The Internet of Things

Remarks by Dr Mawaki Chango

Kara University

DigiLexis Consulting

Definition

- “Internet of Things”: Coined in 1999 by Kevin Ashton a British technology pioneer
  - Context of RFID (Radio-Frequency Identification tags)
- Connecting objects, including everyday items, to the Internet using sensors.
- Definition:
  - Network connectivity
  - Computing capability
  - Objects including sensors and items not generally considered computers
  - Generating, exchanging and consuming enormous data with minimal human intervention

Connectivity models

- March 2015: IAB released architectural guideline (RFC 7452) for networking of smart objects
  - Device-to-Device
  - Device-to-Cloud
  - Device-to-Gateway
  - Back-End Data-Sharing

Device-to-Device

- Home automation scenario
  - Light switch / Light bulb
  - Thermostats
  - Door locks
- Direct communication over various networks, incl.
  - IP networks
  - Bluetooth
  - Z-Wave
  - ZigBee

Device-to-Cloud

- Device connects directly to and can exchange data through the cloud
- Wired Ethernet or Wi-Fi to connect the device to the IP network and ultimately to the cloud service

Device-to-Gateway

- Device-to-application-layer gateway (ALG) model
  - IoT device connects through an ALG service as a conduit to reach a cloud service

- Consumer devices
  - Smart phone running an app
  - Communicating with a device (e.g., personal fitness tracker)
  - Relaying data to a cloud service

Back-End Data-Sharing

- Enables users to export and analyze smart object data from a cloud service in combination with data from other sources
- Supports granting access to the uploaded sensor data to third parties
- Extends the single device-to-cloud communication model and helps avoid data silos (IoT device uploading data only to a single application service provider.)

IoT Issue Areas

- Security
- Privacy
- Interoperability/ Standards
- Legal, Regulatory and Rights
- Emerging Economy and Development Issues

Security

- The more devices are interconnected, greater the vulnerability
- Network security threats also have network power – local risks (security vulnerability) may quickly go global
  - Smart utility power meter
  - Implanted pacemaker
- Network (negative) externalities
- Security is function of risk level, potential threats.
- How can regulation help minimize the risks related to commercialization of devices with known or unknown security flaws?

Privacy

- IoT may challenge traditional expectations of privacy
- User's privacy expectations vs. Scope and use of the data by data collector
- Multiple devices = Multiple data sourcing points = Multiple data streams
- Combining different data streams may give invasive insights about the user
- Increasingly consumer devices record sounds and pictures from their environment

Legal, Regulatory and Rights

- Data protection and crossborder data flows
- Collected data may be beneficial as well as detrimental to the user (when it is used in a discriminatory way)
- Increasing use of IoT devices in legal actions: What are the implications for legal evidence, the manufacturers and for the society?

Emerging economy - Development

- Needs will shape opportunities, meaning the IoT potential is significant for developing economies
  - Water quality and use; waste management; disease and health; natural resource monitoring; climate change; food security; etc.

- Particularly: IoT-enabled "smart agriculture" techniques are envisioned across the entire value chain to improve the sustainability and productivity of the food supply.

Recap

- Definition
- Connectivity models
- Issue areas

Source: *The Internet of Things: An overview. Understanding the issues and challenges of a more connected world*. ISOC, October 2015

Thank you for your attention!

Dr. Mawaki Chango

Kara University

DigiLexis Consulting

@mawakichango