

# TELEMETRÍA EN LA NUBE

Gustavo Alessandrini, Hernán Garcea, Martín Cioffi, Sebastián Barillaro  
**INTI Electrónica e Informática – UT Informática**  
 gusi@inti.gov.ar

## Introducción

Profesionales y expertos de distintas especialidades concuerdan en que el conjunto de tecnologías que se conocen como Internet de las Cosas (*Internet of Things, IoT*), va a producir un enorme impacto en la sociedad, modificando la vida cotidiana, el mundo laboral, negocios y otros hábitos sociales y culturales. Las posibles aplicaciones son incontables: Vehículos, electrodomésticos, luminarias, cámaras, boyas en altamar, ropa (*wearables*) son algunas de las “cosas” que ya se conectan. La difusión del uso de todo tipo de sensores por todas partes, que miden temperatura, humedad, viento, luz, tráfico de personas y vehículos y un sinnúmero de variables más; todos interconectados generan un gigantesco volumen de datos para tomar decisiones sobre clima, tráfico, seguridad, educación, salud, etc. La telemetría detecta, mide y controla de forma automática los datos de un dispositivo remoto. Su principal ventaja es la transmisión de datos desde dispositivos a un punto de control central incluyendo el camino inverso para enviar información de configuración y control a los dispositivos.

La experiencia recogida en la UT Informática a lo largo de más de 20 años -controlador de despacho de cereales<sup>[1]</sup>, pesaje dinámico<sup>[2]</sup>, sistema para certificación de pilas primarias<sup>[3]</sup>, registradores web<sup>[4]</sup>, entre otros- en diseño, desarrollo, operación y evaluación de una gran cantidad de sistemas embebidos, sus comunicaciones y aplicaciones se extiende ahora a este conjunto de tecnologías, abriendo nuevas líneas de trabajo sobre Internet de las cosas y la moderna telemetría.

Estos antecedentes convergen en la construcción de una línea de trabajo dedicada al estudio de las plataformas IoT, haciendo hincapié en las comunicaciones y los accesos a los servicios de la nube (*cloud computing*).

En las siguientes secciones se describen brevemente dos plataformas estudiadas, servicios de la nube y protocolos utilizados. Por último se presentan las conclusiones del trabajo realizado.

## Objetivos

Estudiar, diseñar y poner en marcha distintas plataformas para implementaciones de IoT. Comunicar las plataformas con servicios en la nube, utilizando protocolos abiertos de uso corriente en el ámbito de IoT.

Evaluar los recursos utilizados y los resultados, para trabajar en un laboratorio dedicado a IoT, como impulso y acompañamiento a la visión de INTI en la incorporación del paradigma de Industria 4.0 en la Industria Argentina.

## Descripción

El estudio de las iniciativas relativas a IoT, indican que se puede organizar sus componentes fundamentales como (figura 1):

- Objetos conectados (“cosas”)
- Tecnologías de red
- Protocolos de comunicación
- Plataforma IoT, para el tratamiento inteligente de datos (*Big Data* o *Small Data*)
- Aplicaciones de usuario

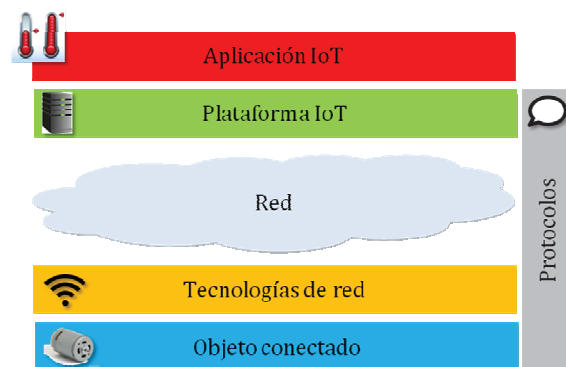


Figura 1. Componentes fundamentales de IoT

Para cumplir con los objetivos planteados, se estudiaron 2 plataformas y 2 servicios de nube:

**Plataforma A:** Se montó sobre una placa de desarrollo de bajo costo basada en un microcontrolador de 32 bits, arquitectura ARM *Cortex M0*, un sensor de temperatura digital y un módulo de WiFi para acceso a Internet. Como servicio de nube se utilizó ThingSpeak<sup>[5]</sup> el cual es un servicio de plataforma de análisis de IoT que permite agregar, visualizar y analizar datos en la nube. Este servicio proporciona visualizaciones instantáneas de los datos enviados por los dispositivos (“cosas”), con la capacidad analizar y procesar en línea los datos a medida que llegan.

El firmware desarrollado lee la temperatura y la envía cada 5 minutos al servicio de nube usando el protocolo HTTP. La información recibida en la nube se puede observar a través de una página web (figura 2) en forma privada o pública según se configure. Se utilizó uno de los servicios implementado, que brinda la

posibilidad de asociar una cuenta de la red social Twitter para generar alarmas que se configuran en función de las variables informadas y los estados de éstas que se quieren señalar como alarmas.

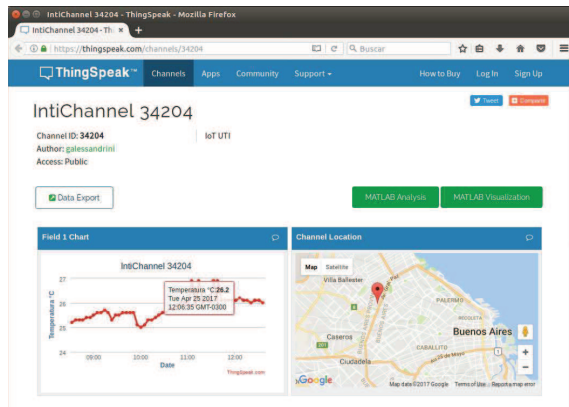


Figura 2. Vista página web de datos de un objeto IoT

**Plataforma B:** Sobre la plataforma Intel Galileo<sup>[6]</sup> que tiene un sistema operativo Linux embebido y conectividad Ethernet, se diseñó un modelo (lectura de temperatura, intensidad de luz, entradas y salidas digitales) para estudiar el protocolo MQTT (*Message Queue Telemetry Transport*)<sup>[7]</sup>, utilizado en IoT. Este protocolo está orientado a la comunicación de sensores, debido a que consume muy poco ancho de banda y puede ser utilizado en la mayoría de los dispositivos embebidos con pocos recursos (CPU y memoria). La arquitectura para MQTT es una topología en estrella (figura 3), con un nodo central que hace de servidor o "broker". Este es el encargado de gestionar la red y de transmitir los mensajes recibidos de los clientes que envían paquetes hacia aquellos clientes que utilizan esos datos. La aplicación de cliente MQTT montada en la plataforma desarrollada, se encarga de recopilar información del dispositivo de telemetría, conectar y publicar la información en el broker. También se suscribe a temas para realizar acciones de configuración y control del dispositivo de telemetría. Otras aplicaciones desarrolladas como clientes suscriptores de MQTT, permiten probar la comunicación tanto con brokers montados en la red del Laboratorio, como con servidores externos.

## Resultados

Se utilizó una metodología de prueba de conceptos sobre las 2 plataformas descritas orientada a obtener datos relevantes para poder caracterizar los métodos implementados y los servicios utilizados.

Las alarmas instauradas para Twitter en la plataforma A, dieron muy buenos resultados para informar situaciones como sobre-temperatura, estados de sensores binarios

(puerta abierta/cerrada, ausencia/presencia de energía, etc.)

La latencia de la red es un tema importante en sistemas de telemetría que incluyen acciones de control sobre los dispositivos remotos. Al ser Internet una red no determinística, se debe evaluar el tiempo máximo de latencia.

Las latencias medidas en la Plataforma B usando servidores MQTT públicos fueron menores a 5 segundos como media normal, detectando casos puntuales mayores a 10 segundos, de acuerdo con los esquemas de calidad de servicio MQTT probados ("transmitir y olvidar", "al menos una vez" y "exactamente una vez").

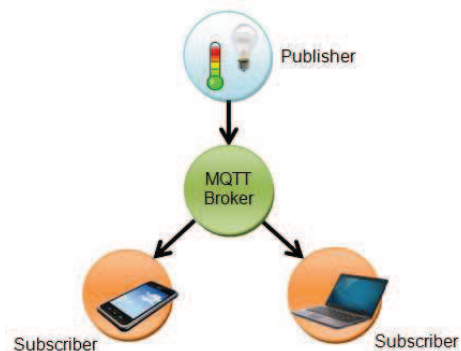


Figura 3. Topología de arquitectura MQTT

## Conclusiones

La computación en la nube permite aumentar el número de servicios basados en la red. Esto genera beneficios tanto para los proveedores, que pueden ofrecer de forma rápida y eficiente, un mayor número de servicios, como para los usuarios que acceden a ellos.

Existen cuestiones relacionadas con la seguridad en los dispositivos conectados. Entre estas se incluyen el no repudio en la transmisión, la autorización de cualquier acción de control y la privacidad de los datos. Para garantizar estos puntos, los datos transferidos entre el objeto conectado y el punto de control remoto mediante MQTT se pueden cifrar mediante *Transport Layer Security* (TLS).

Durante el desarrollo del trabajo se adquirió gran experiencia en las plataformas utilizadas y los servicios de nube usados.

## Referencias

- [1] <http://www-biblio.inti.gob.ar/gsd/collect/inti/index/assoc/HASH01bb.dir/doc.pdf>
- [2] <http://www-biblio.inti.gob.ar/gsd/collect/inti/index/assoc/HASH08090/e1f8c460.dir/doc.pdf>
- [3] <http://www-biblio.inti.gob.ar/trabinti/304765.pdf>, pag 164
- [4] Registrador de datos y sistema de monitoreo web. Tecno INTI 2017.
- [5] [www.thingspeak.com](http://www.thingspeak.com)
- [6] <https://software.intel.com/en-us/iot/hardware/galileo>
- [7] [www.mqtt.org](http://www.mqtt.org)