物聯網通訊與安全

第1章 物聯網
Internet of Things (IoT)

蘇維宗 (Wei-Tsung Su)
suwt@au.edu.tw
564D

歷史版本

版本	說明	日期	負責人
v1.0	初版	2019/02/18	蘇維宗

History

Networked Devices

The concept of a network of smart devices was discussed as early as **1982**, with a modified Coke vending machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold or not.

Source: *Wikipedia*

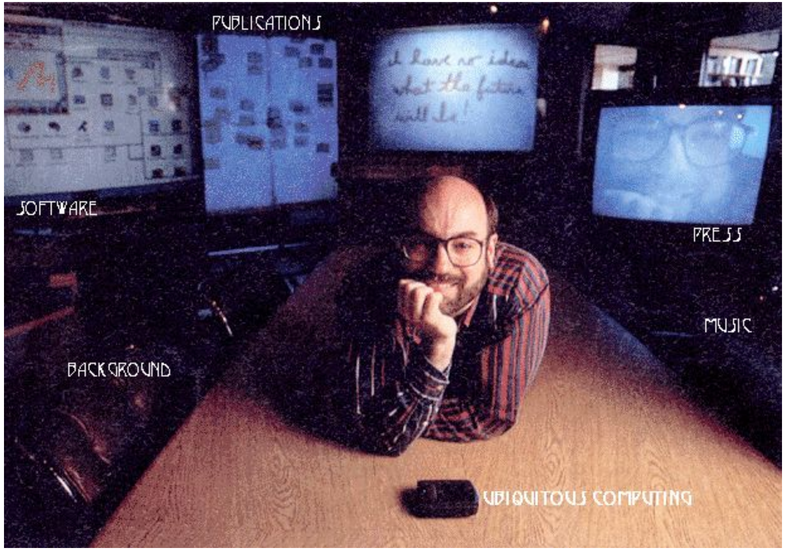
Ubiquitous Computing

The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

Mark Weiser, Chief Scientist, Xerox PARC

The Computer for Twenty-First Century, Scientific American

1991



Source: *Wikipedia*

Inventor of Term "IoT"

Kevin Ashton was the first to use the term Internet of Things (IoT) in **1999** in the context of supply chain management with radio frequency identification (RFID)-tagged or barcoded items (things) offering greater efficiency and accountability to businesses.

Source: *Wikipedia*

Definition from Wikipedia

The Internet of things (IoT) is the network of devices such as vehicles, and home appliances that contain electronics, software, sensors, actuators, and **connectivity** which allows these things to connect, interact and exchange data.

IoT is a multiple-discipline engineering.

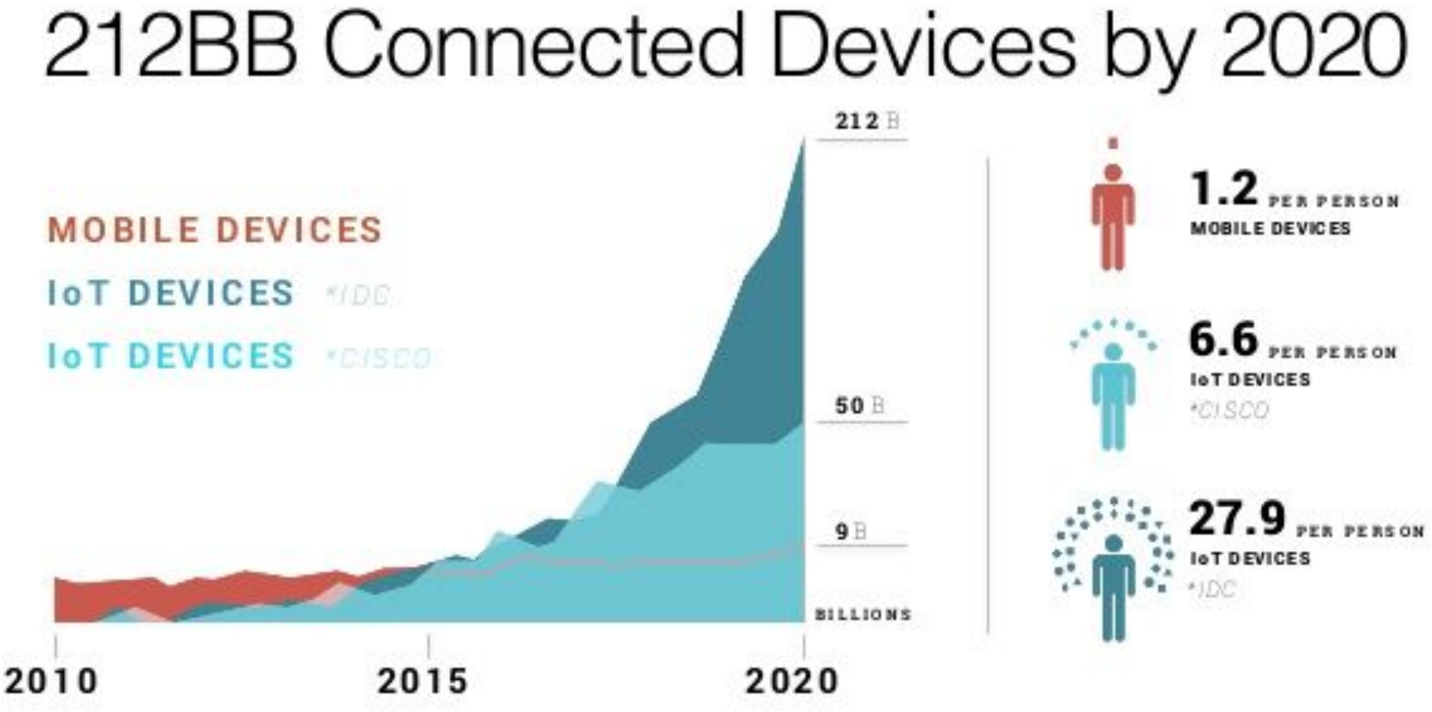
IoT Applications

IoT can be applied to our daily life.

IoT Ecosystem

IoT is heterogeneous in nature.

IoT Trends



IoT is with massive number of devices.

Remark

- IoT is multi-discipline engineering.
- IoT is with massive number of devices.
- IoT can be applied to our daily life.
- IoT is heterogeneous in nature.
    - Most IoT devices are resource-constrained.

Discussion

What are the challenges of deploying an IoT application?

Current IoT Applications

Smart Home

For example,

Amazon Echo
Google Assistant

Smart City

Networked Camera

NEWS ANALYSIS

Skynet in China: Real-life 'Person of Interest' spying in real time

AI married to CCTV surveillance in China uses facial recognition and GPS tracking to overlay personal identifying information on people and cars in real time.

MORE LIKE THIS

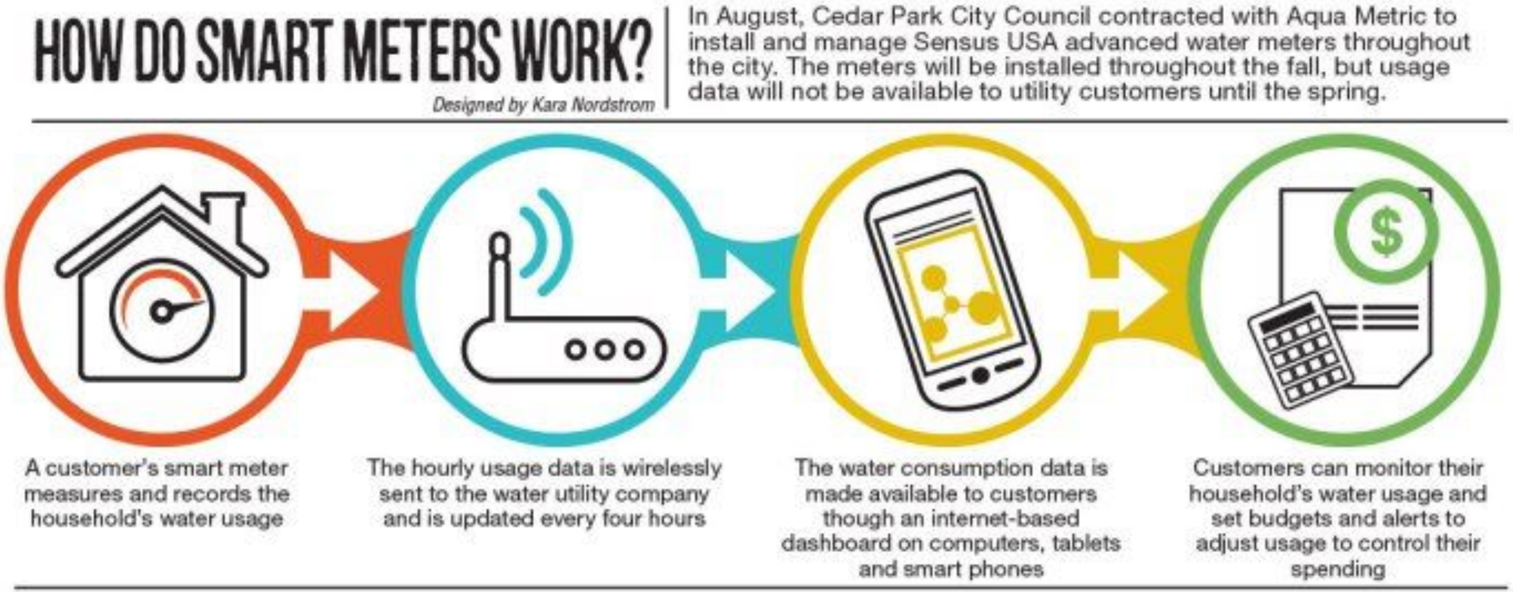

The best of Black Hat: The consequential, the controversial, the canceled


Intellectual property protection: The basics

Video Surveillance and Data Monitoring: The Basics

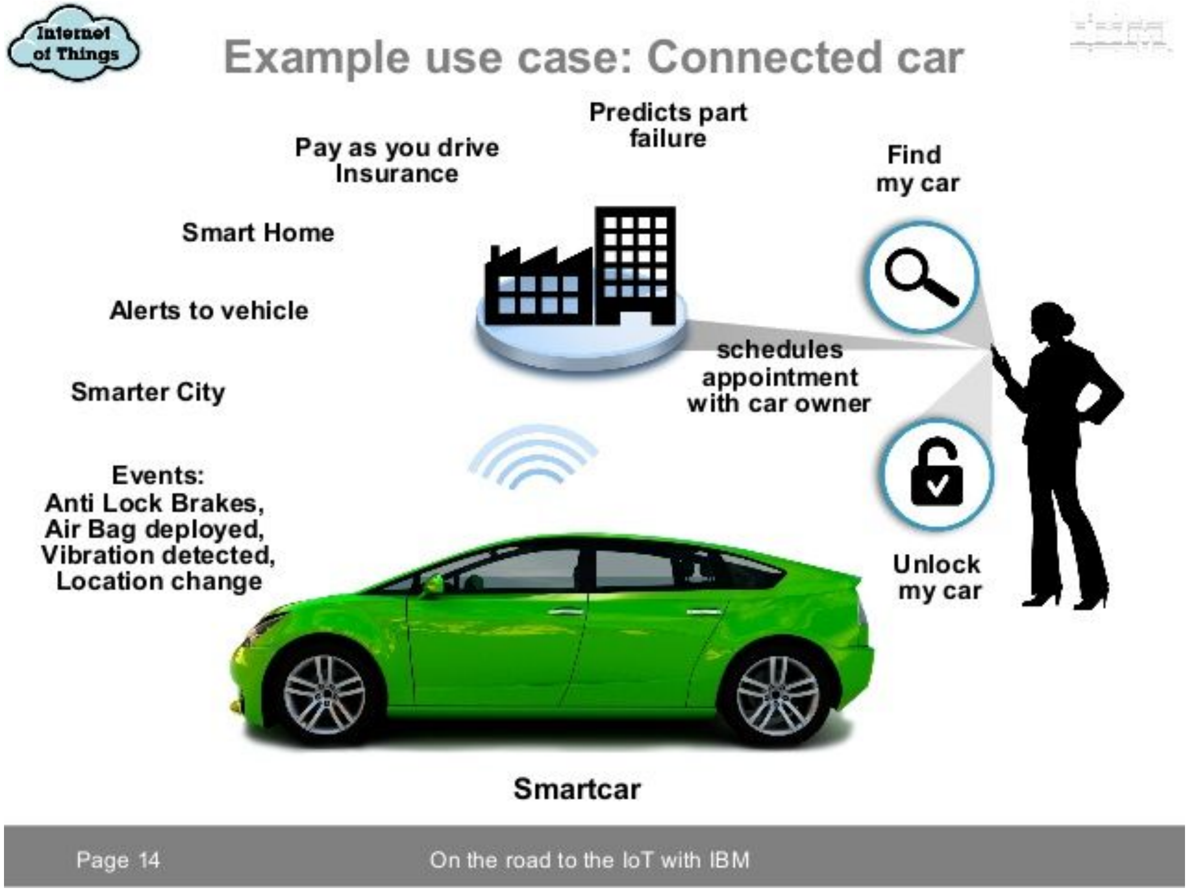
VIDEO
Scammers spoof Office 365, DocuSign and others | Salted Hash Ep 21

Smart City: Smart Meters



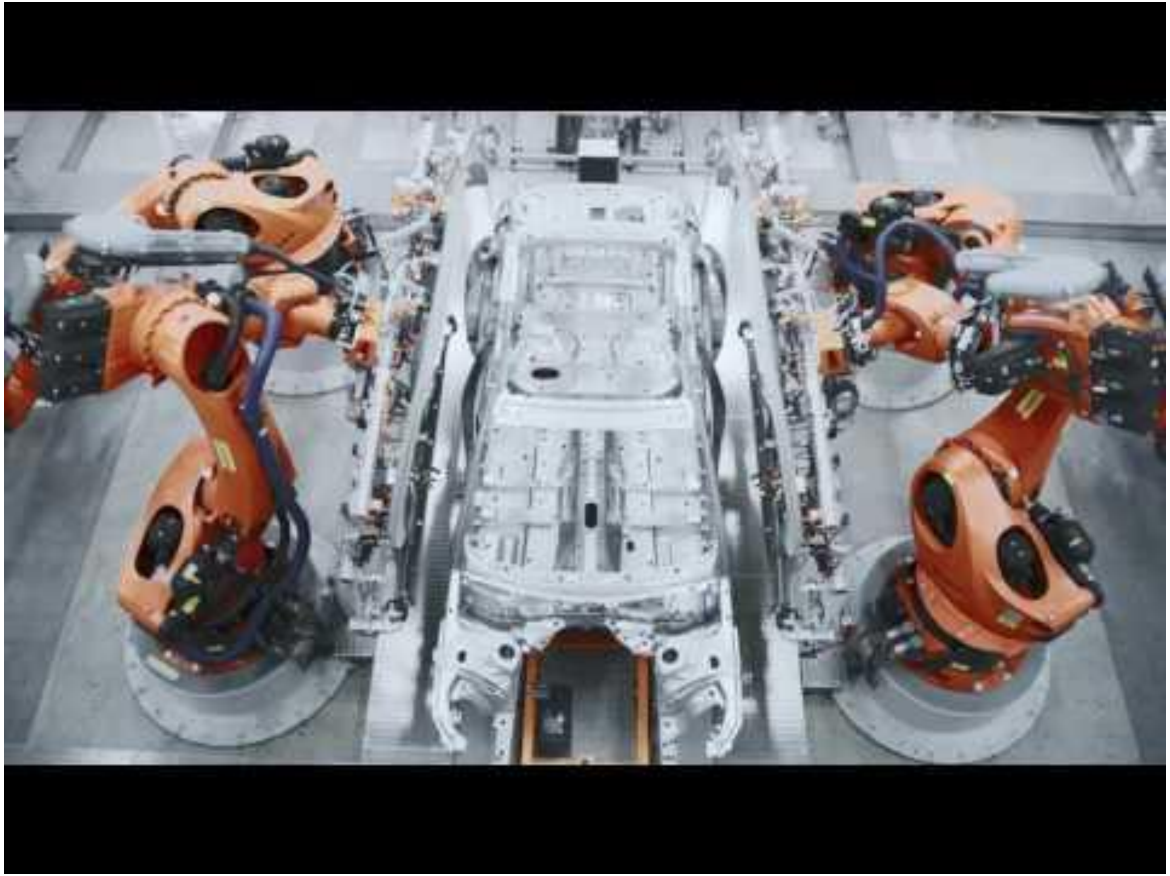
Smart Car

IBM Smart Car



Smart Factory

Audi Smart Factory



IoT is changing our World

Security is Big Issue in IoT

There is Dark Side of IoT

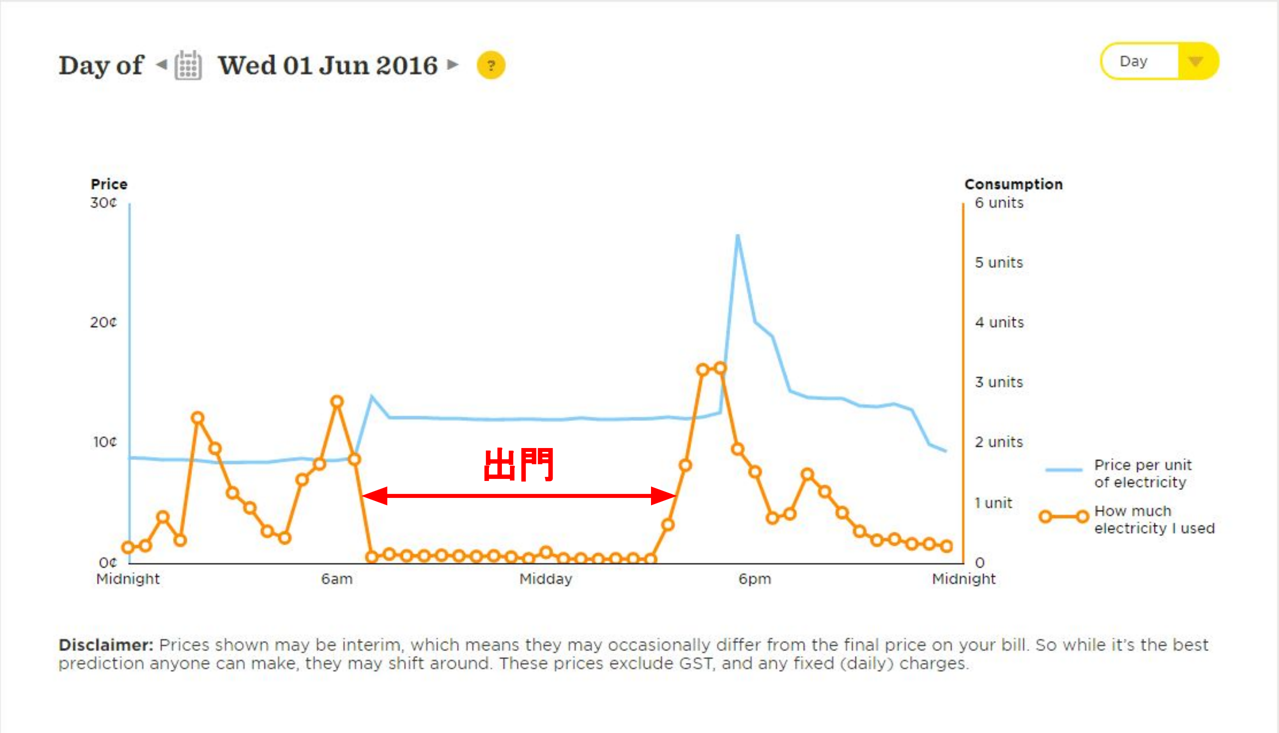
IoT seems wonderful, but ...

Privacy

You may being monitored by IoT devices.

Privacy

IoT data can be utlized to threats in our real life.



Security

Easy to hijack

California Enacts First-in-Nation IoT Security Law

The nation's first IoT security act was just signed into law in California. The law isn't just about the IoT, but billions of small connected devices will have to add critical features if they're sold in the state after Jan. 1, 2020.

Technology

Hackers used hijacked webcams to bring down internet

share

Cyber attackers took down the Dyn DNS using webcams CREDIT: EPA

Security of Smart Car

Hijacking smart car is possible.

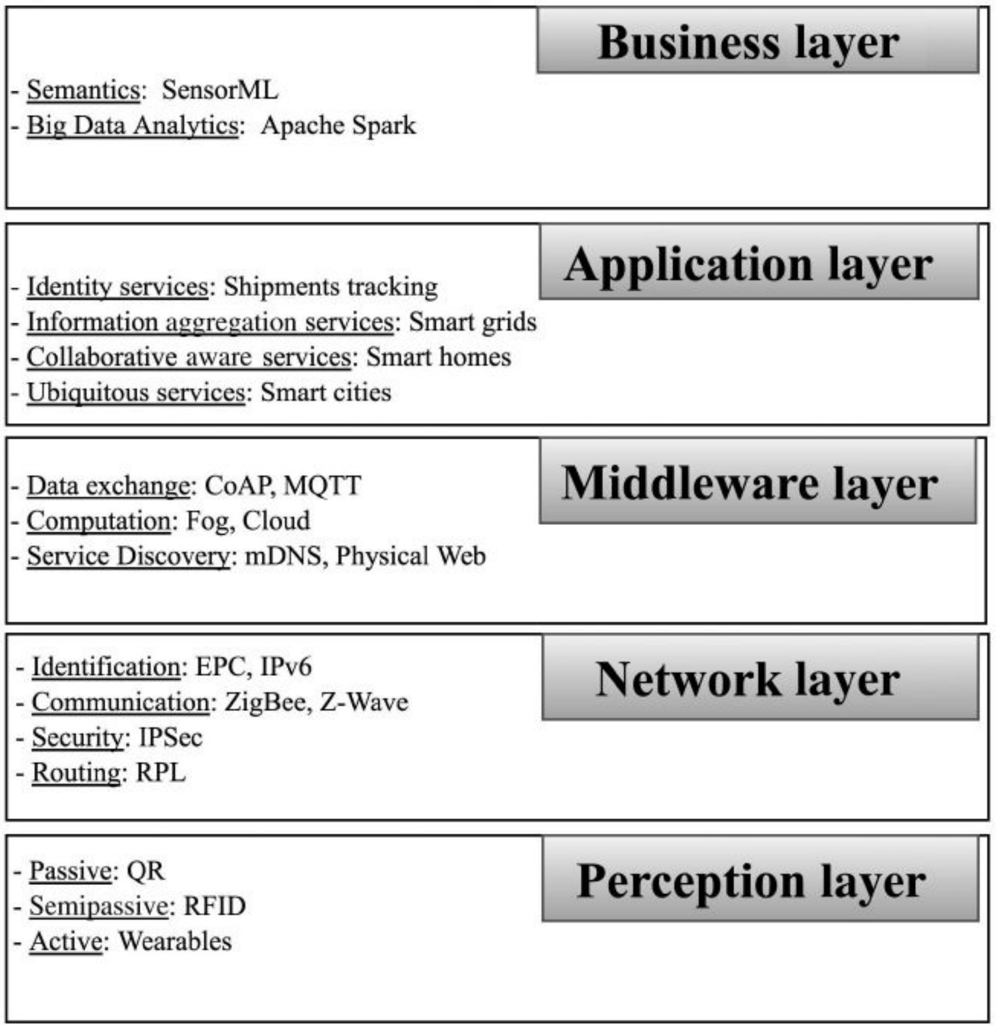
Prequisites for a Good IoT

Vint Cerf and Max Srenges
Taking the Internet to the Next Physical Level
IEEE Computer Magzine, Feb. 2016

Enabling Technologies

IoT Five-layer Model

Each layer has its own functionality and can involve various generic technologies.



Perception Layer Technologies

Passive

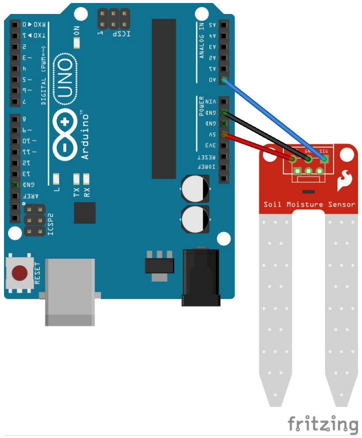
Quick Response (QR) Codes

Passive RFID

Semipassive

Battery-powered RFID

Infrared (IR)



Active

Active RFID

Smart Devices

Network Layer Technologies (Identification)

Naming solutions

Uniform Resource Identifier (URI)
Electronic Product Code (EPC)
Ubiquitous Code (uCode)

Addressing solutions

IPv4
IPv6

Remark

Identification focus on uniquely identifying an IoT device rather than **authenticate** and **authorize** an IoT device.

Network Layer Technologies (Communication)

Wired

Power-Line Communication (PLC)

X10

Wireless

Near-Field Communication (NFC), Ultra-Wide Bandwidth (UWB)

Wi-Fi, IEEE 802.15.4 (Zigbee), Z-Wave, Bluetooth

SigFox, Long-Range Wide-Area Network (LoRaWAN), NB-IoT

ANT+

Light Fidelity (Li-Fi)

Middleware Technologies (Service Discovery)

Service discovery enables requesting services without knowing the underlying infrastructure details.

- Multicast DNS (mDNS)
- DNS Service Discovery (DNS-SD)
- HyperCat (JSON-based)
- Universial Plug and Play (UPnP)

Middleware Technologies (Data Exchange)

Constrained Application Protocol (CoAP)

Extensibel Messaging and Presence Protocol (XMPP)

Message Queue Telemetry Transport (MQTT)

Advanced Message Queuing Protocol (AMQP)

Data Distributed Service (DDS)

Middleware Technologies (Computation)

Local

Local computations are performed using a processing unit or system on a chip (SoC).

(**Reminder:** most IoT devices are resource-constrained.)

Cloud

Cloud computing is preferable for applications in which sensors that reside in different places send generated data to the cloud for centralized processing.

(**Reminder:** IoT is with massive number of devices.)

Fog (or Edge)

A fog computing layer is ideally employed with the cloud to improve performance because it can be deployed near end users or nodes.

Key Challenges of Cloud-Based IoT

High or Unpredictable Latency

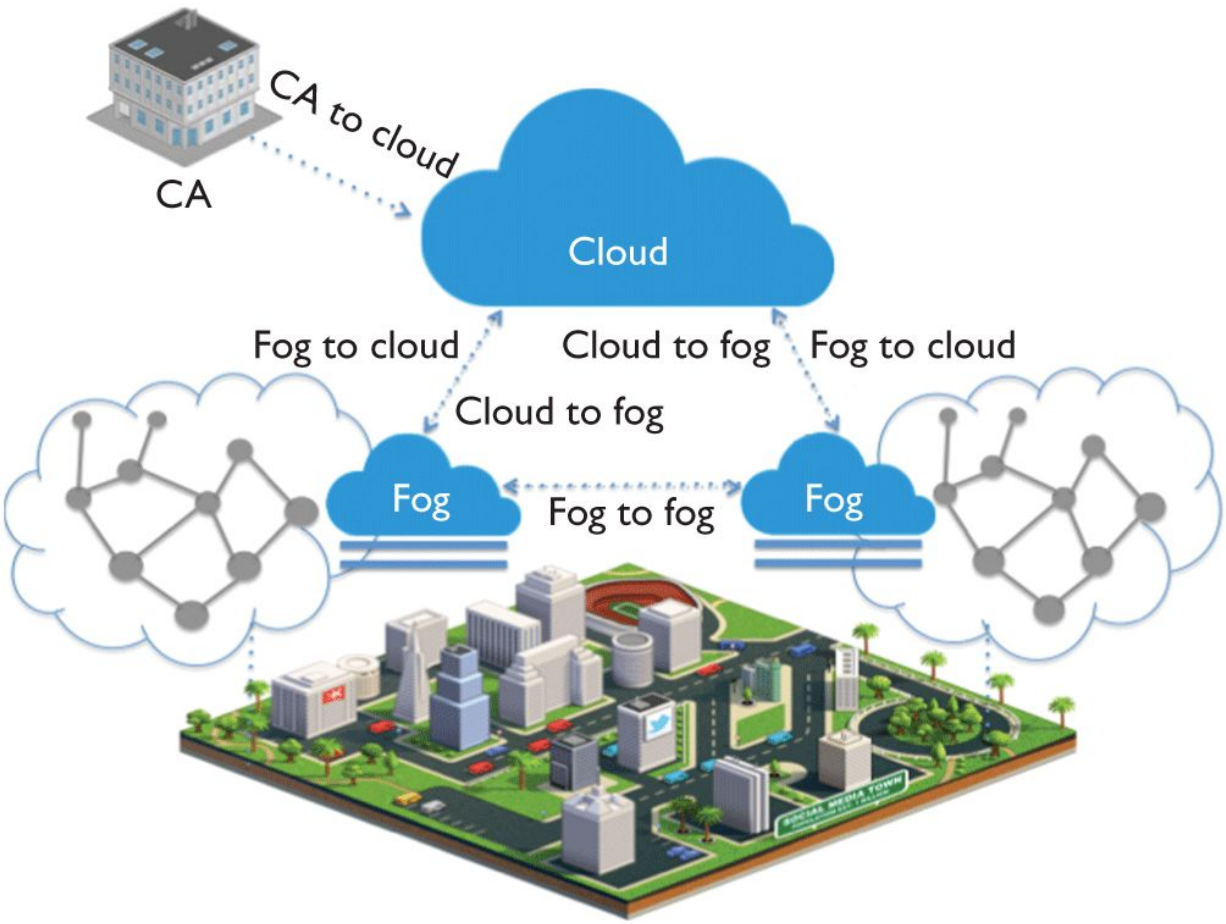
High Uplink Banwidth Requirements

No Filtering or Aggregation

Uninterrupt Internet Connection Required

Privacy and Security Concerns

Fog Computing for IoT, IEEE



Key Challenges of Fog-Based IoT

Technological Interoperability

Semantic Interoperability

Programmability

Scalability

Resilience and Reliability

Application Layer Technologies

Identification Services

Information Aggregation Services

Collaborative Aware Services

Ubiquitous Services

...

Business Layer Technologies (Sematics)

Sensor Model Language (SensorML)

Media Types for Sensor Markup Language (SenML)

Apache IoT Database (Apache IoTDB)

RESTFul API Modeling Language (RAML)

...

Business Layer Technologies (Big Data Analytics)

[Apache Spark]

[Apache Apex] (focus on stramming data)

[Apach Kafka] (streaming middleware)

...

IoT Operation System and Platform

IoT Operation Systems

Android Things (https://developer.android.com/things)

Embedded Linux (eg., Yacto, OpenWrt)

RIOT (https://riot-os.org)

Contiki (http://www.contiki-os.org)

Tiny OS (http://webs.cs.berkeley.edu/tos)

IoT Platform

AWS IoT Core (https://aws.amazon.com/tw/iot-core/)

Google IoT Core (https://cloud.google.com/iot-core/)

Microsoft IoT Hub (https://azure.microsoft.com/zh-tw/services/iot-hub/)

...

IoT Platform Comparison

Platform	Data exchange	Security	Integration	Device management
AWS IoT	MQTT, HTTP	TLS, SigV4[a)], X.509[b)]	REST API	Yes
IBM Watson	MQTT, HTTPS	TLS, IBM Cloud SSO[c)], LDAP[d)]	REST and Real-time APIs	Yes
ThingWorx	MQTT, AMQP, XMPP, CoAP, DDS, WebSockets[e)]	ISO 27001[f)], LDAP	REST API	Yes
Bosch IoT Suite	MQTT, CoAP, AMQP, STOMP[g)]	Unknown	REST API	Yes
Xively	HTTP, HTTPS, WebSocket, MQTT	SSL/TSL	REST API	No
EVRYTHNG	MQTT, CoAP, WebSockets	SSL	REST API	No
Kaa	MQTT, HTTP	RSA and AES	REST API	Yes

What's the next of IoT?

Digital Twin

A **digital twin** is a digital replica of a living or non-living physical entity.

By bridging the physical and the virtual world, data is transmitted seamlessly allowing the virtual entity to exist simultaneously with the physical entity.

Wikipedia

Lightweight and Flexible Security Mechanism

Lightweight Encryption

Adiantum (https://github.com/google/adiantum)

Adiantum-XChaCha20-AES encryption (generic)	37.120 cpb (32069 KB/s)
Adiantum-XChaCha20-AES decryption (generic)	37.123 cpb (32066 KB/s)
AES-256-XTS encryption (generic)	59.634 cpb (19961 KB/s)
AES-256-XTS decryption (generic)	60.136 cpb (19795 KB/s)

Flexible and Extensible Security Mechanism

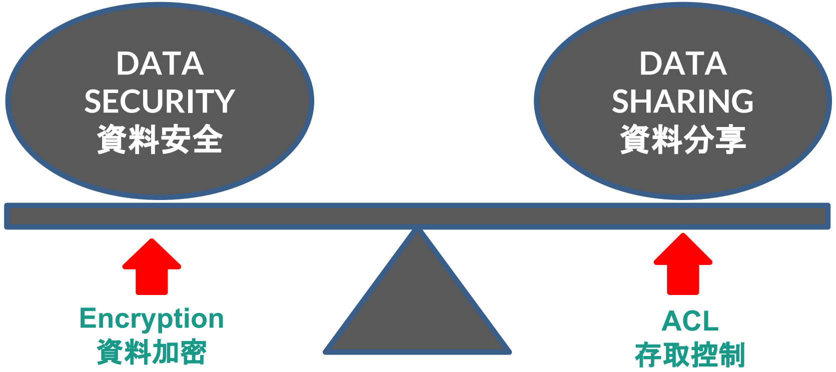
Beebit (https://github.com/beebit-sec)

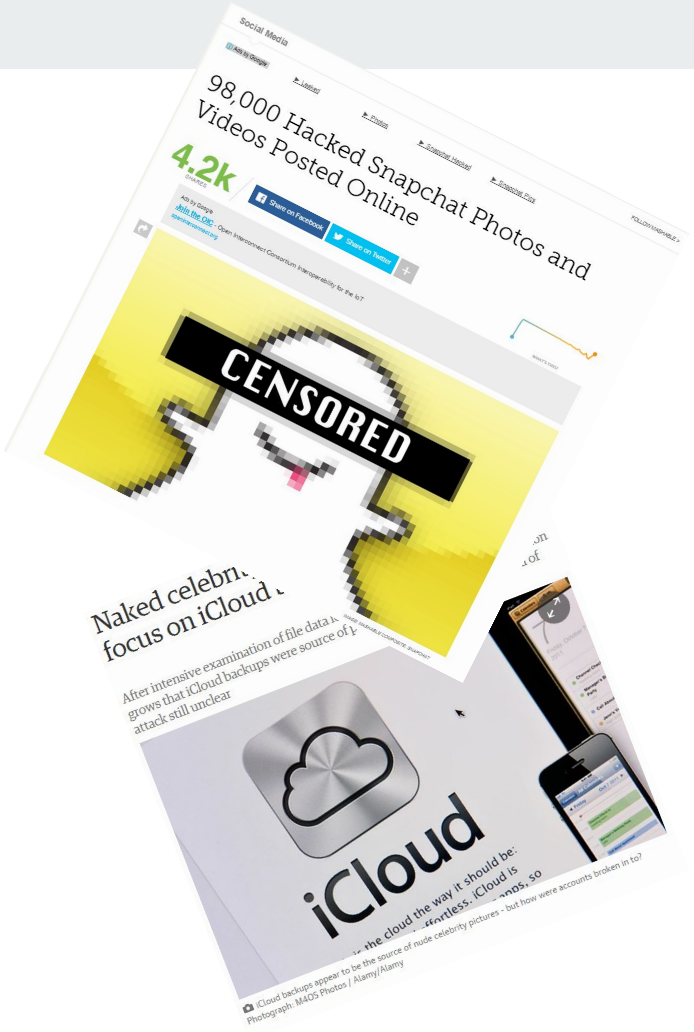
應用性/隱私權

如何在應用性與隱私權之間取得平衡?

運用支援細緻化存取控制的加密系統

Ciphertext-Policy Attribute-Based Encryption (CP-ABE)





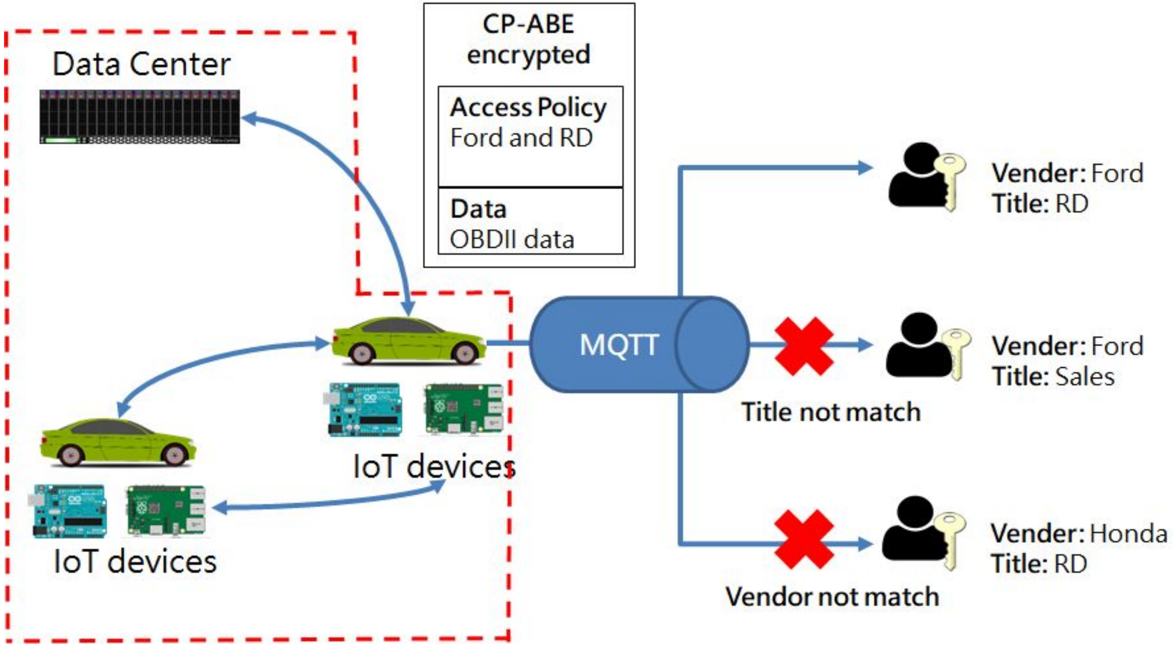
物聯網安全

Beebit (秘密)

開發物聯網安全

相關的開發工具

與系統。



Open Source

https://github.com/ucanlab/beebit-cpabe-sdk

https://github.com/ucanlab/beebit-mqttc-sdk

物聯網裝置具有資源限制

對1MB的資料進行CP-ABE加解密(存取政策使用的屬性個數為1)的過程所需要的時間，如下

Raspberry Pi 3使用了155 ms，其中(加密91ms; 傳輸1ms 解密63ms)
PC (i7-4720HQ, 4GB)使用了34 ms，其中 (加密23ms; 傳輸1ms 解密10ms)

差距近有5倍之多!!!

Discussion

How do you think about the next step of IoT?

Q & A

Computer History Museum, Mt. View, CA