Internet Research Task Force
Internet-Draft
Intended status: Informational
Expires: March 13, 2021

H. Baba
The University of Tokyo
I. Miyake
IoT Square Inc.
J. Matsumura
BizMobile Inc.
Y. Ishida
Japan Network Enabler Corporation

September 9, 2020

Study Report on a Framework for Cloud Inter-connection toward the Realization of IoT
draft-baba-iot-interconnection-04

Abstract

This paper describes issues for solutions through cloud inter-connection to structural problems, which are called as "silo effects" found in cloud-connected electric home appliances, housing equipment and sensors in the face of increasingly accelerated connection of them. Specifically, this paper explains an inter-connection agreement considered to be required for enhancement of cloud inter-connection, what performance guarantee as well as IoT supervising and management should be, necessity of inter-connection HUB which is able to provide inter-connection amongst the preponderance of private cloud groups, and the necessity of a mechanism to avoid threats that cause danger to users when we make the inter-connection.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 13, 2021.

Table of Contents

1. Introduction

To date, based on the results of interviews with "Things" companies, the authors of this paper, the Autors, issued a Problem Statement on IoT [1], and reported on an experiment of WebAPI [2]. With further interviewing and experiments, various requirements specification on a base for securing cloud inter-connection in the anticipated IoT society become clearer.

Currently, the use of various connected devices, hereinafter "IoT Devices" is largely expected to become a using scene of IoT, and such IoT Device manufacturers operates their private cloud groups, the "Cloud", where IoT Devices are connected one after another. It depends on the manufactures whether API of one cloud is open to a third party or whether the cloud remains closed just for itself just like a "silo". However, it is expected that API be open by manufacturers in charge to third parties in the near future and a

large variety of values shall be created through cloud inter-connection of IoT Devices that are connected to the other cloud groups with a similar structure. Several cloud inter-connection services, enabling one cloud with aforementioned IoT Devices to connect with another cloud with IoT Devices, have already been provided.

Thus, by combining cloud-connected IoT Devices, or "connected Things", just like toy blocks being built freely through cloud inter-connection, the era for creating a variety of benefits for users seems to approach us.

As far as users select and handle connected Things on their own response, there are not any significant issues. However, those whom you cannot expect IT literacy like elder people should be able to get access to benefits from IoT. If we stand on such an assumption, there seem to be many open issues.

Furthermore, there is a concern of threats that cause danger to the user's body, property, etc. when we make the inter-connection, and the mechanism to avoid these threats are necessary.

The Authors conducted interviews with 9 market players including IoT service providers and those who were preparing to provide IoT services and undertook research and summarized issues that those players felt with regard to cloud inter-connection. In parallel with other researching experience, we discussed on what framework would be required for doing IoT service provider businesses at smart houses. In addition, we organized the basic concept of the mechanism for avoiding threats when we make the inter-connection. This paper outlines the findings from such discussions.

2. Draft Framework for Cloud Inter-connection

Not assuming the style where users enjoy combination of the use of IoT Devices like DIY but assuming the one where so called service providers offer IoT services to users on a "do-it-for-me (DIFM)" manner, issues different from DIY style become more patent in the light of responsibility for customers and business continuity. Those issues are well diversified but may be summarized into three core categories as follows:

(1) Inter-connection Agreement

Commercial cloud inter-connection requires some kind of contracts without any doubt. Such contracting procedures are very common in the Internet market. However, manufacturers of home appliances and housing equipment have no experience and they feel worried.

(2) Operation Confirmation and Operation Monitoring of IoT Devices

Once being cloud-connected, it is necessary that not products of one manufacture but also ones made by others are operated with commands sent out of one's cloud server. At the development stage of services and during operation of the services, the operation monitoring of one's IoT Devices being connected with other's cloud group just with commands of one's.

(3) Inter-connection Infrastructure

Currently a large number of manufacturers proceed with activities in getting appliances and equipment that used to operate on a standalone basis connected to the Internet. Those pieces of appliances and equipment are independent of each other, namely "silos". Therefore, in case of connecting all those pieces with one another, the number of ways to connect needs to be N(N-1)/2. To do this, much resources shall be required. As was seen in telephone and the Internet, if HUBs connecting with one another are put in place, this issue would be less cumbersome to some extent.

The framework, comprising of above three points, shall be explained in details in the following chapter.

3. Interconnection Agreement

In the era of IoT, it is desirable to facilitate contracting between businesses smoothly by preparing a boilerplate format for an interconnection agreement in advance. As described in the previous chapter, because of the lack of experience in home appliances and housing equipment manufacturers, needless to say, any guidelines or formats would give great comfort to them. The benefits from an interconnection agreement are to define responsibility of each contracting party and clarify consent of the parties.

For example, manufacturers of gas cookers have been working on operational linkage between a gas cooker and air conditioner in order to harness the increase of room temperature. Possibly a universal remote controller may be linked with a gas cooker and then the user can of course operate an air conditioner with the gas cooker controller. However, unless there is consent from the manufacturer of the air conditioner on this link operation, the gas cooker manufacturer seems to hesitate to pursue this due to his feeling that this is not a fair business behavior.

Following precedents in the Internet, the contents of the interconnection agreement include demarcation of responsibility,

procedures in operation and maintenance, cost allocation, technical specifications, and general prohibitions. In addition to such contents, however, the interconnection agreement becomes significantly valuable by proving that participating parties formally agree upon commercial terms of cloud inter-connection.

Of course, the agreement stipulates terms on malfunctioning of IoT Devices. For example, there is a structure where an energy management application located in a cloud group of lighting equipment of Manufacturer A gives a command to a cloud group of air conditioning equipment of Manufacturer B. By chance, one air conditioner starts malfunctioning and the user may call a customer service of Manufacturer A that provides DIFM energy management services to the user. In this case, problems are 1) how the fault can be isolated and 2) how this user's report can be transferred to Manufacturer B if the fault is identified to come from the other service provider, namely Manufacturer B.

In case of one manufacture Authors interviewed with, regarding 1) above, the provider asks the user confirm the lighting operation by its universal remote controller. If operates, the manufacturer process the user's report for the moment as a problem of Manufacturer A. If not operates, the user report could be handled as a problem of Manufacturer B. Manufacture A does not escalate the user's report to Manufacture B in case of 2) above. At a glance, this behavior of Manufacture A may not be sincere, but this is related with the treatment of personal information. Nowadays, manufacturers collect personal information of the user only in case they really need such information. Following this information policy, if a lighting remote controller does not operate the air conditioner, problem of Manufacture B is suspected. However, Manufacturer A does not ask the user for his/her personal information. Instead, they ask the user to call Manufacturer B once again.

Because there are very extraordinary restrictions on transfer of personal information among service providers in many countries, aforementioned treatment of users has to prevail. Contrarily this treatment is totally opposite to a direction of the one-stop services that users generally look for.

Regarding cloud inter-connection, several opinions on issues in business continuity were heard. Namely, in case of formulating DIFM services containing services provided by others, the DIFM service providers are concerned with adverse impacts of the suspension or cancellation of other providers' services on his/her DIFM services. The interconnection agreement does not make other providers promise to continue the provision of the services to the DIFM providers. However, the agreement possibly defines responsibility of advance

notification and a certain lead time for countermeasure formulation. Therefore, the interconnection agreement is meaningful in this regard.

4. IoT Device Operation Confirmation and Monitoring

As was mentioned before, it is prerequisite to secure function of operation confirmation of related IoT Devices in DIFM business in its services development and in processing claims of users during service provision. Even in the experimental service development stage, it is often necessary to identify where a fault occurs and how to isolate the fault in case that IoT Device does not perform as it is expected. This articulates an issue related to inter-operability which is the purpose of inter-connection. Especially, fault identification and capacity to recover the identified faults are very significant issues.

In interviewing with IoT service providers, their capacity to process users' claims involves the following three functions.

1) Monitoring fault incidents;

2) Fault isolation; and

3) On-site fault recovery capability

As of now, generally operational confirmation and monitoring functions comprise the following items.

1) Alive monitoring of IoT Devices through confirmation on ping signal communications;

2) Understanding of fault situations and history by remote reading of equipment log; and

3) Alarm monitoring beyond pre-set threshold levels such as data traffic volume

However, if the number of IoT Devices increases rapidly from now on, a set of aforementioned simple monitoring functions may not be efficient in terms of recovery capacity and cost competitiveness. It is necessary to re-examine the scalability of current operation and monitoring systems carefully and introduce required new technologies for effective operational monitoring of widely proliferated IoT Devices from now on.

5. Interconnection HUB

When a large number of manufacturers start the operation of independent cloud groups, their mutual interconnection becomes more and more complex as is mentioned before. Telephone and the Internet are supported with so called interconnection gateway switch and IX structures, achieving inter-connection among service providers.

Of course, in the IoT world, similar arrangements to connect among cloud groups are possible. There is one difference from the era of telephone and the Internet. This is no existence of inter-connection communication protocols such as SS#7 and BGP4 here.

During the interviews with the providers, no one mentioned the necessity of standardization of inter-cloud interconnection communication protocols. Contrarily, many providers told that they would utilize whatever they can use in an extremely businesslike manner. Actually already existing inter-cloud interconnection services do not specially focus on this issue. So it is considered that interconnection HUBs would necessarily be structured in way HUBs accommodate various different kinds of protocols. In order to connect different protocols that respective cloud group utilize with one another, the HUB side needs to be equipped with a driver module matching each of the cloud groups to be connected. Authors call this as a "printer driver model."

And according to a research of Authors, interconnection services already put in place tend to take similar patterns such as inter-cloud interconnection and application-cloud connection. Therefore it is necessary to proceed with interconnections with different patterns in order to make it more universal.

Service providers as a bussiness that Authors are considering are at least the following four patterns. The University of Tokyo has proceeded a research, recognizing requirements for infrastructures for interconnection of those items.

[Pattern 1] Service providers with their private cloud connecting with IoT devices,

[Pattern 2] preparing device drivers to IoT devices,

[Pattern 3] supplying gateways which connect IoT devices, and

[Pattern 4] application and service providers with with others IoT devices.

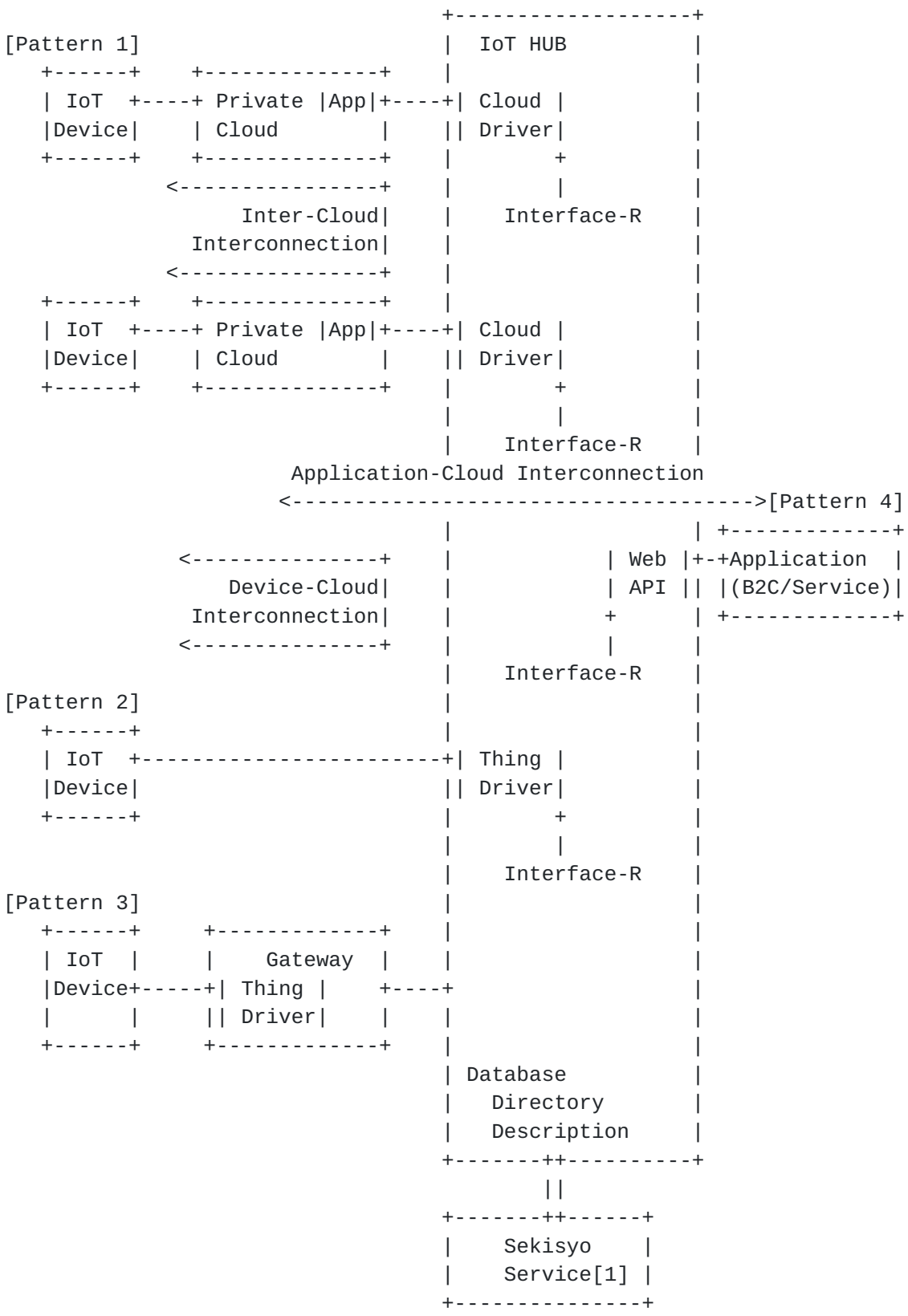

Figure 1: Structure of IoT HUB.

As a result, we verified the effectivness and flexibility of a new architecture. The architecture has a common interface named Interface-R within IoT-HUB, and all devices are connected to the HUB by defining the drivers for R-interface.

6. Flexibility of this method

This method is designed to interconnect IoT Devices, the connectable system is not limited to IoT Device. It can be connected with almost no limitations, such as a block chain engine or a system for data storage. As a result, it can be expected to contribute to the development of new economy such as utilization of data. For example, by setting the unit price for each operation of the IoT Device, costs for deployment of IoT devices are reocovable. Or by using this HUB as a branch point on the data transmission path, new business player such as a data storage provider can be involved in the connection between the IoT Device business companies.

7. Mechanisms to avoid threats when we make the inter-connection

As an example, let us consider a cooperative operation of "If the outside air is fresh, turn off the air conditioner and open the window". In case of humans operate, this behavior does not occur if no one is in the house, however, this behavior can occur in IoT whether the user is in the house or not. And your house can be entered by a thief if you are absence and unlucky.

In this example, the threat of being entered by a thief can occur by competing for the action of "opening the window" and the situation of "absence".

For this reason, a mechanism for avoiding the occurrence of such threats is required when we make inter-connection.

This can be realized by not permitting the target operation when the combination causing the threat as described above. This mechanism checks the movement of operations. In Japan, about 400 years ago, the Shogunate (government) had set up the checkpoints of human traffic, called the "sekisho." So, we are calling tentatively this mechanism SEKISHO after this fact.

8. Security Considerations

Regarding security, pattern 2 of service providers specified in Chapter 5 may contain some vulnerability and thus precaution is required.

9. Privacy Considerations

Regarding privacy, Chapter 2 touches upon concerns on privacy among inter-connected service providers in case of fault isolation after IoT Device malfunctioning.

10. IANA Considerations

This document has no actions for IANA.

11. Acknowledgement

This paper contains findings of the study funded by the Ministry of Internal Affairs and Communications of Japan as well as research activities of IoT Committee of Internet Association Japan. We hereby touch upon such facts and show our gratitude to those who relate to the study and committee activities.

12. Normative References

[1] Baba, H., Ishida, Y., Amatsu, T., Kunitake, K., and K. Maeda, "Problems in and among industries for the prompt realization of IoT and safety considerations", 2020, <draft-baba-iot-problems>.

[2] Baba, H., Ishida, Y., Amatsu, T., Masuda, H., Ogura, S., and K. Kunitake, "Report on Problem Solving Experiment for Realization of Web-API-based IoT", 2020, <draft-baba-iot-webapi>.

Authors' Addresses

Hiroyuki Baba
The University of Tokyo
Institute of Industrial Science
4-6-1 Komaba
Meguro-ku, Tokyo 153-8505
Japan

Email: hbaba@iis.u-tokyo.ac.jp

Izaya Miyake
IoT Square Inc.
Hibiya Parkfront.
2-1-6, Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011
Japan

Email: izmiyake@iot-sq.com

Jun Matsumura
BizMobile Inc.
Kanda Business Cube 3F
5-1, Kandatomiyama-cho
Chiyoda-ku, Tokyo 101-0043
Japan

Email: jumatsum@bizmobile.co.jp

Yoshiki Ishida
Japan Network Enabler Corporation
7F S-GATE Akasaka-Sanno.
1-8-1 Akasaka
Minato-ku, Tokyo 107-0052
Japan

Email: ishida@jpne.co.jp