

# Curso: (62949) Internet para las cosas

Fernando Tricas García

Departamento de Informática e Ingeniería de Sistemas  
Universidad de Zaragoza

<http://webdiis.unizar.es/~ftricas/>

<http://moodle.unizar.es/>

[ftricas@unizar.es](mailto:ftricas@unizar.es)

# La nube

Fernando Tricas García

Departamento de Informática e Ingeniería de Sistemas  
Universidad de Zaragoza

<http://webdiis.unizar.es/~ftricas/>

<http://moodle.unizar.es/>

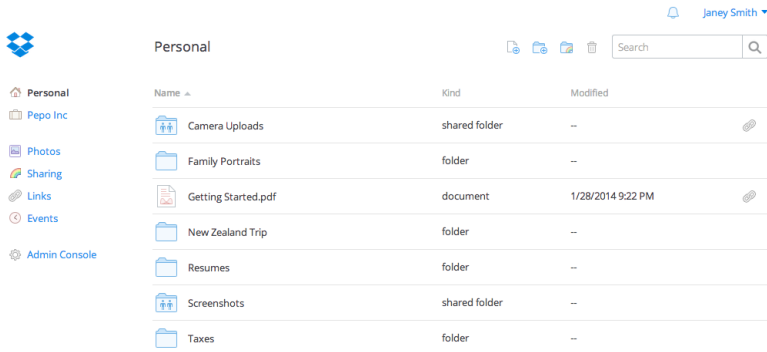
[ftricas@unizar.es](mailto:ftricas@unizar.es)



# ¿Qué es la nube?



# ¿Qué es la nube?



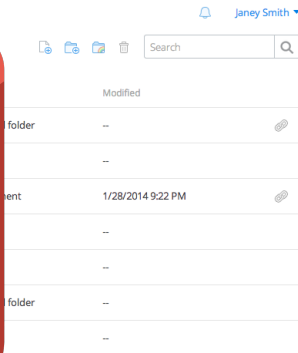
Personal

Janey Smith

Name	Kind	Modified
Camera Uploads	shared folder	--
Family Portraits	folder	--
Getting Started.pdf	document	1/28/2014 9:22 PM
New Zealand Trip	folder	--
Resumes	folder	--
Screenshots	shared folder	--
Taxes	folder	--



# ¿Qué es la nube?

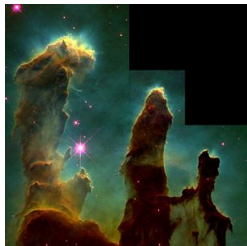


# ¿Qué es la nube?



## ¿Qué es la nube?

*Cloud*: en ciencia, una aglomeración grande de objetos que desde la distancia aparecen visualmente como una nube. Se utiliza para describir un conjunto de elementos a cuyos detalles no se va a prestar atención.



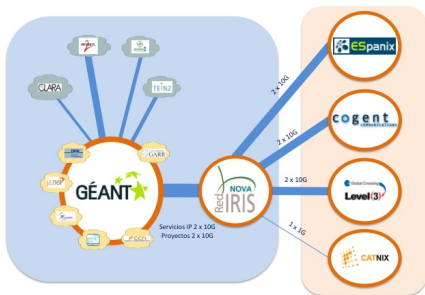
'Nebulosa del Águila (M16)'

Fotografía: <http://es.wikipedia.org/wiki/Nebulosa>

## ¿Qué es la nube?

*Cloud*: en ciencia, una aglomeración grande de objetos que desde la distancia aparecen visualmente como una nube. Se utiliza para describir un conjunto de elementos a cuyos detalles no se va a prestar atención.

También está relacionado con los esquemas que dibujaban algunos programas antiguos para referirse a los servidores.

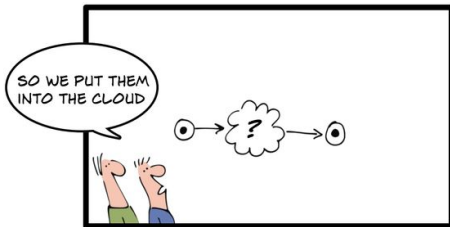
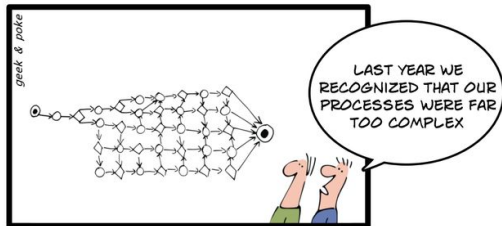


<http://www.rediris.es/lared/externas.html>





# ¿Qué es la nube?



LET THE CLOUDS MAKE YOUR LIFE EASIER

<http://geekandpoke.typepad.com/geekandpoke/2009/03/let-the-clouds-make-your-life-easier.html>

# ¿Qué es la nube?

1970s Tiempo compartido, batch,....

1980s Computador personal

2000s Web 2.0, servicios web, ...



# ¿Qué es la nube?

*Cloud*: servicios informáticos compartidos a través de internet.

- ▶ Servicios: almacenamiento, cálculo (cómputo), servicios, ...



# ¿Por qué?

- ▶ Accesibilidad
- ▶ Robustez
- ▶ Economía
- ▶ Disponibilidad
- ▶ Escalabilidad
- ▶ Time to market



# ¿Sólo ventajas?

- ▶ Dependencia
- ▶ Sensación de pérdida de privacidad/control
- ▶ Necesidad de internet
- ▶ Regulación, leyes, ...
- ▶ ¿Estandarización?
- ▶ Barreras de la organización
- ▶ Adaptación



# ¿Y para qué?

- ▶ El uso más 'popular' es el almacenamiento (Dropbox, Drive, One Drive, ..)
- ▶ Aplicaciones web (GMail y equivalentes, Twitter, Facebook, ...)
  - ▶ Instagram, Netflix, YouTube, ...
  - ...
- ▶ Servicios web (APIs, ...)
- ▶ Computadores como servicio



## Un poco de historia



# La nube al revés

*The “RSA challenge” published in the August 1977 issue of Scientific American (in Martin Gardner’s column) is still open, and the \$100 prize offer still stands. This prize can be won by factoring the RSA modulus published there, which is:*

RSA-129 =

1143816257578888676692357799761466120102182967212423625

<http://www.interesting-people.org/archives/interesting-people/199311/msg00077.html>

Noviembre 1993



Departamento de  
Informática e Ingeniería  
de Sistemas  
Universidad Zaragoza



# Primeros intentos

- ▶ Rivest estimaba  $4 \times 10^{16}$  años de computación para lograrlo
  - ▶ RSA-129, se factorizó el 2 de abril de 1994 (criba cuadrática)
  - ▶ Cálculo distribuido (e-mail y ftp)
  - ▶ Código fuente
  - ▶ 'That said, it runs happily on any Unix box with at least 8Mb of physical memory.'
  - ▶ Unos 600 computadores



# Por si alguien quiere comprobarlo

1143816257578888676692357799761466120102182  
9672124236256256184293570693524573389783059  
7123563958705058989075147599290026879543541

=

34905295108476509491478496199038  
98133417764638493387843990820577

×

32769132993266709549961988190834  
461413177642967992942539798288533

---

[http://www.revistasic.com/revista40/agorarevista\\_40.htm](http://www.revistasic.com/revista40/agorarevista_40.htm)

<http://en.wikipedia.org/wiki/RSA-129>

Para leer la historia:

<http://unaaldia.hispasec.com/2013/10/>

<martin-gardner-rsa-y-otros-pasatiempos.html>



# Resolver los problemas 'a trozos'

¿Puede tener sentido resolver algunos problemas usando procesadores de la gente?

## ▶ SETI@home

- ▶ Público el 17 de mayo de 1999
- ▶ Análisis de señales recibidas en el radiotelescopio de Arecibo



## ▶ Berkeley Open Infrastructure for Network Computing

- ▶ Supercomputador voluntario de propósito 'general'
- ▶ 435,000 computadores, 521 TFlops (12 marzo de 2007)
- ▶ Un montón de proyectos ...



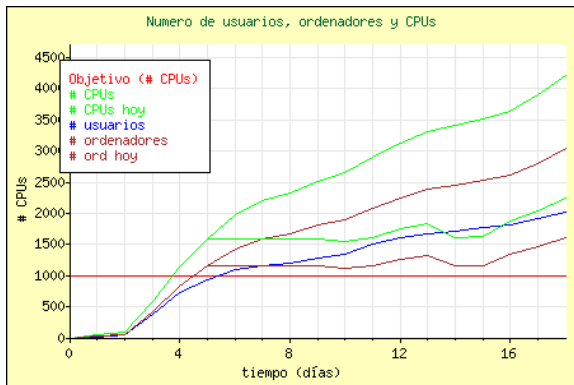
Y claro ...



**Zivis**

<http://www.ibercivis.es/>

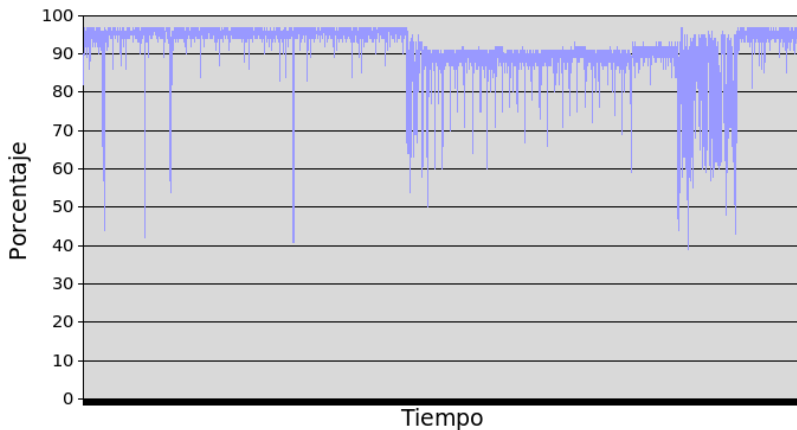
- ▶ Supercomputador ciudadano
- ▶ Confinamiento de partículas en un campo magnético



Departamento de  
Informática e Ingeniería  
de Sistemas  
Universidad Zaragoza

Además ...

## Desuso de mi ordenador



## De hecho, los 'malos' también

- ▶ CIH (1998) de 20 a 80 millones de dólares.
- ▶ Melissa (1999) 300 a 600 millones de dólares
- ▶ ILOVEYOU (2000) de 10 a 15 billones de dólares
- ▶ Code Red (2001) 2.6 billones de dólares.
- ▶ SQL Slammer (2003), 500000 servidores. Poco daño porque era sábado.
- ▶ Blaster (2003)
- ▶ SoBig (agosto 03) de e 5 a 10 billones de dólares y más de un millón de ordenadores infectados.  
1 millón de copias de él mismo en las primeras 24 horas.
- ▶ Bagle (2004) Muchas variantes
- ▶ Sasser (2004) suficientemente destructivo como para colgar algunas comunicaciones satelites de agencia francesas.  
Tambien consiguió cancelar vuelos de numeros compañías aéreas.

No necesitaba acciones por parte del usuario para propagarse.



# ¿Qué pasó con ellos?

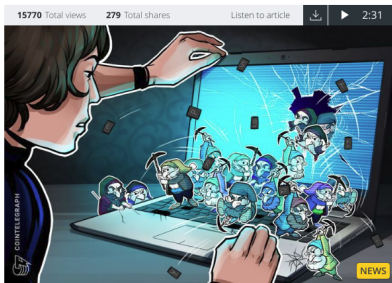
- ▶ Comercialización
- ▶ Botnets, 'llaves mano' para
  - ▶ Molestar
  - ▶ Phishing
  - ▶ Robar
  - ▶ ...







## Cryptojacking Overtakes Ransomware as Top Malware in Some Countries



Cryptojacking, the unauthorized use of another's hardware to mine cryptocurrency, has become the biggest cyber threat in many parts of the world, Bloomberg reported Dec. 14.

<https://cointelegraph.com/news/>

[cryptojacking-overtakes-ransomware-as-top-malware-in-some-countries](https://cointelegraph.com/news/cryptojacking-overtakes-ransomware-as-top-malware-in-some-countries)

# Grid Computing

Colección de recursos de computación distribuidos geográficamente coordinados para obtener algún resultado.

- ▶ Sistemas distribuidos (paralelismo)
- ▶ Heterogéneos
- ▶ 'Middleware'
- ▶ Acoplamiento débil
- ▶ Internet
- ▶ Escalabilidad (¿?)
  - ▶ Confianza
  - ▶ Disponibilidad



# Utility Computing

**Alquilar** recursos computacionales (hw, sw, red,...) en base a las necesidades y bajo demanda.

- ▶ No siempre es distribuido
- ▶ No siempre virtualización

## 1990's



# Software as a Service (SaaS)

Los programas están disponibles bajo un modelo de suscripción, alojados remotamente. También se habla de programas bajo demanda 'on-demand software'.

- ▶ Centralizado (ASP → Application Service Provider).
- ▶ Reducción de costes
- ▶ Puede ser necesario un cliente (normalmente interfaz web).

Palabra clave: suscripción

## 2001



# Cloud Computing

Recursos computacionales compartidos y datos bajo demanda.  
Grid → Utility → SaaS → Cloud Computing



# Algunos tipos

- ▶ Pública. Servicio compartido con otros clientes.
- ▶ Privada. Servicio propio, servidores exclusivos.
- ▶ Híbrida. Mezcla de las dos anteriores.



# Los proveedores

ISP 1.0: conectividad y acceso a la red

- ▶ Servicios básicos de internet (servidor web, correo,...)



# Los proveedores

ISP 2.0: Aumentar servicios

- ▶ Más servicios (aplicaciones, servidor web más complejo, ...)





# Los proveedores

ISP 3.0 (collocation): no sólo servicios, también servidores

- ▶ Hosting/**Housing**



# Los proveedores

ASP (ISP 4.0)

- ▶ Aplicaciones



# Cloud Computing

ISP 1.0 → ISP 2.0 → ISP 3.0 → ASP  
→ Cloud Computing (ISP 5.0)



- ▶ Web Services & SOA (Service Oriented Architecture)
  - ▶ O REST



- ▶ Web Services & SOA (Service Oriented Architecture)
  - ▶ O REST

## Servicios web:

- ▶ Los servicios son componentes de software con interfaces bien definidas (independientes de la implementación).
- ▶ Autocontenidos
- ▶ Descubrimiento dinámico
- ▶ Se pueden crear servicios compuestos

- ▶ Web Services & SOA (Service Oriented Architecture)
  - ▶ O REST

## REST (Representational State Transfer):

- ▶ Cliente/Servidor
- ▶ Conjunto de operaciones (POST, GET, PUT, DELETE)
- ▶ Sintaxis universal, direccionamiento a través de la URL
- ▶ Enlaces

- ▶ Escalabilidad masiva // crecimiento rápido de usuarios
- ▶ APIs estándar (Application Programming Interface)
- ▶ Virtualización
- ▶ Redes rápidas

Palabras clave: interoperabilidad, portabilidad, estandarización, abstracción, reusabilidad, ...



- ▶ Abstracción de recursos
  - ▶ Por software (posible ayuda del hw)
  - ▶ Máquina virtual (computador simulado mediante programas que ejecuta otros programas como si fuera la máquina real).  
Nivel hardware // Nivel sistema operativo // nivel aplicaciones  
// Almacenamiento



- ▶ No consume energía cuando no se usa
- ▶ Gestión más eficiente

## *[SaaS] Software as a Service, los programas*

- ▶ *Servicios*
- ▶ *Más conocido*
- ▶ *La aplicación la proporciona el proveedor*
- ▶ *Google Apps*
- ▶ *Salesfoce (CRM, Customer Relationship Management)*
- ▶ *Flickr, Instagram*
- ▶ *Moodle*
- ▶ *Campus Docente Sigma*
- ▶ *...*

## *[PaaS] Platform as a Service, los programas*

- ▶ *Los desarrolladores utilizan la infraestructura según las necesidades de los servicios que crean.*
- ▶ *Amazon E2C (Elastic Compute cloud)*
- ▶ *Microsoft Azure*
- ▶ *Sistema operativo*
- ▶ *Persistencia de datos, almacenamiento*
- ▶ *Servidores*
- ▶ *Alojamiento (hosting)*



## *[IaaS] Infrastructure as a Service, los servidores*

- ▶ *Capacidad para alquilar (centros de datos y servidores)*
- ▶ *Evolución de alojamiento de servidores*
- ▶ *Amazon E2C & S3*
- ▶ *Rackspace*
- ▶ *Azure*



# Hay más

*[NaaS] Network as a Service*

- ▶ *Abstracción de la red*
- ▶ *Akamai*

DaaS (Data), CaaS (Communication)



## Seguridad

Control, prestaciones, soporte, bloqueo del vendedor, personalización, velocidad para activar servicios,...



# La seguridad

- ▶ Leyes internacionales sobre privacidad
- ▶ Propiedad de los datos
- ▶ Garantía de servicio
- ▶ Seguridad de las máquinas virtuales
- ▶ Fallos
- ▶ Cifrado
- ▶ Alojamiento de datos personales
- ▶ Planificación frente a contingencias / recuperación



# Casos de uso

**SaaS** Primer paso sencillo (algunas aplicaciones)

**PaaS** Empresas pequeñas y nuevas (sin coste de adquisición)

**IaaS** Nueva aproximación Utility Computing // Escalar con un proveedor externo para cargas puntuales.





¿Qué ejecutamos dónde y  
cómo?  
¿Cómo lo gestionamos?





The Internet Toaster – John Romkey (1989)

[http://www.livinginternet.com/i/ia\\_myths\\_toast.htm](http://www.livinginternet.com/i/ia_myths_toast.htm)

TCP/IP<sup>1</sup> – SNMP<sup>2</sup>

---

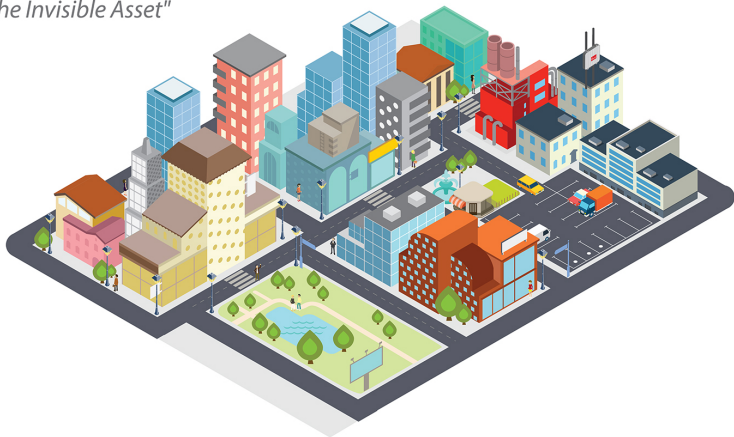
<sup>1</sup>Transmission Control Protocol/Internet Protocol

<sup>2</sup>Simple Network Management Protocol

# IoT Security Infographic

Privacy, Authenticity, Confidentiality and Integrity  
of the Sensor Data

*"The Invisible Asset"*

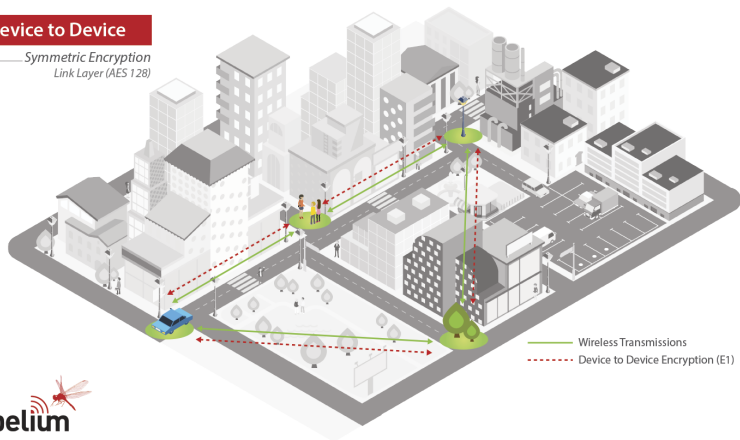


Centro de  
Investigación en  
Sistemas de Ingeniería  
Universidad Zaragoza

# IoT (Ejemplo Smart city)

## Device to Device

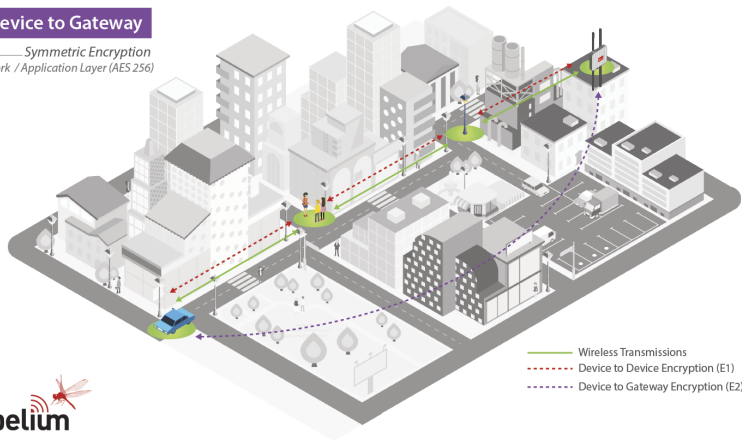
Symmetric Encryption  
Link Layer (AES 128)



# IoT (Ejemplo Smart city)

## Device to Gateway

— Symmetric Encryption  
Network / Application Layer (AES 256)

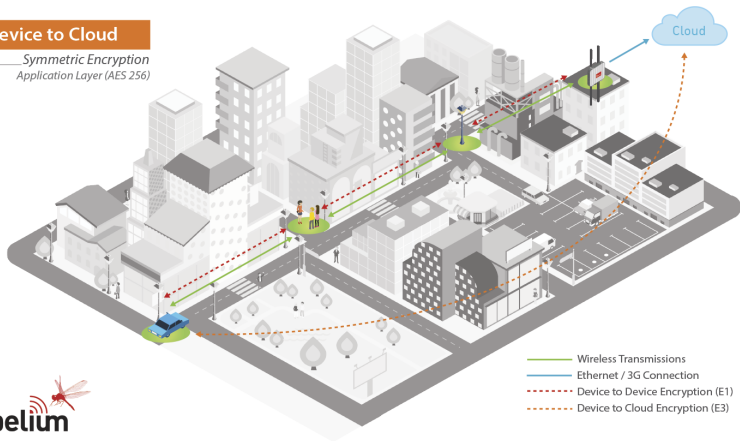


- Wireless Transmissions
- - - Device to Device Encryption (E1)
- - - Device to Gateway Encryption (E2)

# IoT (Ejemplo Smart city)

## Device to Cloud

*Symmetric Encryption*  
Application Layer (AES 256)



# IoT (Ejemplo Smart city)

## Gateway to Cloud

Secure Web Server  
Application Layer (SSL, HTTPS)



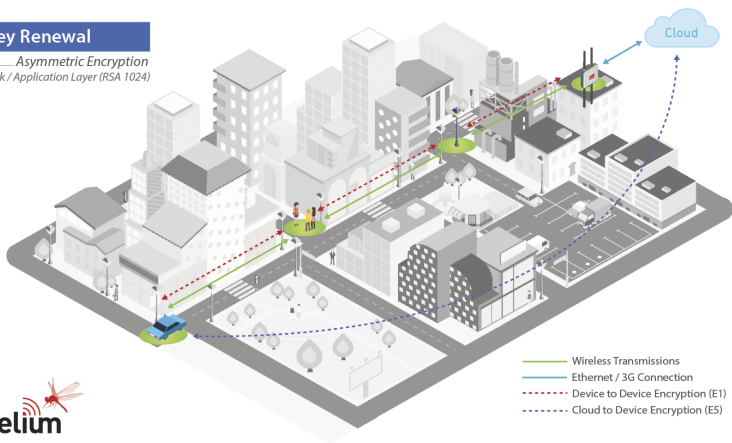
— Ethernet / 3G Connection  
- - - Gateway to Cloud Encryption (E4)



# IoT (Ejemplo Smart city)

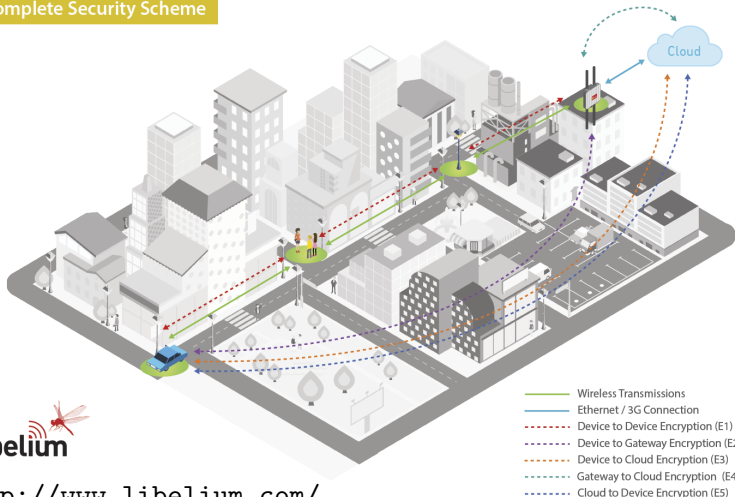
## Key Renewal

*Asymmetric Encryption*  
Network / Application Layer (RSA 1024)





## Complete Security Scheme



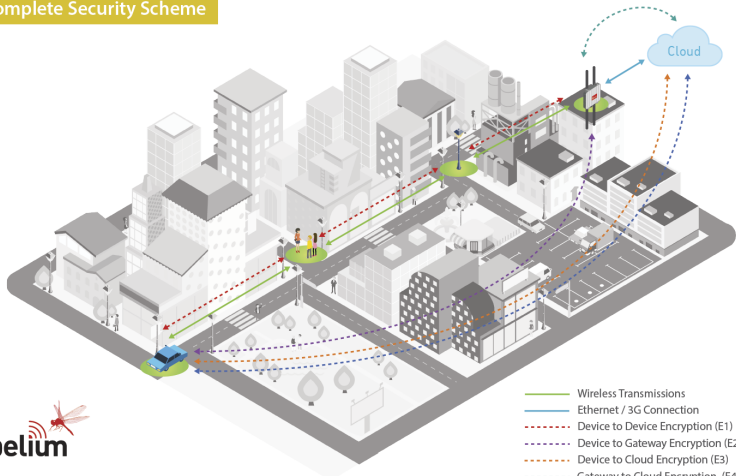
<http://www.libelium.com/>

iot-security-infographic-privacy-authenticity-confidentiality

IoT Security Infographic – Privacy, Authenticity, Confidentiality

# IoT (Ejemplo Smart city)

## Complete Security Scheme

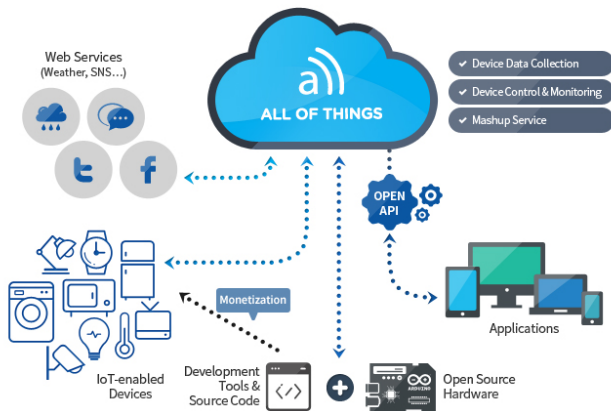


<http://www.libelium.com/>

iot-security-infographic-privacy-authenticity-confidentiality

IoT Security Infographic – Privacy, Authenticity, Confidentiality

# IoT cloud



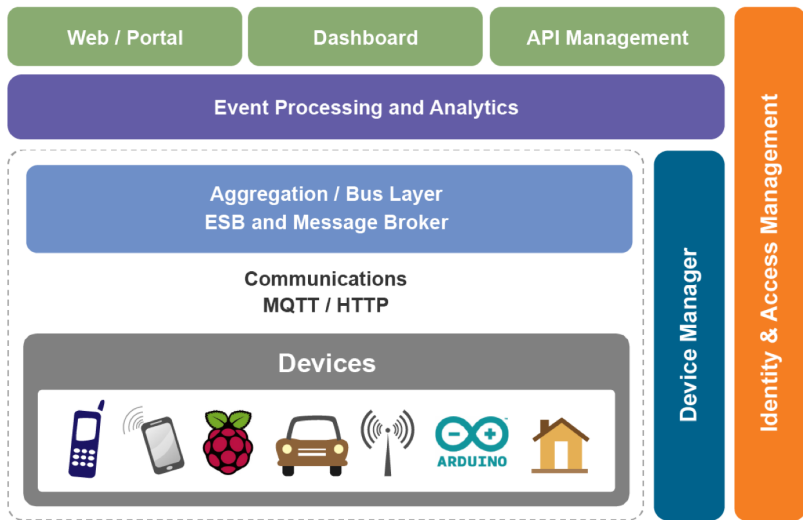
<http://www.ntels.com/en/press-20150708/>



Departamento de  
Informática e Ingeniería  
de Sistemas  
Universidad Zaragoza

# IoT Reference Architecture

## IoT Reference Architecture



WSO2 <http://wso2.com/>



Departamento de  
Sistemas de Ingeniería  
Universidad Zaragoza

# HTTP/MQTT

## HTTP

Hyper Text Transfer Protocol

## MQTT

MQ Telemetry Transport. Protocolo de publicación/transporte de mensajes cliente/servidor.

- ▶ Ligero
- ▶ Abierto
- ▶ Simple y diseñado para que sea fácil de implementar



# Gestión de mensajes

(Por completitud)

ESB

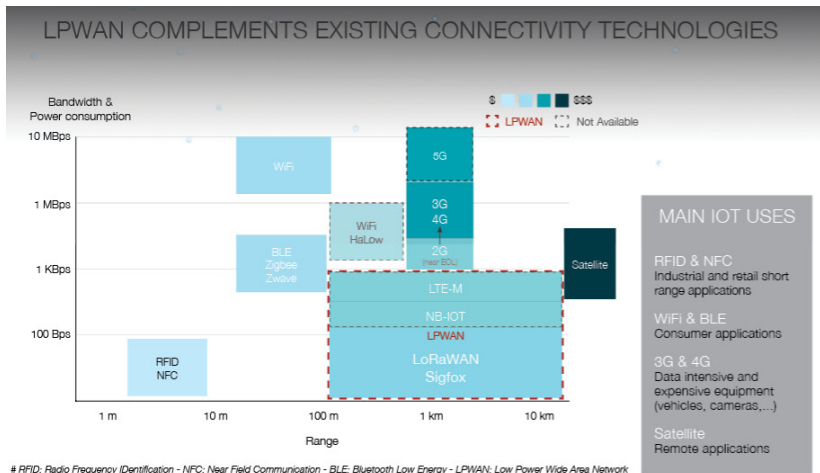
Enterprise Service Bus

Message Broker

Gestor de mensajes



# Conectividad



IoT Connectivity – Comparing NB-IoT, LTE-M, LoRa, SigFox, and other LPWAN Technologies

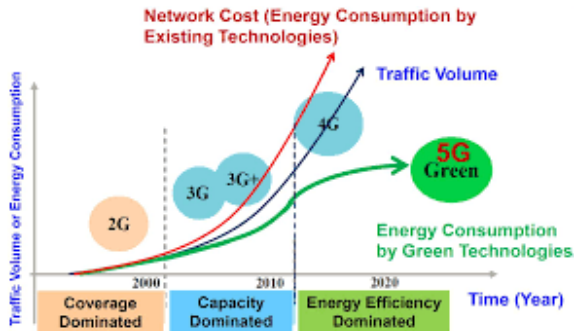
<https://www.ietfforall.com/>

[iot-connectivity-comparison-lora-sigfox-rpma-lpwan-technologies/](https://www.ietfforall.com/iot-connectivity-comparison-lora-sigfox-rpma-lpwan-technologies/)



Departamento de  
Informática e Ingeniería  
de Sistemas  
Universidad Zaragoza

# Conectividad y consumo

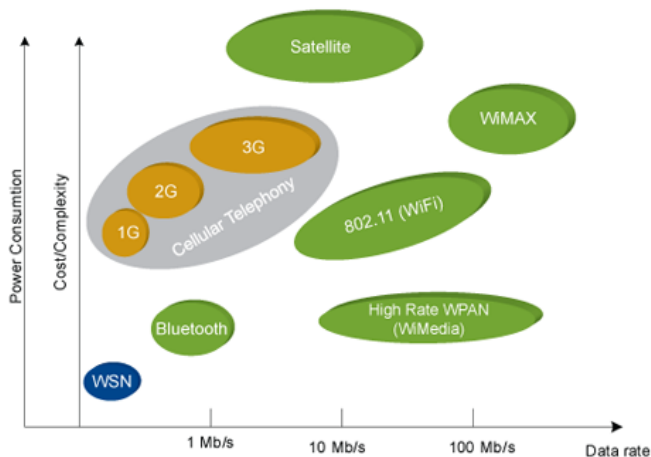


5G Wireless Communication – Vision & Challenges (Nov. 2017)

<http://gcek.ac.in/ece/fdp/materials/0/Day1.pdf>



# Conectividad y consumo



Standards & Feature Comparison - WSN Technology - A.N. Solutions

<http://www.an-solutions.de/images/standarts.html>  
(No disponible)



# Algunas características de los dispositivos IoT

- ▶ Duración (¿actualizaciones?)
- ▶ Tamaño (¿capacidades?)
- ▶ Es un dispositivo (¿gestión?)
- ▶ Datos (a menudo personales)
- ▶ La percepción (¿electrodomésticos?)



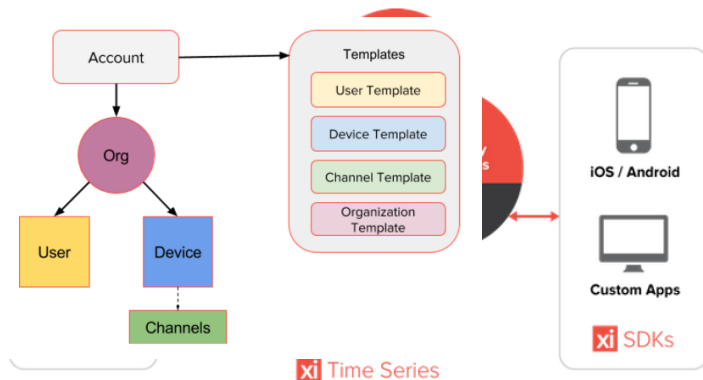
Xively<sup>3</sup> (<https://xively.com/>)



<sup>3</sup>2007 Pachube, 2011 LogMeIn → Cosm, 2013 Xively, marzo 2018 comprado por Google



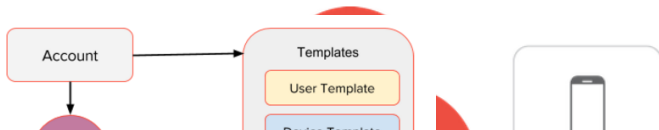
Xively<sup>3</sup> (<https://xively.com/>)



<sup>3</sup>2007 Pachube, 2011 LogMeIn → Cosm, 2013 Xively, marzo 2018

comprado por Google

Xively<sup>3</sup> (<https://xively.com/>)



## Example

```
mosquito_sub
-p 8883
-h broker.xively.com
-i 5d1e827d-bc31-48d7-bd37-f6bf13146d32
-u 5d1e827d-bc31-48d7-bd37-f6bf13146d32
-P sr845jg03lfv35=4kgk3rksdfmmlw34342mfcsdf34vn
-t xi/blue/v1/kb133d3d-1234-5fb1-ba4v-492daac5481c/d/6df62b2c-38af-45b0-bae8-95e56191a381/fanspeed
--cafile ~/Desktop/ca-certificates-gsrl.crt
```

<sup>3</sup>2007 Pachube, 2011 LogMeln → Cosm, 2013 Xively, marzo 2018  
comprado por Google



# Subscripción

## Example

```
mosquitto_sub
-p 8883
-h broker.xively.com
-i 5d1e827d-bc31-48d7-bd37-f6bf13146d32
-u 5d1e827d-bc31-48d7-bd37-f6bf13146d32
-P sr845jg03lfv35=4kgk3rksdfmmlw34342mfc sdf34vn
-t xi/blue/v1/kb133d3d-1234-5fb1-ba4v-492daac5481c/d/6df62b2c-38af-45b0-bae8-95e56191a381/fanspeed
--cafile ~/Desktop/ca-certificates-gsr1.crt
```

- ▶ -i Client ID
- ▶ -u Username
- ▶ -P Password
- ▶ -t Topic name



# Publishing

## Example

```
mosquitto_pub
-p 8883
-h broker.xively.com
-i 6df62b2c-38af-45b0-bae8-95e56191a381
-u 6df62b2c-38af-45b0-bae8-95e56191a381
-P 238tjglf/f=2o9ymbvo3klfm3owfft4g3fvdfg-594kf
-t xi/blue/v1/kb133d3d-1234-5fb1-ba4v-492daac5481c/d/6df62b2c-38af-45b0-bae8-95e56191a381/fanspeed
--cafile ~/Desktop/ca-certificates-gsr1.crt
-m '[
{"name":"controlcommand","value":"1"},
{"name":"message","value":"Hello. My Name is Inigo Montoya."}
]'
```

- ▶ -i Client ID
- ▶ -u Username
- ▶ -P Password
- ▶ -t Topic name
- ▶ -m Message



## ThingSpeak (<https://thingspeak.com/>)



### Luz y temperatura cada 1 minuto

Channel ID: **82841**  
Author: **oskimac**  
Access: **Public**

<http://weather.msfc.nasa.gov/cgi-bin/get-goes?satellite=GOES-E%20FULL&lat=-24&lon=-66&zoom=1&palette=ir10.pal&info=vis&past=0>  
direccion para ver imagenes satelitales  
📌 registrar, control, Temperatura, computadora, Arduino, oscar, Uruguay, luz, cada 60 segundos

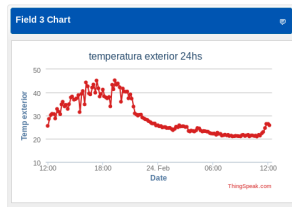
Data Export

More Information

MATLAB Analysis

MATLAB Visualization

More Apps



<https://thingspeak.com/channels/82841> (viejo)

<https://thingspeak.com/channels/210101>

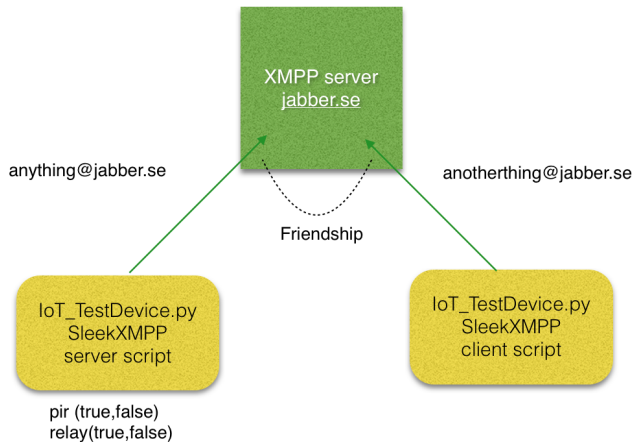
<https://thingspeak.com/channels/406174>





# Lo único necesario es Internet

XMPP-IOT (<http://www.xmpp-iot.org/>)



# ¿Cloud?

- ▶ Integración de datos de varias fuentes
- ▶ Recolección automatizada
- ▶ ¡Análisis!



## Google IoT Cloud

### Solutions

Send feedback

Learn  
Why Google  
Customer successes  
Partners  
Products  
Resources

### Internet of Things

There is the potential for 50 billion connected devices by 2020. Google Cloud Platform gives you the tools to scale connections, gather and make sense of data, and provide the reliable customer experiences that hardware devices require.

TRY IT FREE



Send feedback

### Solutions

Learn  
Why Google for Big Data  
Customer successes  
Partners  
Products  
Resources

### Big Data

Today's applications are generating more and more data all the time. And this data is being generated faster. Use the products and services on Google Cloud Platform to help you collect, ingest, and analyze your data. With Google Cloud Platform, you can take advantage of Google's scale and speed to quickly and cost effectively use your data to benefit your application.

TRY IT FREE



<https://cloud.google.com/solutions/iot/>



Departamento de  
Informática e Ingeniería  
de Sistemas  
Universidad Zaragoza

**Fog Computing:** utilizar los dispositivos (que tienen cada vez más capacidades) para hacer parte del procesado/almacenamiento/comunicaciones.

**Table 2**

Cloud Computing	Fog Computing
Data and applications are processed in a cloud, which is time consuming task for large data.	Rather than presenting and working from a centralized cloud, fog operates on network edge. So it consumes less time.
Problem of bandwidth, as a result of sending every bit of data over cloud channels.	Less demand for bandwidth, as every bit of data's were aggregated at certain access points instead of sending over cloud channels.
Slow response time and scalability problems as a result of depending servers that are located at remote places.	By setting small servers called edge servers in visibility of users, it is possible for a fog computing platform to avoid response time and scalability issues.

<http://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing>



# La niebla

- ▶ Reducción en el movimiento de datos (coste, latencia, ...)
- ▶ Descentralización (eliminación del punto de fallo).
- ▶ Mejoras en la seguridad
- ▶ Velocidad pero también un buen nivel en escalabilidad, confiabilidad, tolerancia a fallos
- ▶ Menos ancho de banda



# Referencias

'Introduction to Cloud Computing'

[http://www.slideshare.net/DSPIP/  
cloud-computing-introduction-2978287](http://www.slideshare.net/DSPIP/cloud-computing-introduction-2978287)

'Introduction to Cloud Computing'

[http://www.slideshare.net/ProfEdge/  
introduction-to-cloud-computing-23970527](http://www.slideshare.net/ProfEdge/introduction-to-cloud-computing-23970527)

'Llegando a la Industria 4.0 a través del IoT'

[http://www.slideshare.net/BrunoCendn/  
llegando-a-la-industria-40-a-travs-del-iot](http://www.slideshare.net/BrunoCendn/llegando-a-la-industria-40-a-travs-del-iot)

