositivos *IoT* [81]), simuladores [74] y *Gateways*, que en su mayoría se ofrecen como productos de código abierto y con entorno gráfico de programación.

Las redes *WSN* son uno de los principales componentes de aplicaciones *IoT*, que permiten conectar, detectar y controlar los objetos de forma remota usando nodos de sensores inalámbricos (*Wireless Sensor Nodes, WSND*). Karray *et al.* [82] realizan un estudio de los componentes de diseño de los nodos y las tendencias de aplicación. Los autores encontraron que para la implementación de estos nodos se utilizan diferentes tecnologías como *Arduino* [79], *Waspmote nodes*, *Meshlium* [83], *WISE IoT Nodes*, *Raspberry Pi* [1], [12], [26], [28], [48], [49], [51], [61], [64], [66], [75], [78], [79], *Zigbee Radio* [40], [47], [76], *SoC(System-on-a-Chip)-based IoT node* [51], [64], [78], entre otras. Afirman que la mayoría de los primeros nodos implementados utilizan un microcontrolador (*MCU*), por ejemplo *NodeMCU* [84] y que se componen principalmente de un transmisor-receptor de radio [85], una antena, un procesador, una unidad de memoria, sensores o interfaces de sensores y una batería. También mencionan que existen otros nodos que usan los procesadores de señal digital (*Digital Signal Processors, DSP*) [76] que ejecutan algoritmos de procesamiento de señales de manera rápida. Su arquitectura se implementa utilizando el *DSP* como coprocesador o como procesador principal. Otra manera de implementar los nodos es usar *FPGAs* (*Field-Programmable Gate Array*) [38], que son circuitos integrados programables y contienen un conjunto de puertas lógicas y sus conexiones.

Otro hallazgo del estudio de Karray *et al.* [82] es que en muchas propuestas se implementan arquitecturas híbridas en los nodos usando microcontroladores junto con dispositivos programables como *FPGA* [38], *CPLD* (*Complex Programmable Logic Devices*) y *FPAA* (*field-programmable analog array*). Esto permite un mejor rendimiento asociando las tareas simples al *MCU* y las tareas complejas al dispositivo programable que actúa como un coprocesador; esta técnica es muy común en redes *WSN*. Otra alternativa que plantean, es la de diseñar nodos basados en *ASICs* (*Application Specific Integrated Circuit*) [38], [86] y *SoCs* (*System on Chip*) [51], [64], [78] que son circuitos diseñados e integrados en un sólo circuito.

Otros tipos de sensores son los ubicuos, que se basan en la tecnología de las redes WSN y se distribuyen en el entorno real, recogen datos y los transmiten a los centros de procesamiento mediante redes de comunicación móviles o de Internet [87].

Un nuevo paradigma llamado *Dynamic Wireless Sensor Network* (*D-WSN*) [88] incluye los componentes *IoT* como componentes interconectados de forma inalámbrica e introduce funcionalidades desvinculadas físicamente de los dispositivos. Este paradigma presenta tres contribuciones principales: i) funcionalidad de red a componentes individuales que se asocien dinámicamente con nodos de sensores activos, para así aumentar sus capacidades según sea necesario; ii) reingeniería de la operación de las redes *WSN* en el *IoT*, básicamente para adaptarse a arquitecturas dinámicas que evolucionan con el tiempo para aumentar la resiliencia y la vida útil, principalmente basadas en componentes individuales en lugar de nodos WSN estáticos; y iii) un modelo determinista estrechamente acoplado para la vida funcional de redes *WSN* en el *IoT*.

En los hogares inteligentes los sensores se implementan como actuadores o como controladores [62]. Los actuadores permiten cambiar el estado de los dispositivos en el hogar como interrumpir el suministro de agua, emitir advertencias de riesgos o ajustar la intensidad de luz. Los controladores permiten manipular los dispositivos de acuerdo con parámetros elegidos por el usuario [50].

La computación de borde es una arquitectura distribuida de tecnologías de la información en la que el almacenamiento de datos, los servicios y las aplicaciones se trasladan total o parcialmente desde los nodos centralizados hasta nodos cerca al usuario final. El concepto de arquitecturas de computación de borde para aplicaciones *IoT* (*edge-computing architectures for IoT applications, ECAs-IoT*) [2], [53], [55], [67], [89] abarca dispositivos *IoT*, de borde y de computación en la nube, *software* y protocolos de red e infraestructura interconectados para así ofrecer determinados servicios. Según Hamdan *et al.* [81] existen tres maneras para la distribución y uso de los componentes *ECAs-IoT*: i) *Cloudlet* [41], que es un grupo de computadores llamados nodos *cloudlet* que actúan como un pequeño centro de datos que proporciona servicios a dispositivos *IoT* dentro de una misma área geográfica; ii) *Fog computing* [62], [90]–[92], que es una infraestructura descentralizada de nodos heterogéneos (*switches*, controladores industriales y *access points*) que se sitúan en cualquier lugar entre los usuarios finales y la nube [51], [74], [90]–[92]; y iii) *Mobile edge computing (MEC)* [55], que hace referencia a una red que proporciona servicios de computación en la nube a los dispositivos móviles en el borde de una red móvil para reducir la latencia.

Un paradigma distribuido llamado *mobile crowdsensing* se está convirtiendo en uno de los componentes principales de los servicios *IoT* y se basa en redes de sensores a gran escala en las cuales los individuos comparten datos y extraen información para medir y mapear fenómenos de interés común. Este paradigma crea una nueva forma de percibir el mundo y permite implementar una nueva generación de redes inteligentes interconectando cosas con cosas, cosas con personas y personas con personas [93]. El resumen del análisis de los componentes se muestra en la Tabla X.

C. Métodos para la Creación de Sistemas IoT

Muchas organizaciones están tratando de implementar métodos de *software* para el desarrollo de sistemas *IoT* [43],

TABLA X
COMPONENTES DE *hardware* Y *software* EN *IoT*

Componente	Referencias	Tipo
Virtual sensor	[14], [64], [74]	*Software*
Raspberry Pi	[1], [12], [26], [28], [48], [49], [51], [61], [64], [66], [75], [78], [79], [82], [90]	*Hardware*
Arduino	[1], [12], [40], [42], [45], [47], [49], [51], [61], [64], [66], [75], [79], [84], [90]	*Hardware*
Sensor nodes	[27], [37], [45], [47], [48], [51], [57], [58], [61], [64], [82], [87], [88], [90]	*Hardware*
Gateways	[2], [23], [28], [37], [40], [46]–[50], [68], [94]	*Hardware*
Actuators	[14], [23], [34], [42], [48]–[51], [54], [56], [77], [91]	*Hardware*
Controllers	[39], [48], [50], [51], [57], [69], [81]	*Hardware*
Microcontrlador MCU	[1], [27], [38], [51], [82], [84], [88]	*Hardware*
Wireless Sensor Nodes (WSN)	[27], [51], [82]	*Hardware*
FPGAs (Field-Programmable Gate Array)	[38], [82]	*Hardware*
Hubs	[1], [25], [53], [55], [81], [88]	*Hardware*
Android	[12], [28], [41], [47], [48], [50], [51], [66], [74], [82], [84], [90]	*Software*
IOS	[12], [41], [47], [48], [66], [82]	*Software*
IP Camera	[21], [28], [29], [32], [47], [49], [51]	*Hardware*
Smartphones	[22], [28], [32], [35], [42], [54], [66], [68], [70], [94]	*Hardware*
GNU/Linux	[1], [26], [32], [34], [38], [42], [51], [70], [74], [77], [78], [82], [91]	*Software*
MySQL	[28], [38], [49], [58], [78], [89]	*Software*

[44], [86], [95]–[97], pero se requiere de soluciones que se adapten a los retos de desarrollo e implementación en temas de computación distribuida, redes de dispositivos *IoT*, seguridad y análisis de datos [5], [62].

Merzouk *et al.* [13] comparan tres métodos ágiles de desarrollo de *software* (*Scrum*, *Kanban* y *SAFe*) contra dos métodos *IoT* como *IGNITE* [98] y *IoT Methodology* [5], [99]. En este análisis se concluye que *Kanban*, *Scrum* y *SAFe* se diseñan para desarrollar *software* y no *hardware*, lo que dificulta su implementación en sistemas *IoT*. Por su parte, *IGNITE* y *IoT methodology* son métodos monolíticos, que no cubren todas las fases y problemáticas resultantes en el desarrollo de sistemas *IoT* en áreas como la seguridad, operabilidad, escalabilidad, rentabilidad y modelos de negocio en *IoT* [100].

Fortino *et al.* [14] analizan doce métodos propuestos para *IoT*. Los autores afirman que la mayoría se enfocan en el proceso de análisis y diseño, se desarrollan para propósitos generales y vienen de proyectos académicos. Mencionan que pocos abordan la fase de simulación [101], [102], que no integran plataformas *IoT* existentes [103] y permiten desarrollar aplicaciones *IoT* descentralizadas a gran escala [101]. En la Tabla XI se presentan los doce métodos analizados.

Existen otros métodos propuestos que se centran en mejorar el rendimiento de sistemas *IoT* inalámbricos [63], [76], [104] y con ello solucionar los problemas de seguridad [105], [106]. El resumen del análisis de estos métodos se muestra en la Tabla XII.

Para sintetizar las respuestas con los hallazgos de la Revisión Sistemática de Literatura, se presenta un mapa mental con los temas relevantes de cada pregunta de investigación, así como el número de referencias bibliográficas donde se relacionan (Fig. 1).

TABLA XI
MÉTODOS *IoT* [14]

Método	Propósito	Proceso	Origen	Licencia
ACOSO-Meth [102]	General	A, D, I, S	Academia	Abierta
Manate *et al.* [107]	General	A, D	Academia	Abierta
INTER-METH [103]	Específico	A, D, I	Project	Abierta
Ayala *et al.* [83]	General	A, D	Academia	Abierta
Casadei *et al.* [101]	Específico	A, D, I, S	Academia	Abierta
Spanoudakis *et al.* [108]	General	A, D, I	Project	Abierta
IDEA [109]	General	A, D	Academia	Abierta
IGNITE [98]	General	A, D	Company	Propietaria
Collins *et al.* [110]	General	A, D	Company	Propietaria
Patel *et al.* [111]	General	A, D, I	Academia	Abierta
SEM [112]	General	A, D, I	Academia	Abierta
THING-ML [80]	General	A, D, I	Academia	Abierta

(A = Análisis, D = Diseño, I = Implementación, S = Simulación)

TABLA XII
OTROS MÉTODOS *IoT*

Método	Propósito	Proceso	Origen	Licencia
da Costa & Baltus [76]	Específico	A, D	Academia	Abierta
Janhunen *et al.* [104]	Específico	A, D, I	Academia	Abierta
Wang *et al.* [63]	Específico	A, D	Academia	Abierta
Josyla & Gupta [105]	Específico	A, D	Academia	Abierta
ERAMIS [106]	General	A, D, I	Academia	Abierta
Jacob *et al.* [113]	Específico	S	Academia	Abierta

(A = Análisis, D = Diseño, I = Implementación, S = Simulación)

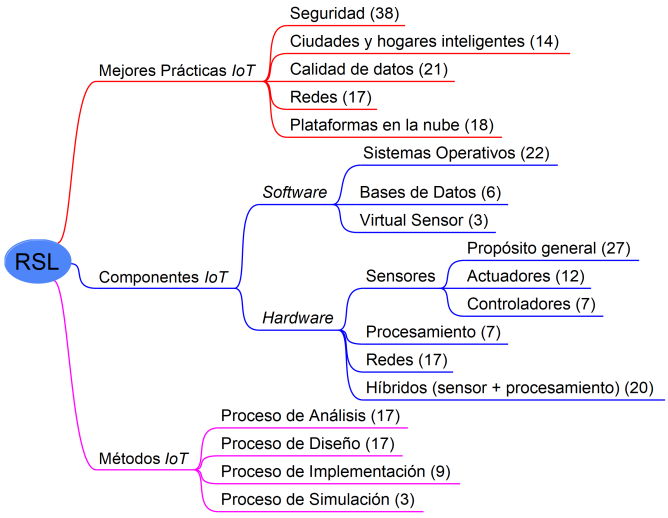

Fig. 1. Resumen RSL. Fuente: Elaboración propia.

V. DISCUSIÓN

El objetivo de este artículo es realizar una revisión sistemática de literatura en revistas indexadas utilizando el método de Kitchenham [11] para identificar las mejores prácticas, los componentes de *hardware* y *software* actuales y los métodos para crear sistemas *IoT*. Esta investigación sirve como base teórica para crear mejores sistemas *IoT* en las organizaciones y reducir costos. Utilizar el método de Kitchenham para la revisión sistemática de literatura tiene las siguientes fortalezas: existe diversidad de literatura relacionada, tiene una estructura con fases bien definidas, permite analizar con profundidad los temas de estudio y facilita responder con claridad las preguntas de investigación. Algunos de los estudios analizados desarrollan revisiones estructuradas sin definir con claridad el método implementado.

Existe diversidad de prácticas para la implementación de

sistemas *IoT*. Cada organización estructura sus propias prácticas de acuerdo con sus necesidades. Esto hace que muchas prácticas sean comunes pero se desarrollan con métodos diferentes. Tener un escenario común donde se definan las mejores prácticas en *IoT* permitiría a los involucrados en el análisis, desarrollo e implementación de estos sistemas, compartir sus experiencias, tomar mejores decisiones y construir métodos propios para solucionar problemáticas específicas en su entorno.

VI. Conclusiones

Existen diferentes enfoques para abordar la implementación de sistemas *IoT*. La mayoría de los métodos, modelos y arquitecturas encontradas en la literatura se enfocan en mejorar aspectos relacionados con la seguridad de la información desde la captura de los datos hasta su procesamiento y revisión de la calidad. Las ciudades y hogares inteligentes, la instalación, configuración y medición de rendimiento de las redes de sensores y la implementación de los servicios *IoT* en contextos particulares, son temas que los investigadores en esta área están explorando para aprovechar el potencial de los sistemas *IoT*. En este artículo se identificaron las mejores prácticas, los componentes de *software* y *hardware* y los métodos para crear sistemas *IoT*. Luego de este estudio es posible dar respuesta a las preguntas de investigación formuladas en la Sección A1.

a. *¿Cuáles son las mejores prácticas empleadas en la actualidad para el desarrollo de sistemas IoT?*
   Se encontraron muchas propuestas para la aplicación de mejores prácticas en la implementación de sistemas *IoT*. En el área de la seguridad se propone utilizar protocolos de normas vigentes, proteger mensajes sensibles implementando cifrado, impedir el acceso no autorizado a los dispositivos, minimizar la recopilación de datos, deshabilitar servicios y puertos innecesarios en los dispositivos, restringir el acceso físico a los dispositivos, realizar capacitaciones para concientizar a los usuarios en temas de seguridad en *IoT*, implementar parches de seguridad tanto a nivel de *OS/firmware* como de aplicaciones y utilizar una única clave criptográfica por dispositivo. También se destacan mejores prácticas como implementar dispositivos en las redes mediante la segmentación y segregación, utilizar técnicas de análisis de big data para recopilar, gestionar y analizar grandes volúmenes de datos, mejorar el consumo de energía de los dispositivos y utilizar los servicios de *cloud computing* para almacenar y procesar datos.
b. *¿Cuáles son los principales componentes de software y hardware empleados en la actualidad para el desarrollo de sistemas IoT?* Los componentes de *hardware* usados actualmente para la construcción de soluciones *IoT* involucran dispositivos con capacidad de procesamiento, almacenamiento y comunicación (inalámbrica en la mayoría de las veces) que buscan reducir el consumo de energía y el tiempo de respuesta en el intercambio y procesamiento de los datos. Los más relevantes encontrados en el estudio son *Arduino*, *Raspberry Pi*, *sensor nodes*, *gateways*, *actuators*, *controllers*, microcontroladores (*MCU*), *Wireless Sensor Nodes (WSN)*, *FPGAs (Field-Programmable Gate Array)*, *Hubs*, cámaras *IP*, y *smartphones*.
   Los componentes de *software* hallados incluyen sistemas operativos (*Android*, *IOS*, *GNU/Linux*), motores de bases de datos (*MySQL*) y sensores virtuales.
c. *¿Qué métodos se desarrollan para la creación de sistemas IoT?* Para lograr el acoplamiento entre estas mejores prácticas y los componentes, se usan métodos que evolucionaron desde una simple adaptación de esquemas de desarrollo de *software* en sistemas *IoT*, hasta una implementación robusta de métodos propuestos que tienen en cuenta todos los aspectos y etapas propias de soluciones *IoT* como se muestra en la Tabla XI y Tabla XII.

En este artículo se mostró la actualidad de los sistemas *IoT* con base en la identificación de mejores prácticas, los componentes y los métodos usados para su implementación y se destacan las características generales. Sin embargo, se evidencia la falta de un marco de trabajo común que sirva de guía para que los involucrados (usuarios, fabricantes de *software* y *hardware*, ejecutivos y académicos) abarquen todos los problemas en el desarrollo de soluciones *IoT* en áreas como la seguridad, operabilidad, escalabilidad y rentabilidad. Como trabajo futuro se tiene la intención de estructurar algunas de las mejores prácticas en *IoT* para compartirlas con los interesados en el desarrollo de sistemas *IoT* en un dominio común.

Agradecimentos

Este artículo es un producto del proyecto de investigación con código CI-021-04 de la Universidad Católica de Pereira, también es parte del proyecto con código 52499 de la Universidad Nacional de Colombia Sede Medellín y de un proyecto de Maestría en Ingeniería de Sistemas y Computación de la Universidad Tecnológica de Pereira. Los autores agradecen a la estudiante Tania Largo por su aporte en el desarrollo del estudio.

Referencias

[1] S. Nižetić, P. Šolić, D. L.-d.-I. González-de Artaza, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," *Journal of Cleaner Production*, vol. 274, Nov. 2020.
[2] M. Aly, F. Khomh, Y. Guéhéneuc, H. Washizaki, and S. Yacout, "Is Fragmentation a Threat to the Success of the Internet of Things?," *IEEE Internet of Things Journal*, vol. 6, pp. 472–487, Feb. 2019.
[3] J. Tournier, F. Lesueur, F. L. Mouël, L. Guyon, and H. Ben-Hassine, "A survey of IoT protocols and their security issues through the lens of a generic IoT stack," *Internet of Things*, vol. 16, Dec. 2021.
[4] F. Zambonelli, "Key Abstractions for IoT-Oriented Software Engineering," *IEEE Software*, vol. 34, pp. 38–45, Jan. 2017.
[5] I. Jacobson, I. Spence, and P.-W. Ng, "Is there a single method for the internet of things?: Essence can keep software development for the IoT from becoming unwieldy.," *Communications of the ACM*, vol. 60, pp. 46–53, Oct. 2017.
[6] G. Giray, B. Tekinerdogan, and E. Tüzün, "Adopting the Essence Framework to Derive a Practice Library for the Development of IoT Systems," in *Connected Environments for the Internet of Things: Challenges and Solutions* (Z. Mahmood, ed.), pp. 151–168, Cham, Switzerland: Springer International Publishing, 2017.
[7] C. Bellman and P. C. v. Oorschot, "Best Practices for IoT Security: What Does That Even Mean?," *CoRR*, vol. abs/2004.12179, Apr. 2020.

[8] A. Gyrard, M. Serrano, and G. A. Atemezing, "Semantic web methodologies, best practices and ontology engineering applied to Internet of Things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, (Milan, Italy), pp. 412–417, Dec. 14–16, 2015.

[9] E. Benkhelifa, T. Welsh, and W. Hamouda, "A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3496–3509, 2018.

[10] A. Beltramen, "Prototipado rápido de proyectos IoT sin programación," in *XXI Concurso de Trabajos Estudiantiles (EST) - JAIIO 47 (CABA, 2018)*, (La plata, Argentina), pp. 174–182, Sociedad Argentina de Informática e Investigación Operativa, Sept. 2018.

[11] B. A. Kitchenham, P. Brereton, M. Turner, M. K. Niazi, S. Linkman, R. Pretorius, and D. Budgen, "Refining the systematic literature review process—two participant-observer case studies," *Empirical Software Engineering*, vol. 15, pp. 618–653, Dec. 2010.

[12] N. B. A. Kamaludeen, S. P. Lee, and R. M. Parizi, "Guideline-Based Approach for IoT Home Application Development," in *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, (Atlanta, GA, USA), pp. 929–936, July 14–17, 2019.

[13] S. Merzouk, A. Cherkaoui, A. Marzak, and S. Nawal, "IoT methodologies: comparative study," *Procedia Computer Science*, vol. 175, pp. 585–590, Jan. 2020.

[14] G. Fortino, C. Savaglio, G. Spezzano, and M. Zhou, "Internet of Things as System of Systems: A Review of Methodologies, Frameworks, Platforms, and Tools," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, pp. 223–236, Jan. 2021.

[15] B. A. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," Technical Report EBSE 2007-001, Keele University and Durham University Joint Report, Keele, UK, July 2007.

[16] G. Scholar, "Data Mining & Analysis - Google Scholar Metrics." https://scholar.google.es/citations?view_op=top_venues&hl=en&vq=eng_dataminінganalysis.

[17] S. J. . C. Rank, "SJR : Scientific Journal Rankings." https://www.scimagojr.com/journalrank.php.

[18] J. O. A. Gamboa, "Bases de datos y calidad de las revistas científicas: la aportación de Latindex.," *ESPACIO I+D: Innovación más Desarrollo*, vol. VI, pp. 8 – 28, Dec. 2017.

[19] H. Nieto-Chaupis, "Interpretation of Scimago Ranking in Terms of Success Probabilities," in *2019 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, (Valparaiso, Chile), pp. 1–4, Oct. 29–31, 2019.

[20] T. Todorov, "Practical aspects of journal indexing in scientific databases," in *2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, (Ankara, Turkey), pp. 233–236, Oct. 21–23, 2021.

[21] A. Dingman, G. Russo, G. Osterholt, T. Uffelman, and L. J. Camp, "Poster Abstract: Good Advice That Just Doesn't Help," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, (Bloomington, IN, USA), pp. 289–291, Apr. 17–20, 2018.

[22] R. Pérez Colón, S. Navajas, and E. Terry, "IoT IN LAC 2019: Taking the Pulse of the Internet of Things in Latin America and the Caribbean," tech. rep., Inter-American Development Bank, Washington D.C., USA, Oct. 2019.

[23] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of Security and Privacy for the Internet of Medical Things (IoMT)," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, (Santorini, Greece), pp. 457–464, May 29–31, 2019.

[24] B. Javed, M. W. Iqbal, and H. Abbas, "Internet of things (IoT) design considerations for developers and manufacturers," in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, (Paris, France), pp. 834–839, May 21–25, 2017.

[25] B. Momenzadeh, H. Dougherty, M. Remmel, S. Myers, and L. J. Camp, "Best Practices Would Make Things Better in the IoT," *IEEE Security Privacy*, vol. 18, pp. 38–47, July 2020.

[26] J. Sainz-Raso, S. Martin, G. Diaz, and M. Castro, "Security Vulnerabilities in Raspberry Pi–Analysis of the System Weaknesses," *IEEE Consumer Electronics Magazine*, vol. 8, pp. 47–52, Nov. 2019.

[27] D. Yuan, S. S. Kanhere, and M. Hollick, "Instrumenting Wireless Sensor Networks — A survey on the metrics that matter," *Pervasive and Mobile Computing*, vol. 37, pp. 45–62, June 2017.

[28] N. Kalbo, Y. Mirsky, A. Shabtai, and Y. Elovici, "The security of ip-based video surveillance systems," *Sensors*, vol. 20, pp. 1–27, Aug. 2020.

[29] Y. I. Khan and M. U. Ndubuaku, "Ontology-based automation of security guidelines for smart homes," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, (Singapore), pp. 35–40, Feb. 5–8, 2018.

[30] M. Trnka, T. Cerny, and N. Stickney, "Survey of Authentication and Authorization for the Internet of Things," *Security and Communication Networks*, vol. 2018, June 2018.

[31] G. Nebbione and M. Calzarossa, "Security of IoT application layer protocols: Challenges and findings," *Future Internet*, vol. 12, Mar. 2020.

[32] B. R. Payne and T. T. Abegaz, "Securing the Internet of Things: Best Practices for Deploying IoT Devices," in *Computer and Network Security Essentials*, pp. 493–506, Cham, Switzerland: Springer International Publishing, 2018.

[33] J. Whitter-Jones, "Security review on the Internet of Things," in *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*, (Barcelona, Spain), pp. 163–168, Apr. 23–26, 2018.

[34] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis," *Sensors*, vol. 20, June 2020.

[35] F. Pereira, R. Correia, P. Pinho, S. Lopes, and N. Carvalho, "Challenges in resource-constrained iot devices: Energy and communication as critical success factors for future iot deployment," *Sensors*, vol. 20, Nov. 2020.

[36] B. Oniga, V. Dadarlat, E. D. Poorter, and A. Munteanu, "Analysis, design and implementation of secure LoRaWAN sensor networks," in *2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP)*, (Cluj-Napoca, Romania), pp. 421–428, Sept. 7–9, 2017.

[37] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things*, vol. 14, June 2021.

[38] M. G. Samaila, J. B. F. Sequeiros, T. Simões, M. M. Freire, and P. R. M. Inácio, "IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space," *IEEE Access*, vol. 8, pp. 16462–16494, 2020.

[39] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," *Arabian Journal for Science and Engineering*, vol. 42, pp. 425–441, Feb. 2017.

[40] A. Martín-Garín, J. A. Millán-García, A. Baïri, M. Gabilondo, and A. Rodríguez, "IoT and cloud computing for building energy efficiency," in *Start-Up Creation (Second Edition)* (F. Pacheco-Torgal, E. Rasmussen, C.-G. Granqvist, V. Ivanov, A. Kaklauskas, and S. Makonin, eds.), Woodhead Publishing Series in Civil and Structural Engineering, pp. 235–265, Cambridge, UK: Woodhead Publishing, Mar. 2020.

[41] S. K. Datta, J. Härri, and C. Bonnet, "IoT Platform for Precision Positioning Service for Highly Autonomous Vehicles," in *2018 22nd International Computer Science and Engineering Conference (ICSEC)*, (Chiang Mai, Thailand), pp. 1–6, Nov. 21–24, 2018.

[42] A. Celesti, M. Fazio, F. Galan Marquez, A. Glikson, H. Mauwa, A. Bagula, F. Celesti, and M. Villari, "How to Develop IoT Cloud e-Health Systems Based on FIWARE: A Lesson Learnt," *Journal of Sensor and Actuator Networks*, vol. 8, p. 7, Jan. 2019.

[43] B. A. Mozzaquatro, C. Agostinho, R. Melo, and R. Jardim-Goncalves, "A Model-Driven Adaptive Approach for IoT Security," in *Model-Driven Engineering and Software Development* (S. Hammoudi, L. F. Pires, B. Selic, and P. Desfray, eds.), Communications in Computer and Information Science, (Rome, Italy), pp. 194–215, Springer International Publishing, Feb. 19–21, 2016.

[44] J. B. F. Sequeiros, F. T. Chimuco, M. G. Samaila, M. M. Freire, and P. R. M. Inácio, "Attack and System Modeling Applied to IoT, Cloud, and Mobile Ecosystems: Embedding Security by Design," *ACM Computing Surveys*, vol. 53, pp. 1–32, Mar. 2020.

[45] M. S. Islam, M. T. Islam, A. E. Almutairi, G. K. Beng, N. Misran, and N. Amin, "Monitoring of the Human Body Signal through the Internet of Things (IoT) Based LoRa Wireless Network System," *Applied Sciences*, vol. 9, May 2019.

[46] J. Bugeja, A. Jacobsson, and P. Davidsson, "Is your home becoming a spy?: A data-centered analysis and classification of smart connected home systems," in *IoT 2020 - 10th International Conference on the Internet of Things*, (Malmö, Sweden), Association for Computing Machinery, Oct. 2020.

[47] I.-I. Pătru, M. Carabaş, M. Bărbulescu, and L. Gheorghe, "Smart home IoT system," in *2016 15th RoEduNet Conference: Networking*

in Education and Research, (Bucharest, Romania), pp. 1–6, Sept. 7–9, 2016.

[48] A. Zaidan, B. Zaidan, M. Qahtan, O. Albahri, A. Albahri, M. Alaa, F. Jumaah, M. Talal, K. Tan, W. Shir, and C. Lim, "A survey on communication components for IoT-based technologies in smart homes," *Telecommunication Systems*, vol. 69, pp. 1–25, Mar. 2018.

[49] A. Iqbal, F. Ullah, H. Anwar, K. S. Kwak, M. Imran, W. Jamal, and A. u. Rahman, "Interoperable Internet-of-Things platform for smart home system using Web-of-Objects and cloud," *Sustainable Cities and Society*, vol. 38, pp. 636–646, Apr. 2018.

[50] I. Machorro-Cano, G. Alor-Hernández, M. A. Paredes-Valverde, L. Rodríguez-Mazahua, J. L. Sánchez-Cervantes, and J. O. Olmedo-Aguirre, "HEMS-IoT: A Big Data and Machine Learning-Based Smart Home System for Energy Saving," *Energies*, vol. 13, Jan. 2020. Number: 5 Publisher: Multidisciplinary Digital Publishing Institute.

[51] I. Froiz-Míguez, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "Design, Implementation and Practical Evaluation of an IoT Home Automation System for Fog Computing Applications Based on MQTT and ZigBee-WiFi Sensor Nodes," *Sensors*, vol. 18, Aug. 2018.

[52] M. A. Abdullah, T. Al-Hadhrami, C. W. Tan, and A. H. Yatim, "Towards Green Energy for Smart Cities: Particle Swarm Optimization Based MPPT Approach," *IEEE Access*, vol. 6, pp. 58427–58438, 2018.

[53] M. A. Ahad, S. Paiva, G. Tripathi, and N. Feroz, "Enabling technologies and sustainable smart cities," *Sustainable Cities and Society*, vol. 61, Oct. 2020.

[54] M. Weber and I. P. Zarko, "A Regulatory View on Smart City Services," *Sensors*, vol. 19, Jan. 2019.

[55] K. Kuru and D. Ansell, "TCitySmartF: A Comprehensive Systematic Framework for Transforming Cities Into Smart Cities," *IEEE Access*, vol. 8, pp. 18615–18644, 2020.

[56] G. D'Amico, P. L'Abbate, W. Liao, T. Yigitcanlar, and G. Ioppolo, "Understanding Sensor Cities: Insights from Technology Giant Company Driven Smart Urbanism Practices," *Sensors*, vol. 20, Aug. 2020.

[57] R. Perez-Castillo, A. G. Carretero, M. Rodriguez, I. Caballero, M. Piattini, A. Mate, S. Kim, and D. Lee, "Data Quality Best Practices in IoT Environments," in *2018 11th International Conference on the Quality of Information and Communications Technology (QUATIC)*, (Coimbra, Portugal), pp. 272–275, Sept. 4–7, 2018.

[58] T. Anh Khoa, N. Quang Minh, H. Hai Son, C. Nguyen Dang Khoa, D. Ngoc Tan, N. VanDung, N. Hoang Nam, D. Ngoc Minh Duc, and N. Trung Tin, "Wireless sensor networks and machine learning meet climate change prediction," *International Journal of Communication Systems*, vol. 34, Feb. 2021.

[59] J. C. Blandón A., J. A. López, and L. E. Tobón Llano, "Routing in wireless sensor networks using bio-inspired algorithms," *Entre Ciencia e Ingeniería*, vol. 12, pp. 130–137, May 2019.

[60] H. Wang, Y. Liu, Y. Wei, Y. He, K. F. Tsang, L. L. Lai, and C. S. Lai, "LP-INDEX: Explore the Best Practice of LPWAN Technologies in Smart City," in *2020 IEEE International Smart Cities Conference (ISC2)*, (Piscataway, NJ, USA), pp. 1–5, Oct. 2020.

[61] N. Silva, J. Mendes, R. Silva, F. N. dos Santos, P. Mestre, C. Serôdio, and R. Morais, "Low-Cost IoT LoRa®Solutions for Precision Agriculture Monitoring Practices," in *Progress in Artificial Intelligence* (P. Moura Oliveira, P. Novais, and L. P. Reis, eds.), Lecture Notes in Computer Science, (Vila Real, Portugal), pp. 224–235, Springer International Publishing, Sept. 3–6, 2019.

[62] N. Magaia, P. Gomes, L. Silva, B. Sousa, C. X. Mavromoustakis, and G. Mastorakis, "Development of Mobile IoT Solutions: Approaches, Architectures, and Methodologies," *IEEE Internet of Things Journal*, vol. 8, pp. 16452–16472, Nov. 2021.

[63] J. Wang, W.-C. Yeh, N. N. Xiong, J. Wang, X. He, and C.-L. Huang, "Building an Improved Internet of Things Smart Sensor Network Based on a Three-Phase Methodology," *IEEE Access*, vol. 7, pp. 141728–141737, 2019.

[64] E. Navarro, N. Costa, and A. Pereira, "A Systematic Review of IoT Solutions for Smart Farming," *Sensors*, vol. 20, July 2020.

[65] P. Leelavinodhan, F. Antonelli, M. Vecchio, and A. Maestrini, "Energy-neutral weather stations for precision agriculture: Challenges and approaches," in *2020 IEEE International Workshop on Metrology for Agriculture and Forestry (MetroAgriFor)*, (Trento, Italy), pp. 24–28, Nov. 4–6, 2020.

[66] P. Ganguly, "Selecting the right IoT cloud platform," in *2016 International Conference on Internet of Things and Applications (IOTA)*, (Pune, India), pp. 316–320, 2016.

[67] S. Wang, S. Valluripally, R. Mitra, S. S. Nuguri, K. Salah, and P. Calyam, "Cost-Performance Trade-Offs in Fog Computing for IoT Data Processing of Social Virtual Reality," in *2019 IEEE International Conference on Fog Computing (ICFC)*, (Prague, Czech Republic), pp. 134–143, June 24–26, 2019.

[68] I. Machorro-Cano, G. Alor-Hernández, M. A. Paredes-Valverde, U. Ramos-Deonati, J. L. Sánchez-Cervantes, and L. Rodríguez-Mazahua, "PISIoT: A Machine Learning and IoT-Based Smart Health Platform for Overweight and Obesity Control," *Applied Sciences*, vol. 9, July 2019. Number: 15 Publisher: Multidisciplinary Digital Publishing Institute.

[69] J. Park, T. Kim, and C.-s. Lee, "Development of Thermal Comfort-Based Controller and Potential Reduction of the Cooling Energy Consumption of a Residential Building in Kuwait," *Energies*, vol. 12, Jan. 2019. Number: 17 Publisher: Multidisciplinary Digital Publishing Institute.

[70] K. Matsui, "An information provision system to promote energy conservation and maintain indoor comfort in smart homes using sensed data by IoT sensors," *Future Generation Computer Systems*, vol. 82, pp. 388–394, May 2018.

[71] S. J. Miah, N. Hasan, R. Hasan, and J. Gammack, "Healthcare support for underserved communities using a mobile social media platform," *Information Systems*, vol. 66, pp. 1–12, June 2017.

[72] B. Keswani, A. G. Mohapatra, A. Mohanty, A. Khanna, J. J. P. C. Rodrigues, D. Gupta, and V. H. C. de Albuquerque, "Adapting weather conditions based IoT enabled smart irrigation technique in precision agriculture mechanisms," *Neural Computing & Applications*, vol. 31, pp. 277–292, Jan. 2019.

[73] A. Sinha, G. Shrivastava, and P. Kumar, "Architecting user-centric internet of things for smart agriculture," *Sustainable Computing-Informatics and Systems*, vol. 23, pp. 88–102, Sept. 2019.

[74] A. Kertesz, T. Pflanzner, and T. Gyimothy, "A Mobile IoT Device Simulator for IoT-Fog-Cloud Systems," *Journal of Grid Computing*, vol. 17, pp. 529–551, Sept. 2019.

[75] D. Tadeus, Yuniarto, and F. Mangkusasmito, "LoRa Gateway as Internet of Things (IoT) Infrastructure Components on Undip Vocational School," in *IOP Conf. Series: Materials Science and Engineering.*, vol. 771, (Yogyakarta, Indonesia), IOP Publishing Ltd, Mar. 18, 2020.

[76] C. M. d. Costa and P. Baltus, "Design Methodology for Industrial Internet-of-Things Wireless Systems," *IEEE Sensors Journal*, vol. 21, pp. 5529–5542, Feb. 2021.

[77] G. P. Jesi, E. Benetti, and G. Mazzini, "Building an IoT Public Network Infrastructure," in *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, (Split, Croatia), pp. 1–5, Sept. 19–21, 2019.

[78] R. K. Kodali and A. Valdas, "MQTT Based Monitoring System for Urban Farmers Using ESP32 and Raspberry Pi," in *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)*, (Bangalore, India), pp. 395–398, Aug. 16–18, 2018.

[79] A. E. A. Tivani, R. M. Murdocca, C. F. S. Paez, and J. D. D. Gazzano, "Didactic Prototype for Teaching the MQTT Protocol Based on Free Hardware Boards and Node-RED," *IEEE Latin America Transactions*, vol. 18, pp. 376–382, Feb. 2020.

[80] B. Morin, N. Harrand, and F. Fleurey, "Model-Based Software Engineering to Tame the IoT Jungle," *IEEE Software*, vol. 34, pp. 30–36, Jan. 2017.

[81] S. Hamdan, M. Ayyash, and S. Almajali, "Edge-Computing Architectures for Internet of Things Applications: A Survey," *Sensors*, vol. 20, Nov. 2020.

[82] F. Karray, M. W. Jmal, A. Garcia-Ortiz, M. Abid, and A. M. Obeid, "A comprehensive survey on wireless sensor node hardware platforms," *Computer Networks*, vol. 144, pp. 89–110, Oct. 2018.

[83] I. Ayala, M. Amor, L. Fuentes, and J. M. Troya, "A Software Product Line Process to Develop Agents for the IoT," *Sensors*, vol. 15, pp. 15640–15660, July 2015.

[84] E. Boonchieng, O. Chieochan, and A. Saokaew, "Smart farm: Applying the Use of NodeMCU, IOT, NETPIE and LINE API for a lingzhi mushroom farm in Thailand," *IEICE Transactions on Communications*, vol. E101.B, pp. 16–23, Jan. 2018.

[85] S. A. Nauroze, J. G. Hester, B. K. Tehrani, W. Su, J. Bito, R. Bahr, J. Kimionis, and M. M. Tentzeris, "Additively Manufactured RF Components and Modules: Toward Empowering the Birth of Cost-Efficient Dense and Ubiquitous IoT Implementations," *Proceedings of the IEEE*, vol. 105, pp. 702–722, Apr. 2017.

[86] H. Koziolek, A. Burger, M. Platenius-Mohr, J. Rückert, and G. Stomberg, "OpenPnP: a plug-and-produce architecture for the industrial internet of things," in *Proceedings of the 41st International Conference on Software Engineering: Software Engineering in Practice*, ICSE-

SEIP '19, (Montreal, QC, Canada), pp. 131–140, IEEE Press, May 25–31, 2019.
[87] C. Yin, S. Zhang, J. Wang, and N. N. Xiong, "Anomaly Detection Based on Convolutional Recurrent Autoencoder for IoT Time Series," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, pp. 112–122, Feb. 2020.
[88] S. M. A. Oteafy and H. S. Hassanein, "Resilient IoT Architectures Over Dynamic Sensor Networks With Adaptive Components," *IEEE Internet of Things Journal*, vol. 4, pp. 474–483, Apr. 2017.
[89] T. Leppänen, C. Savaglio, L. Lovén, W. Russo, G. Di Fatta, J. Riekki, and G. Fortino, "Developing Agent-Based Smart Objects for IoT Edge Computing: Mobile Crowdsensing Use Case," in *Internet and Distributed Computing Systems* (Y. Xiang, J. Sun, G. Fortino, A. Guerrieri, and J. J. Jung, eds.), Lecture Notes in Computer Science, (Tokyo, Japan), pp. 235–247, Springer International Publishing, Oct. 11–13, 2018.
[90] M. Celaya-Echarri, I. Froiz-Miguez, L. Azpilicueta, P. Fraga-Lamas, P. Lopez-Iturri, F. Falcone, and T. Fernandez-Carames, "Building Decentralized Fog Computing-Based Smart Parking Systems: From Deterministic Propagation Modeling to Practical Deployment," *IEEE Access*, vol. 8, pp. 117666–117688, 2020.
[91] P. Krishnan, S. Duttagupta, and K. Achuthan, "SDN/NFV security framework for fog-to-things computing infrastructure," *Software-Practice & Experience*, vol. 50, pp. 757–800, May 2020.
[92] P. G. Vinueza Naranjo, Z. Pooranian, M. Shojafar, M. Conti, and R. Buyya, "FOCAN: A Fog-supported smart city network architecture for management of applications in the Internet of Everything environments," *Journal of Parallel and Distributed Computing*, vol. 132, pp. 274–283, Oct. 2019.
[93] J. Liu, H. Shen, H. S. Narman, W. Chung, and Z. Lin, "A Survey of Mobile Crowdsensing Techniques: A Critical Component for The Internet of Things," *ACM Transactions on Cyber-Physical Systems*, vol. 2, June 2018.
[94] F. Mancini, G. Lo Basso, and L. de Santoli, "Energy Use in Residential Buildings: Impact of Building Automation Control Systems on Energy Performance and Flexibility," *Energies*, vol. 12, Jan. 2019. Number: 15 Publisher: Multidisciplinary Digital Publishing Institute.
[95] Y. Y. Jusoh, S. Abdullah, I. M. Ali, M. H. M. Noh, M. H. Mazlan, C. S. Bouh, and T. Z. Sheng, "Adoption of Agile Software Methodology Among the SMEs Developing an IOT Applications," in *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*, (Johor Bahru, Malaysia), pp. 1–6, Dec. 2–3, 2019.
[96] L. J. Moukahal, M. A. Elsayed, and M. Zulkernine, "Vehicle Software Engineering (VSE): Research and Practice," *IEEE Internet of Things Journal*, vol. 7, pp. 10137–10149, Oct. 2020.
[97] R. Jabangwe and A. Nguyen-Duc, "SIoT Framework: Towards an Approach for Early Identification of Security Requirements for Internet-of-things Applications," *E-Informatica-Software Engineering Journal*, vol. 14, no. 1, pp. 77–95, 2020.
[98] F. Puhlmann and D. Slama, "An IoT solution methodology," tech. rep., Bosch Software Innovations GmbH, Berlin, Germany, 2017.
[99] R. van Kranenburg, "IoT Methodology – The Internet of Things project lifecycle guide for creative, technical and business people." http://www.iotmethodology.com/, 2015.
[100] M. Barenkamp, J. Schoenke, N. Zarvic, and O. Thomas, "IoT Best Practices: Fallstricke bei der Realisierung von (Industrial) Internet of Things (IIoT)-Projekten frühzeitig erkennen und adressieren," *HMD Praxis der Wirtschaftsinformatik*, vol. 56, pp. 1157–1177, Dec. 2019.
[101] R. Casadei, C. Tsigkanos, M. Viroli, and S. Dustdar, "Engineering Resilient Collaborative Edge-Enabled IoT," in *2019 IEEE International Conference on Services Computing (SCC)*, (Milan, Italy), pp. 36–45, July 8–13, 2019.
[102] G. Fortino, W. Russo, C. Savaglio, W. Shen, and M. Zhou, "Agent-Oriented Cooperative Smart Objects: From IoT System Design to Implementation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, pp. 1939–1956, Nov. 2018.
[103] C. Savaglio, G. Fortino, R. Gravina, and W. Russo, "A Methodology for Integrating Internet of Things Platforms," in *2018 IEEE International Conference on Cloud Engineering (IC2E)*, (Orlando, FL, USA), pp. 317–322, Apr. 17–20, 2018.
[104] J. Janhunen, K. Mikhaylov, J. Petäjäjärvi, and M. Sonkki, "Wireless Energy Transfer Powered Wireless Sensor Node for Green IoT: Design, Implementation and Evaluation," *Sensors*, vol. 19, Dec. 2018.
[105] S. K. Josyula and D. Gupta, "A new security methodology for internet of things," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, (Greater Noida, India), pp. 613–618, May 5–6, 2017.
[106] P. Kearney and R. Asal, "ERAMIS: A Reference Architecture-Based Methodology for IoT Systems," in *2019 IEEE World Congress on Services (SERVICES)*, vol. 2642-939X, (Milan, Italy), pp. 366–367, July 8–13, 2019.
[107] B. Manate, F. Fortiş, and P. Moore, "Applying the Prometheus Methodology for an Internet of Things Architecture," in *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, (London, UK), pp. 435–442, Dec. 8–11, 2014.
[108] N. Spanoudakis and P. Moraitis, "Engineering ambient intelligence systems using agent technology," *IEEE Intelligent Systems*, vol. 30, pp. 60–67, May 2015.
[109] B. Costa, P. F. Pires, and F. C. Delicato, "Modeling IoT Applications with SysML4IoT," in *2016 42th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, (Limassol, Cyprus), pp. 157–164, Sept. 2016.
[110] T. Collins, "A methodology for building the Internet of Things." http://www.iotmethodology.com/, 2017.
[111] P. Patel and D. Cassou, "Enabling high-level application development for the Internet of Things," *Journal of Systems and Software*, vol. 103, pp. 62–84, May 2015.
[112] F. Cicirelli, G. Fortino, A. Guerrieri, G. Spezzano, and A. Vinci, "Metamodeling of Smart Environments: from design to implementation," *Advanced Engineering Informatics*, vol. 33, pp. 274–284, Aug. 2017.
[113] R. Jacob, C. A. Boano, U. Raza, M. Zimmerling, and L. Thiele, "Towards a methodology for experimental evaluation in low-power wireless networking," in *Proceedings of the 2nd Workshop on Benchmarking Cyber-Physical Systems and Internet of Things*, CPS-IoTBench '19, (Montreal, QC, Canada), pp. 18–23, Association for Computing Machinery, Apr. 15, 2019.

Carlos Mario Medina Otálvaro Systems and Computing Engineer from Universidad Tecnológica de Pereira, Colombia. Master's student in Engineering, Systems and Computing emphasis at Universidad Tecnológica de Pereira. He is currently an hour teacher chair at Universidad Tecnológica de Pereira and Universidad Católica de Pereira in Colombia. More than ten years of experience in web development especially in Backend technologies. His interests of research are related to Software Engineering and Programming Languages.

Juan Carlos Blandón Andrade System Engineer at Universidad Cooperativa de Colombia. Master in Engineering focused on systems and computation, Javeriana University Cali Colombia. Ph.D. in Engineering—systems and computing at Universidad Nacional de Colombia Medellín. Associate Professor at Universidad Católica de Pereira, Colombia. His research interests are focused in Software Engineering, Artificial Intelligence focused on Natural Language Processing and Pedagogy in Engineering.

Carlos Mario Zapata Jaramillo Civil Engineer, Information System Management Specialist, M.Sc. in System Engineering, Ph.D. in Engineering focused on Systems, Universidad Nacional de Colombia. Full Professor at Computer and Decision Science Department, Faculty of Mines, Universidad Nacional de Colombia, Medellín, Colombia. He is, moreover, President of the Executive Committee of the Latin American Chapter of Semat and one of the official translators of the book "The Essence of Software Engineering: applying the Semat kernel". His research interests are focused in Software Engineering, Requirements Engineering, Computational Linguistics and Didactical Strategies for Teaching Engineering.

Jorge Iván Ríos Patiño Industrial Engineer from Universidad Tecnológica de Pereira, Colombia. Master in Computer Science from the Polytechnic University of Madrid (Spain). Master in Knowledge Engineering from the Polytechnic University of Madrid (Spain). Nowadays he is a professor at the Universidad Tecnológica de Pereira. Among his areas of interest are: Artificial Intelligence, Theory of Computation, Optimization and Metaheuristics.