Problems in and among industries for the prompt realization of IoT and safety considerations

(https://datatracker.ietf.org/doc/html/draft-baba-iot-problems-04)

November 13th, 2017

Hiroyuki BABA

The University of Tokyo

Yoshiki ISHIDA

Japan Network Enabler Corporation

Agenda

1. Introduction
2. Objectives of activity
3. Meeting
4. Contents of I-D
5. Problems in and among industries for the prompt realization of IoT / Highlights
6. Safety considerations
7. TEST BED at the University of Tokyo

1. Introduction

- Motivation for writing this I-D
  - Sharing comments from Things players about IoT
  - Clarifying the barriers for deployment of IoT
  - Prototyping an open referable document of these barriers.

2. Objectives of activity

- What are challenges for realizing IoT ?

- ICT industry players

(ICT industry:communication carriers, ICT equipment vendors, the Internet service providers, application vendors, and software houses)

- Things industry players

(Things industry:home and housing equipment manufacturers, infrastructure providers such as railways companies and power companies, and manufacturers of home appliances such as air conditioners and refrigerators)

- What is safety issue in things world in IoT era ?

3. Meeting (held in 2015)

- Meeting with major players and asking questions
  - ✓ Telecommunications Carrier (ICT)
  - ✓ Global IC chip vender (ICT)
  - ✓ Railway Company (Things)
  - ✓ Electric Power Company (Things)
  - ✓ Home and housing equipment manufacturer (Things)
  - ✓ (Two) Home appliance manufacturer (Things)
  - ✓ Medical equipment manufacturer (Things)
  - ✓ Automobile parts manufacturer (Things)
  - ✓ Precision machinery manufacturer (Things)

4. Contents of I-D

1. Introduction
2. Technical Challenges
   2.1. Safety, Security and Privacy
      2.1.1. Challenges in protecting lives and property from IoT-related threats (IoT Safety)
         2.1.1.1. Safety of body/life
         2.1.1.2. Safety of equipment
         2.1.1.3. Proper performance of equipment
      2.1.2. Information Security
      2.1.3. Privacy in acquiring data
   2.2. Challenges posed by data acquisition, data distribution, data management and data quantity
      2.2.1. Traffic patterns
      2.2.2. Acquired mass data
      2.2.3. Explosive increase and diversity of data
   2.3. Mapping of the physical world and the virtual world
      2.3.1. Physically handling acquired data
      2.3.2. Data calibration

4. Contents of I-D(Cont'd)

2.4. Product lifetime, generation management, and the cost of equipment updates
 2.4.1. Product lifetime
 2.4.2. Introducing IoT equipment into commodity equipment
2.5. Too many related standards and the speed of standardization
 2.5.1. Too many related standards
 2.5.2. Speed of standardization
2.6. Interoperability, fault isolation, and total quality assurance
 2.6.1. Interoperability
 2.6.2. Fault isolation
 2.6.3. Quality assurance
2.7. Product design policy
 2.7.1. Changes in design policy
2.8. Various technology restrictions within actual usage
 2.8.1. Using radio waves
 2.8.2. Batteries
 2.8.3. Wiring
 2.8.4. Being open

4. Contents of I-D(Cont'd)

3. Non-technical Challenges
   3.1. Changing the product paradigm
      3.1.1. Ecosystems
      3.1.2. Coordination and significant changes in strategy
      3.1.3. Competition with existing industries
   3.2. Benefits
      3.2.1. Rising costs and monetization
   3.3. Information security and privacy of social systems
      3.3.1. Classification of ownership, location, and the usage of data
   3.4. Disclosure of data
      3.4.1. Side effects and malicious use potentially caused by the disclosure of data
   3.5. Preparing social support
      3.5.1. Regulations
      3.5.2. Corporate social responsibility
      3.5.3. Customization for individual customers
      3.5.4. IoT literacy of the users
      3.5.5. Individual vs. family
4. Information Security Considerations
5. Privacy Considerations
6. Acknowledgments

Problems in and among industries for the prompt realization of IoT

5. Highlight -1

2.1.2. Information Security

For example, there is a product available for connecting the entrance door to the network. In ICT security technology, increasing the key length of the encryption makes it much harder to break.
But even if the latest information security technology is used when it is installed, the information security technology will become obsolete and even pose a risk about halfway through the twenty- to thirty-year lifetime of the entrance door. As has been explained in other items, the ICT sense of time is completely different from that of Things.

IfyouuseLongkey//fkl93q039wruei@r@30fiz;lvjklaf^oaafieq@40[1.....

It's easy to break electronic key in 20 years!

5. Highlight -2

2.1.3. Privacy in acquiring data

Another huge challenge is the ownership of data. Up until now, there has been a divided debate on whether data belonged to the company or to the users. Likewise, the relationship inside a small user group is also extremely diverse and complicated. One specific example is of a company that had obtained permission from the head of the household to use the data when it carried out an HEMS trial. Later on, the spouse of the head of the household disagreed and as a result permission to use the data was withdrawn.

In this case: Who is the "USER" ?

5. Highlight -3

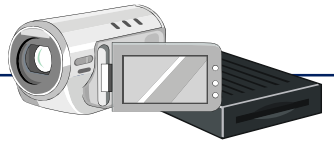
2.2.1. Traffic patterns

routinely or temporarily sending or receiving data through a huge number of various sensors and devices presents a very different kind of Internet traffic. However, questions such as how much traffic will come from what kind of Things, and how will they superimpose each other have not been sufficiently studied. There is no concrete explanation about the backbone design and operation of traffic, and there have been many cases in which the unclear specifications for IoT traffic made the design difficult on the communication company side. There are many challenges related to the set up and Management of IoT equipment. We have heard from the construction companies that the configuration of IoT equipment with a large number of sensors involves a lot of hard work.

5. Highlight -4

2.3.1. Physically handling acquired data
2.3.2. Data calibration

The acquired data simply represents certain kinds of digital value, and it is important to uncover the meaning of this data. As described previously, configuration of IoT equipment, such as the large number of installed sensors, requires a lot of hard work. An even greater amount of effort will be needed to determine the meaning of the data and connect it to the physical world.
Another important thing is calibration. This involves properly linking the data sent from Things to the Things concerned, and (for) correctly indicating the operating conditions.



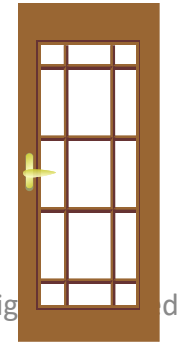
How can we manage too much work ?
…… configuration -> determine the meaning of the data -> calibration on all of many many many IoT devices such as sensors and etc.

5. Highlight -5

2.4.1. Product lifetime

The life of most ICT equipment is about 5 years or less, while the life of IoT equipment and devices is at least 10 years. There is a clear gap between these two types of equipment.
In the example of the entrance door connected to the network mentioned earlier, the door is often used for about twenty to thirty years after installed. If it is connected to a network, the communication technology and communication service will most likely have undergone numerous generation changes in that twenty- to thirty-year time span (of door). This presents a large gap between the ICT industry and the Things industry.

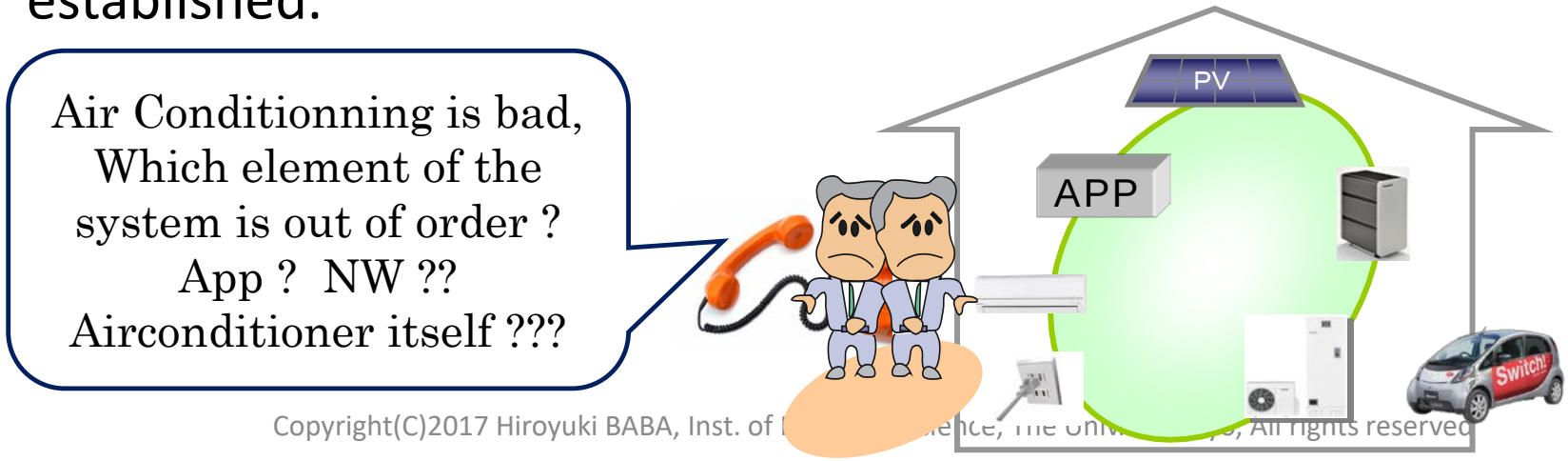
5 years VS 20～30 years



5. Highlight -6

2.6.2. Fault isolation

If users are left to isolate the fault on their own, they may not know which manufacturer they contact for repairs if they are unable to isolate the fault on their own, or the manufacturer may refuse to perform repairs because they fall outside the scope of their responsibility. As can be seen, the issue is an important challenge that will determine whether the B2C specific IoT world can be established.



5. Highlight -7

2.8.1. Using radio waves

There are many cases that have provided us with insight about issues related to the use of radio waves in IoT (such as the wave traveling range and whether or not it travels further than stated in assumptions available). The suppliers or providers who configure IoT are not always wave communication technology experts. People who are unfamiliar with radio waves seem to think that waves travel from antenna to antenna in a straight line, and that they can be blocked by obstacles. As a result, they often ask questions about how many meters radio waves can travel or whether radio waves can actually travel. Few people understand the fact that the emitted radio waves are reflected from various locations and are superimposed at the reception point where they are received, or that depending on how waves are reflected a change in the reception signal intensity, called fading, may occur. The lack of engineers who can advise on specialized matters such as these poses a major obstacle.

5. Highlight -8

2.8.4. Being open

A single company alone cannot make all the commodities for IoT. The IoT world needs to be open, and this can only be achieved with the cooperation of many different industries. Up until now, companies in the Things industry have developed products in a closed loop process, seeking to capture users with their company's own products. For this reason, they lack an open design concept of interoperability. Today, an entirely new design concept is needed to design products that can interconnect with the products of other companies.

5. Highlight -9

3.1.1. Ecosystems

While the goal of setting up IoT is to generate new value, it may actually lead to the destruction of the ecosystems in which industries operate. In the IoT era, the traditional vertically integrated way of producing Things in manufacturing industries will consume too much time and cost. This approach also makes it difficult to incorporate the ideas of other cultures. The need for paradigm shift is easy to understand, but difficult to implement. Promoting this shift will pose a management challenge that requires a considerable amount of skill and effort to overcome.

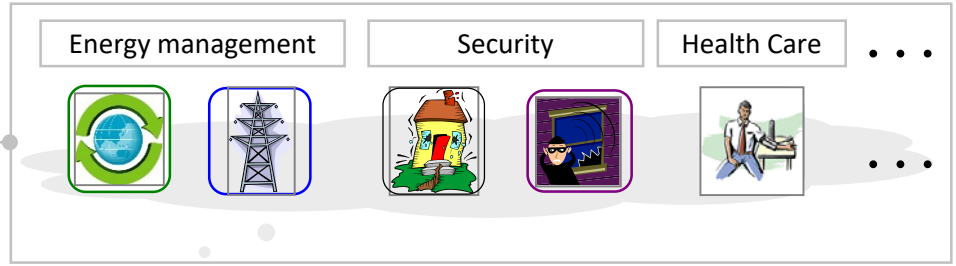
Safety considerations

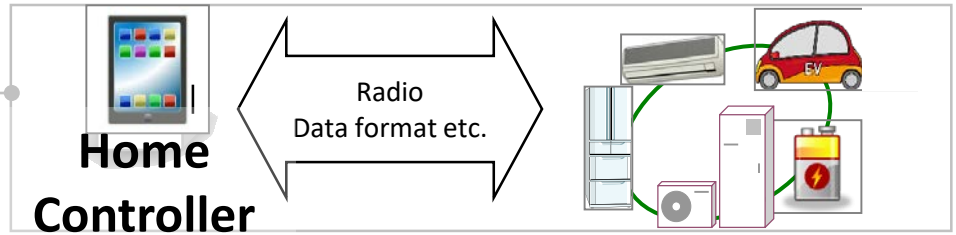
2.1.1. Challenges in protecting lives and property from IoT-related threats (IoT Safety)

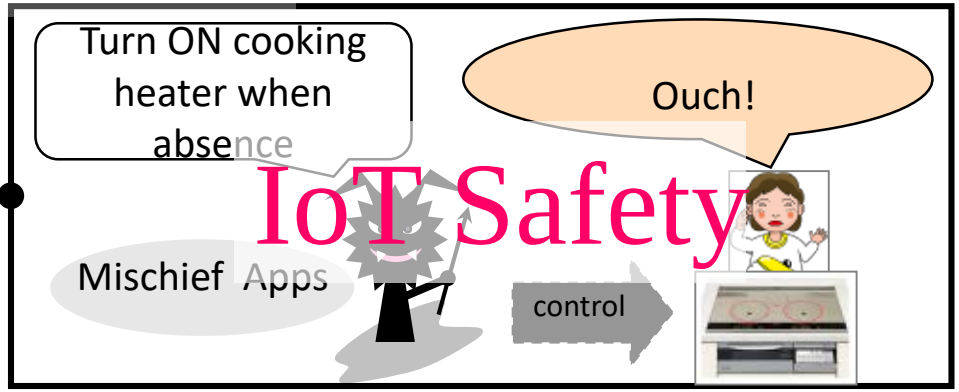
The introduction of IoT may generate threats to "Safety" through the actual operation of mechanical devices, in addition to the Information Security problems discussed in Section 2.1.2 below. For example, the spread of applications for visualizing electric power consumption allows for mischief in device operation without the use of identity fraud or hacking. In addition, there is the potential for problems to arise in the normal operation of individual devices that are not caused by abnormal current or voltage, another troubling aspect of the introduction of IoT. These issues cannot be resolved with ordinary information security measures for Network Layer 4 or lower. In another case, a command to an IoT device is proper by itself, but it may conflict with the other commands or its environmental status. Therefore, the authors consider it necessary to have a system for interpreting the details of operations of many appliances and preventing operations according to the necessity in Layer 7 (what the authors tentatively call "Sekisyo".)

Safety issue in Things world

4	Service Energy management, Elderly care・・・
3	apps Energy management, Elderly care ・・・
2	Cyber Security Protect hacking …etc.
1	OS、Com.Protocol Android™、Windows Mobile™ ECHONET Lite ™、Zigbee™
0	Product Liability Law, etc.・・・ What control do you permit for third party apps.



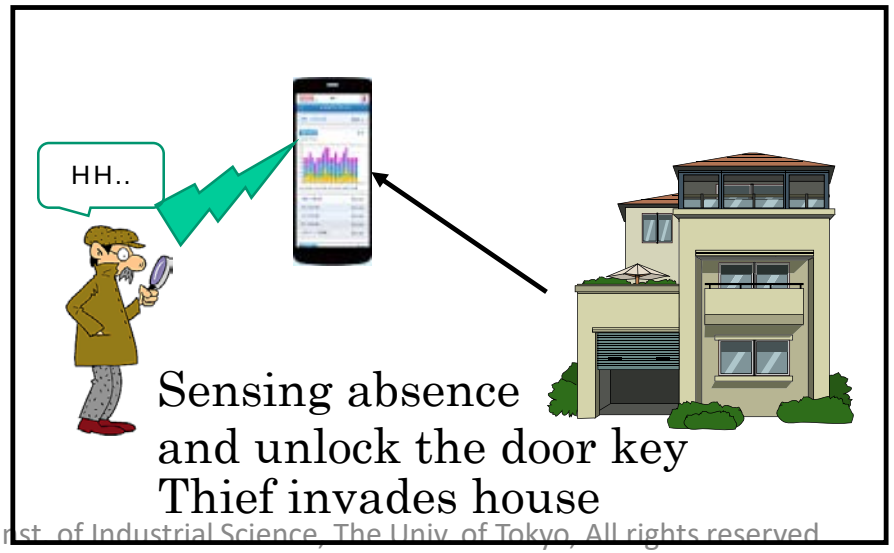




Android: Registered trademark of Google Inc. Windows Mobile: Registered trademark of Microsoft Corporation ECHONET Lite: Registered trademark of ECHONET Consortium
ZigBee: Registered trademark of ZigBee Alliance, Inc.

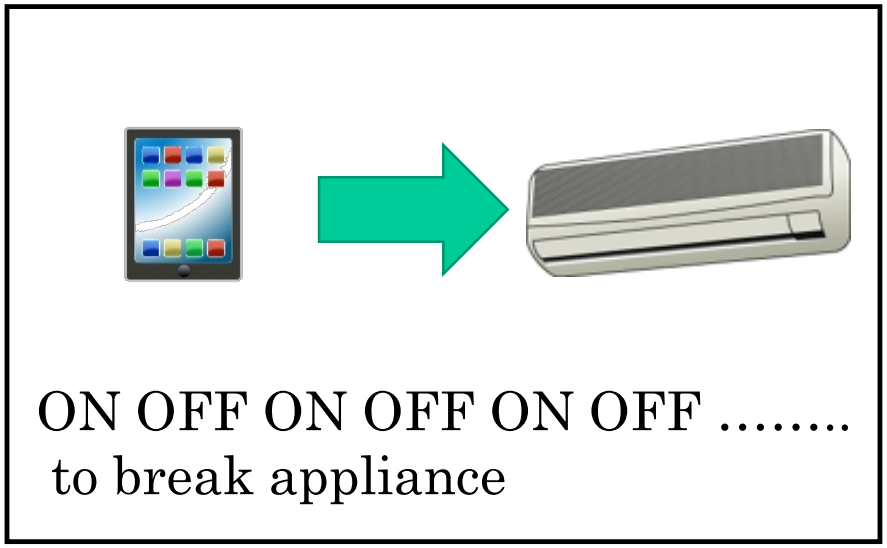
2.1.1.1. Safety of body/life

Information on things such as the use of faucets and housing equipment, the locking of the front doors and windows, and the state of electric power consumption based on the smart meter is used by smart houses to regulate homes. This information is (also) used to determine whether anyone is at home, and the electronic lock of the front door and windows is unlocked and a notice of absence is issued to a thief.



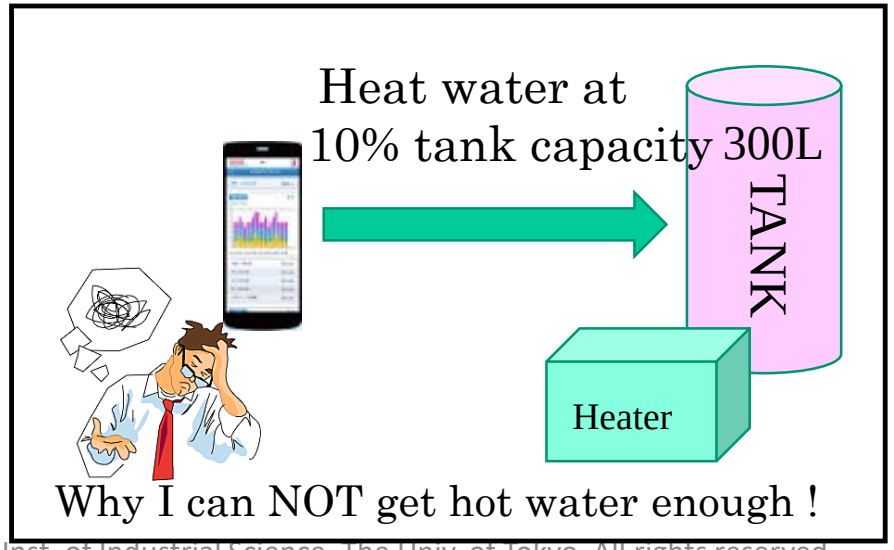
2.1.1.2. Safety of equipment

Air conditioners and other equipment that normally are not expected to be frequently started or stopped each a day can be caused to break down by repeatedly turning them on and off as many as hundreds of times a day.



2.1.1.3. Proper performance of equipment

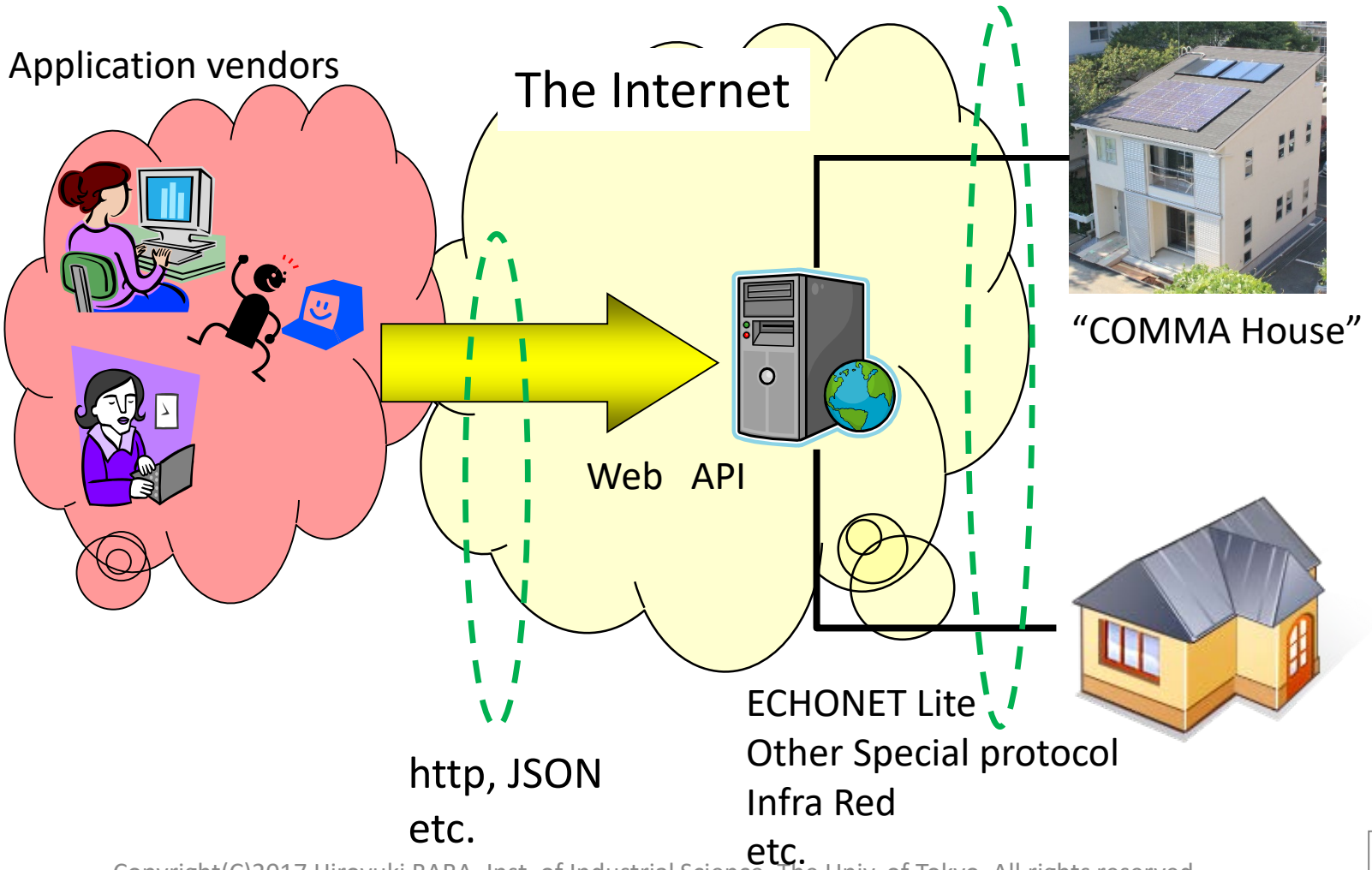
Water heaters containing a hot well can be caused to operate erratically. This is done by frequently transmitting signals from the mischief application instead of operation panel to tell the water heater that only 10% of the normal amount of hot water is needed, leaving the water heater perpetually low on water.



TEST BED at the University of Tokyo

TEST BED to develop IoT Technology

Application vendors can get access to the real world via Web API



Open Innovation Scheme at COMMA House

- ✓Promoting collaboration among different industries
- ✓Promoting participation of start-up enterprises
- ✓Enabling trials before the relevant eco-system is established
- ✓Prototyping

Thank you for your attention

(https://datatracker.ietf.org/doc/html/draft-baba-iot-problems-04)

Hiroyuki BABA

E-Mail: hbaba@iis.u-tokyo.ac.jp