J Inf Process Syst, Vol.17, No.2, pp.284~296, April 2021
https://doi.org/10.3745/JIPS.04.0212

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Reference Architecture and Operation Model for PPP (Public-Private-Partnership) Cloud

Youngkon Lee* and Ukhyun Lee**

Abstract

The cloud has already become the core infrastructure of information systems, and government institutions are rapidly migrating information systems to the cloud. Government institutions in several countries use private clouds in their closed networks. However, because of the advantages of public clouds over private clouds, the demand for public clouds is increasing, and government institutions are expected to gradually switch to public clouds. When all data from government institutions are managed in the public cloud, the biggest concern for government institutions is the leakage of confidential data. The public-private-partnership (PPP) cloud provides a solution to this problem. PPP cloud is a form participation in a public cloud infrastructure and the building of a closed network data center. The PPP cloud prevents confidential data leakage and leverages the benefits of the public cloud to build a cloud quickly and easily maintain the cloud. In this paper, based on the case of the PPP cloud applied to the Korean government, the concept, architecture, operation model, and contract method of the PPP cloud are presented.

Keywords

Cloud Operational Model, Cloud Reference Model, PPP Cloud

1. Introduction

In recent times, the cloud has played a key role in the fourth industrial revolution, such as service innovation and new value creation through new technology combinations, and the accumulation and management of large-scale data. Most of the latest IT technologies, such as artificial intelligence (AI), big data, and blockchain, are implemented and utilized in the cloud. Developed countries, such as the United States and Europe are trying to introduce the cloud into the government sector, and cloud global companies are working to preoccupy the global cloud market by actively investing.

Despite government's efforts to introduce cloud services, government institutions still prefer to use private clouds only for non-critical services and build their own cloud because of security and reliability issues. When government institutions use public clouds, there is concern that even if institutions directly perform security control, sensitive data may be exposed to the public. When using a public cloud for institutions, it is necessary to consider all laws and regulations that should be followed.

Government institutions continue to expand the scope of institutions' use of private clouds and transition from cloud building and ownership models to private service models. They also plan to

Manuscript received September 14, 2020; first revision February 1, 2021; accepted February 4, 2021.
Corresponding Author: Ukhyun Lee (uhlee@shinhan.ac.kr)
* Dept. of Business Management, Korea Polytechnic University, Siheung, Korea (yklee2002@gmail.com)
** Dept. of School of IT Convergence Engineering, Shinhan University, Uijeongbu, Korea (uhlee@shinhan.ac.kr)

introduce various types of cloud models (hybrid, multi-cloud, public security cloud, etc.) for collaboration between institutions and the public sector. Security problems remain a stumbling block in the journey of an institution from a self-contained cloud to a private cloud or a new model, such as a hybrid. The public-private-partnership (PPP) cloud has been proposed as an alternative to solve these problems. The PPP cloud is a way to overcome the difficulties that could be encountered when converting information resources of institutions into the public cloud temporarily.

It takes at least 2 years for a company or institution to adopt a private cloud. The PPP cloud can be installed within a maximum of two months. Consequently, the cost of introducing a PPP cloud can be reduced to one-tenth by adopting a private cloud of the same size.

In this paper, we present a reference model that can be utilized when a government institution wants to introduce and operate a private cloud in the PPP model. Therefore, we present the status and problems of various domestic and international clouds. In addition, the concept and characteristics of PPP cloud and the necessary review points, technical model, operation model, and contract model are presented when introducing the PPP cloud.

2. Related Work

In the Federal IT Modernization President's Report [1], various ways to promote private cloud were announced to strengthen the security of the federal government of the United States. One way is to bring the government to the public cloud, and the other is to bring the public cloud to the government. The way to bring the government to the public cloud implies that the government will use the infrastructure of the public cloud operators, and it is important to have thorough security and control technology, because the infrastructure should be shared with customers other than the government. There are two ways of bringing clouds to the government. The first is to provide the cloud provider's servers to government-owned infrastructure [2], which is the model we propose in this paper. The second is to separate the cloud provider's servers and the infrastructure for government use. Both the implementation types for the PPP cloud are summarized in Table 1.

Table 1. Implementation method for PPP cloud

Method	Contents
Bring the Government to the Cloud	Used by the government for the infrastructure (building, server, network, application system, etc.) owned and operated by the cloud service provider e.g. SaaS, IaaS, etc.
	Default recommended, enlarged model
	Sharing infrastructure with non-government customers (however, government data require security and protection measures such as encryption)
Bring the Cloud to the Government	Provide servers owned and operated by cloud service provider in government-owned and operated infrastructure (e.g., buildings, networks, etc.)
	Suitable for non-Internet networks (e.g., closed networks, etc.)
	First use cases in information agencies (e.g., CIA, etc.) [3]
	Enabling the government to separate and use vendor-owned and operated infrastructure and servers
	Sharing logical spaces (servers, buildings, networks, personnel, etc.) among government agencies (e.g., AWS Secret Region)

2.1 MS Azure Stack

On August 8, 2017, Microsoft released the Azure Stack, a hybrid cloud platform that provides cloud continuity [4] implying that Azure's IaaS and PaaS in an on-premise environment is provided. If a company wants to use an on-premise system connected with Azure cloud, it implements a hybrid cloud platform that can retain and take advantage of Microsoft's public cloud Azure capabilities. A company that wants to use the cloud but has not been able to, can integrate Microsoft Azure with its infrastructure, and build a hybrid cloud to obtain advantage of the latest cloud features.

Azure Stack provides continuity without the need for any migration through integrated operation rather than the existing hybrid cloud, by providing compatibility between its data center and the cloud. Hybrid clouds support the compatibility between private and public clouds but do not guarantee complete continuity. Azure Stack ensures continuity by enabling customers to use the applications and services they use in a public cloud environment, even in a hybrid environment.

2.2 AWS Outpost

The Amazon Web Services (AWS) outpost aims to provide a hybrid cloud environment by internet-working with the AWS cloud. AWS services are available on-premises and support the AWS infrastructure and operations [5].

A key feature of the AWS Outpost is that companies build and use on-premises with the same services as the AWS cloud. The infrastructure is provided in the form of a fully managed service maintained and managed by AWS, and companies can choose between computing, memory, and storage. In addition, monitoring, updates, and patches for on-premise systems are automatically performed by the AWS Outpost. The AWS Outpost platform includes the API, management console, and automation.

By means of the AWS Outpost, customers use the same API and control panel used in AWS, and the scope of support includes EC2 (computing), EBS (storage), ECS (container), and EMR (big data). By using AWS's control panel in the same form on-premises, companies can take advantage of the same features and environments as AWS.

2.3 NBP Cloud-as-a-Service

NBP's cloud-as-a-service (CaaS) is a service that builds and uses the cloud infrastructure and cloud platform stack of Naver Cloud Platform, a public cloud service, in an on-premises environment [6]. In general, public cloud services provide multiple zones, allowing users to select zones and create and use computing resources and platform software. Zones generally represent a data center environment, and providing multiple zones in a region representing a region or country corresponds to a public cloud in multiple data centers in a region or country. It has the same meaning as operating and providing services, that is, the user selects a data center in which his service will be executed.

NBP's CaaS service is logically similar to setting up a cloud zone in an institution's data center or on-premises environment, in addition to a cloud data center operated by a cloud operator. In other words, if a cloud data center provides a public cloud zone, it is equivalent to providing a private cloud zone to an on-premises data center.

3. Concept of PPP Cloud

A PPP cloud refers to a private-public cooperation cloud method of renting, building, and operating a public cloud inside a government, local government, or government institution [7]. In other words, it is a

method of renting and building a cloud inside a government, local government, or institution for a system that cannot use a public cloud. The PPP cloud is a model that is established in the private sector and managed by public clouds. In the PPP cloud, management aspects include security control and operation [8]. In general, security controls can be performed by an institution, and operations can be performed remotely or internally by a cloud operator. The institution can use one of two ways to build a PPP cloud inside an institution. First, the cloud server is installed inside the institution, and the institution pays only the usage fee annually. Second, the construction of cloud infrastructure is provided by the public cloud on behalf of the institution in accordance with the requirements, and the risks that may occur when carrying out the project are shared. The first method is for a cloud operator to install a pre-fabricated cloud server inside the institution with minimum changes. It is mainly used for small- and medium-sized cloud construction using the HCI (hyper-converged infrastructure)—is an appliance that integrates and provides servers, storage, network, virtualization solutions, and orchestration management solutions from a single vendor in a single rack-like form. Fig. 1 shows the concept of the PPP cloud when public clouds are employed in the government data centers with network interfaces.

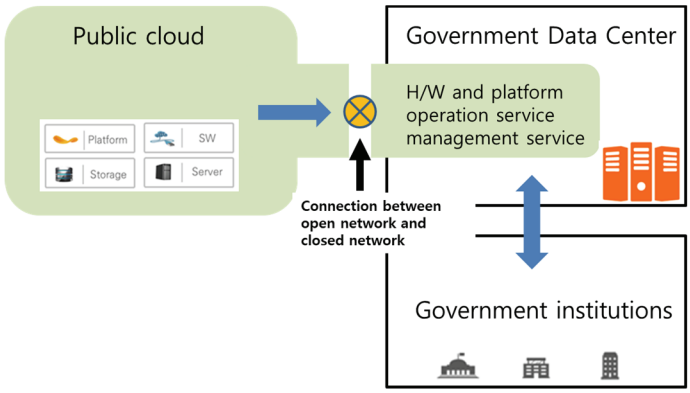

Fig. 1. The concept of PPP cloud.

The second method is to accept the institution's requirements under the consensus of cloud service provider (CSPs) and build a cloud. This is employed for building large-scale clouds. The PPP cloud is located in the data center of an institution and works with the existing institutional network and computing infrastructure. Because the PPP cloud is located inside the institution's security network, it has the same security level as the cloud that it builds. However, the operation can be performed directly by a public cloud operator remotely or by a cloud management service provider entrusted by a private cloud operator. Security control should be performed directly by the institutions. In principle, the PPP cloud is charged based on the monthly usage time. For this, a billing agent module that monitors and measures the hours of use of the institution is required. The monthly payment system is a simple model.

The PPP cloud has several advantages over the self-built method or the private cloud. First, building its own cloud has limitations in the introduction of advanced cloud technologies. Cloud technology is rapidly developing, and public cloud operators want to adopt the latest technology to meet market demands. However, the institution prefers a stable operation rather than installing the latest technology after the cloud is built. Therefore, it is difficult to introduce advanced cloud technologies. Second, building a cloud may have challenges in securing stable quality. It is probable that the internal managers of the institution are not cloud experts and therefore do not know how to respond appropriately when a

problem occurs. The institution may lack experience or knowledge of stable cloud operations. Third, it takes at least two years for an institution to build its own cloud. This may result in a significant overhead for the institution. There is a possibility of information being leaked or public cloud operators exposing confidential data. Therefore, the PPP cloud is a new cloud model that can satisfy both high security and advanced technology, operational experience, and knowledge of a private cloud by being located in the internal network.

4. Characteristics of PPP Cloud

The public cloud usually provides the service at a low cost, without a separate construction, and there are almost no issues related to quality or operation for services [9,10]. The self-constructed cloud has the most evident security advantages, but it has the disadvantages of being expensive to build and challenging to update it with the latest technology.

The PPP cloud combines the advantages of a public cloud and a self-built cloud. In other words, by installing the cloud system directly inside a government institution with the technology and cloud operation experience of a public CSP, there is an advantage that both security and technical aspects can be utilized. In addition, by building and operating a private cloud in the public, flexible operation, guaranteed high-quality service, and professional maintenance support are possible.

Once a private cloud is installed, depreciation occurs over time and technology continues to deteriorate, prompting it to be disposed after a certain period of time. However, because the PPP cloud installs a public cloud in the private sector, the public cloud continues to be upgraded systematically and technologically. In this respect, it can be concluded that the sustainability of the PPP cloud is much better than that of the private cloud.

Because the PPP cloud is built and operated inside the institution, it can comply with the institution's unique security policy and has the advantage of being able to operate within each institution's security environment [11-13]. CSPs can operate the PPP cloud directly or remotely, however security management must follow the security policy set by the institution. In principle, security control is performed directly by the institution's administrator within the security environment. Table 2 shows that the PPP cloud is superior in some aspects compared to the private cloud.

Table 2. Comparison between private cloud and PPP cloud

	Private cloud	**PPP cloud**
High-tech sustainability	Low	**High**
Stable service quality	Middle	**High**
Cloud construction time	At least 2 years	**Available immediately**
Budget efficiency	Low	**Middle**
Security safety	High	High

The PPP cloud has a rack-based all-in-one configuration for servers, networks, storage, etc., which enables rapid cloud configuration and support. An advantage is that it is possible to build a cloud in a short time by installing an all-in-one system built in a ready-made form by a CSP in an institution with minimum customization. The PPP cloud is a high-quality cloud service verified by a professional CSP with extensive experience in building and technology. Although the PPP cloud is installed inside the institution, it is difficult to obtain the same functions or characteristics as the public cloud, but the

experience and technology of the public cloud can be highly guaranteed.

The PPP cloud is built and operated by public cloud providers, making it easy to respond to changes in advanced technology. Public cloud companies are rapidly adopting technology changes and developments, and through contracts, these can be applied almost identically to the PPP cloud. The PPP cloud can minimize the investment cost in comparison to the cost of construction. The PPP cloud is borrowed from a CSP, and after a certain contract period, an institution returns the cloud system to the CSP. Therefore, the possibility of continuing the contract is an advantageous aspect from the viewpoint of the institution, and this minimizes the investment cost owing to the construction by entering into a contract considering the needs of the institution.

In summary, the PPP cloud has proven to provide high-quality service and a stable operating environment, and can be an alternative to improve public cloud construction and operation by reducing the time required and cost reduction when building a cloud.

5. Reference Model for PPP Cloud

The PPP cloud is a method of renting and building an on-premise cloud infrastructure provided by the public cloud within the government, local governments, and public institutions. PPP cloud users and administrators use and manage the PPP cloud through the portal (Fig. 2). To this end, the PPP cloud provides a user portal for users and an administrator portal for the administrators. The user portal provides functions such as service request and monitoring, history management, and the administrator portal provides service approval, service resource management, integrated control, and metering and billing functions. The PPP cloud provides a cloud service management platform that offers service composition, resource allocation, performance measurement, capacity management, and user authentication management functions. The PPP cloud is of two types:

- A model that installs the infrastructure configuration (appliance) formed by a professional cloud company inside the institution.
- A model that installs the infrastructure (e.g., server, storage, network, and software) of a CSP that has obtained public cloud security certification (CSAP) inside the institution.

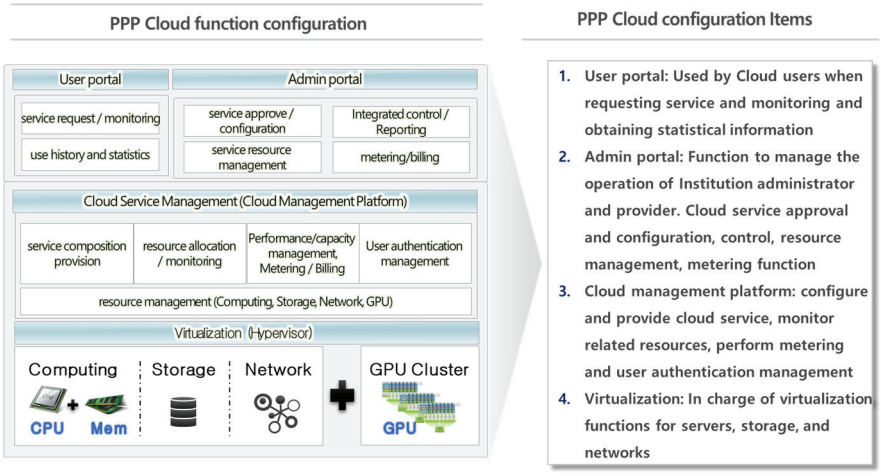

Fig. 2. PPP cloud function configuration.

5.1 Infrastructure Configuration Model Provided by Cloud Appliance Provider

This model configures a cloud infrastructure (appliance) and installs it inside an institution by applying open source and commercial virtualization software based on general hardware or HCI equipment, CSP, cloud managed service provider (MSP), and solution/equipment. Fig. 3 shows the PPP cloud implemented by cloud appliances.

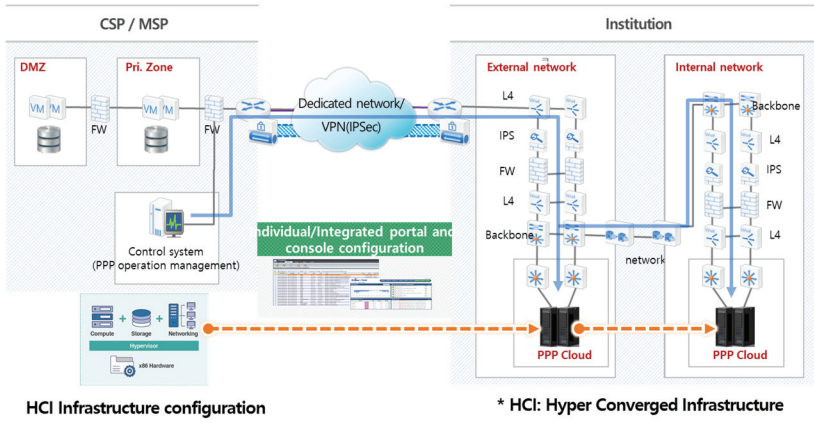

Fig. 3. HCI based model.

The PPP cloud is an appliance-type infrastructure that integrates servers, storage, network, and software (virtualization software and platform), virtualizes physical resources through a hypervisor, and configures various storages such as Block, NFS, iSCSI, and HDFS.

Hypervisors that can be applied to this model include Openstack KVM, VMware vSphere, Microsoft Hyper-V, and Citrix XenServer, and companies select and apply appropriate hypervisors according to their budget and scale. This model provides virtual resource creation and management functions through the cloud service portal and management platform, and consists of logically separating external service and business, management, and storage networks using network switches (L2).

The cloud portal is classified into a user portal and an administrator portal, comprising functions for institutional managers and operation management of the operators. Functions for institutional managers include virtual resource monitoring, account management, user approval for resource creation, and functions for operation management include PPP cloud virtual resources, server/storage/network physical resource usage, and failure prevention. The institution defines the authority of the portal user/ administrator in the early stages of cloud configuration, and the functions and screens are divided according to the authority.

Institutions using PPP cloud need to select the appropriate infrastructure through the scale of the cloud conversion system, the characteristics of the service (business), and RoI analysis, and the infrastructure shape recommends one of the two types of infrastructure.

The HCI appliance is employed when constructing a small- to medium-sized infrastructure and is suitable for systems or development systems that require infrastructure flexibility using step-by-step cloud transition of individual systems and expansion of new service (business) types.

The cloud appliance base is factored when configuring a medium-to-large (e.g., AI/big data system) infrastructure and is suitable for cloud conversion that integrates multiple systems with low volatility in resource utilization.

User organizations considering the PPP cloud-based hybrid cloud (including multi-cloud) configuration need to review the configuration and introduction of the integrated portal for integrated monitoring, efficiency of resource creation/management, and operational convenience. In this case, the organization may hesitate to develop an integrated portal because of the cost and time required to construct an integrated portal. However, in the future, if a hybrid/multi-cloud form is built using various operators' clouds, the integrated portal must be reviewed to ascertain the efficiency and convenience of management.

Institution users use the integrated portal solutions of several operators provided in the market to form an integrated portal. The institution can interoperate with the integrated portal solution by utilizing the API provided for management of the PPP cloud, and if the provided API function is limited, the functions of the integrated portal are also limited. The institutions may require additional development to link with the integrated portal depending on the virtualization software and platform of the PPP cloud infrastructure being introduced. Therefore, when selecting a PPP cloud, institutions should conduct a preliminary review on the possibility of moving to a hybrid or multi-cloud in the future, and if there is a possibility of conversion, considerations regarding the implementation of the integrated portal should be made.

Table 3. Functions required in user portal and administrator portal

Function	Contents
User portal	
Service request	Service catalog based virtual resource usage application function
Monitoring	Topology and usage status monitoring of virtual resources (server, storage, network, etc.) in use
Alarm management	After setting the threshold of use of virtual resources, when the conditions are met, alarm sent through email, message, etc.
User login	Based on user account and authority information, access (login) function (OTP function application, etc.) and management function through log collection for access information
Usage history and statistics	Providing usage status and statistics for each period of virtual resources (virtual server, CPU, memory, disk, storage, etc.) per user account
Administrator portal	
Admin login	Management function through log collection for access (login) function (applied OTP function) and access information based on account/authority information in charge of technology/management
Service approval	Approval function for the service requested by the user
Authentication/permission management	User/administrator's account-specific authentication function and management functions such as function permission registration/storage for resources
Virtual resource management (server, network, storage)	Management function for physical/virtual resources Virtual server (VM), storage, network (virtual router/switch), etc. Including management for domains (or zones)
Integrated monitoring	Monitoring of overall usage status of physical/virtual resource usage status by user account
Dashboard	Providing status and topology of virtual resource usage and user account in graphical form and figures in GUI form
Control/reporting	Infrastructure/security control function and periodic (monthly, etc.) usage status reporting function
Metering/billing	Ability to accurately measure the amount of use of virtual resources and a function to set billing and cost policies accordingly
Statistics management	Providing statistical information on usage by user/per household member/per period (by time)

The integrated portal consists of user and administrator portals, and the core functions that must be included in the selection and development of the integrated portal solution are listed in Table 3.

5.2 Infrastructure Configuration Model Provided by Security Certified Cloud Service Provider

This model is a method of installing the infrastructure (server, storage, network, and software) of the CSP that has obtained public cloud security certification (CSAP)—a system that supports users to use cloud services with confidence by evaluating and certifying compliance with information protection standards by a certification body—inside the institution, and the PPP cloud infrastructure is subjected to technical security. Therefore, the PPP cloud built by this model has already been checked and evaluated for security management from an operational point of view, and is remotely operated and managed by a business operator (CSP) with a professional operating system, thereby enhancing security and ensuring high reliability. Fig. 4 shows the PPP model with a security-certified cloud system.

The security certified cloud infrastructure configuration is an infrastructure with enhanced technical security, such as vulnerability check for virtualization infrastructure, portal of IaaS, and simulation penetration test of virtual environment (VM).

- Vulnerability check: Diagnosis of software security vulnerabilities for OS and application-specific vulnerabilities apart from IaaS portals and functions.
- Mock penetration test: Penetration test through external internet and penetration test into hypervisor or other VM through user VM.

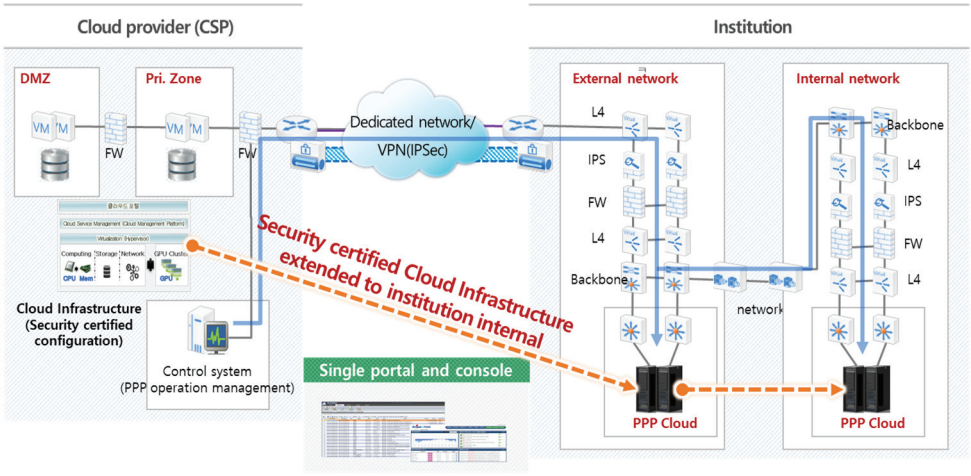

Fig. 4. PPP model with security certified cloud.

Institutions can use the secure authentication cloud model using a unified (provided by CSP) cloud service portal and console, enabling rapid hybrid cloud configuration, and using public clouds when additional resources are required. In addition, when reviewing the security of the National Intelligence Service for the introduction of the PPP cloud, a rapid review can be conducted for an infrastructure with technical protection measures.

5.3 Classification by PPP Cloud with Connection Multiplicity

In addition to the two PPP cloud types mentioned in Sections 5.1 and 5.2, a detailed classification of the PPP cloud is possible depending on whether the PPP cloud service provider is single or multiple, and whether the provided cloud is a connected or standalone type. Fig. 5 shows the detailed PPP cloud types.

Classification	Independent		Connected	
	Single provider	Multi provider	Single Hybrid	Multi Hybrid
Cloud appliance provider	Individual portal	Integrated portal	Integrated portal	Integrated portal
Cloud Security certified(CSAP) service provider	Individual portal	Integrated portal	Individual portal	Integrated portal

Fig. 5. Classification by PPP cloud with connection multiplicity

6. Operational Model for PPP Cloud

6.1 Operation and Security Control

Operation control is a service provided through a PPP CSP or a specialized private enterprise, MSP. A remote operation control is provided, and the user organization is resident in consideration of the security level of the target system to be converted to the PPP cloud. The institution can review a model that mixes the operational control model with remote/resident operating control. In general, it is possible to introduce an operation control service through a PPP cloud provider; however, it is also possible to consider selecting a separate professional company that provides an operation control service.

Because the operational control model is divided according to the role of operators, the operational control service scope and SLA standards are different for each remote/resident model, and the roles and responsibilities of operators that provide PPP cloud services vary depending on the model, as shown in Fig. 6.

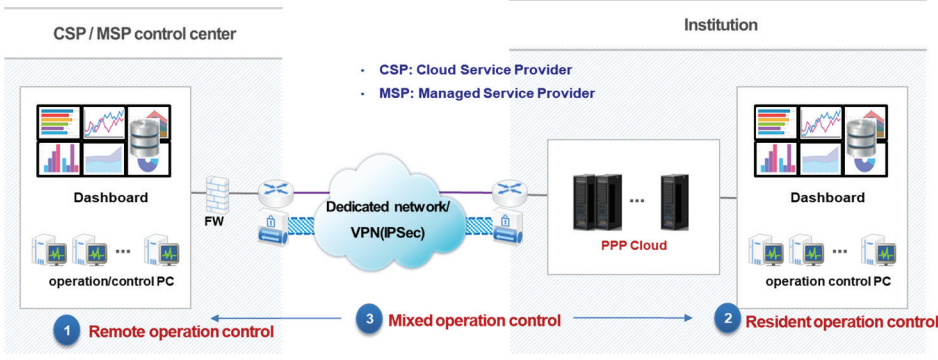

Fig. 6. Operation type for PPP cloud.

When the institution selects the remote/resident operating control model, depending on whether the operating control organization and network are separated within the institution, by securing the operating control personnel, the security level of the system to be converted to the PPP cloud, that is, the importance of data and the occurrence of an error/information leakage should be considered.

Service costs increase and decrease depending on the operation control model, scope, and time, and the institution needs to select the PPP cloud installation and operation control model in consideration of the cost. Therefore, it is necessary to use contracts and services by separating the scope of operational control services (e.g., technical support, monitoring, fault handling, and security measures) and service levels over time (e.g., basic, advanced, and customized).

6.2 Operation Scope

The scope of operational control includes technical support and monitoring, fault handling, security measures, and security control. However, CSP should provide security measures for the PPP cloud infrastructure itself, and CSP and MSP should provide operational control services that comply with IaaS security certified protection measures and similar administrative/technical protection measures.

Technical support: Support for configuring and changing infrastructure such as virtual servers/storage, and installing various middleware, applications, and security solutions.

- Middleware such as Web/WAS/DB, various application installations, and technical support. Application and management of security solutions such as server security (vaccine), system access control, DB encryption/access control, web shell, and personal information filtering and monitoring necessary for application and data security.

Monitoring: Real-time monitoring and control of infrastructure resource usage.

- Monitoring items: physical/virtual resource status information and utilization (e.g., CPU, memory, disk, network, etc.), process status information and utilization, TCP connection, and Ping/Port Check.
- It is necessary to classify and manage the monitoring items according to the managers, operation control service providers, and users. In other words, the status of physical resources is monitored by operators and managers, and users are considered irrelevant here.
- In the case of the remote operation control model, monitoring at the infrastructure and OS levels is central, and at the center of the resident operation control, middleware and application level monitoring may be necessary.
- The operator's role in monitoring and controlling is to set appropriate thresholds for each item and includes prompt response measures when the thresholds are exceeded.

Fault handling: Measures such as quick recovery of faults generated through real-time monitoring, control, and cause analysis.

- Measures for infrastructure degradation, errors, and failures caused by controllable technical factors, such as OS defects and hardware defects, such as OS, virtualization software, and portals.
- Classify the disability item and level (grade), and reflect it in the SLA, such as the urgency and action time according to the disability phenomenon.
- Provide report on obstacles, including impact on the occurrence of failures, analyzed causes, and future preventive measures.

7. Conclusion

In this paper, we present a reference and operational model for government institutions that are planning to introduce a PPP cloud. To this end, the current status of domestic and foreign public clouds was analyzed, and PPP cloud concepts and characteristics, as well as domestic and foreign PPP cloud case studies were considered. Based on this analysis, we present the review points for PPP cloud introduction, PPP cloud technical reference model, and PPP cloud operation model.

The PPP cloud is the optimal alternative for institutions to solve the most difficult complementary issues when adopting a public cloud. Institutions can take advantage of the advanced technology and cloud operation capabilities of public clouds. The institutions want their confidential data to remain invisible, regardless of what happens on the cloud. Considering this, the PPP cloud can be viewed as an intermediate cloud encompassing the features of both the private cloud and the public cloud. The PPP cloud, as suggested in the case analysis, is the preferred cloud form for governments and institutions.

The most recommended model for organizations to adopt a cloud is to use a public cloud. Using a public cloud can best utilize the characteristics and advantages of the cloud. However, both domestically and internationally, there are many laws and regulations with regard to the cloud, and the as the government agencies are stringent, it is not an easy option to incorporate a public cloud from the beginning. Thus, it is necessary to propose a method to gradually move to the public cloud after institutions experience the stability and technical advantages through the PPP cloud.

In this paper, two reference models for the introduction of the PPP cloud are presented. The first is a method to configure and apply a cloud appliance by a cloud professional company, and the second is to install a cloud shape of a CSAP-certified company in a user institution. The PPP cloud user can select and build an appropriate model according to the situation and scale of the two models.

It is true that the PPP cloud is inferior in terms of operation compared to the public cloud. There are difficulties in maintenance, such as scale-up of computing resources, and when an error occurs, the operator may have difficulty responding immediately. In addition, operators need more effort than public clouds to maintain SLA quality levels. Therefore, the user organization should consider these parts when introducing the PPP cloud.

Because the PPP cloud is usually located in the internal network of the institution, the administrator should carry out security control. The PPP user organization must establish security systems, including intrusion detection or firewalls, and security policies, including user access rights. In addition, these contents should be clearly presented in the contract with the providers delivering the PPP cloud.

In the cloud, multi-cloud or hybrid clouds have become the dominant trend. The PPP cloud will probably go through a process of converting to a hybrid cloud, if it is riding on this trend in the near future. When a user institution adopts a PPP cloud, it is desirable to form an integrated portal with the transition to a hybrid cloud in the future.

The PPP cloud has obvious strengths in terms of security, however, it is gaining strength by undermining some of the strengths of the public cloud. The biggest problem is that the PPP cloud cannot guarantee the convenience in the operation and management of public clouds. In addition the PPP cloud has limitations in continuous technology upgrades after its introduction. Continuous research is required to compensate for these shortcomings. If research is conducted in terms of security in cloud connection, it will be possible to develop a model that allows connection between the PPP cloud and public cloud in the form of a hybrid cloud.

References

[1] https://www.whitehouse.gov/articles/final-modernization-report/, White house, USA (2017).

[2] Government of the United Kingdom, "Cloud guide for the public sector," 2021 [Online]. Available: https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector.

[3] https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html (2018).

[4] http://www.qvrex.co.kr/wp-content/uploads/2017/07/Microsoft-Azure-Overview.pdf, Microsoft (2017).

[5] Amazon Web Services, "AWS outposts: user guide," 2021 [Online]. Available: https://docs.aws.amazon.com/outposts/latest/userguide/outposts.pdf, Amazon (2019).

[6] Naver Cloud Platform, "Now and future of Hybrid cloud service for promoting business," 2019 [Online]. Available: https://seminar.citrixevent.com/FWT2019KR/download/PTDeck/2_NBP_HybridCloud_Strategy.pdf.

[7] National Information Society Agency, "2018 Public Sector Cloud Leading Project Casebook," 2019 [Online]. Available: https://www.ceart.kr/web/board/BD_board.view.do?domainCd=2&bbsCd=1031&bbscttSeq=20190605142239481.

[8] Ministry of the Interior and Safety, "Guidelines for the use of private clouds for public administration," 2019 [Online]. Available: https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000015&nttId=75072.

[9] J. H. Qiang, D. W. Ning, T. J. Feng, and L. W. Ping, "Dynamic cloud resource reservation model based on trust," *Journal of Information Processing Systems*, vol. 14, no. 2, pp. 377-395, 2018.

[10] Y. Song and Y. Pang, "How to manage cloud risks based on the BMIS model," *Journal of Information Processing Systems*, vol. 10, no. 1, pp. 132-144, 2014.

[11] M. G. Jaatun, C. Lambrinoudakis, and C. Rong, "Special issue on security in cloud computing," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 1, article no. 17, 2012. https://doi.org/10.1186/2192-113X-1-17.

[12] N. Gonzalez, C. Miers, F. Redigolo, M. Simplicio, T. Carvalho, M. Naslund, and M. Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 1, article no. 11, 2012. https://doi.org/10.1186/2192-113X-1-11.

[13] K. Hashizume, D. G. Rosado, E. Fernandez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, article no. 5, 2013. https://doi.org/10.1186/1869-0238-4-5.

Youngkon Lee **https://orcid.org/0000-0002-8427-2542**

He is a Professor in the Department of Business Management, Korea Polytechnic University. His research interests include IT service QoS, cloud service computing, and knowledge search based on ontology. He has recently been involved in large scale consulting on the integration of government IT systems into the cloud, and has been performing considerable research on the effective operation of open platform-based clouds. In addition, he is pursuing studies in cloud-based big data analysis and cloud performance improvement, with great interest.

Ukhyun Lee **https://orcid.org/0000-0002-4938-8881**

She received the B.S. degree in Department of Computer Science, Ewha Womans University in 1992 and M.S. degree in Department of Information and Communication Engineering, KAIST in 1997, and Ph.D. degree in Department of Computer Science, Chonnam National University in 2003. She is a Professor in School of IT Convergence Engineering, Shinhan University. Her current research interests include the effective operation of open platform-based cloud and AI data processing and data modeling.