THE MINISTRY OF RESEARCH, TECHNOLOGY AND HIGHER EDUCATION
THE REPUBLIC OF INDONESIA

DIPONEGORO UNIVERSITY
FACULTY OF SCIENCE AND MATHEMATICS

CERTIFICATE

Decree of Dean Number : 1440/UN7.5.8/HK/2017

This is to certify that

Guruh Aryotejo

as

PRESENTER

In the 7th International Seminar on New Paradigm and Innovation of Natural Science and Its Application (ISNPINSA-7) held on 17 October 2017 at Grand Candi Hotel Semarang Indonesia

with paper entitled as follows:

Hybrid Cloud: Bridging of Private and Public Cloud Computing

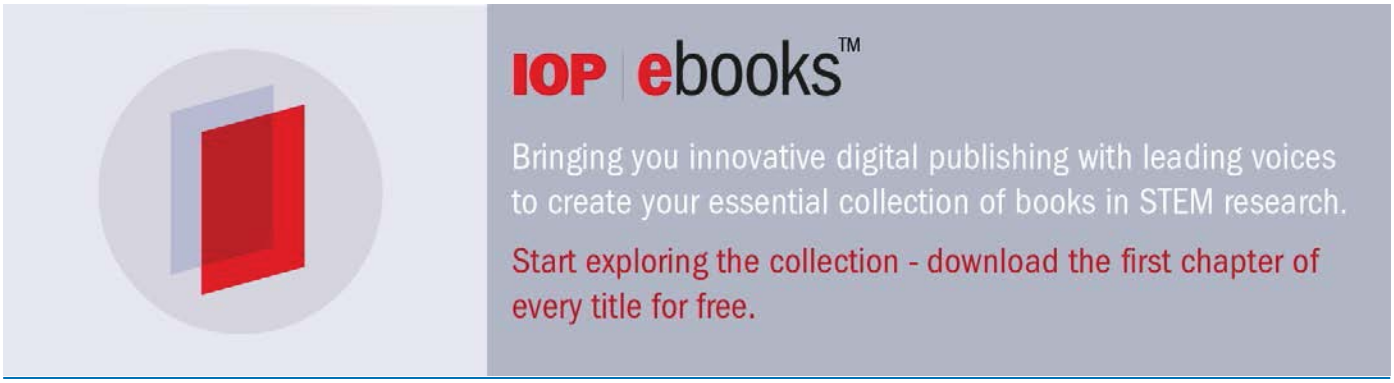
DEAN OF FSM UNDIP

Prof. Dr. Widowati, S.Si, M.Si.
NIP. 196902141994032002

7th ISNPINSA COMMITTEE, CHAIRMAN

Dr. Budi Warsito, S.Si, M.Si.
NIP. 19750824199903 1003

Hybrid cloud: bridging of private and public cloud computing



IOP Conf. Series: Journal of Physics: Conf. Series **1025** (2018) 012091 doi:10.1088/1742-6596/1025/1/012091

Hybrid cloud: bridging of private and public cloud computing

Guruh Aryotejo[1], **Daniel Y Kristiyanto**[2], **Mufadhol**[3]

[1]Information System of Sekolah Tinggi Elektronika dan Komputer, Majapahit 561, 50192, Semarang, Indonesia
[2]Computer Engineering of Sekolah Tinggi Elektronika dan Komputer, Majapahit 561, 50192, Semarang, Indonesia
[3]Information Technology of Sekolah Tinggi Elektronika dan Komputer, Majapahit 561, 50192, Semarang, Indonesia

Abstract. Cloud Computing is quickly emerging as a promising paradigm in the recent years especially for the business sector. In addition, through cloud service providers, cloud computing is widely used by Information Technology (IT) based startup company to grow their business. However, the level of most businesses awareness on data security issues is low, since some Cloud Service Provider (CSP) could decrypt their data. Hybrid Cloud Deployment Model (HCDM) has characteristic as open source, which is one of secure cloud computing model, thus HCDM may solve data security issues. The objective of this study is to design, deploy and evaluate a HCDM as Infrastructure as a Service (IaaS). In the implementation process, Metal as a Service (MAAS) engine was used as a base to build an actual server and node. Followed by installing the vsftpd application, which serves as FTP server. In comparison with HCDM, public cloud was adopted through public cloud interface. As a result, the design and deployment of HCDM was conducted successfully, instead of having good security, HCDM able to transfer data faster than public cloud significantly. To the best of our knowledge, Hybrid Cloud Deployment model is one of secure cloud computing model due to its characteristic as open source. Furthermore, this study will serve as a base for future studies about Hybrid Cloud Deployment model which may relevant for solving big security issues of IT-based startup companies especially in Indonesia.

Keyword: Cloud Computing, Hybrid Cloud, Data Center, start-up, MAAS, IaaS

1. Introduction

Progress in the field of Information Technology (IT) allowing the development of software or hardware occur in a relatively short time. Some start-up companies moving to the cloud computing business solution as it eliminates the need for planning ahead for provisioning, and allows companies to start from small resources and increase resources only when needed [1]. Most companies do not have the resources to build IT infrastructure [2], newly established companies, especially startups, tend to have no centralized way of storing and exchanging data, and also have no data flow (storage or exchange). These situations make data difficult to access and verify. The difficulties of data verification lead to unpredictable and potential disrupt the company's business processes [3].

The security of digital data is also one of the problems of startup in today's digital age. Most of startup founders in Indonesia do not have technical IT background. This causes negligence in maintaining data security. One of the studies claimed that computer networks were vulnerable to

attacks and proposed the idea of securing data when the network had been penetrated [4]. However, if the front door has been penetrated then it is only a matter of time to retrieve valuable goods.

Cloud Computing is considered as the future of computing, where software, hardware and network play a major role. The collective effort of the entity makes it possible to create Cloud Computing. HCDM, stands for Hybrid Cloud Model that is a combination of private cloud and internet, is created by using Open Source applications. The purpose of this study is to design, deploy and evaluate a *Hybrid Cloud Deployment Model* (HCDM), in which Infrastructure as a Service (IAAS) can apply it further. The establishment of HCDM is further expected to provide a valuable contribution to the strengthening of IT-based startup companies in Indonesia.

2. Theoretical Background

2.1. Cloud Computing

HCDM is one of cloud computing model, which is included combination of the use of computer technology in a network with the development of computer-based network or the Internet (cloud). It has a function to run applications through interconnected computer at the same time [5]. The way of cloud computing works is that users can access files, data, programs and services on an internet browser via the internet. Pay per use services and computing resources are the main advantage of cloud computing [6].

Cloud computing use three pieces of unification technology, namely Data Center, Virtualization and Utility/On-Demand Computing [7]. Data Center is the center of computing, storage and applications. Virtualization is a technology that enable an IT infrastructure to operate like some IT infrastructure, thus may minimize the organization's CapEx and OpEx [2-7]. Whereas, Utility Computing is a service delivery model that provides computing services according to customer needs, it attracts no cost at a fixed price but in accordance with its use [8].

There are four deployment models, such as Private, Public, Community and Hybrid Cloud. Some of the available Cloud Computing service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) [6-10], and even X as a Service (XaaS) where X can be any services [2]. In addition, the implementation of cloud computing on some companies have big security issues. Table 1 below reveals comparison of cloud computing based on deployment models [14][15].

Table 1. The comparison of cloud deployment model

Deployment models	Holder	Security	Scalability	Cost
Private Cloud	Single private organization	Higher than other deployment models	Limited	High
Community Cloud	Two or more private organizations with identical requirements	Lower than Private Cloud and higher than Public and Hybrid Cloud	Limited	medium
Public Cloud	Cloud Service Provider (CSP)	Lower than other deployment models	Very High	Pay-per-use
Hybrid Cloud	CSP and private organizations	Lower than Private and Community Cloud and higher than Public Cloud	High	Pay-per-use

Research community have made numerous studies related to cloud computing. Two studies about deployment method of Private Cloud have been conducted, the result revealed that deployment method of Private Cloud using Eucalyptus and OpenStack had been deployed successfully [17][18]. Our paper extend these results related to the security and performance issues of Private Cloud versus Public Cloud.

2.2. Cloud Computing Security

Nowadays, the data transfer trend outside of a controlled environment is one of big security issues. P. Rajendran, et al [10] has proposed and implemented intrusion detection system for private cloud using Microsoft Azure, which is a public cloud. The result shows those proposed model is less efficient when implemented properly in public cloud.

Data stored in the cloud should be secure, yet some studies reveal that there is always a way to bypass CSP security [11], some of cloud users had reported have security issues [12] and most businesses choose CSP to adopt Cloud Computing, which could decrypt their data [13]. Using hybrid cloud model (HCDM) through combining private cloud and internet may solve those security issues problems.

3. Result and Discussion

3.1. Design for HCDM Hardware setup

Hardware used in this study consist of 6 Acer Servers, TP-Link TL-SG1016D and a Mikrotik RB450G as mentioned in table 2. Each of the Acer server, except Acer VTM480G, used Intel Advanced Management Technology (AMT). AMT is able to control computers that are shutdown physically or has no operating system installed. These AMT interfaces act as a virtual interface on the first Ethernet interface, and configured in one of the Basic Input/Output System (BIOS) menus.

Table 2. Hardware specification for HCDM implementation

Hardware	Purpose	CPU Cores	RAM (GB)	HDD Quantity	HDD (GB)	Ethernet
Mikrotik RB450G	Router	1	-	-	-	5
TP-Link TL-SG1016D	Switch	-	-	-	-	12
Acer VTM480G	MaaS Region/Cluster Controller	4	4	1	250	2
Acer S6610G	MaaS Node 1	4	4	1	320	1
Acer S6610G	MaaS Node 2	4	2	1	360	1
Acer S680G	MaaS Cluster Controller	4	2	1	250	1
Acer S680G	MaaS Node 3	4	2	1	160	1
Acer S680G	MaaS Node 4	4	2	1	250	1

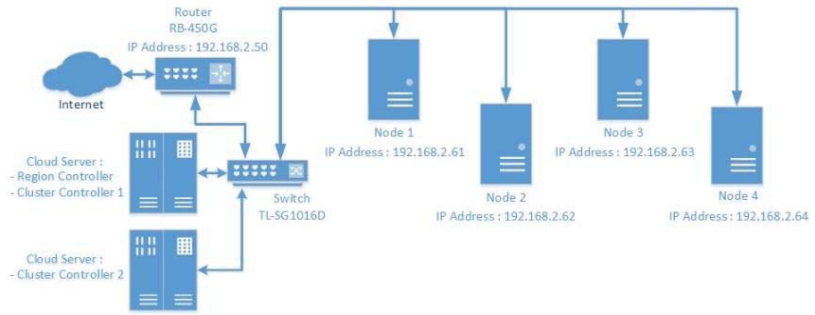


Figure 1. The logical topology that was applied for HCDM design

Figure 1 show the logical topology of this study, in order to enable communicate between hardware, Mikrotik and TP-Link are applied. Whereas, Cluster Controller 1 was applied as a main server.

3.2. Design for HCM/HCDM Software Setup

Software used in this study was Open Source software. There are three software installed, uBuntu, MAAS and JUJU. As a popular Debian-based Linux operating system, uBuntu was used as HCDM operating system. Due to capable of providing physical server automation for data centre operations, Metal as a Service (MAAS) was implemented as a server provisioning application of HCDM. MAAS task is to manage the machine, while JUJU manages the service running on the machine as shown in figure 2.

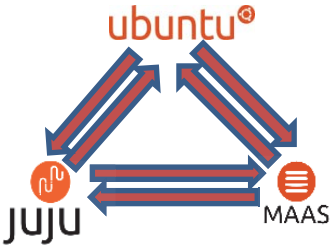


Figure 2. The implementation of uBuntu, JUJU and MAAS Software for HCDM software set up

The 14.04 LTS uBuntu Server version was installed on the Region/Cluster Controller 1 server. Followed by installing 1.9.4 MAAS version through typing *sudo apt-get install maas* and configuring user name and password by typing *sudo dpkg-reconfigure maas-region-controller* and *sudo dpkg-reconfigure maas-cluster-controller,* respectively.

The BIOS nodes must have configured correctly before the implementation begin. First, enable PXE boot on the first interface through the Integrated Peripherals menu. Second, completely disable any boot options from the hard drives, make sure that only the Network Boot selected. Third, In Advanced Chipset option, enable the Intel AMT. Fourth, during the Power On Self-Test (POST) process, press the shift-p key to enter the AMT menu and make sure the Dynamic Host Configuration Protocol (DHCP) option for network configuration is enabled.

According to the logical topology as shown in figure 1, the 5e Unshielded Twisted Pair (UTP) cable, connect between each hardware to internet main server. We accessed the MAAS configuration page through entering MaaS Region/Cluster Controller's IP address. After entering the username and password, MAAS will open the main page. Through visiting image menu on MAAS configuration page, the image was downloaded automatically, followed by enabling DHCP server on Clusters page.

MAAS must register a node to provision a server. Registration process have two stages, namely enlistment and commission. Enlistment begins by turning on nodes one at a time and it will boot through Preboot Execution Environment (PXE). Region Controller automatically receive the hardware information about the node, such as the architecture and MAC address, and store it to the database. MAAS configuration page will display successfully registered node, followed by manually selected the node to enter the commission stage.

The final step was installing the application to verify whether the MAAS was working properly or not. First, we installed JUJU, which is responsible for coordinating the applications within the MAAS, through typing *sudo apt-get install juju-core juju-quickstart juju-deployer* and use *sudo juju bootstrap* to bootstrap it. We evaluated MAAS using vsftpd through typing *sudo juju deploy vsftpd*

3.3. HCDM as Cloud Computing with IaaS

Based on this research result, revealed that the HCDM has a key role as a server provisioning system that simplify local-based cloud computing application via online. Regarding to Figure 3 and 4 reveals that HCDM as cloud computing acted as private cloud, consists of two (2) modules, Region Controller and Cluster Controller, connected to the internet. Region Controller is responsible for looking after node and user management, network communications and interaction between different Clusters Controller. On the other hand, Cluster Controller is to oversee nodes, deploy the operating systems and manage the images and power states. Region Controller can have more than one Cluster Controller.

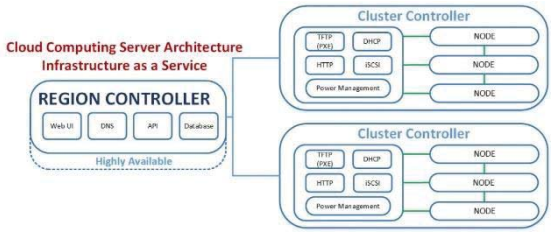


Figure 3. The design of Private Cloud Model

Figure 4. The design of Hybrid Cloud Deployment Model

The Region Controller was included various sub-applications, such as Web UI, Domain Name System (DNS), Application Programming Interface (API) and Database. Web UI is a web-based self-service portal to interact with underlying MaaS Engine. At the region controller, the DNS task forward internet request from Cluster Controller to forwarder. The API control and query the MaaS Engine using HTTP request. Whereas, the database task track availability of node and MaaS engine status.

In order to evaluate the security of HCDM, preliminary of security access was performed, the client was facilitated a connection to HCDM and Public Cloud, followed by connection analysis. As shown in figure 5, HCDM was used Secure Shell (SSH) as a protocol, connections occurred to HCDM were within Private IP Address range. Whereas, Public Cloud used Quick UDP Internet Connections (QUIC) as a protocol, connections occurred were within Public IP Address (Figure 6). Moreover, SSH was used 128-bit encryption, and the connection characteristic of client to HCDM used Private IP Address. The result shows HCDM have a more secure connection than Public Cloud. This result is in line with S.R.M.Krishna *et al.* (2011) research result revealed that the SSH protocol provides the safeguard such as the client transmits its authentication information to the server using 128-bit encryption. [16]

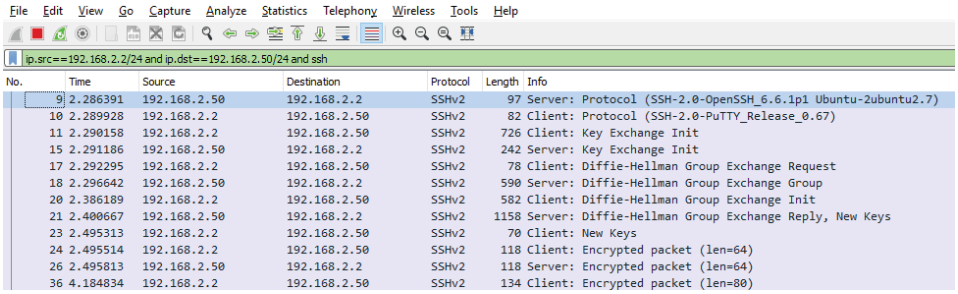


Figure 5. The security simulation result of client to HCDM

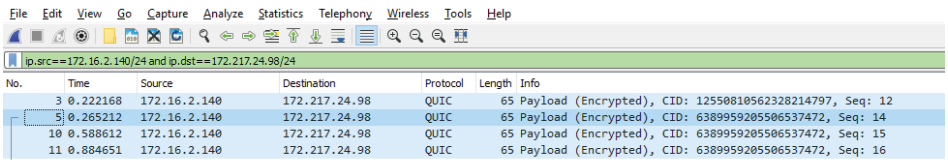


Figure 6. The security simulation result of client to Public Cloud.

Furthermore, to analyse the performance of HCDM, the simulation on data transfer speed was conducted. In condition of low usage internet traffic, the client data was uploaded into HCDM and Public Cloud, based on figure 7(a) and 7(b) show that HCDM had a speed of 11,453 KB/s, and Public Cloud had a speed of 106 KB/sec. This indicate that HCDM is 100 times faster than Public Cloud in

term of data transfer speed. According to our research results, HCDM have two advantages, it is more secure and able to transfer data faster than public cloud.

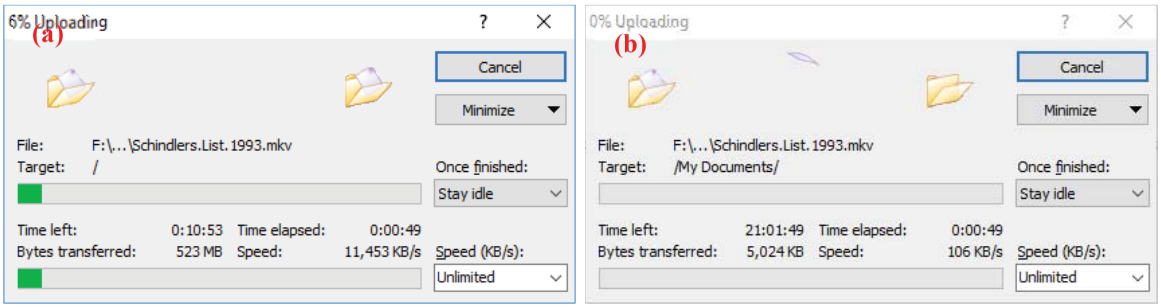


Figure 7. The transfer speed simulation result of client to HCDM (a), and client to Public Cloud (b)

Cloud Computing advantages are the resources, such as data, picture, video and application deployed on remote servers, that can be accessed and utilized anytime and anywhere. While the disadvantages of cloud computing tend to overlook the security aspect due to have not enough information about it. The combination of private cloud and internet, to become HCDM, could mitigate this disadvantage and will optimally improve the cloud computing security. In our future study, it might be possible to further applied HCDM for IaaS.

4. Conclusion

In this study, the design and deployment of HCDM were conducted successfully. In order to evaluate HCDM, we have performed preliminary of security and data transfer speed analysis. In comparison with Public Cloud, that have a QUIC Protocol and is within Public IP Address range, we found that HCDM have a SSH protocol and is within Private IP Address range, it could be concluded HCDM has more secure connection. Furthermore, we analyze data transfer speed between client to HCDM and client to public cloud. Notably, HCDM is able to perform data transfer speed of 100 times higher than public cloud. To the best of our knowledge, this finding enhance our knowledge of cloud computing. It may serve as a base for future studies about Hybrid Cloud Deployment model which may relevant for solving big security issues of IT-based startup companies especially in Indonesia.

Acknowledgement

The authors would like to acknowledge to DRPM-DIKTI for their financial support for this research through RDP scheme in 2017.

References

[1] Avram M G 2014 Advantages and challenges of adopting cloud computing from an enterprise Perspective. *Procedia Tech.* **12** 529-534. doi: 10.1016/j.protcy.2013.12.525
[2] Dhar S 2012 From outsourcing to Cloud computing: evolution of IT services. Manag. Resea. Review **35** (8) 664–675. https://doi.org/10.1108/01409171211247677
[3] Lueg R, Malinauskaite L and Marinova I 2014 The vital role of business processes for a business model: the case of a startup company *Probl. Perspect. Manag* **12** 213–220
[4] Khlaif M, Talb M 2013 Digital Data Security and Copyright Protection Using Cellular Automata *Internat. Journ. of Comp. Scien. and Netw* **2** (3) 1–4
[5] Hurwitz J, Bloor R, Kaufman M, and Halper F 2010 *Cloud Computing for Dummies* (Wiley Publishing, Inc., Indianapolis, Indiana)
[6] Jadeja Y, Modi K 2012 Cloud Computing - Concepts, Architecture and Challenges *Inter. Conf. on Comp., Elect. and Electri. Tech.* 877-880 https://doi.org/10.1109/ICCEET.2012.6203873
[7] Chandrasekaran K 2015 *Essentials of Cloud Computing* (CRC Press Taylor & Francis Group)
[8] Anand H S, Kamayani 2015 scope of cloud computing in education sector : a review **2** 150–152

[9] Du Z, He L, Chen Y, Xiao Y, Gao P, and Wang T 2017 Robot Cloud: Bridging the power of robotics and cloud computing *Futur. Gener. Comput. Syst.*, **74**, 337–348
[10] Rajendran P K, Muthukumar B and Nagarajan G 2015 Hybrid intrusion detection system for private cloud: A systematic approach *Procedia Comput. Sci.* **48** 325–329
[11] Padhy R, Patra M, and Satapathy S 2011 Cloud Computing: Security Issues and Research Challenges *Inte. Jour. of Comp. Scie. and Info. Techn. & Secu.* **1** 136–146
[12] Tomison A, Hutchings A, Smith R G and James L 2013 Cloud computing for small business: Criminal and security threats and prevention measures *Tren. & issu. in crim. and crim. just.* **456** 1-8
[13] Azeem A and Sprott C R 2012 Let me in the cloud: analysis of the benefit and risk assessment of cloud platform *J. Financ. Crime* **20** 6–24
[14] Venkat T, Rao N, Naveena K, David R, and Narayana M 2015, A New Computing Environment Using Hybrid Cloud *Jour. of Info. Scie. and Comp. Tech.* **3** 180-185
[15] Goyal S 2014 Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review *Inter. Journ. of Comp. Netw. and Info. Secur.* **6** **2**0-29 Doi: 10.5815/ijcnis.2014.03.03
[16] Krishna S R M, Paradeep S J, Priya K P, Vishnu P H 2011 Enhancing the Communication Channel Through Secure Shell And Irrational DES *Inter. Journ. of Comp. Scie. and Engi.* **3** 1020-1027
[17] Mirajkar N, Barde M, Kamble, Harshal A, Rahul S and Kumud 2012 Implementation of private cloud using eucalyptus and an open source operating system *Inter. Jour. of Comp. Scie.Issu.* **9** 360-364
[18] Islam S, Husain A, Zaki H M 2017 Pooling of Computing Resources in Private Cloud Deployment *Inter. Jour. of Engin. Resea. in Comp. Scien. and Engin.* **4** 92-98