

Hub Of Things: Concentrador para el Internet de las Cosas

Ricardo Brea¹, Daniel Skrie¹, Marisa Panizzi¹

¹Escuela de Sistemas. Universidad Argentina John F. Kennedy.
Bartolomé Mitre 1411, Ciudad Autónoma de Buenos Aires (C1037ABA), Tel: 5236-1200
brea.ricardo@gmail.com; dskrie@yahoo.com.ar; marisapanizzi@outlook.com

RESUMEN

En la actualidad, cada vez encontramos más dispositivos electrónicos conectados a internet, monitoreados y controlados en forma remota. La diversidad tecnológica y la cantidad de dispositivos dificulta la integración de los mismos para su control, monitoreo e interacción. Las plataformas basadas en microcontroladores o de procesamiento reducido como *Arduino*, no brindan una conexión con niveles aceptables de seguridad. La privacidad constituye una dificultad, ya que los usuarios desconocen si los distintos proveedores de soluciones *IoT* utilizan sus datos o los venden a terceros. La latencia también es un problema. Muchos de los proveedores de soluciones en la nube no tienen servidores locales, lo que degrada el tiempo de reacción ante determinado evento. Se propone el *Hub Of Things* o *HoT* como una solución que integre localmente o en la nube, el control y monitoreo de los dispositivos. Proveerá además una interface de control, segura y homogénea, tanto gráfica como de programación. Será escalable porque contemplará un método que amplía la variedad de dispositivos a integrar y monitorear, posibilitando su interacción con otros sistemas. El *HoT* intentará solucionar los problemas de la diversidad tecnológica, por medio de una interface homogénea y segura. Sirviendo de mediador entre los dispositivos y el usuario.

Palabras clave: Internet de las Cosas, *Fog computing*, Seguridad, *MQTT*.

CONTEXTO

Este trabajo se desarrolla en la Escuela de Sistemas de la Universidad John F. Kennedy, en el marco de la asignatura Taller de Trabajo Final Integrador de la carrera Licenciatura en Sistemas

1. INTRODUCCION

El término “Internet de las Cosas” o *IoT* por sus siglas en inglés, es un concepto acuñado en 1999 por Kevin Ashton investigador de MIT [1]. Originalmente los datos disponibles en internet eran ingresados o generados por humanos, con la incorporación de sensores y conectividad más accesible. Los dispositivos o “cosas” son capaces de generar datos y pueden ser muy diversos: teléfonos inteligentes, bandas inteligentes (*SmartBands*), estaciones meteorológicas, automóviles, etc.

El *IoT* genera grandes posibilidades de crecimiento, no solo en el ámbito hogareño, también en el industrial conocido como Industria 4.0, o bien en la planificación urbana bajo el concepto de ciudad inteligente o *Smart Cities*.

En la Tabla 1, se representan las distintas proyecciones para el crecimiento de *IoT*, que promedian 25,7 billones de dispositivos para 2020.

Tabla 1 Pronósticos de crecimiento del IoT

Fuente	Billones de Dispositivos
Cisco [2]	26.3
Ericsson [3]	28
Gartner [4]	20.8
Goldman Sachs [5]	28

Con un pronóstico de crecimiento tan optimista es importante detectar los problemas que actualmente presenta el IoT. *Acquity Group* (División de *Accenture* dedicada a la estrategia digital y marketing) realizó en el año 2014 una encuesta a 2000 consumidores de los Estados Unidos, que conociendo los dispositivos *IoT*, no los adquirirían por los siguientes motivos;

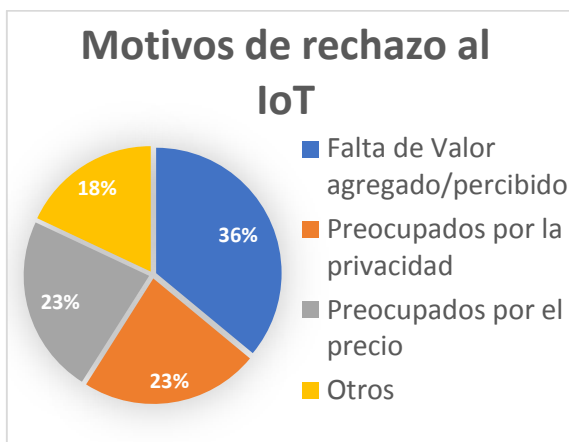


Figura 1. Motivos de rechazo del IoT [6]

La falta de valor agregado es percibida, entre otros motivos, a partir de las dificultades de integración con soluciones similares o existentes.

La preocupación por la privacidad es un elemento inherente a las soluciones en la nube. Los proveedores de estos servicios mitigan el problema con un contrato de privacidad.

La preocupación por el precio responde a varios elementos, como por ejemplo el desconocimiento de las tecnologías y la incertidumbre en los costos de los servicios que formarán parte del costo fijo.

Hay aspectos técnicos que impiden la implementación del *IoT*, como la latencia, el tiempo de respuesta de la solución. Los grandes proveedores de servicios en la nube (Microsoft, Amazon, Oracle e IBM) tienen sus servidores fuera del país y en soluciones industriales, el tiempo de reacción es un factor importante. Para reducir la latencia inherente de las soluciones en la nube surge el

concepto de *Fog Computing* [7] o *Edge Computing* que se refiere a:

- Analizar los datos más sensibles en el *Edge*, el borde, donde se generan los datos, sin necesidad de enviar grandes volúmenes de datos a la red.
- Reaccionar a la información generada en el rango de milisegundos.
- Enviar la información a la nube para su análisis y almacenamiento a largo plazo.

El objetivo del *Hub Of Things* es proveer una plataforma segura, homogénea, extensible y abierta, que opera en el *Fog Computing* y ser utilizada como base en nuevas soluciones *IoT* para el control y monitoreo de dispositivos conectados a internet. El *Hub Of Things* plantea una solución de bajo costo frente a los motivos de rechazo al IoT.

En la figura 2, se presenta que el *Hub Of Things* como un *IoT Gateway*, una solución de software y hardware que serviría de intermediario entre los dispositivos y otros sistemas, ya sea que estén implementados localmente (*On-Premise*) o en la Nube. Se incrementaría la seguridad y estabilidad, reduciéndose la latencia. Se considera que al brindar una capa de abstracción, se reduce el acoplamiento con servicios *IoT* en la nube y permite adaptar otros protocolos de comunicación como *LoRa*, *BLE*, *Modbus*, etc. a un único protocolo, que en este caso es *MQTT*.

MQTT (*Message Queue Telemetry Transport*), es un protocolo usado para la comunicación *machine-to-machine* (*M2M*) en *IoT*. Está orientado a la comunicación de sensores, debido a que minimiza la información adicional a cada mensaje que envía y puede ser utilizado en la mayoría de los dispositivos embebidos y de pocos recursos. *MQTT* sigue una topología de estrella, con un nodo central que hace de servidor o *bróker* y distribuye los mensajes utilizando el patrón *publiser-subscriber* [8].

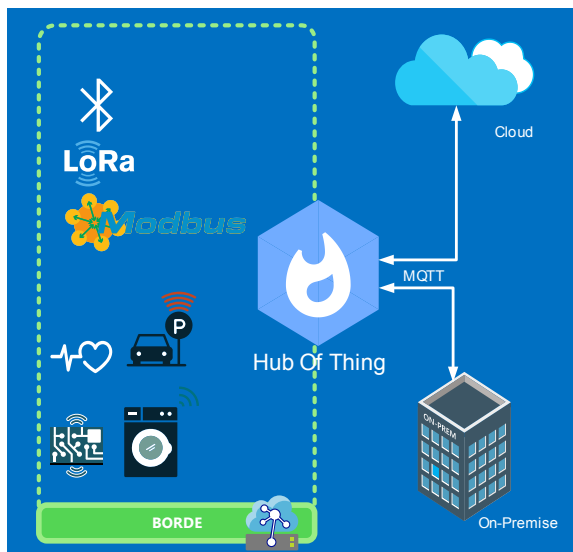


Figura 2 - Arquitectura de alto nivel - HoT

Internamente el *Hub Of Things* contemplará la siguiente arquitectura:

Capa de adaptación: El objetivo de esta capa será proveer una interface de programación, *API*, que permitirá adaptar cualquier protocolo al sistema de mensajes similar a *MQTT*, es decir en tuplas <<*TOPIC, PAYLOAD*>>.

MQTT Bróker: Se implementará con una librería abierta denominada Mosca que implementa el protocolo MQTT sobre TCP y *WebSockets* facilitando la comunicación con clientes JavaScript.

Interface HTML: La capa de presentación se encontrará programada en *HTML5* y *JavaScript* utilizando el *framework Angular* para aplicaciones de una sola página o “*SPA*”. El diseño de la página seguirá la directiva *Material Desing* de Google [9], que se asemeja a los controles del sistema operativo *Android*. Dichas directivas existen para diseñar interfaces de usuario intuitivas, homogéneas y fáciles de utilizar. Otras características de la interface HTML son; Interface *Responsive*, adaptable a varios tipos de dispositivos y gráficos *SVG*, vectoriales que consumen menos espacio y son visibles en cualquier resolución [10].

2. LINEAS DE INVESTIGACION Y DESARROLLO

El *Hub Of Things* es una herramienta que constituye un punto de inicio para otras soluciones *IoT*, vinculadas a problemas particulares o como integradora de soluciones que implementan protocolos no TCP/IP. Las líneas de investigación se verán orientadas a la recopilación de datos y la integración de sistemas. Si bien cada línea puede enfocarse como un trabajo independiente, son mencionadas por que utilizarán el *Hub Of Things* como elemento central.

A saber:

- Integración de sistemas de procesamiento de imágenes como el índice de vegetación de diferencia normalizada o NVDI [11].
- Medición de consumo eléctrico hogareño.
- Monitoreo de variables ambientales urbanas como la concentración de CO₂ o el nivel de ruido ambiente.
- Integración de sistemas inalámbricos *IoT* de largo alcance con *LoRa*.
- Integración de sistema cableados *Modbus*.

3. RESULTADOS OBTENIDOS / ESPERADOS

El objetivo principal de este trabajo es proveer una solución segura, homogénea, extensible y abierta para el control y monitoreo de dispositivos conectados a internet.

Los objetivos de este trabajo son:

- Proveer una *API* que permita la integración de otros dispositivos y protocolos al sistema.
- Brindar flexibilidad a las estructuras de datos para almacenar la configuración de los dispositivos integrados, de forma tal que se pueda incorporar una gran variedad de datos, dada la diversidad de opciones

- Implementar un *Bróker MQTT* integrado con capacidad de conectarse en modo puente a otro *Bróker* central.
- Implementar autenticación en todas las interfaces.
- Desarrollar interface web de usuario intuitiva y flexible tanto a nivel usuario como de programación.
- Implementar seguridad a nivel de transporte. Es decir cifrar las comunicaciones siempre que sea posible desde y hacia los clientes.
- Utilizar componentes propios o de terceros con el único requisito de que sean de código fuente abierto. Para mantener el costo de licencias en cero.
- Definir una arquitectura simple para que pueda ser utilizado tanto en *PC* o *SBC* (computadoras en una placa) como *Raspberry Pi*.

La Pregunta Problema:

¿La incorporación de una solución abierta, homogénea, segura y de bajo costo incrementara la adopción de soluciones IoT en los mercados hogareños (*Smart home*), corporativos (*Smart buildings*), urbano (*Smart Cities*) e industriales (Industria 4.0)?

4. FORMACION DE RECURSOS HUMANOS

En este trabajo que se desarrolla en la Escuela de Sistemas de la Universidad John F. Kennedy, participan un alumno avanzado de la carrera Licenciatura en Sistemas que se encuentra desarrollando su trabajo de fin de carrera, el docente a cargo de la asignatura y la Directora de la Escuela.

5. BIBLIOGRAFIA

- [1] K. Ashton, «That 'Internet of Things' Thing,» 22 JUN 2012. [En línea]. Available: <http://www.rfidjournal.com/articles/view?4986>. [Último acceso: FEB 2016].
- [2] Cisco, «Cisco Visual Networking Index Predicts Near-Tripling of IP Traffic by 2020,» 07 JUN 2016. [En línea]. Available: <https://newsroom.cisco.com/press-release-content?type=press-release&articleId=1771211>. [Último acceso: FEB 2018].
- [3] Ericsson, «Ericsson Mobility Report November 2015,» NOV 2015. [En línea]. Available: <https://www.ericsson.com/assets/local/news/2016/03/ericsson-mobility-report-nov-2015.pdf>. [Último acceso: FEB 2018].
- [4] Gartner, «Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016,» 10 NOV 2015. [En línea]. Available: <https://www.gartner.com/newsroom/id/3165317>. [Último acceso: FEB 2018].
- [5] S. Jankows, J. Covello, H. Bellini, J. Ritchie y D. Costa, «The Internet of Things: Making sense of the next mega-trend,» 3 SEP 2014. [En línea]. Available: <http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf>. [Último acceso: FEB 2018].
- [6] Accenture: Acquity Group, «IoT: The Future of Consumer Adoption,» 2014. [En línea].: https://www.accenture.com/t20150624_T211456_w_/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.pdf. [Último acceso: NOV 2016].
- [7] Cisco, «Fog Computing and the Internet of Things,» 2015. [En línea]: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf. [Último acceso: FEB 2016].
- [8] OASIS, «MQTT Version 3.1.1,» OCT 29 2014. [En línea]. Available: <http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html>. [Último acceso: ENE 2016].

- [9] Google, «Material Design - Guidelines,» 2014. [En línea]. Available: <https://material.io/guidelines/>. [Último acceso: NOV 2016].
- [10] D. Strazzullo, D. D. Dailey and J. Frost, *Building Web Applications with SVG*, Sebastopol, California: O'Reilly Media, Inc., 2012.
- [11] J. Weier y D. Herring, «NASA-Earthobservatory-Measuring Vegetation (NDVI & EVI),» 30 AUG 2000. [En línea]. Available: https://earthobservatory.nasa.gov/Features/MeasuringVegetation/measuring_vegetation_1.php. [Último acceso: JUN 2017].