

Internet of Things



MATERI 1: Internet of Things (IoT) Introduction

What we learn today ...

- Internet of Things Concept
- Internet of Things Architecture
- Internet of Things Layers



TODAY	TOMORROW	10 DAYS
Today Thunderstorm	100%	32° 23°
Wednesday, Jan 1 Thunderstorm	100%	31° 23°
Thursday, Jan 2 Thunderstorm	100%	31° 23°
Friday, Jan 3 Thunderstorm	80%	32° 23°
Saturday, Jan 4 Thunderstorm	90%	32° 24°
Sunday, Jan 5 Thunderstorm	80%	31° 23°
Monday, Jan 6 Thunderstorm	80%	32° 23°
Tuesday, Jan 7 Thunderstorm	80%	31° 23°

The term IoT can most likely be attributed to Kevin Ashton in 1997 with his work at Proctor and Gamble using RFID tags to manage supply chains. The work brought him to MIT in 1999 where he and a group of like-minded individuals started the Auto-ID center research consortium.

Since then, IoT has taken off from simple RFID tags to an ecosystem and industry that by 2020 will cannibalize, create, or displace five trillion out of one hundred trillion global GDP dollars, or 6% of the world GDP.

Perry Lea,
Internet of Things for Architects,
Packt Pub, 2018

The concept of things being connected to the Internet up through 2012 was primarily connected smartphones, tablets, PCs, and laptops. Essentially, things that first functioned in all respects as a computer.

Since the humble beginnings of the Internet starting with ARPANET in 1969, most of the technologies surrounding the IoT didn't exist. Up to the year 2000, most devices that were associated with the Internet were, as stated, computers of various sizes.

Perry Lea,
Internet of Things for Architects,
Packt Pub, 2018

Year	Device	Reference
1973	Mario W. Cardullo receives the patent for first RFID tag	US Patent US 3713148 A
1982	Carnegie Mellon internet-connected soda machine	https://www.cs.cmu.edu/~coke/history_long.txt
1989	Internet-connected toaster at Interop '89	IEEE Consumer Electronics Magazine (Volume: 6, Issue: 1, Jan. 2017)
1991	HP introduces HP LaserJet III Si: first Ethernet-connected network printer	http://hpmuseum.net/display_item.php?hw=350
1993	Internet-connected coffee pot at University of Cambridge (first internet-connected camera)	https://www.cl.cam.ac.uk/coffee/qsf/coffee.html
1996	General Motors OnStar (2001 remote diagnostics)	https://en.wikipedia.org/wiki/OnStar
1998	Bluetooth SIG formed	https://www.bluetooth.com/about-us/our-history
1999	LG Internet Digital DIOS refrigerator	https://www.telecompaper.com/news/lg-unveils-internetready-refrigerator--221266

Perry Lea,
Internet of Things
for Architects,
Packt Pub, 2018

2000	First instances of <i>Cooltown</i> concept of pervasive computing everywhere: HP Labs, a system of computing and communication technologies that, combined, create a <i>web-connected experience for people, places, and objects</i>	https://www.youtube.com/watch?v=U2AkkuIVV-I
2001	First Bluetooth product launched: KDDI Bluetooth-enabled mobile phone	http://edition.cnn.com/2001/BUSINESS/asia/04/17/tokyo.kddiblue tooth/index.html
2005	United Nation's International Telecommunications Union report predicting the rise of IoT for the first time	http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf
2008	IPSO Alliance formed to promote IP on objects, first IoT-focused alliance	https://www.ipso-alliance.org
2010	The concept of Smart Lighting formed after success in developing solid-state LED light bulbs	https://www.bu.edu/smartlighting/files/2010/01/BobK.pdf
2014	Apple creates iBeacon protocol for beacons	https://support.apple.com/en-us/HT202880

Perry Lea,
Internet of Things
for Architects,
Packt Pub, 2018

The Internet of Things (IoT) paradigm promises **to make “things”** including consumer electronic devices or home appliances, such as medical devices, fridge, cameras, and sensors, **part of the Internet environment.**

This paradigm opens the doors to new innovations **that will build novel type of interactions among things and humans**, and enables the realization of smart cities, infrastructures, and services for enhancing the quality of life and utilization of resources.

Rajkumar Buyya and Amir Vahid Dastjerdi,
Internet of Things Principles and Paradigms,
Elsevier, 2016

The IoT is believed to be the future **Internet for the new generation**, which integrates various ranges of technologies, including **sensory, communication, networking, service oriented architecture (SoA), and intelligent information processing** technologies.

Shancang Li and Li Da Xu,
Securing the Internet of Things,
Elsevier, 2017

The Internet of Things or, as commonly referred to and now universally used, IoT has two keywords: **things and Internet**. The very idea of IoT consists **allowing things to connect to the (existing) Internet**, thus allowing the **generation of information** and, on the reverse, the **interaction of the virtual world with the physical world**.

Simone Cirani, et. al.,
Internet of Things Architecture, Protocol, and Standards,
Wiley, 2019

1. How to **connect things**
2. How to **gather data from things**
3. Things are considered **not operated by humans**;
4. Being **connected to the internet** means the things become neighbors with all the world's criminals, hackers, and curious teenagers at once.

Peter Waher, *Mastering Internet of Things*, 2018

It is a general concept involving an autonomous device communicating directly to another autonomous device. Autonomous refers to the ability of the node to instantiate and communicate information with another node without human intervention. The form of communication is left open to the application. It may very well be the case that an M2M device uses no inherent services or topologies for communication. This leaves out typical internet appliances used regularly for cloud services and storage. An M2M system may communicate over non-IP based channels as well, such as a serial port or custom protocol.

Perry Lea,
Internet of Things for Architects,
Packt Pub, 2018

1. M2M

- Autonomous device
- Communicating with other autonomous device
- May communicate over non-IP based channel

- IoT
- May incorporate some M2M nodes
- Aggregates data to an edge gateway
- Serve the entry point onto the Internet

IoT systems may incorporate some M2M nodes (such as a Bluetooth mesh using non-IP communication), but aggregates data at an edge router or gateway. An edge appliance like a gateway or router serves as the entry point onto the internet. Alternatively, some sensors with more substantial computing power can push the internet networking layers onto the sensor itself. Regardless of where the internet on-ramp exists, the fact that it has a method of tying into the internet fabric is what defines IoT.

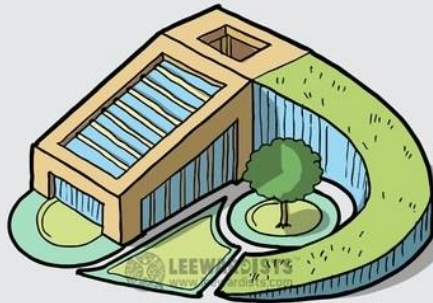
Perry Lea,
Internet of Things for Architects,
Packt Pub, 2018

M2M vs. IoT: What's the difference?

M2M	IoT
Machines	Sensors
Hardware-based	Software-based
Vertical applications	Horizontal applications
Deployed in a closed system	Connects to a larger network
Machines communicating with machines	Machines communicating with machines, humans with machines, machines with humans
Uses non-IP protocol	Uses IP protocols
Can use the cloud, but not required to	Uses the cloud
Machines use point-to-point communication, usually embedded in hardware	Devices use IP networks to communicate
Often one-way communication	Back and forth communication
Main purpose is to monitor and control	Multiple applications; multilevel communications
Operates via triggered responses based on an action	Can, but does not have to, operate on triggered responses
Limited integration options, devices must have complementary communication standards	Unlimited integration options, but requires software that manages communications/protocols
Structured data	Structured and unstructured data



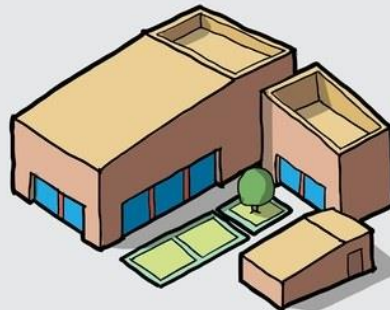
Concept Sketch



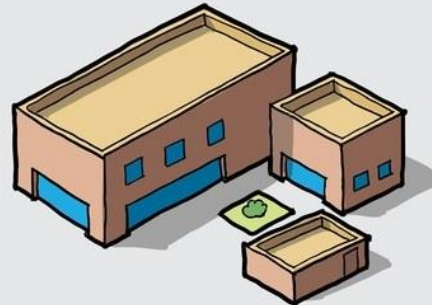
After meeting with Client

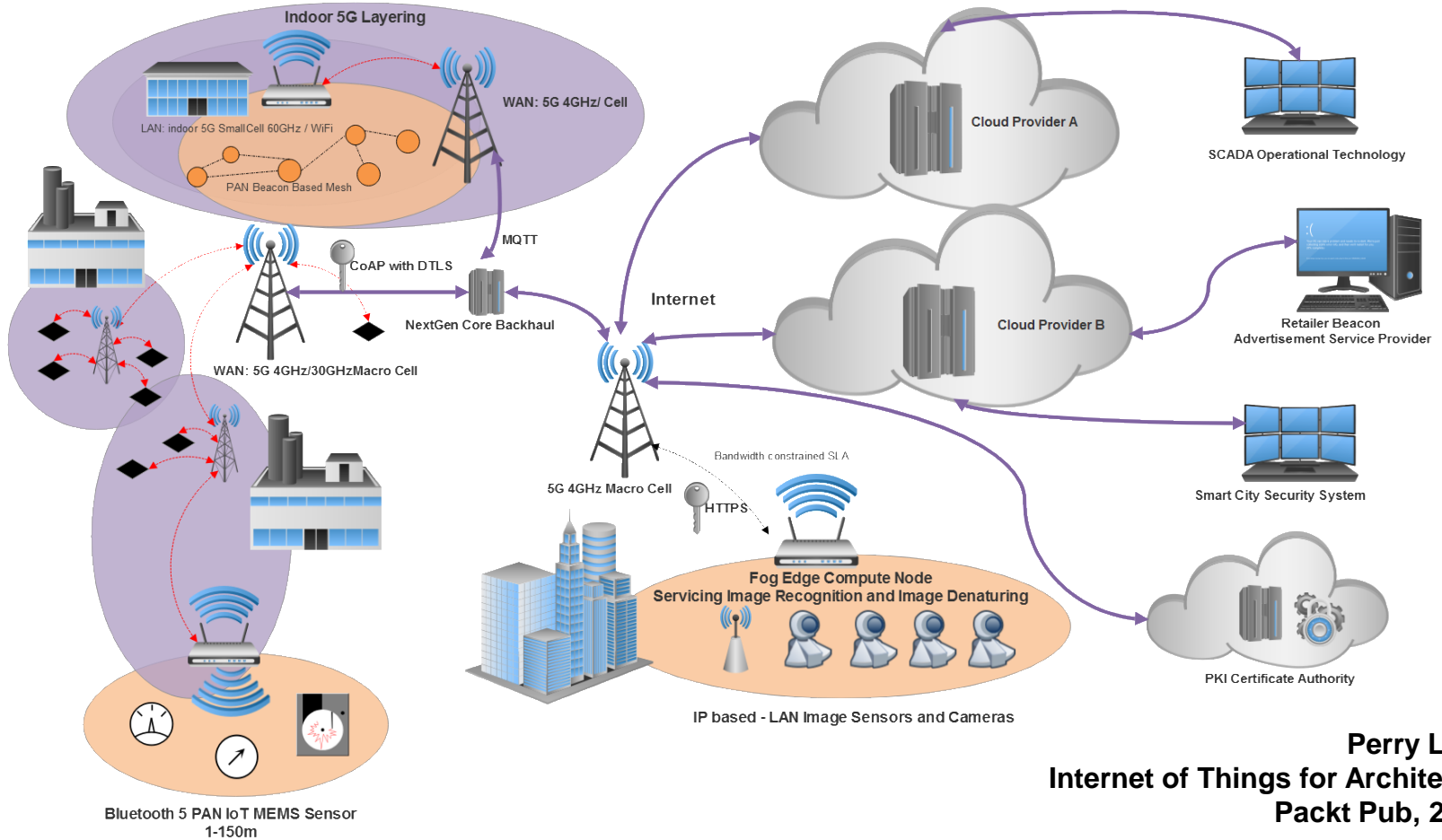


After Working Drawings



After Construction





Perry Lea,
Internet of Things for Architects,
Packt Pub, 2018

The IoT Architecture aimed

- To Understand the impact choosing a certain design aspect of the systems.
- To consider resiliency and how costly the loss of data
- To choice the internet protocols and the other peripheral to support them
- To manage the sensor data and power usage
- To manage the security and their maintenance

The IoT Architecture parts

1. Sensing and Power
2. Data communication
3. Internet routing and protocols
4. Fog and edge compute, analytic, and machine learning
5. Threat and security in IoT

The sensor outputting a stream time-correlated data. They must be **transmitted securely, possibly analyzed, and possibly stored.**

Sensing devices comes in a variety of forms and complexities ;

- Thermocouples and temperature sensors
- Photoelectric sensors
- PIR sensors
- LiDAR
- MEMS sensors
- Smart IoT endpoints : Vision systems

Energy sources and power management :

- Power management
- Energy harvesting
 - . Solar Harvesting
 - . Thermal harvesting
- Energy storage
 - . Batteries
 - . Supercapacitor
 - . Radioactive

The fact, the starting point of the IoT isn't sensors or the applications, but it's about **connectivity**.

The data communications ;

1. Near-range and near-meter systems ; PAN
2. Wireless local area network ; IEEE 802.11 Wi-Fi systems
3. IP-Based communications systems
4. Long-range communication ; 4G

To bridge the sensors to the internet, they need ;

1. Gateway routers
2. Supporting IP-Based protocol

The router has important role in **securing**, **managing**, and **steering data**.

The protocols used in IoT such as MQTT, CoAP, and AMPQ are several example that given more efficient and power consumable protocols.

Consider what to do with the data from the edge point to the cloud service.

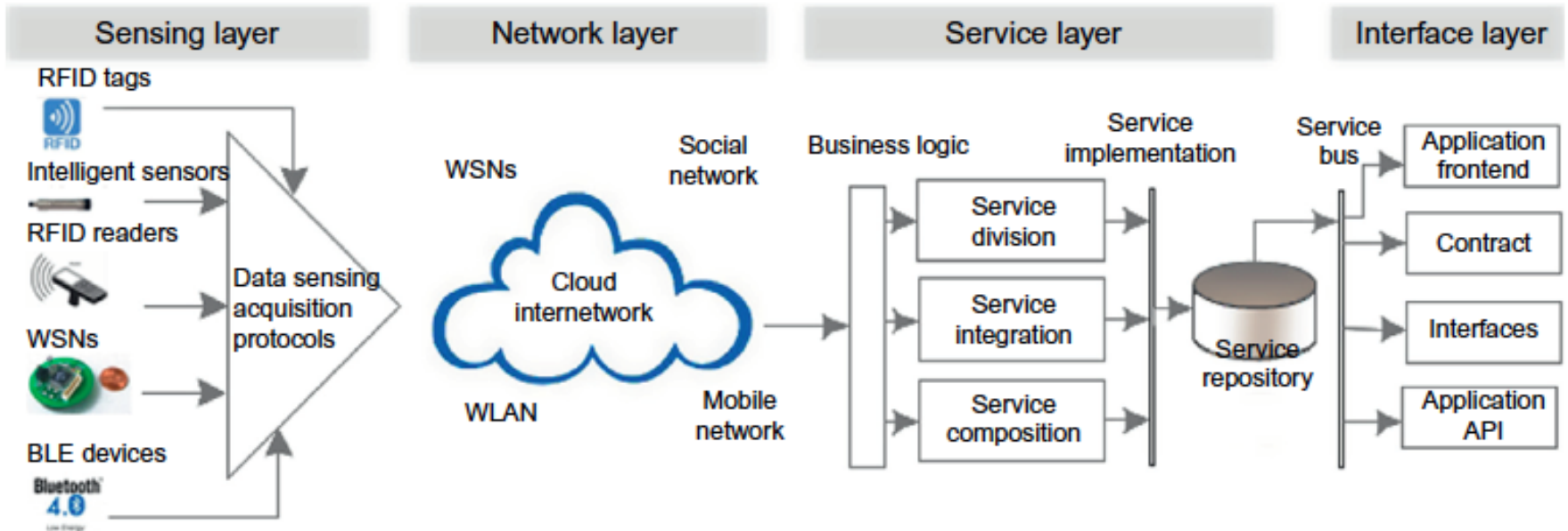
There three cloud architecture : SaaS, IaaS, PaaS. The right choice of the cloud architecture can maintain the latency.

The measurable cost in moving all IoT data to the cloud versus processing in the edge (edge processing), or extending cloud services downward to edge router (fog computing)

The security need to be aware are :

1. Confidentiality
2. Availability
3. Integrity
4. Authenticity
5. Authority





Shancang Li and Li Da Xu,
 Securing the Internet of Things,
 Elsevier, 2017

Generic SoA for IoT, which consists of four layers:

1. **Sensing layer** is integrated with end components of IoT to sense and acquire the information of devices;
2. **Network layer** is the infrastructure to support wireless or wired connections among things;
3. **Service layer** is to provide and manage services required by users or applications;
4. **Application interfaces layer** consists of interaction methods with users or applications.

Shancang Li and Li Da Xu,
Securing the Internet of Things,
Elsevier, 2017

We will touch on nearly every segment in information technology, as they all have a role in IoT:

1. **Sensors:** Embedded systems, real-time operating systems, energy-harvesting sources, Micro-Electro-Mechanical Systems (MEMS).
1. **Sensor communication systems:** Wireless personal area networks reach from 0 cm to 100 m. Low-speed and low-power communication channels, often non-IP based have a place in sensor communication.
1. **Local area networks:** Typically, IP-based communication systems such as 802.11 Wi-Fi used for fast radio communication, often in peer-to-peer or star topologies.

Perry Lea,
Internet of Things for Architects,
Packt Pub, 2018

4. **Aggregators, routers, gateways:** Embedded systems providers, cheapest vendors (processors, DRAM, and storage), module vendors, passive component manufacturers, thin client manufacturers, cellular and wireless radio manufacturers, middleware providers, fog framework providers, edge analytics packages, edge security providers, certificate management systems.
4. **WAN:** Cellular network providers, satellite network providers, Low-Power Wide-Area Network (LPWAN) providers. Typically using internet transport protocols targeted for IoT and constrained devices like MQTT, CoAP, and even HTTP.
4. **Cloud:** Infrastructure as a service provider, platform as a service provider, database manufacturers, streaming and batch processing manufacturers, data analytics packages, software as a service provider, data lake providers, Software- Defined Networking/Software-Defined Perimeter providers, and machine learning services.

Perry Lea,
Internet of Things for Architects,
Packt Pub, 2018

- 7. Data analytics:** As the information propagates to the cloud en-mass. Dealing with volumes data and extracting value is the job of complex event processing, data analytics, and machine learning techniques.
- 7. Security:** Tying the entire architecture together is security. Security will touch every component from physical sensors to the CPU and digital hardware, to the radio communication systems, to the communication protocols themselves. Each level needs to ensure security, authenticity, and integrity. There cannot be the weak link in a chain, as the IoT will form the largest attack surface on earth.

Perry Lea,
Internet of Things for Architects,
Packt Pub, 2018



Task

- Fill this task in link google form :
<https://forms.gle/DFNa9hu1oopVJktU6>
- Time limit : 15 Minutes

Prepare for every next meeting

- Make group with maximum two people in one group.
- Every meeting in your class will be in groups with your group.
- Prepare the hardware and tools for every group.

What you need to prepare for our next week ?

6. Potentiometer
7. LED(s)
8. Resistor(s) 10 K Ohm
9. Installed Arduino IDE on your computer
10. Please install the ESP8266 plugin if you choose the ESP as your micro controller (<https://github.com/esp8266/Arduino>)

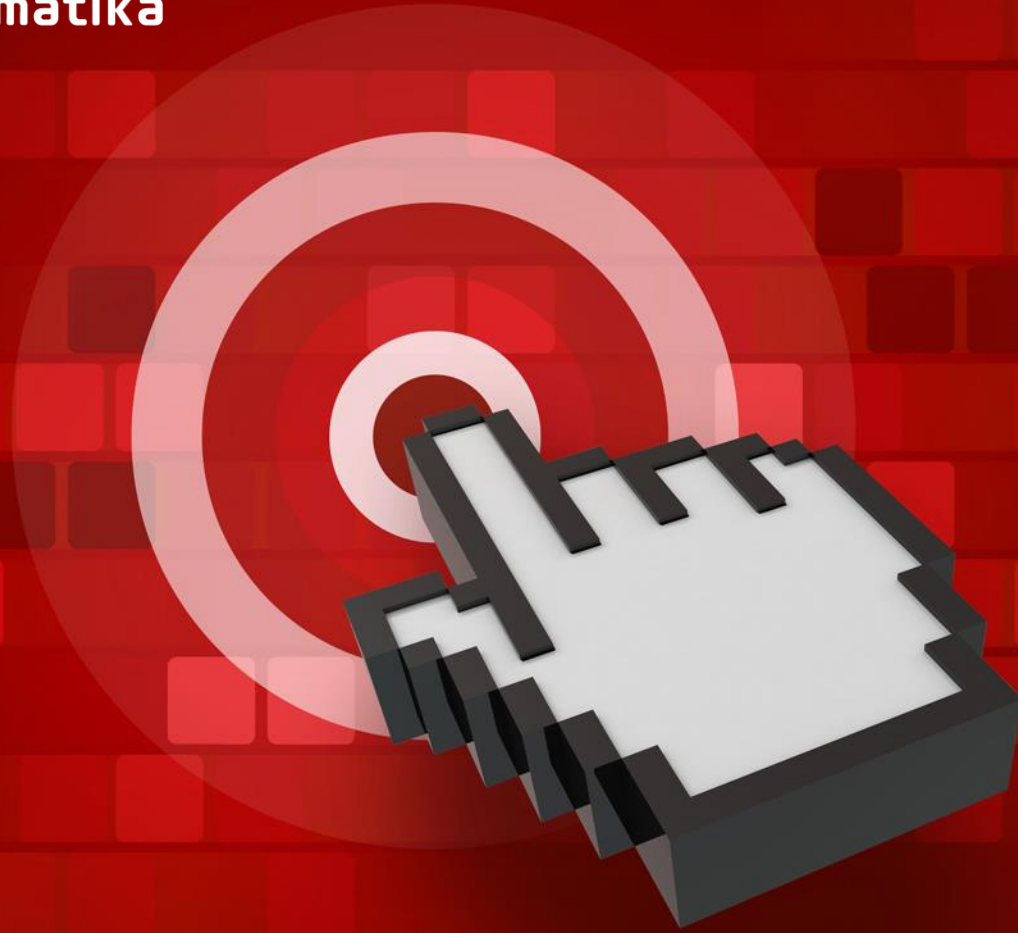


What you need to learn at home ?

- Working on module 1, the module will be sent to the head of class email.



Fakultas Informatika
School of Computing
Telkom University



THANK YOU