Análisis de las principales plataformas IoT y su adecuación a la normativa ISO/IEC 30141

José Antonio de la Torre las Heras, Fernando Rincón Calle, Julián Caba Jiménez, Jesús Barba Romero y Juan Carlos López López[1]

Resumen— **La proliferación en el número de fabricantes y tecnologías ha provocado una gran heterogeneidad en los despliegues IoT. Esta tendencia está provocando que la aceptación de estos sistemas esté viéndose frenada. Por otro lado, la gran cantidad de dispositivos conectados hace que el modelo de volcado al *Cloud* deba evaluarse y plantear nuevas soluciones como el modelo híbrido Edge-Cloud. En este trabajo se analiza en primer lugar los estudios previos realizados sobre los dispositivos que hacen de pasarela o *Gateway* entre el Edge, el Cloud y los dispositivos finales valorando su adecuación a la normativa ISO/IEC 30141 que define los requisitos que deben tener las plataformas IoT. Como resultado de ese análisis se han valorado las principales plataformas y se han identificado las principales carencias en las que se debe trabajar para mejorar la adecuación de los sistemas a la norma ISO/IEC 30141.**

Palabras clave— **IoT, IoT Platforms, Edge Computing, IoT Gateways, ISO/IEC 30141**

I. Introducción

El término *Internet Of Things* (IoT) ha revolucionado la industria y la academia en lo últimos años (Ver Figura 1). Según Cisco, en base a su informe anual [1], se espera que para 2023 haya más de 29.3 billones de dispositivos conectados a Internet.

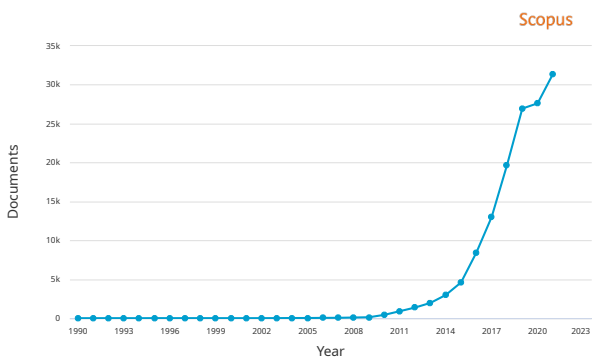

Fig. 1: Resultados de búsqueda de la cadena: "Internet of Things" OR "IoT" en Scopus

Gracias a la aparición de nuevas tecnologías de comunicación como LoRaWAN, 5G, Sigfox, NarrowBand, entre otras, las redes de sensores (WSN) han evolucionado a sistemas con grandes capacidades para generar información valiosa y actuar sobre su entorno de manera inteligente. Estas nuevas capacidades brindan nuevas oportunidades en muchos sectores como la Industria 4.0, ambiente sanitario, casas inteligentes o agricultura inteligente, entre otros.

[1]Dpto. de Tecnologías y Sistemas de la Información, Escuela Superior de Informática de Ciudad Real, Universidad de Castilla-La Mancha

En los primeros años de explotación de la tecnología IoT la principal preocupación ha sido la gestión de la información generada. Inicialmente, los dispositivos carecían de capacidad de cómputo y memoria y esta gestión se centralizaba en los servidores en el *Cloud*. Según los dispositivos han ido mejorando sus capacidades, se han desarrollado nuevas casos de uso que requieren de una menor latencia, como en el caso del coche autónomo. Estos nuevos requisitos han obligado a la industria a buscar soluciones donde el tiempo de comunicación se reduzca el máximo posible. Es aquí donde aparecen las arquitecturas en el *Edge/Fog*.

Finalmente, en los últimos años el foco se ha fijado en otros aspectos como el de la seguridad, que en un inicio no se planteaba de manera integral, llevando a escenarios de riesgo como los estudiados en [2]. Además, la creciente preocupación por la privacidad de los datos está obligando a que la industria busque soluciones donde el usuario final tenga el control sobre los datos que genera.

En paralelo a esta evolución, las plataformas de gestión IoT también se han tenido que adaptar a estos requisitos cambiantes.

En este trabajo se analizarán las arquitecturas de las plataformas IoT más relevantes en la actualidad en base a métricas definidas por diferentes organismos estandarizadores. Como resultado, se obtiene una medida de la alineación de dichas plataformas con los estándares con el fin de definir una futura arquitectura de referencia para despliegues IoT.

El trabajo se estructura en un primer estudio del contexto (Sección II) que rodea a los *gateways* y su relación con el "Nodo IoT" así como la computación en el Edge. En la Sección III se analizan otros trabajos que han evaluado este tipo de plataformas y se plantean los criterios de selección para el estudio. Finalmente, en la Sección IV se realiza el análisis de las plataformas seleccionadas, para terminar en la Sección V con las conclusiones sobre el estado actual de las plataformas IoT y el trabajo futuro que se debe realizar para mejorar los aspectos más alejados de la norma.

II. Contexto

En la literatura el término más utilizado para referirse al dispositivo que realiza la labor de agregación, filtrado y gestión en el Edge es el de gateway siendo la "plataforma IoT" el software de gestión del mismo. No obstante, en los últimos años otro término que está ganando popularidad es el de Nodo IoT.

En parte esta popularidad se debe a la normativa UNE-178108. Esta norma plantea al Nodo IoT como la composición de dos términos: pasarela IoT o gateway y computación en el Edge.

La norma define principalmente los requisitos que debe cumplir un Nodo IoT que van desde los aspectos funcionales y el software de gestión, hasta la interconexión con la capa superior que, en el caso de la norma (UNE-178108), es la ciudad inteligente. Aunque la norma se defina en el dominio de la ciudad inteligente, es directamente aplicable a cualquier despliegue IoT. Por otro lado, la normativa hace especial énfasis en la necesidad de aplicar técnicas que permitan la computación local (Edge/Fog) así como mecanismos para la agregación y federación en múltiples dominios de control. El objetivo final de la norma es que en todos los edificios de nueva creación en España se incluya un Nodo IoT con las capacidades anteriormente expuestas.

Como ya hemos adelantado, el Nodo IoT se puede ver como la **composición** de una **pasarela IoT** y un conjunto de capacidades que permitan el cómputo en el **Edge/Fog**.

En la literatura se pueden encontrar multitud de definiciones del término "pasarela IoT" o "IoT Gateway". No obstante, desde nuestra experiencia la más acertada y completa es la propuesta en [3] que define a la pasarela como: "Dispositivo que realiza tareas como: obtención de datos, preprocesamiento y filtrado de dichos datos, gestión de la seguridad de los dispositivos IoT y gestión de la privacidad de los datos que generan". Esta definición se centra en el aspecto más inmediato de la pasarela que es la de agregación de datos y la gestión de los dispositivos. No obstante, la pasarela también debe poder formar parte de un sistema mayor y delegar determinados servicios mediante técnicas de federación.

Así, el Cloud será una capa más (ver Figura 2) dentro de la arquitectura de la solución IoT a la que la pasarela puede conectarse para proporcionar servicios más complejos (que requieran de mayor capacidad de cómputo, memoria, inteligencia).

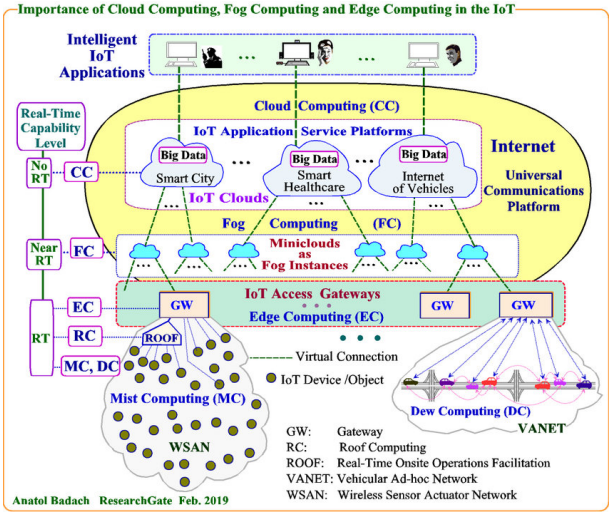

Fig. 2: Arquitectura Cloud, Edge, Fog [4]

La pasarela, de forma transversal a toda esta funcionalidad, tiene que garantizar la seguridad incluyendo mecanismos que no solo cumplan con las políticas locales donde se despliegue sino que sean capaces de alinearse con las políticas de seguridad de la solución global donde se encuentre desplegado. En despliegues reales con más de 6000 dispositivos, donde hemos tenido la oportunidad de trabajar, hemos observado como en la mayoría de casos hay que duplicar las credenciales y roles de acceso y, en muchos de estos casos, los roles no están alineados por los que se pone en riesgo la información y la seguridad del despliegue.

La capacidad de cómputo en el Edge es otro de los aspectos claves de la normativa. Una de las definiciones de Edge en la que mejor se refleja el concepto principal es [5]: "La computación en el Edge consiste en el conjunto de tecnologías que permiten que el cómputo se realice en el borde de la red, en nombre del Cloud para los datos que se envían a fuera, o en nombre de los dispositivos para los datos que se envían desde dentro" Es decir, la computación en el Edge debería permitir que aquellos servicios que originalmente se realizan en el Cloud, se realicen cerca del usuario, en el borde de la red. Esto añade muchos beneficios como:

- Mejora en los tiempos de respuesta
- Mayor confianza de los usuarios en la solución IoT ya que tienen el control sobre los datos
- Optimización energética

La computación en el Edge crea una serie de retos, identificados en [5] y para los que la pasarela o Nodo IoT puede ser una gran oportunidad para la implementación de su solución.

El organismo estandarizador ISO/IEC ha recogido todos estos detalles arquitecturales en la normativa ISO/IEC 30141:2016 [6] que define las características más importantes del IoT para, más adelante, abstraerlas en un modelo conceptual. En base a este modelo la norma propone una plataforma de referencia de alto nivel basándose en la interpretación del modelo conceptual desde cinco perspectivas diferentes. Esta norma será de vital importancia, tal y como se verá más adelante, para poder evaluar, de una manera sistemática, las diferentes plataformas IoT.

III. Trabajo previo en pasarelas IoT

Durante nuestro trabajo en diferentes despliegues IoT hemos tenido la oportunidad de tratar con diferentes tecnologías para plataformas IoT. También hemos desarrollado plataformas IoT específicas para el problema del cliente (ad hoc) que actualmente están gestionando miles de dispositivos IoT en diferentes partes del mundo. Estos despliegues nos han permitido identificar la gran cantidad de detalles que se deben tener en cuenta a la hora de gestionar un gran volumen de dispositivos.

Se pueden encontrar tanto plataformas IoT comerciales como otras desarrolladas en el ámbito académi-

co. En esta sección se analizará el trabajo previo realizado sobre estas plataformas IoT y se realizará una primera selección de aquellas que más tarde se analizarán cualitativamente.

Los criterios de inclusión para este trabajo se han basado en:

- **C.1 Madurez del proyecto**: Para la valoración de este criterio nos hemos basado en el conocimiento experto y una serie de marcadores como la continuidad en su desarrollo (varias versiones con cambios sustanciales), APIs y SDKs estables sin cambios significativos que rompan la compatibilidad hacia atrás, despliegue en entornos reales y bajo carga y despliegue en diferentes casos de uso como por ejemplo ciudades inteligentes o agricultura inteligente.
- **C.2 Continuidad**: Muchas propuestas finalmente no tienen la tracción suficiente, lo que interrumpe su desarrollo y deja el proyecto en un punto donde no puede ser implementado en escenarios reales sin un estudio previo y actualización. Por ejemplo, algunos trabajos teóricos únicamente se acompañan de un repositorio de código sin más actualizaciones después de la publicación.
- **C.3 Código o documentación abierta**: Con el objetivo de analizar la plataforma o plantear una arquitectura de referencia basándonos en el trabajo previo realizado por la plataforma, es necesario el acceso al código fuente o a la documentación para poder analizar las decisiones tomadas arquitecturalmente.
- **C.4 Desplegable en dispositivos de bajo recursos**: El objetivo de la pasarela IoT es que sea capaz de desplegarse en todo tipo de instalaciones IoT con un coste bajo por lo que los requisitos mínimos de despliegue no deberían ser mayores a los de un *Single Board Computer* (SBC) o dispositivo similar.
- **C.5 Gestión del nodo y los dispositivos**: Es importante que las tecnologías desplegadas en el nodo tengan en consideración desde el inicio la posibilidad de actualizar todos sus componentes, dotando al usuario de la capacidad para desplegar nuevas versiones del firmware de los dispositivos así como de los propios servicios del gateway.

En base a estos criterio de inclusión se han seleccionado para su evaluación las plataformas mostradas en Tabla I. Las plataformas mostradas en Tabla II se han estudiado, pero no cumplen algunos de los requisitos. Uno de los problemas a los que nos hemos tenido que enfrentar para hacer este estudio ha sido la poca transparencia en los trabajos académicos a la hora de publicar el código o documentación de referencia que permita estudiar la implementación propuesta además del artículo. Este tipo de práctica complica la capacidad de reproducción de resultados de los trabajos [12].

Tabla I: Plataformas elegidas

Plataforma	Tipo	Ref
Thingsboard	Comunidad	[7]
Home Assistant	Comunidad	[8]
Edge X	Industria	[9]
Bosch IoT Suite	Industria	[10]]
Kura	Comunidad	[11]

Tabla II: Plataformas excluidas

Ref	Tipo	C.1	C.2	C.3	C.4	C.5
[13]	A			X	✓	X
[14]	A			X	✓	X
[15]	A			X	✓	X
[16]	I	✓	✓	X	X	
[17]	I	✓	✓	X	X	
[18]	I	✓		✓	✓	X
[19]	A	✓	X	✓	✓	✓
[20]	I	✓	✓	✓	✓	X
[21]	A	✓		✓	✓	X

IV. Evaluación de plataformas

La evaluación de una arquitectura de pasarela IoT es una tarea compleja debido a la multitud de variables que diferencian cada caso de uso. No obstante, a lo largo de estos años se han desarrollado normas y recomendaciones por los principales centros de estandarización como International Telecommunication Union (ITU), Insitute of Electrical and Electronics Engineers (IEEE) o International Organization for Standardization (ISO). Estas recomendaciones sirven como referencia para la evaluación de arquitecturas para las pasarelas.

En este trabajo basaremos en el estudio realizado en [22] en el que se desarrolla un sistema de evaluación basado en el estándar ISO/IEC 30141:2016 [6].

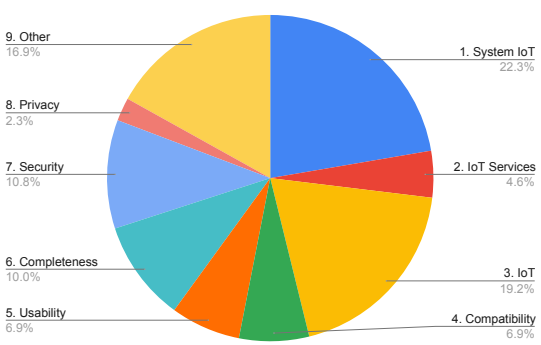

Fig. 3: Distribución de la puntuación asignada a cada epígrafe.

En la Tabla III se toma como base una arquitectura de referencia que define la calificación máxima para cada uno de los apartados de la norma. Sobre esta arquitectura de referencia se evaluarán cada una de las plataformas de la Tabla I. Se examina cada criterio (C_i) pudiéndose dividir éste en varios subapartados ($C_{i,j}$). Cada apartado tiene un peso ($W_{i,j}$) de 1 a 5 basado en el conocimiento experto de los autores. En base a la adecuación de la plataforma a cada criterio se le asigna un valor del 0 al 9 ($V_{i,j}$)

que, multiplicado por el peso del criterio dará lugar al valor complejo ($CV_{i,j}$).

Analizando el trabajo anterior se puede observar (Figura 3) la distribución que se ha realizado a la hora de asignar los pesos o importancia de cada uno de los apartados (C_i) de la tabla. De este modo, los apartados de "System IoT Characteristics" así como "IoT Components Characteristics" son los más importantes. Estos apartados de la norma se centran, principalmente en las capacidades de cara al usuario final del sistema. Se evalúan aspectos como la habilidad para poder realizar tareas en tiempo real, gestionar redes heterogéneas o el soporte a aplicaciones de terceros con capacidad de tener sistemas de suscripción en la propia plataforma. También se valora las posibilidades de sustituir módulos manteniendo la misma funcionalidad, es decir, una arquitectura desacoplada y abierta a cambios.

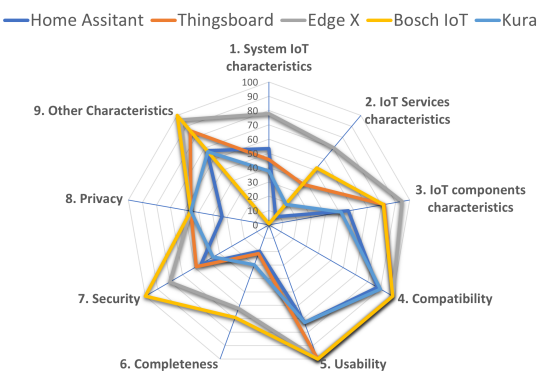

Fig. 4: Resultados obtenidos

Para cada una de las plataformas de la Tabla I se ha aplicado la metodología obteniendo los resultados mostrados en la Figura 4. La figura muestra la puntuación relativa a la plataforma de referencia. Analizando la gráfica se puede ver como hay ciertos apartados donde la mayoría de las plataformas están alejadas de los requisitos impuestos por la norma. Por ejemplo, el apartado "IoT Services" define la capacidad de la plataforma para enriquecer los datos con información contextual así como actuar de forma planificada y en tiempo acotado. Todas las plataformas estudiadas carecen de la capacidad para dar respuesta en un tiempo acotado estricto. Otro aspecto donde las plataformas deben mejorar es en el de privacidad, que, aunque mejora la privacidad ofrecida por el Cloud, todavía carece de mecanismos para etiquetar y proteger de forma activa la información. Ninguna de las plataformas estudiadas tiene la capacidad de etiquetar información sensible y filtrar o avisar al usuario de su uso. Por último, desde el punto de vista funcional todas las plataformas, carecen de mecanismos para autodiagnosticarse e informar de la "salud" del sistema. En este sentido, en los últimos años se ha realizado mucho trabajo en el ámbito de los sistemas ciberfísicos como en [23]

V. Conclusiones y trabajo futuro

Tras el análisis de las diferentes plataformas podemos concluir que todavía queda un gran trabajo para adecuar las tecnologías a los requisitos impuestos por los organismos de estandarización.

Uno de los puntos donde más distancia hay entre la normativa y las implementaciones es la implementación de mecanismos de tiempo real así como mecanismos que aseguren la privacidad de las soluciones desplegadas. En nuestra opinión esto se debe a que, hasta ahora, las soluciones IoT se han desplegado como un mecanismo complementario a instalaciones previas y no como un sustituto de las mismas, delegando las responsabilidades correspondiente al tiempo real a las soluciones tradicionales de la industria. No obstante, en nuevas instalaciones esto puede acarrear un incremento en costes debido a la necesidad de mantener dos sistemas.

En el aspecto de la privacidad ninguna de las plataformas estudiadas implementa ningún mecanismo **explícito** que permita acotar y estudiar el flujo de información de carácter privado. La razón por la que creemos que este apartado no está reforzado es la gran variabilidad en las normativas y la complejidad a la hora de definir qué es la información personal ya que esta puede ser definida no solo por un dato si no por el contexto en el que se produce el dato. En los últimos años se ha trabajado activamente en este aspecto como se puede ver en el trabajo [24] donde se analizan y caracterizan los retos sobre la privacidad en el ecosistema IoT.

En cuanto a las tecnologías usadas por las plataformas hemos observado que hay un consenso en torno al uso de sistemas de componentes software basados en OSGi. Este tipo de tecnología es muy conveniente debido a la facilidad para desarrollar componentes desacoplados pero bien comunicados. No obstante, otras aproximaciones como Edge X que plantean la solución desde un punto de vista basado en contenedores y tecnologías de orquestación que, aunque complican la labor de integración, ayudan a mejorar puntos como los descritos en la norma en los epígrafes: 3.1, 3.2, 3.3, 3.4, 3.5.

Tras este análisis pormenorizado del estado actual en las plataformas IoT podemos concluir que:

- Se debe mejorar los procedimientos para etiquetar y asegurar la privacidad desde el origen del dato.
- Se requiere de una mayor atención a tareas que tengan requisitos temporales o de tiempo real.
- Se debe mejorar la "conciencia" del sistema sobre su estado y proporcionar estrategias de contención para situaciones anómalas.
- Se requiere de una mayor transparencia tanto en la academia como en la industria para mejorar la aceptación de las soluciones propuestas.
- Atendiendo a los resultados de la Figura 4 creemos que se deben tomar como plataformas de referencia para desarrollar futuros trabajos Edge X y Bosch IoT con 995 y 957.

Tabla III: Tabla de referencia para la evaluación de plataformas IoT

Criteria for Evaluation of IoT Reference Architecture	Reference platform		
	Weight	Value	Complex Value
1. System IoT characteristics	29		**261**
1.1 Automatic configuration	5	9	45
1.2 Distinguishing between functional and control resources	3	9	27
1.3 High level of distribution	2	9	18
1.4 Networking Communication	5	9	45
1.5 Control and functioning of the network	2	9	18
1.6 Real time possibility	3	9	27
1.7 Automatic Description	4	9	36
1.8 Subscription for services	5	9	45
2. IoT Services characteristics	6		**54**
2.1 Content information	2	9	18
2.2 Context information	2	9	18
2.3 Temporality	2	9	18
3. IoT components characteristics	25		**225**
3.1 Interchangeability	4	9	36
3.2 Detectability	4	9	36
3.3 Modularity	3	9	27
3.4 Network connectivity	5	9	45
3.5 Sharing	4	9	36
3.6 Unique identification	5	9	45
4. Compatibility	9		**81**
4.1 Support for previous technologies	4	9	36
4.2 Well-Defined components	5	9	45
5. Usability	9		**81**
5.1 Flexibility	4	9	36
5.2 Manageability	5	9	45
6. Completeness	13		**117**
6.1 Authenticity	5	9	45
6.2 Reliability	4	9	36
6.3 Sustainability	4	9	36
7. Security	14		**126**
7.1 Availability	4	9	36
7.2 Confidentiality	5	9	45
7.3 Integrity	4	9	36
7.4 Safety	1	9	9
8. Privacy	3	9	**27**
9. Other Characteristics	22		**198**
9.1 Data - Volume, speed, reliability, variability and diversity	5	9	45
9.2 Heterogeneity	4	9	36
9.3 Compliance with regulatory systems	5	9	45
9.4 Scalability	4	9	36
9.5 Confidentiality	4	9	36
Total			**1170**

Agradecimientos

Financiado parcialmente por el Ministerio de Economía y Competitividad (MINECO) del Gobierno de España (proyecto TALENT-BELIEF, no. PID2020-116417RB-C44), por el programa Europeo Horizonte 2020 bajo el proyecto SHAPES (GA Nº 857159).

Referencias

[1] "Cisco annual internet report (2018–2023) white paper," `https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html`, Accessed 2022-20-05.

[2] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh, "Iot security: Ongoing challenges and research opportunities," in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, 2014, pp. 230–234.

[3] Mohammad Aazam and Eui Nam Huh, "Fog computing and smart gateway based communication for cloud of things," *Proceedings - 2014 International Conference on Future Internet of Things and Cloud, FiCloud 2014*, pp. 464–470, 12 2014.

[4] Anatol Badach, *IIoT – Intelligent IoT*, p. 23, WEKA Media, 03 2019.

[5] Weisong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[6] ISO/IEC, "Internet of Things (IoT) - Reference Architecture," Standard, International Organization for Standardization, Geneva, CH, Aug. 2018.

[7] "Thingsboard open-source iot platform," https://thingsboard.io, Accessed 2022-20-05.

[8] "Home assistant platform," `https://www.home-assistant.io`, Accessed 2022-20-05.

[9] "Edge x foundry," `https://www.edgexfoundry.org`, Accessed 2022-20-05.

[10] "Bosch iot suite," `https://bosch-iot-suite.com/`, Accessed 2022-20-05.

[11] "Kura the extensible open source java/osgi iot edge framework," `https://www.eclipse.org/kura/`, Accessed 2022-20-05.

[12] Jesús M. González-Barahona and Gregorio Robles, "On the reproducibility of empirical software engineering studies based on data retrieved from development repositories," *Empirical Software Engineering*, vol. 17, no. 1-2, pp. 75 – 89, 2012, Cited by: 59; All Open Access, Hybrid Gold Open Access.

[13] Tomislav Vresk and Igor Čavrak, "Architecture of an interoperable iot platform based on microservices," in *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2016, pp. 1196–1201.

[14] Diana Cecilia Yacchirema Vargas and Carlos Enrique Palau Salvador, "Smart iot gateway for heterogeneous devices interoperability," *IEEE Latin America Transactions*, vol. 14, no. 8, pp. 3900–3906, 2016.

[15] Daniel Bimschas, Horst Hellbrück, Richard Mietz, Dennis Pfisterer, Kay Römer, and Torsten Teubler, "Middleware for smart gateways connecting sensornets to the internet," in *Proceedings of the 5th International Workshop on Middleware Tools, Services and Run-Time Support for Sensor Networks*, New York, NY, USA, 2010, MidSens '10, p. 8–14, Association for Computing Machinery.

[16] "Fog horn," `https://www.foghorn.io`, Accessed 2022-20-05.

[17] "Thingworx," `https://www.ptc.com/en/products/thingworx`, Accessed 2022-20-05.

[18] "Ubiworx," `https://ubiworx.com`, Accessed 2022-20-05.

[19] "Agile iot h2020 project," http://agile-iot.eu/, Accessed 2022-20-05.

[20] "Mainflux," `https://mainflux.com`, Accessed 2022-20-05.

[21] Eneko Olivares Gorriti, *Especificación y desarrollo de una pasarela física y virtual para interoperabilidad de dispositivos heterogéneos en el ámbito de Internet de las Cosas*, Ph.D. thesis, Universitat Politecnica de Valencia, 2021.

[22] Luben Boyanov, Valentin Kisimov, and Yavor Christov, "Evaluating iot reference architecture," *2020 International Conference Automatics and Informatics, ICAI 2020 - Proceedings*, 2020.

[23] Ana Petrovska, Stefan Kugele, Thomas Hutzelmann, Theo Beffart, Sebastian Bergemann, and Alexander Pretschner, "Defining adaptivity and logical architecture for engineering (smart) self-adaptive cyber–physical systems," *Information and Software Technology*, vol. 147, pp. 106866, 2022.

[24] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle, "Privacy in the internet of things: Threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728 – 2742, 2013, Cited by: 304; All Open Access, Bronze Open Access, Green Open Access.