공학석사 학위논문

Economic Analysis on IoT-as-a-Service Federation Model

IoT-as-a-Service Federation 모델의 경제성 분석

2019년 2월

서울대학교 대학원

M.S. Technology Management, Economics and Policy

Shin Dong Hyuk

Economic Analysis on IoT-as-a-Service Federation Model

지도 교수 Jörn Altmann

이 논문을 공학석사 학위논문으로 제출함

2018 년 12 월

서울대학교 대학원

TEMEP

Shin Dong Hyuk

Shin Dong Hyuk의 석사 학위논문을 인준함

2018 년 12 월

위 원 장 ______________________ (인)

부위원장 ______________________ (인)

위 원 ______________________ (인)

Abstract

Economic Analysis on IoT-as-a-Service Federation Model

Shin Dong Hyuk

M.S. Technology Management, Economics and Policy

The Graduate School

Seoul National University

Like other emerging technologies, Internet-of-Things is becoming "as-a-Service" integrated with the existing cloud platforms. Still, it has several technical issues with respect to scalability, geographic limitations, and interoperability. Studies have been proposed to adopt the concept of cloud federation to address these limitations. Although cloud federation has been envisioned to be a solution for IoT-as-a-Service, there is a paucity of studies from business and economic perspective. The research objective of this paper is to analyze IoT-as-a-Service federation model, which allows IoT providers to join and leave a federation, regarding the value that is created for IoT providers. An Agent-Based Model (ABM) with preparatory modeling schemes have been implemented, to conduct simulations of different federation scenarios. Simulation results demonstrate that this new concept of technology can contribute to the economic utility and technical efficiency by reducing costs, making better resource allocation, improving the Quality of

Service experienced by end users.

Keywords: Internet-of-Things, Cloud Federation, IoT-as-a-Service, Agent Based Modeling, Ecosystem Modeling, Resource Allocation

Student Number: 2017-21802

Contents

List of Tables

List of Figures

1. Introduction

Internet-of-Things, IoT, integrates the physical world and the virtual world through a number of devices distributed everywhere. This evolving technology of today generates a tremendous amount of data and introduces many novel applications, which can deliver new values to various participants in the IoT ecosystem. As time goes on, more and more IoT devices are being connected to the ecosystem, and interactions between the stakeholders are increasing rapidly.

Similar to other emerging technologies, IoT is also evolving to "as-a-Service" with the cloud computing paradigm. This transformation is mainly motivated by the complementarity of two different technologies, IoT and Cloud, leading disruptive innovation with new application scenarios (Botta, 2016). As the cloud is becoming an essential part of IoT implementations, most IoT solutions in the future are expected to be built and become dependent on the cloud-native architecture (Aguzzi, 2013).

However, there are still several technology issues of the existing IoT-as-a-Service platforms. First, scalability issue. As the number of IoT devices continues to increase steeply as well as the amount of generated data, dynamic cloud scalability is required since the capacity of a single IoT Cloud service provider is unable to meet the demands. Second, geographic limitations. Massive IoT-as-a-Service distributed in a large geographical area requires global-level service coverage (e.g., logistics, environment sensing), but current IoT Cloud service provider can only cover a limited land area.

Third, interoperability problems. The IoT ecosystem has intricate characteristics as a heterogeneous environment on which many types of devices, technologies, and applications operate simultaneously. As they are not always able to communicate over standards, the interoperability problem is a growing issue as the size of the ecosystem becomes larger.

To address the above limitations, several studies have been proposed to adopt the concept of cloud federation to IoT. Cloud federation is a strategic alliance of independent cloud providers for providing shared resources to deal with varying demands from users (Haile, 2015, May). In general, a single cloud service provider has a limited capability to accommodate large-scale applications and complex platforms incorporating various standards and technologies. Cloud federation provides more advanced scalability and availability with virtually unlimited shared resources on geographically distributed clouds (Airaj, 2013, December). Also, enhanced interoperability allows flexible service execution independent of the nature of the platform. The economic benefits of cloud federation have been discussed from a perspective of profitability of service providers (Goiri, 2010, July), and also with relevant economic theories (Kim, 2014).

Thus, the limitations of IoT-as-a-Service can be solved by the introduction of cloud federation. The federation in infrastructure and platform layers will cope with the issues of data expansion and scalability, geographic limitations of cross-border scale applications as well as interoperability issues in the heterogeneous environment. The federation in software layer will enable the integration of various applications to provide users with improved usability and novel services. The benefits of conventional cloud federation concept were mostly studied from a resource economics viewpoint, whereas federation in the IoT area can further enhance the flexibility of services.

Since cloud federation has been envisioned to be a solution for IoT-as-a-Service, yet little research has been conducted on business perspective and its impact on technical implementation. The widespread adoption of IoT requires a novel approach to the business model, which is distinct from traditional applications (Dijkman, 2015). In the IoT ecosystem, there are extensive interactions among various types of stakeholders, which transform the existing value chain more stereoscopically (Bilgeri, 2015). Hence, there is an absence of ideas on how to construct a value chain and profit model for the federation of specialized service, especially IoT. The prior research on IoT cloud federation is focusing on technical architecture (Celesti, 2016, March), energy resource management (Giacobbe, 2015, Sep), emerging storage (Fazio, 2014) and security (Barreto, 2015) issues. In order for this novel technology to generate actual economic values in reality, research on how business perspective determine the technical requirements and implementation of IoT-as-a-Service federation is in great need.

The research objective of this paper is to analyze IoT-as-a-Service federation model, which allows IoT providers to join and leave a federation, with respect to the value that is created for IoT providers. Based on this objective, the research questions were formulated as follows:

1. How are values created and delivered among the stakeholders in the IoT Cloud ecosystem, assuming IoT-as-a-Service federation?

2. How to model the dynamics of IoT-as-a-Service federation triggered by business requirements, i.e., the frequent establishment and termination of federations?
3. What will be benefits of IoT-as-a-Service federation in cost reduction and resource allocation?

To develop a research model for IoT-as-a-Service Federation, we considered Agent-Based Modeling (ABM) as a main methodology for the following reasons. First, IoT-as-a-Service federation model involves intricate interactions between heterogeneous stakeholders in the ecosystem. Second, this model is appropriate to demonstrate the dynamics of IoT-as-a-Service federation triggered by business requirements, especially the frequent establishment and termination of federations. For an elaborate implementation of agent-based modeling from the software engineering perspective, the ecosystem modeling using Stakeholder Network Diagram and the technical implementation using UML Sequence Diagram were implemented as preparatory steps.

We built two operating scenarios on the Stakeholder Network Diagram: Scenario A from the IaaS/PaaS perspective: A large multi-national logistics platform (for geographic coverage) and Scenario B from the SaaS perspective: A meta application in the smart city (for integration). Next, we constructed the Sequence Diagram with Unified Modeling Language (UML) to architect an actual technical implementation of IoT-as-a-Service federation model. Two types of implementations were considered, which are 1) Without federation and 2) With federation, and there is also a subtype of implementation 2-1) With federation (Dynamic Resource Allocation).

Based on the analysis of the two types of diagrams above, we implemented the agent-based model using NetLogo program. Through the comparison of two cases (i.e., without federation and with federation), detailed simulations are conducted by adjusting several parameters.

Consequently, we conducted an economic analysis on IoT-as-a-Service federation model through agent-based modeling and a couple of preliminary modeling schemes. This model can contribute to a better understanding of how economic values are created and delivered among the stakeholders in the ecosystem. Simulation analysis with specific federation scenarios demonstrates that IoT-as-a-Service federation can increase the economic utility and technical efficiency by maximizing profits, making better resource allocation, improving the Quality of Service experienced by end users. The results from the simulation can be used as a motivation for decision makers to invest in IoT-as-a-Service federation platform as well as IoT service itself. The more IoT-as-a-Service federation ecosystem grows, the more innovative large-scale application services will become a reality.

The remainder of the paper is summarized as follows: Section 2 reviews related literature and works. The research model for IoT-as-a-Service federation is presented in Section 3. Section 4 discusses the detailed results of the simulation with agent-based modeling. Finally, the paper concludes with a discussion of the results, contribution, and limitations in Section 5.

2. State-of-the-Art

2.1. IoT(Internet-of-Things)-as-a-Service

Like many emerging technologies that drive the fourth industrial revolution, IoT is also becoming “as-a-Service” consolidated with the existing cloud platforms. Previous studies have proposed several alternatives to complement the inherent shortcomings of this tiny hardware-centric technology with limited capability, but the integration with cloud computing has emerged as the most powerful solution. This is due to the mutually complementary properties of IoT and Cloud, which can give many advantages to each other in terms of storage, computation, and communication resources (Botta, 2016). For instance, if applications are running on an IoT device where computational resources are limited, it can adapt its settings with the environment to improve resource efficiency through the cooperation with the cloud (Jeferry, 2015). Besides, rapid delivery of services, high flexibility, and reduced costs are attracting many IoT providers into the cloud environment, and more and more IoT solutions are being implemented on the cloud-native architecture (Aguzzi, 2013). Cloud-native implementation enables a huge number of IoT devices to be efficiently managed and controlled in real time through the Internet. In addition, since most cloud platforms of today offer a variety of different applications, IoT-as-a-Service can be combined with them to create new business opportunities for service providers. Big data coming out of the widespread IoT networks can also generate new values and insights to the clients through the analytics platforms on the cloud.

However, there are still few technical issues of the existing IoT-as-a-Service platforms. First, IoT data is expanding exponentially. As the amount of data from a vast number of IoT devices explosively increases, current scalability of the existing cloud platform begins to hit the limits. This phenomenon has been predicted for a long time, but the growth rate of IoT devices far exceed the prediction. It is forecasted that the number of IoT devices will rise from 9 billion in 2017 to over 55 billion by 2025 (BI Intelligence, 2018). On the contrary, the most prestigious cloud providers that are currently leading the market have a definite limit on their infrastructure capacity and have too much data to process even beyond IoT. As a result, the lack of scalability causes the entire system going down and the service outages in a wide area are increasingly occurring.

Second, there are geographic limitations. The business requirements of recent IoT applications are becoming more complex and diverse, demanding global coverage to capture cross-border business opportunities. Especially like Massive-IoT, which refers to the billion scale number of devices requiring real-time connections even from the most remote regions (Qualcomm, 2017) needs adequate cloud resources to deal with geographically distributed service requests. However, the single cloud service provider has a clear limit with respect to such resource provisioning capabilities. Even market-leading cloud providers do not operate their data centers in all regions, which can cause the degradation or failure of services in some areas.

Third, the interoperability problems. The IoT ecosystem is characterized by a heterogeneous environment, on which numerous types of devices, technologies, applications are operating simultaneously. Since they are not always capable of communicating with each other, the interoperability problem becomes a big issue as the size of the ecosystem grows larger. The problem of fragmentation between different IoT environments hinders the entry of new stakeholders and the advent of cross-platform applications (Bröring, 2017). The lack of interoperability also causes the lock-in effect of the current platform, which can reduce the productivity of the provider and the end user's satisfaction (Haile, 2018). As such, interoperability has a profound impact on business as well as technical aspects. However, the single cloud service provider is not sufficient to resolve these intricate problems, which means collaboration with other cloud platforms is strongly required.

2.2. Cloud Federation

Cloud Federation is an advanced solution for conventional cloud computing, which can efficiently settle the problems diagnosed in 2.1. As the word implies, it is a strategic alliance between independent cloud service providers that jointly provide their resources to address the diverse service requirements of users (Haile, 2015, May). The limited capabilities of the single cloud service provider make it challenging to handle large-scale applications and complex platforms incorporating multiple standards and technologies. Cloud federation can actively cope with a variety of changing demands from users by allocating shared resources dynamically and can increase the profit of the provider, also by renting spare resources (Goiri, 2010, July). Besides, improved interoperability facilitates flexible service execution independent of the nature of the platform. These benefits of cloud federation can also be proven from an economic perspective, a reduction in costs due to the achievement of economies of scale and an increase in utility due to the enhancements in network externalities (Kim, 2014).

In order for individual cloud providers to actively join in cloud federation, it is essential to make them perceive their potential benefits for the participation. In this regard, the cloud federation platform, or the federated cloud provider performs a variety of roles to manage cloud federation to operate successfully and fairly. These roles include resource provider management, business logic and mechanism, efficient resource allocation, and application management (Altmann, 2017, September). It is important to guarantee a fair division of revenue for the participants in proportion to their contribution to the federation (Aryal, 2017, September). A rational revenue sharing model can drive sustainable value creation for relevant stakeholders and make their ecosystem grow up (Haile, 2016, Feb).

For users, as their behaviors and application requirements change over time, the cloud federation platform should allocate proper virtual machines dynamically for the whole application lifecycle, not only the initial stage (Aryal, 2018, April). Consistent and appropriate resource allocation is essential to increase the revenue opportunity for service provider since users' willingness-to-pay for services is measured through the time that they spent on services (Haile, 2016, May). Likewise, the total cost of running services can be minimized through an optimal service placement algorithm on the federated hybrid cloud (Altmann, 2014). Cloud federation for IoT-as-a-Service should incorporate appropriate management schemes that take into account the unique characteristics of IoT technology and applications.

2.3. IoT-as-a-Service Federation

The limitations of existing IoT-as-a-Service platforms discussed above can be overcome with the introduction of a Cloud Federation concept. The federation in infrastructure and platform layers will address issues related to data expansion and scalability, geographic limitations of cross-border scale applications as well as interoperability issues in the heterogeneous environment. Moreover, the federation in software layer signifies that various sorts of applications can be integrated to improve usability and provide novel services. Through the federation at each layer, we can consider a variety of unique service scenarios.

The benefits of traditional cloud federation concept were mostly discussed from a resource economics perspective, whereas federation in the IoT area can further improve the service flexibility. Since the IoT applications have been built across a wide range of fragmented domains, the federation idea can make it available to provide innovative services through developing cross-domain applications (Soursos, 2016, June). The implementation of federation architecture is actualized with container virtualization technology, and related scenarios have been discussed (Celesti, 2016, March). Further discussion is needed for diverse application scenarios of IoT-as-a-Service federation in the real world.

3. Research Model

3.1. Literature Research on Methodology

To develop an appropriate research model for IoT-as-a-Service Federation, we considered Agent-Based Modeling (ABM) as a main methodology. With agent-based modeling, we can model and simulate the complex system in which autonomous agents operate according to pre-set rules, bringing information about a variety of dynamic interactions between the agents like in the real world (Bonabeau, 2002). In this research, agent-based modeling is considered as a priority over other modeling schemes for the following reasons. First, IoT-as-a-Service federation model involves complex interactions between heterogeneous stakeholders in the ecosystem. Second, this model also allows setting the dynamics of IoT-as-a-Service federation triggered by business requirements, especially the frequent establishment and termination of federations. For a sophisticated implementation of agent-based modeling from the software engineering perspective, 3.2. Ecosystem Modeling using Stakeholder Network Diagram and 3.3. Technical Implementation using UML Sequence Diagram were implemented as preparatory steps.

3.2. Ecosystem Modeling (Stakeholder Network Diagram)

By building the Stakeholder Network Diagram, we identified various types of stakeholders and services they provide in the ecosystem. There are mainly three types of stakeholders in the diagram, which are Cloud/IoT Provider, IT

Service Provider, and End User. Accordingly, there are mainly two types of services which are Cloud/IT Service and IoT Device Service. And we also identified the exchange of services and economic values between each stakeholder interactively. For different purposes, we built two operating scenarios on the diagram like followings.

3.2.1. Scenario A from the IaaS/PaaS Perspective: A large multi-national logistics platform (for geographic coverage)

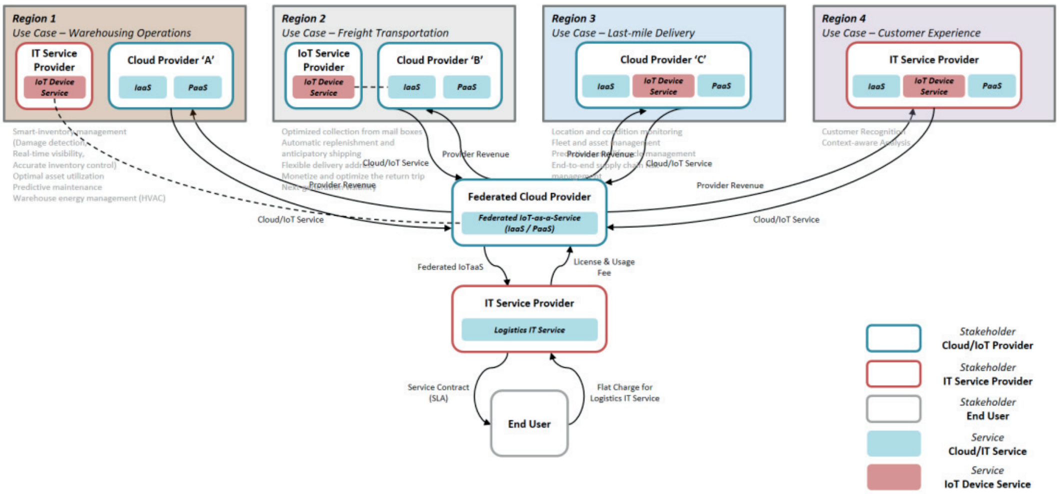

Figure 1. Stakeholder Network Diagram for Scenario A

Scenario A was constructed from the IaaS (Infrastructure-as-a-Service) / PaaS (Platform-as-a-Service) perspective. In this scenario, the application domain is a large multi-national logistics platform, and the purpose is to expand geographic coverage to the global reach. IT service provider could be a logistics service provider (e.g., DHL, UPS, etc.) in this scenario. Multiple cloud providers from four different regions are federated to provide a federated IoT-as-a-Service (IaaS/PaaS) for a single IT service provider. The configuration of the service providers in each area was created differently. In region 1 (warehousing operations), IT service provider provides IoT device service. In region 2 (freight transportation), IoT service provider provides IoT device service. In region 3 (last-mile delivery), cloud provider provides its own IoT device service. In region 4 (customer experience), IT service provider provides its own IoT device service. With this configuration, each service provider can implement their own logistics applications in their respective areas (Macaulay, 2015).

Stakeholders who were provided services are willing to pay economic values in the form of licenses and usage fees, which become the revenue of the provider. Federated cloud provider distributes the revenue based on the number and service time of the virtual machines deployed by each Cloud/IoT provider.

3.2.2. Scenario B from the SaaS Perspective: A meta application in the smart city (for integration)

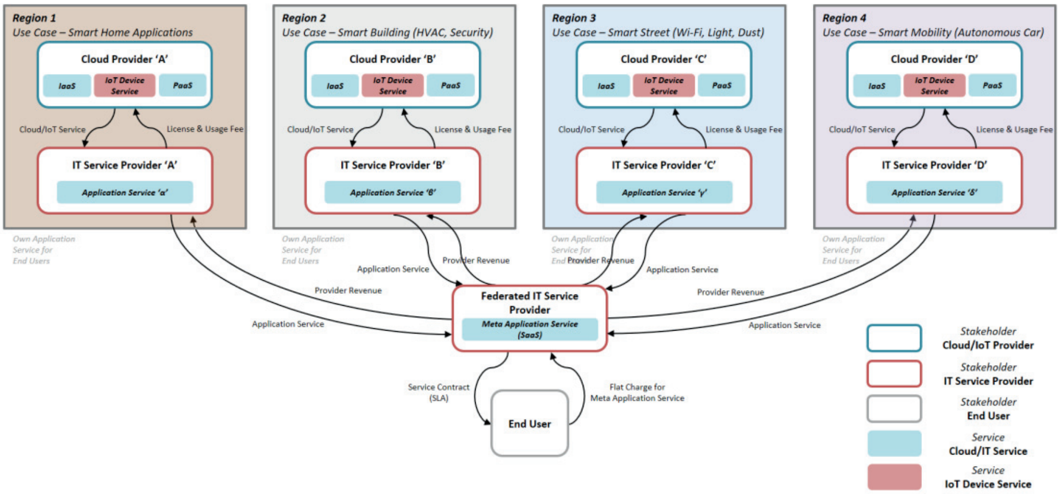

Figure 2. Stakeholder Network Diagram for Scenario B

Scenario B was constructed from the SaaS (Software-as-a-Service) perspective. In this scenario, the application domain is a meta application in the smart city and the purpose is to integrate heterogeneous applications services. IT service providers could be smart city service providers (e.g., smart home, building, etc.) in this scenario. Multiple IT service providers from different regions are federated to provide a meta application service (SaaS) for end user. The configuration of the service providers in each area was created identically. Each IT service provider has its own application service and each cloud provider provides its own IoT device service. In region 1, smart home applications are provided. In region 2, smart building

(HVAC, security) applications are provided. In region 3, smart street (light, Wi-Fi) applications are provided. In region 4, smart mobility (autonomous car) applications are provided. With this configuration, each IT service provider can implement their own smart city applications in their respective areas.

Stakeholders who were provided services are willing to pay economic values in the form of licenses and usage fees, which become the revenue of the provider. Federated IT service provider distributes the revenue based on the number and service time of the virtual machines deployed by each Cloud/IoT provider.

3.3. Technical Implementation (Sequence Diagram)

We constructed the Sequence Diagram with Unified Modeling Language (UML) to architect an actual technical implementation of IoT-as-a-Service federation model. Two types of implementations were considered, which are 1) Without federation and 2) With federation, and there is also a subtype of implementation 2-1) With federation (Dynamic Resource Allocation). The ecosystem stakeholders and their technical interactions identified in the Stakeholder Network Diagram are demonstrated in these sequence diagrams. Each diagram consists of four technical steps: a) provider registration, b) service request, c) service execution, and d) service termination. There is a significant difference in detailed operation according to whether the federation option is on or off, especially dynamic resource allocation.

3.3.1. Without Federation

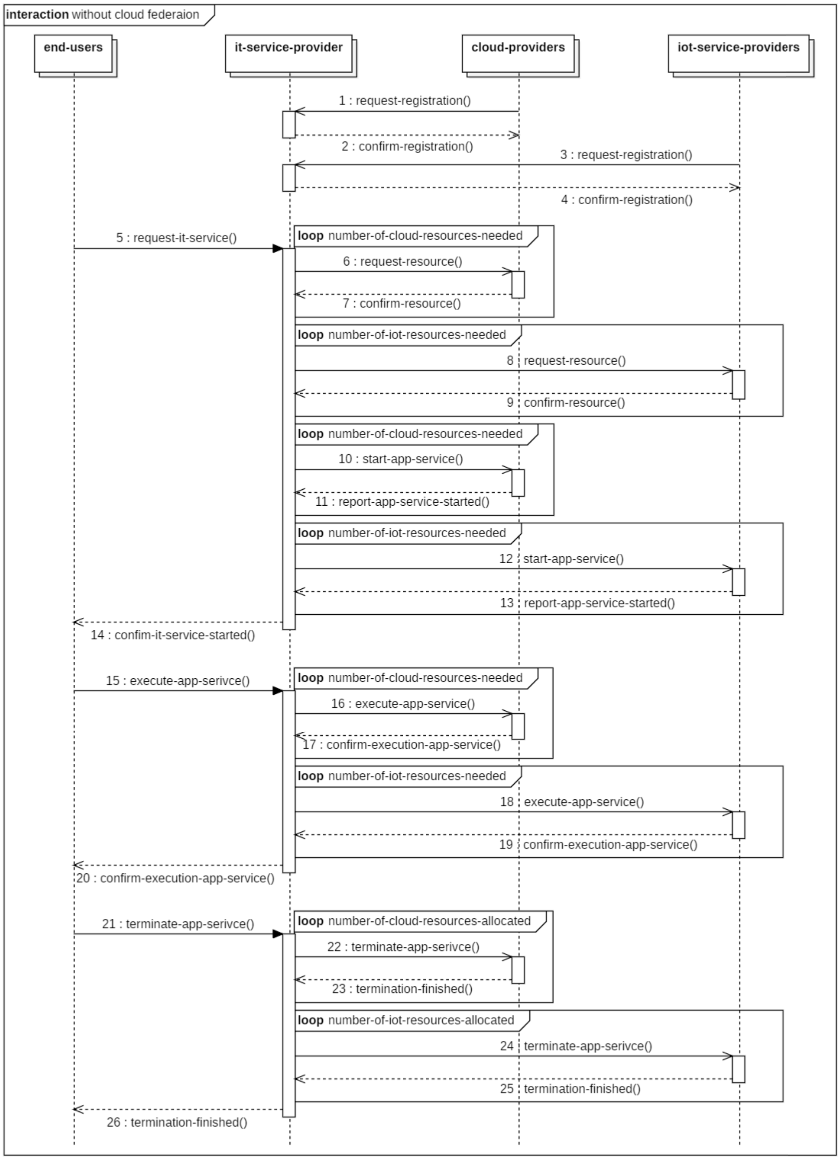

Figure 3. Sequence Diagram for Without Federation Case

In this implementation, IT service provider should manage every registration and connection with each of Cloud/IoT providers. Since IT service provider is a stakeholder who receives Cloud/IoT service to provide IT service, it is difficult to handle all of these connections throughout the service periods. Directly managing all resources, services, and applications incurs a lot of overhead costs for IT service provider. If there is more than one IT service provider, the costs of Cloud/IoT providers will also increase rapidly as the number of connections increases.

3.3.2. With Federation

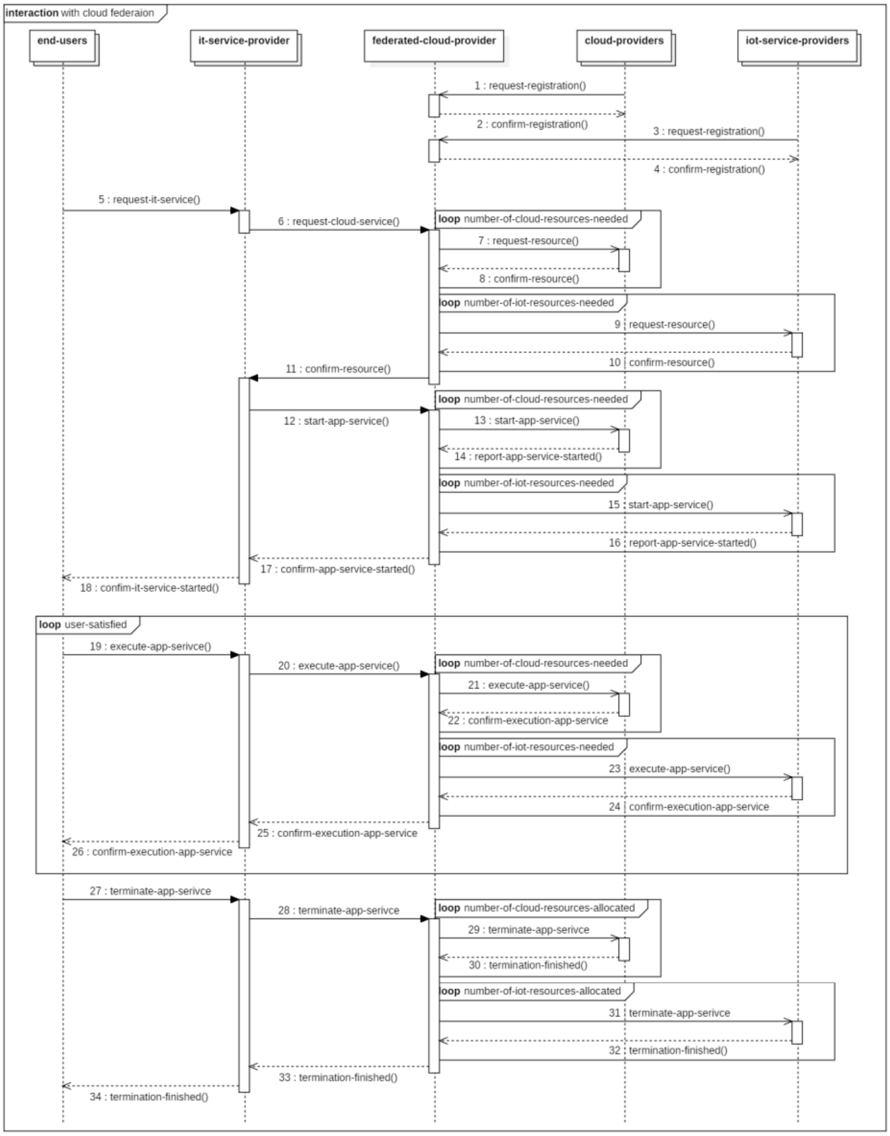

Figure 4. Sequence Diagram for With Federation Case

In this implementation, there is federated cloud provider who can manage every registration and connection with each of Cloud/IoT providers. Now, IT service providers can fully concentrate on their own tasks of proving IT service while maintaining a single connection with federated cloud provider. We assumed that this implementation could significantly reduce the costs of stakeholders compared to without federation case. This implementation also makes dynamic resource allocation possible, which we will discuss in detail on the next diagram.

3.3.3. With Federation (Dynamic Resource Allocation)

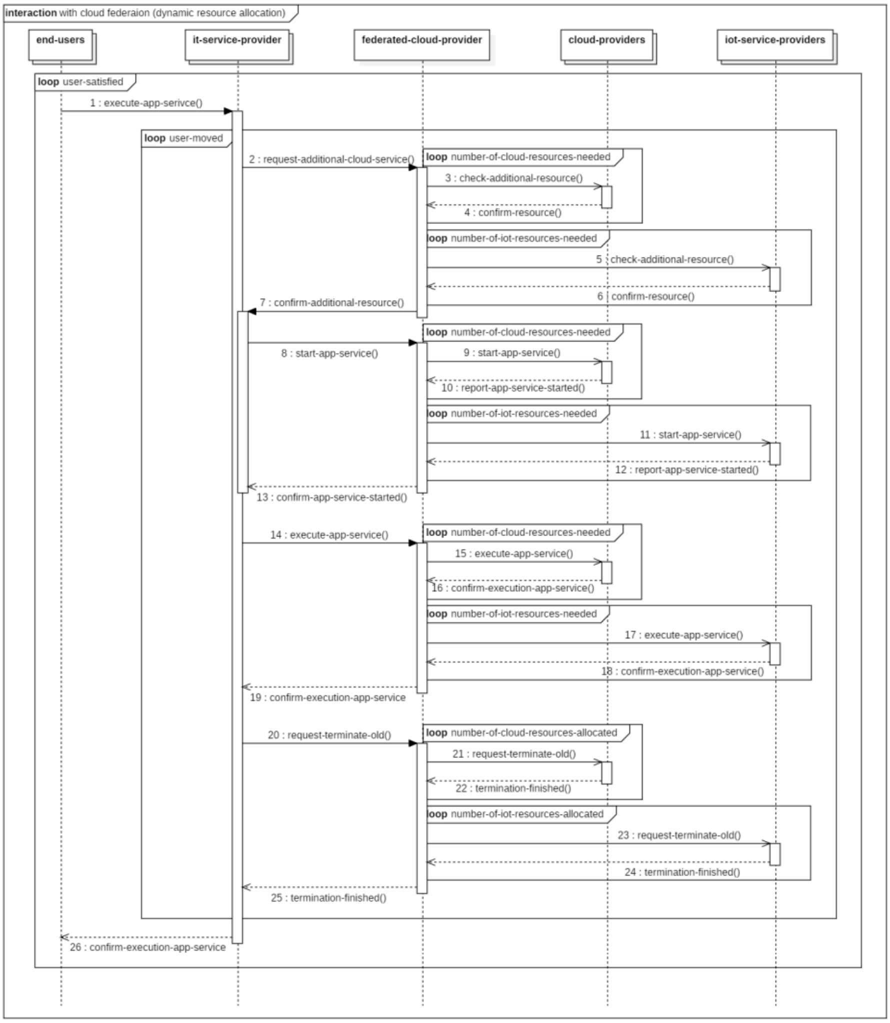

Figure 5. Sequence Diagram for Dynamic Resource Allocation

With this dynamic resource allocation function, federated cloud provider can manage various resources in real time and dynamic manner. It allows each of Cloud/IoT providers to join and leave a federation dynamically by business requirements. For example, if end user moved and gets out of service coverage, federated cloud provider automatically searches for additional resource providers in real time. After it confirms that the existing application is running successfully on the new resource provider, then it terminates the connection with the old resource provider. In this way, end user can be provided with seamless services regardless of its location.

3.4. Simulation Setup with Agent-Based Modeling

Based on the analysis of the two types of diagrams above, we implemented the agent-based model using NetLogo program. For the basic settings, various types of stakeholders in the ecosystem were declared by agentset breeds. 1) The arrow-shaped agent represents End User, white means no resources allocated, sky blue means cloud resources allocated, and green means IoT resources allocated. These end users move through the world in NetLogo to get resources. 2) Blue box indicates Federated Cloud Provider and red box indicates IT Service Provider. 3) The star-shaped agent represents a resource provider, sky blue for Cloud Provider and green for IoT Provider. The circle around a resource provider means service coverage in the physical world. If more end users than the predefined IoT capacity enter into the service coverage, the color of the IoT provider changes to red, and it is no longer available to allocate new resources. 4) The link breeds between stakeholders mean connections, but also can be costs. 5) There are three main regions in the world, and in the middle region, federated cloud provider and IT service provider manage the connections between stakeholders. In the Region A, agents operate under the 'without federation' implementation. In the Region B, agents operate under the 'with federation' implementation with dynamic resource allocation.

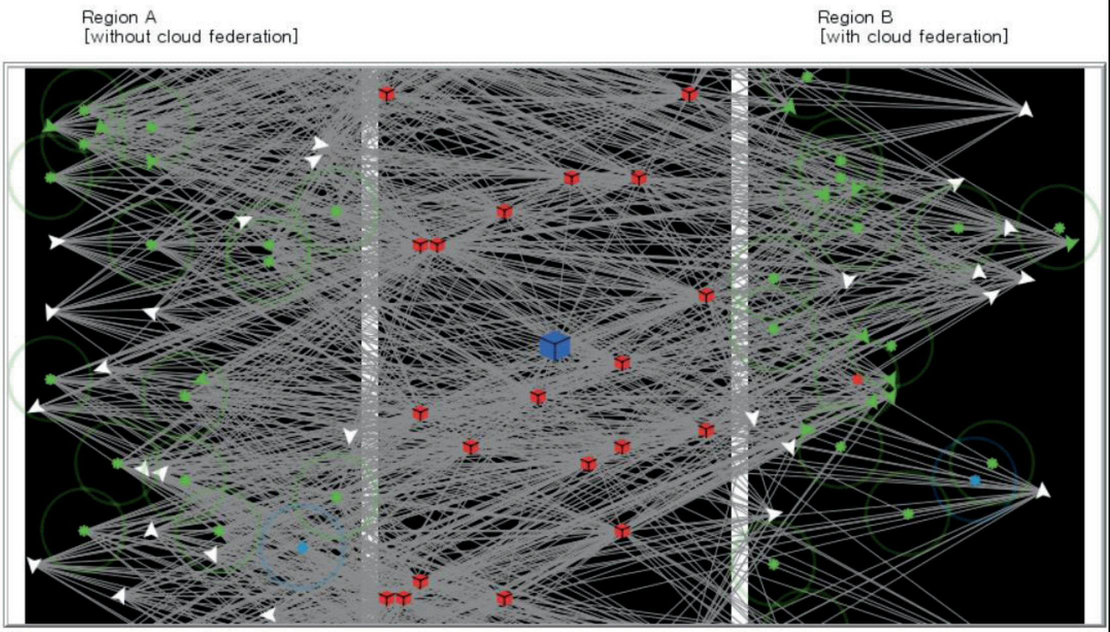

Figure 6. Simulation with NetLogo Program

Through this comparison of the two regions, detailed simulations are conducted by adjusting various types of variables. We will control the number of each stakeholder and also the capacity parameter of IoT provider. In the next section, we will analyze and discuss the simulation results.

4. Simulation Results

4.1. Basic Settings

For the simulation, the following numbers of agents are considered in Table 1. The number of agents can be adjusted for each purpose in the simulation.

Table 1. Number of Agents used in the Simulation

Federated Cloud Provider	IT Service Provider	Cloud Provider	IoT Provider	Static End User	Dynamic End User
1	50	1	50	25	25

In order to focus on the behavior of IoT providers and the value generated thereby, the deployment of a relatively large number of IoT providers compared to the cloud providers was considered. Static end user is a type of user who does not move and receive/not receive resources constantly in an area, and dynamic end user is a type of user who moves around the physical world and participates in establishment and termination of federations. The number of IT service providers was set equal to the total number of end users because it was identified as a moderate number that did not bias the IoT-as-a-Service federation.

4.2. Cost Analysis

In this simulation, we compared the costs in Region A (without federation case) and Region B (with federation case) to evaluate the economic utility of IoT-as-a-Service Federation. The link connecting each type of agent is cost itself, and each type of link has a different price. In 3.3., we assumed that Federated cloud provider could significantly reduce the costs of stakeholders.

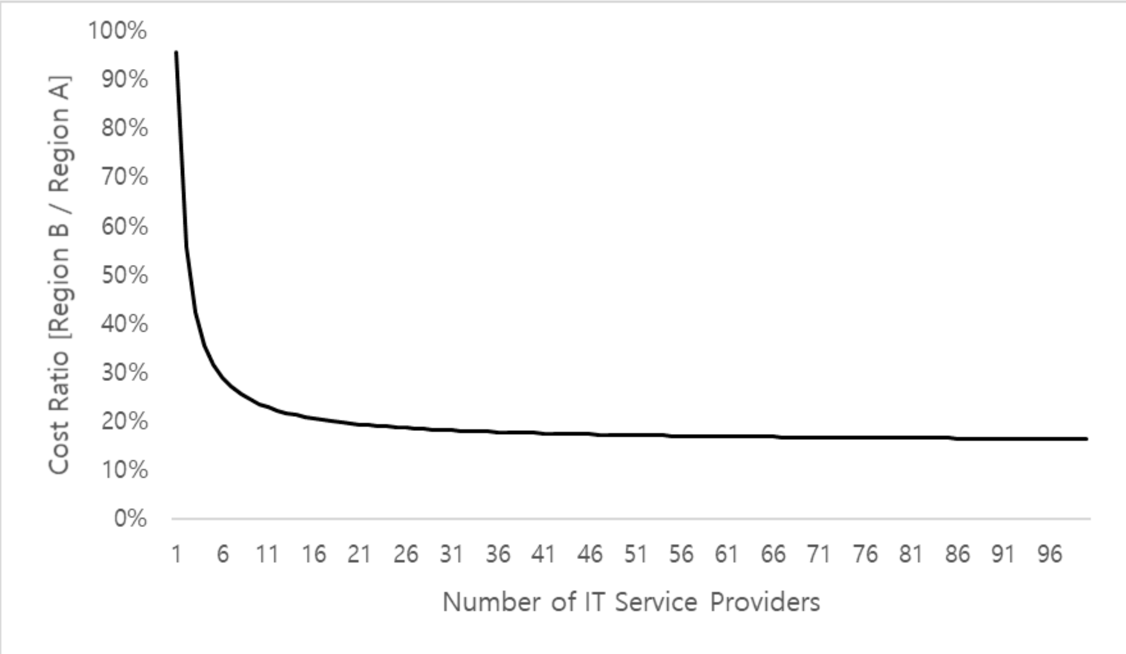

Figure 7. Cost Analysis for Region A and B

Figure 7 shows the cost difference between the two regions by calculating the cost ratio of Region B / Region A. Remarkable cost reduction was achieved in IoT with federation case compared to without federation case. This difference goes even more significant as the number of IT service providers increases, which can be explained as follows. First, the difference in the number of links. As discussed earlier in Section 3.3., federated cloud provider operates as a resource broker between IT service providers and Cloud/IoT providers in IoT with federation case, thereby significantly reducing the number of nodes required. It can also be checked by the density of the links on the NetLogo world. Second, the price difference per link. IT service provider lacks the ability to perform professional resource brokerage because it has its own business of providing IT service. In this simulation, we assumed that the connection cost between IT service provider and Cloud/IoT provider is 25% higher than the connection cost between federated cloud provider and Cloud/IoT provider. Even though the cost of single connection between IT service provider and federated cloud provider is considerably high, the total cost-savings due to the decrease in the number of nodes are significantly greater which result in substantial cost differences of the two regions.

4.3. Resource Allocation

In this simulation, we compared the resource allocation levels in Region A (without federation case) and Region B (with federation case) to assess the technical efficiency of IoT-as-a-Service Federation and derive business insights for decision makers. Various kinds of results were measured by adjusting several key parameters. Each of simulation results will be discussed below.

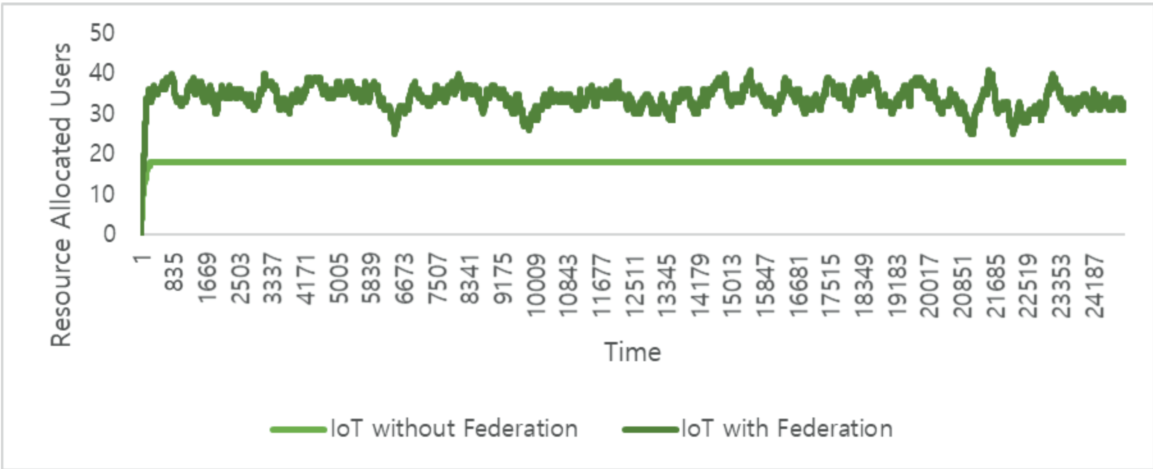

Figure 8. Resource Allocation of IoT without/with Federation

Figure 8 depicts the resource allocation levels of IoT without/with federation cases. All parameters were fixed at default settings. Over 25,000 ticks, end users in IoT with federation case have been allocated with an average of 85% more resources. This is because dynamic resource allocation function allows dynamic(moving) users to continue to receive resources regardless of its location.

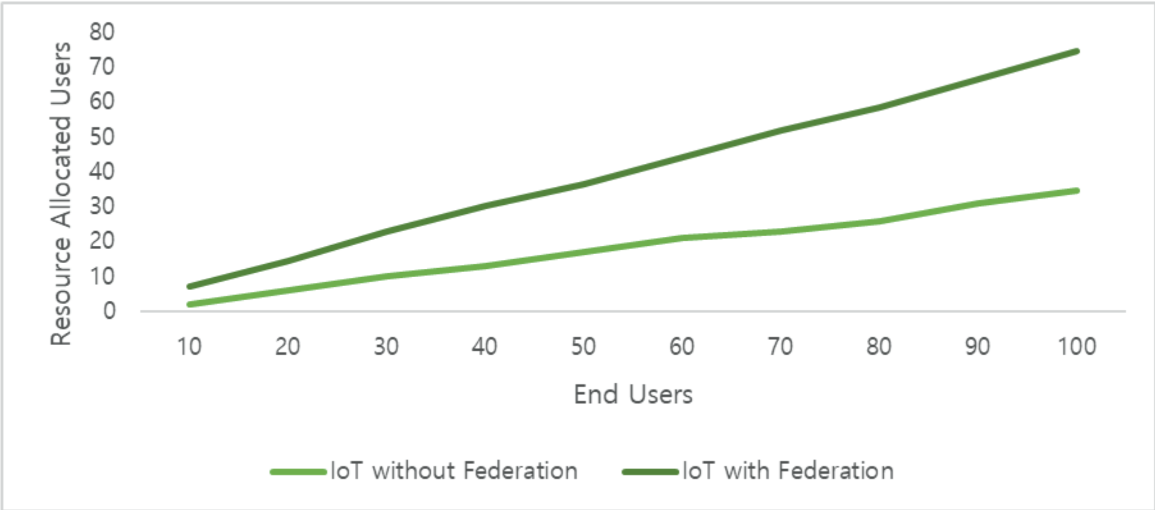

Figure 9. Resource Allocation by Increasing End Users

Figure 9 shows the resource allocation levels of IoT without/with federation cases by increasing the number of end users. The remaining parameters were fixed at the default setting. We see that the gap in resource allocation between the two cases identified in Figure 8 is going even greater as end users increase. This tendency is maintained until the number of end users reaches 100.

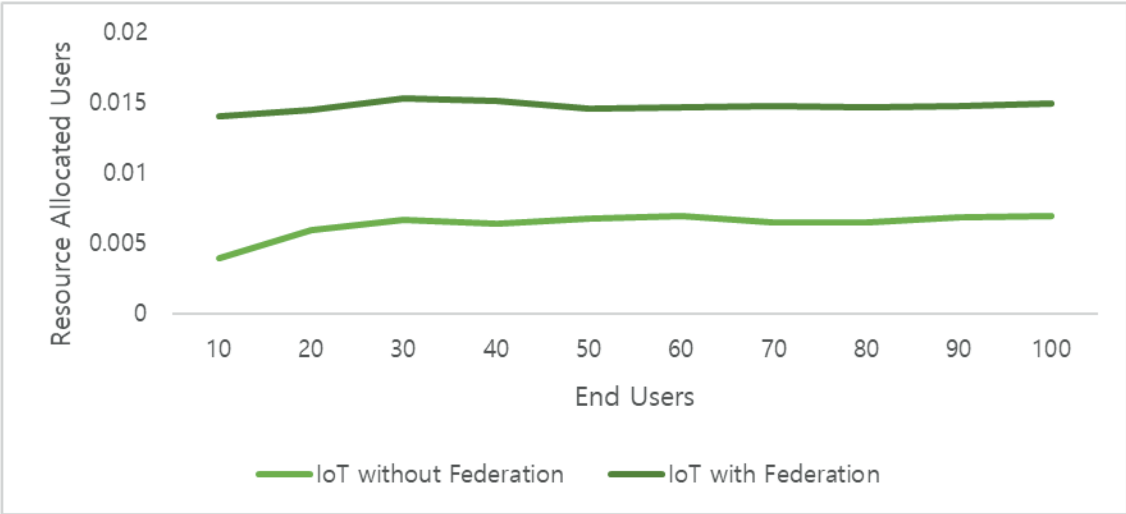

Figure 10. Maximum Capacity of IoT Providers

Figure 10 shows the maximum capacity of IoT providers in the two cases by increasing the number of end users. Maximum capacity was calculated by Resource Allocation / (IoT Providers * End users). This is a measure to see how the maximum resource capacity of IoT provider changes as end users increase. The average maximum capacity in IoT with federation case is more than twice as much as that of IoT without federation case. Even if the number of end users increases to 100, it shows that there is no notable volatility in the maximum capacity.

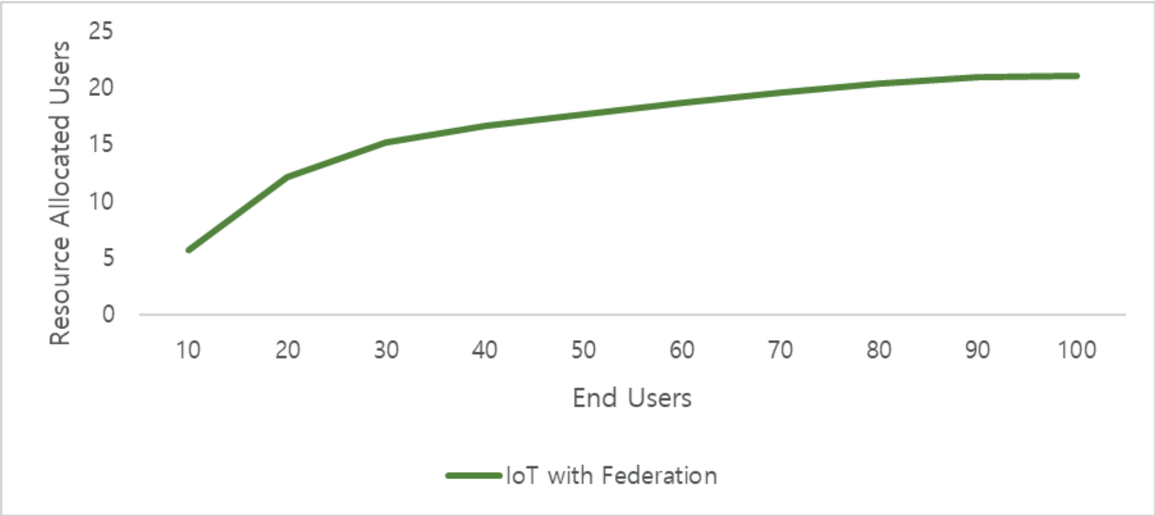

Figure 11. Resource Allocation when IoT Capacity = 1

Figure 11 shows the resource allocation levels when IoT capacity is limited to 1. This means that if more than one end user enters into the service coverage, IoT provider is no longer available to allocate new resources. As the number of end users increases, the increment of the resource allocation level gradually decreases and eventually the level reaches a certain limit, the maximum empirical capacity.

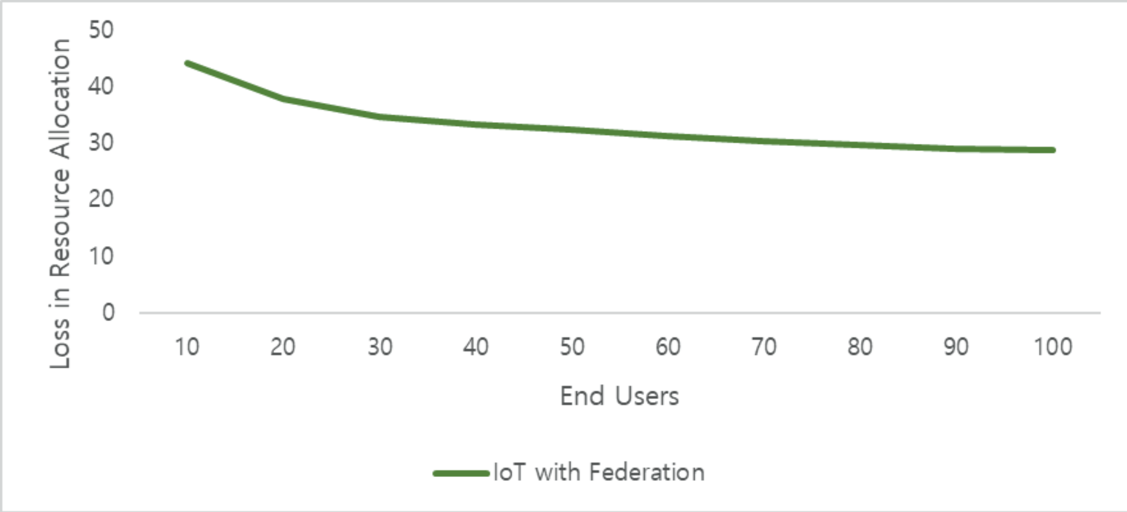

Figure 12. Loss in Resource Allocation (Theoretical)

Figure 12 shows the loss in resource allocation when IoT capacity is limited to 1. This is a measure to see how many end users did not get services. The loss was calculated by subtracting the resource allocation levels identified in Figure 11 from the maximum theoretical capacity, which is the number of deployed IoT providers. As the number of end users increases, the loss in resource allocation also shows a slow decline.

4.4. Profit Maximization Condition

From the simulation results of cost analysis (Section 4.2.) and resource allocation (Section 4.3.), we calculated the revenue, cost, and profit of IT service provider to figure out the profit maximization condition.

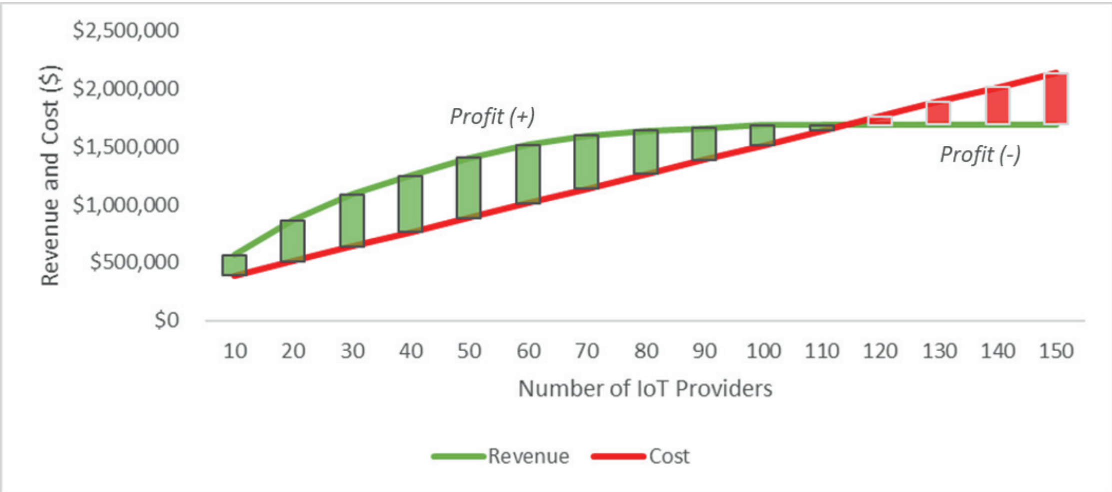

Figure 13. Revenue, Cost, and Profit by Increasing IoT Providers

Figure 13 depicts the revenue, cost, and profit of IT service provider who pays for federations with Cloud/IoT providers through federated cloud provider and provides their own services to end users. Their revenue is proportional to the level of allocated resources on which their applications are running, while cost is proportional to the number of links connected with resource providers. Once IT service provider establishes more federations with IoT providers, the revenue and cost will increase, and profit will be changed accordingly. However, as cost increases linearly while the rate of increase in revenue gradually decreases, profit will be changed to a negative value if the number of IoT providers exceeds a specific number. This is because the resource allocation level is reaching its limit. In this simulation, where we set the number of end users to 50, if the number of IoT providers exceeds 110, then IT service provider will suffer an economic loss.

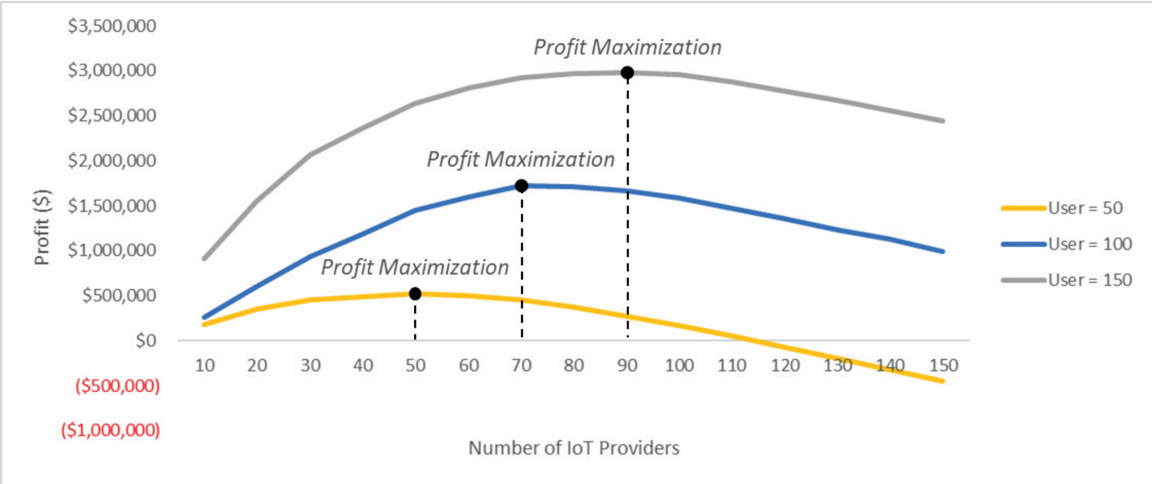

Figure 14. Profits per each number of End Users

Figure 14 expresses profits by increasing IoT providers per each number of end users. As discussed in Figure 13, profit varies with the number of IoT providers, and its curve has inverted U-shape. That is, each curve has a unique profit maximization point. (e.g., If the end user is 50, profit is maximized when IoT provider is also 50. Same for 100-70 and 150-90.) For profit maximization, IT service provider should establish federations with the proper number of IoT providers considering the number of end users in the ecosystem.

5. Discussion and Conclusion

5.1. Discussion

In the cost analysis simulation (Section 4.2.), we were able to discover a significant cost reduction in IoT with federation case compared to without federation case. This result comes from the federated cloud provider's specialized attribute as a resource broker, which has greatly reduced the number of connections required to build the service architecture and also the cost per link. We can consider a new business model for IoT-as-a-Service federation with these advantages, particularly as a resource broker. It can be formulated by building the federated cloud provider as 1) an independent stakeholder or 2) an affiliated stakeholder of IT service provider. Theoretically, the outcome of cost-saving reaches the maximum when the number of federated cloud providers is just one. If the number of federated cloud providers increases over one, the complexity of the overall network also becomes higher and likely to reduce the cost-saving effects.

From the comparison of resource allocation simulations in both cases (Section 4.3.), it is revealed that IoT with federation case results in better resource allocation. This difference originates from the existence of dynamic resource allocation function, which allows dynamic end users to receive resources consistently regardless of location. The distinction is more evident in the comparison of maximum capacity. In this way, it is expected that dynamic users in the real world can be continuously provided with various kinds of resources without being dependent on specific IoT provider. This will improve usability and enable innovative large-scale services for end users. Another critical factor to consider with regard to resource allocation is the capacity. As shown in Figure 11 and Figure 12, if the capacity of the IoT provider is limited, the resource allocation level cannot go out of certain bounds, and some part of the end users are not able to receive the service properly. Thus, IT service provider should consider the capacity and attributes of IoT provider when they are looking for proper resources on which they will run their applications for end users.

In section 4.4, we identified a profit maximization condition that reflects the simulation results of cost and resource allocation. If the number of IoT provider increases, cost continues to rise linearly, but there is a certain limit for the increase in revenue which is proportional to the resource allocation level. Thus, the profit graph for IT service provider represents an inverted U-shape and has a unique point for profit maximization. This means that more allocation of resources than necessary for running service will result in a decrease of profit. For the maximization of profit, IT service provider needs to establish federations with the appropriate number of IoT providers considering the number of end users in the ecosystem. In this regard, federated cloud provider can contribute to the profit maximization of IT service provider and assure the Quality of Service of end users by implementing federation level auto-scaling through real-time resource monitoring.

5.2. Summary and Contribution

Economic analysis on IoT-as-a-Service federation models has been performed with agent-based modeling and a couple of preparatory modeling schemes, leading to a better understanding of how economic values are created and delivered among the stakeholders in the ecosystem. Simulation analysis with different federation scenarios demonstrates that this new concept of technology can contribute to the economic utility and technical efficiency by maximizing profits, making better resource allocation, improving the Quality of Service experienced by end users.

These results can be utilized as a motivation for decision makers to invest more in IoT-as-a-Service federation technology and IoT services. The simulations performed in different conditions give them insights on the decisive factors they should consider to maximize profits. When an IT company or IT service provider build new IoT ecosystem under various scenarios and industries, a better business model strategy can be developed if they deeply understand the potential interactions and dynamics between the stakeholders and how to structure the stakeholder network efficiently. This study supports their decision making and leads all stakeholders in the ecosystem to benefit as well. For a certain number of stakeholders participating in the model, the economic utility of all agents can be maximized, and consequently, contribute to overall ecosystem growth. Growth in IoT-as-a-Service federation ecosystem will enable novel application services that were previously difficult to implement with scale and geographic limitations.

5.3. Limitations

IoT providers in the real world have many own attributes such as standards, protocols, coverage, and specialized application areas. However, only a single type and same capability of IoT provider were considered in this paper. In future studies, more realistic results can be obtained through models considering various characteristics of IoT. Furthermore, we want to address the interoperability problem that may arise from considering heterogeneous types of IoT through building advanced version of simulations.

Federated cloud provider can perform functions specific to application management such as knowledge extractor and edge SLA manager in addition to resource brokerage and resource allocation discussed in this paper (Altmann, 2017). The next study will explore ways to improve the economic utility and technical efficiency of IoT-as-a-Federation further, taking into account these additional functions.

Bibliography

Aguzzi, S., Bradshaw, D., Canning, M., Cansfield, M., Carter, P., Cattaneo, G., ... & Stevens, R. (2013). Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination. Final Report, European Commission, SMART, 37, 2013.

Airaj, M., Blanchet, C., Kenny, S., & Loomis, C. (2013, December). Appliance management for federated cloud environments. In Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on (Vol. 1, pp. 232-239). IEEE.

Altmann, J., Al-Athwari, B., Carlini, E., Coppola, M., Dazzi, P., Ferrer, A. J., ... & Psomakelis, E. (2017, September). BASMATI: An Architecture for Managing Cloud and Edge Resources for Mobile Users. In International Conference on the Economics of Grids, Clouds, Systems, and Services (pp. 56-66). Springer, Cham.

Altmann, J., & Kashef, M. M. (2014). Cost model based service placement in federated hybrid clouds. Future Generation Computer Systems, 41, 79-90.

Aryal, R. G., & Altmann, J. (2018, April). Dynamic application deployment in federations of clouds and edge resources using a multiobjective optimization AI algorithm. In Fog and Mobile Edge Computing (FMEC), 2018 Third International Conference on (pp. 147-154). IEEE.

Aryal, R. G., & Altmann, J. (2017, September). Fairness in Revenue Sharing for Stable Cloud Federations. In International Conference on the Economics of Grids, Clouds, Systems, and Services (pp. 219-232). Springer, Cham.

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49-69.

Barreto, L., Celesti, A., Villari, M., Fazio, M., & Puliafito, A. (2015, October). Security and IoT Cloud Federation: Design of Authentication Schemes. In International Internet of Things Summit (pp. 337-346). Springer, Cham.

Bilgeri, D., Brandt, V., Lang, M., Tesch, J., & Weinberger, M. (2015). The IoT business model builder. A White Paper of the Bosch IoT Lab in collaboration with Bosch Software Innovations GmbH.

Bonabeau, E. (2002). Agent-based modeling: Methods and techniques for simulating human systems. Proceedings of the National Academy of Sciences, 99(suppl 3), 7280-7287.

Botta, A., De Donato, W., Persico, V., & Pescape, A. (2016). Integration of cloud computing and internet of things: a survey. Future Generation Computer Systems, 56, 684-700.

BI Intelligence. (2018). THE INTERNET OF THINGS 2018 REPORT.

Bröring, A., Schmid, S., Schindhelm, C. K., Khelil, A., Kabisch, S., Kramer, D., ... & Teniente López, E. (2017). Enabling IoT ecosystems through platform interoperability. IEEE software, 34(1), 54-61.

Carlini, E., Dazzi, P., Mordacchini, M. (2016). A holistic approach for high-level programming of next-generation data-intensive applications targeting distributed heterogeneous computing environment. Procedia Comput. Sci. 97, 131–134.

Celesti, A., Fazio, M., Giacobbe, M., Puliafito, A., & Villari, M. (2016, March). Characterizing cloud federation in IoT. In Advanced Information Networking and Applications Workshops (WAINA), 2016 30th International Conference on (pp. 93-98). IEEE.

Coronado, J. P. R., & Altmann, J. (2017, September). Model for Incentivizing Cloud Service Federation. In International Conference on the Economics of Grids, Clouds, Systems, and Services (pp. 233-246). Springer, Cham.

Dash, S. K., Mohapatra, S., & Pattnaik, P. K. (2010). A survey on applications of wireless sensor network using cloud computing. International Journal of Computer Science & Emerging Technologies, 1(4), 50-55.

Dijkman, R. M., Sprenkels, B., Peeters, T., & Janssen, A. (2015). Business models for the Internet of Things. International Journal of Information Management, 35(6), 672-678.

Ericsson. (2017). Cellular networks for massive IoT. Ericsson Mobility Report.

Fazio, M., Celesti, A., Villari, M., & Puliafito, A. (2014, May). The need of a hybrid storage approach for iot in paas cloud federation. In Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference on (pp. 779-784). IEEE.

Fox, G. C., Kamburugamuve, S., & Hartman, R. D. (2012, May). Architecture and measured characteristics of a cloud based internet of things. In Collaboration Technologies and Systems (CTS), 2012 International Conference on (pp. 6-12). IEEE.

Gebregiorgis, S. A., & Altmann, J. (2015). IT service platforms: Their value creation model and the impact of their level of openness on their adoption. Procedia Computer Science, 68, 173-187.

Giacobbe, M., Celesti, A., Fazio, M., Villari, M., & Puliafito, A. (2015, September). A sustainable energy-aware resource management strategy for IoT Cloud federation. In Systems Engineering (ISSE), 2015 IEEE International Symposium on (pp. 170-175). IEEE.

Goiri, I., Guitart, J., & Torres, J. (2010, July). Characterizing cloud federation for enhancing providers' profit. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on (pp. 123-130). IEEE.

Gordijn, J., Akkermans, H., & Van Vliet, J. (2001). Designing and evaluating e-business models. IEEE intelligent Systems, 16(4), 11-17.

Haile, N., & Altmann, J. (2018). Evaluating investments in portability and interoperability between software service platforms. Future

Generation Computer Systems, 78, 224-241.

Haile, N., & Altmann, J. (2016, May). Structural analysis of value creation in software service platforms. Electronic Markets, 26(2), 129-142.

Haile, N., & Altmann, J. (2016, Feb). Value creation in software service platforms. Future Generation Computer Systems, 55, 495-509.

Haile, N., & Altmann, J. (2015, May). Risk-Benefit-Mediated Impact of Determinants on the Adoption of Cloud Federation. In PACIS (p. 17).

Jeferry, K., Kousiouris, G., Kyriazis, D., Altmann, J., Ciuffoletti, A., Maglogiannis, I., ... & Zhao, Z. (2015). Challenges emerging from future cloud application scenarios. Procedia Computer Science, 68, 227-237.

Kim, K., Kang, S., & Altmann, J. (2014). Goliath vs. a federation of Davids: a two-sided market analysis of competition between clouds. In GECON (Vol. 8914, pp. 45-56). Springer.

Macaulay, J., Buckalew, L., & Chung, G. (2015). Internet of things in logistics. A collaborative report by DHL and Cisco on implications and use cases for the logistics industry, Pub. DHL Customer Solutions & Innovation, Troisdorf.

Matthyssens, P., Pauwels, P., & Vandenbempt, K. (2005). Strategic flexibility, rigidity and barriers to the development of absorptive capacity in business markets: Themes and research perspectives. Industrial Marketing Management, 34(6), 547-554.

Hao Xu (2017). LTE IoT is starting to connect the massive IoT today, thanks to eMTC and NB-IoT. Qualcomm.

The Economist Intelligence Unit. (2013). The Internet of Things business index. InTechnical report.

Ray, P. P. (2016). A survey of IoT cloud platforms. Future Computing and Informatics Journal, 1(1-2), 35-46.

Rao, B. P., Saluia, P., Sharma, N., Mittal, A., & Sharma, S. V. (2012, December). Cloud computing for Internet of Things & sensing based applications. In Sensing Technology (ICST), 2012 Sixth International Conference on (pp. 374-380). IEEE.

Soursos, S., Žarko, I. P., Zwickl, P., Gojmerac, I., Bianchi, G., & Carrozzo, G. (2016, June). Towards the cross-domain interoperability of IoT platforms. In Networks and Communications (EuCNC), 2016 European Conference on (pp. 398-402). IEEE.

Westerlund, M., Leminen, S., & Rajahonka, M. (2014). Designing business models for the internet of things. Technology Innovation Management Review, 4(7), 5.

Yao, D., Yu, C., Jin, H., & Zhou, J. (2013, September). Energy efficient task scheduling in mobile cloud computing. In IFIP International Conference on Network and Parallel Computing (pp. 344-355). Springer, Berlin, Heidelberg.

Abstract (Korean)

여러 이머징 테크놀로지와 마찬가지로, 사물인터넷(Internet-of-Things) 또한 기존 클라우드 플랫폼과 통합되어 "as-a-Service" 형태로 진화하고 있다. 하지만 확장성, 지형적 한계, 상호운용성 등의 기술적 이슈가 존재하기 때문에 이를 극복하기 위해 클라우드 연합(Cloud Federation)의 개념을 접목하려는 연구들이 제안되었다. 비록 클라우드 연합이 IoT-as-a-Service의 솔루션으로 고려되었지만, 아직 비즈니스 및 경제적 관점에서의 연구는 부족한 현실이다. 이 논문의 연구 목적은 IoT 서비스 제공자들에게 창출되는 가치의 관점에서, 그들이 연합에 참여하고 나가는 것을 가능하게 하는 IoT-as-a-Service 연합 모델을 분석하는 것이다. 여러 다른 연합 시나리오의 시뮬레이션을 수행하기 위해 예비 모델링 기법들과 더불어 행위자 기반 모형(Agent-Based Model)이 구현되었다. 시뮬레이션의 결과는 이 새로운 기술 개념이 비용을 절감하고, 자원 할당을 개선하며, 최종 사용자의 서비스 품질을 향상시킴으로써 행위자들의 경제적 효용 및 기술적 효율에 기여할 수 있음을 보여준다.

주요어 : 사물인터넷, 클라우드 연합, IoT-as-a-Service, 행위자 기반 모형, 생태계 모형, 자원 할당
학 번 : 2017-21802