Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 10, October-2022

Hybrid Cloud Computing: A Perspective

Amit Kumar Jain
Computer Science
Delhi University, Delhi, India

***Abstract*— In recent years, cloud computing has quickly emerged as a promising paradigm, particularly for the commercial world. Additionally, cloud computing is commonly used by startup companies in information technology (IT) to expand their businesses through cloud service providers. However, because some Cloud Service Providers (CSP) could decrypt customer data, the majority of enterprises have low levels of awareness regarding data security risks. Because the Hybrid Cloud Deployment Model (HCDM) is open source and one of the secure cloud computing models, it may be able to address data security challenges. Designing, deploying, and evaluating an HCDM as Infrastructure as a Service is the goal of this project (IaaS). A real server and node were constructed during the implementation phase using the Metal as a Service (MAAS) engine as a foundation. The vsftpd application, which acts as an FTP server, is then installed after that. Public cloud adoption occurred via public cloud interface as opposed to HCDM. As a result, the design and deployment of HCDM went smoothly. In addition to having high security, HCDM was able to transfer data substantially faster than public clouds. To the best of our knowledge, the open source nature of the hybrid cloud deployment strategy makes it one of the most secure cloud computing models. Additionally, this work will provide as a foundation for subsequent research on the hybrid cloud deployment strategy, which may be important for resolving significant security challenges.**

Keywords—Cloud computing, Hybrid Cloud Architecture

I. INTRODUCTION

The development of software or hardware is now possible in a relatively short amount of time because to advancements in information technology (IT). Some startup businesses are switching to the cloud computing business model because it eliminates the need for provisioning planning in advance and enables them to start with little resources and add more as needed [1]. Most businesses lack the funds necessary to invest in IT infrastructure [2], and newly founded businesses, particularly startups, frequently lack a centralized method of data storage and exchange as well as any kind of data flow. These circumstances make it challenging to access and validate data. The challenges of data verification result in unpredictability and the potential for business operations to be disrupted [3].

One of the difficulties facing startups in the current digital era is the protection of digital data. The majority of Indonesian company founders lack technical IT backgrounds. As a result, data security is not maintained properly. One study asserted that computer networks were attack-prone and suggested safeguarding data once the network had been breached [4]. However, if the front door has been broken into, it will only take a short while to recover valuables. The future of computing is thought to lie in cloud computing, where hardware, software, and networks all play significant roles. The ability to construct cloud computing is made feasible by the entity's combined efforts. HCDM, which stands for Hybrid Cloud Model and combines the internet and private clouds, is made possible by leveraging open source software. This study's goal is to develop, test, and further use a hybrid cloud deployment model (HCDM) so that infrastructure as a service (IAAS) can use it.

II. BACKGROUND

A. Cloud Computing

The HCDM model of cloud computing combines the usage of computer technology in a network with the growth of computer-based networks, such as the Internet (cloud). It provides the ability to simultaneously run apps on several connected computers [5]. Users can access files, data, programs, and services on an internet browser via the internet thanks to cloud computing. The primary benefit of cloud computing is pay-per-use services and computing resources [6].

Data centers, virtualization, and utility/on-demand computing are the three technologies that make up cloud computing [7]. The hub of computers, storage, and applications is the data center. Technology known as virtualization allows an organization's CapEx and OpEx to be reduced by making one IT infrastructure behave like another IT infrastructure [2–7]. Utility Computing, on the other hand, is a method of service delivery that offers computing services in accordance with consumer needs without charging a fixed fee but rather according to usage [8].

There are four types of cloud deployment models: private, public, community, and hybrid. 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 service, are some of the Cloud Computing service models that are now accessible. Additionally, there are significant security concerns with certain businesses' adoption of cloud computing. The comparison of cloud computing based on deployment models is shown in Table 1 below [14][15].

TABLE I. 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	Lower than Private Cloud and higher than Public and	Limited	Medium

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 10, October-2022

	requirements	Hybrid Cloud		
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

Numerous studies of cloud computing have been conducted by the research community. Two studies on private cloud deployment techniques were undertaken, and the findings showed that Eucalyptus and OpenStack were successful in deploying private cloud techniques [17][18]. These findings about the performance and security differences between private and public clouds are expanded in our study.

B. Cloud Computing Security

One of the major security concerns of the present is the tendency of data transfer outside of a regulated environment. Using the public cloud Microsoft Azure, P. Rajendran, et al. [10] have developed and deployed an intrusion detection system for private clouds. The outcome demonstrates that when correctly applied in public clouds, the proposed models are less efficient.

Although studies show that there is always a way to get around CSP security [11], some cloud users have reported having security difficulties [12], and most businesses pick CSP to adopt cloud computing, which might decrypt their data [13], data kept in the cloud is supposed to be secure. Using the hybrid cloud model (HCDM), which combines the private cloud and the internet, may be able to address such security concerns.

III. RESULT AND DISCUSSION

A. Design for HCDM Hardware setup

In this study, hardware such as six Acer servers, a TP-Link TL-SG1016D, and a Mikrotik RB450G were employed. All Acer servers used Intel Advanced Management Technology, with the exception of Acer VTM480G. (AMT). Computers with no operating system installed or that have been physically shut down can be controlled via AMT. These AMT interfaces are set up in one of the Basic Input/Output System (BIOS) menus and function as a virtual interface on the first Ethernet interface.

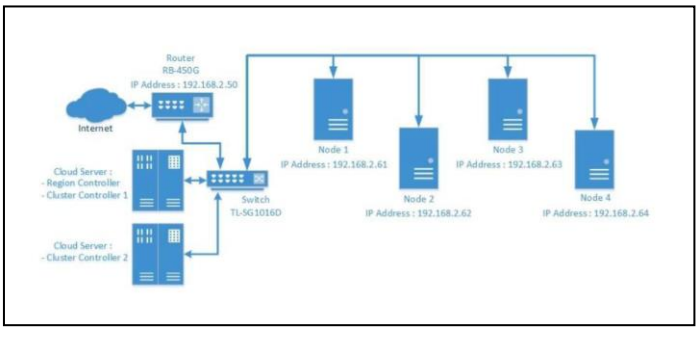

Fig. 1. The logical topology that was applied for HCDM design

Figure 1 depicts the study's logical topology. Mikrotik and TP-Link are used to facilitate hardware communication. While Cluster Controller 1 served as the primary server.

B. Design for HCM/HCDM Software Setup

Open Source software was used in this study. Three programs have been set up: uBuntu, MAAS, and JUJU. uBuntu was picked as the HCDM operating system since it is a well-liked Debian-based Linux operating system. Metal as a Service (MAAS) was implemented as a server provisioning application of HCDM due to its ability to provide physical server automation for data center operations. While JUJU manages the service that is running on the machine, MAAS manages the machine.

The Region/Cluster Controller 1 server has uBuntu 14.04 LTS installed on it. Then type sudo apt-get install maas to install the 1.9.4 MAAS version, and sudo dpkg-reconfigure maas-region-controller and sudo dpkgreconfigure maas-cluster-controller to set the user name and password. Before the implementation can start, the BIOS nodes must be correctly configured. The first step is to use the Integrated Peripherals option to allow PXE boot on the first interface. Second, make sure that just Network Boot is selected and deactivate all hard disk boot options completely. Third, turn on Intel AMT in the Advanced Chipset option. Fourth, verify that the Dynamic Host Configuration Protocol (DHCP) option for network configuration is active in the AMT menu by entering it with the shift-p key while the Power On Self-Test (POST) process is running.

In accordance with the logical topology, 5e Unshielded Twisted Pair (UTP) cables connect each piece of hardware to the Internet's primary server. We entered the MAAS configuration page by providing the IP address of the MaaS Region/Cluster Controller. After inputting the login and password, the MAAS homepage will load. The image was automatically downloaded after visiting the image menu on the MAAS configuration page and enabling the DHCP server on the Clusters page. MAAS must register a node for server provisioning. The registration procedure consists of two phases: enrollment and commissioning. Enlistment commences with the activation of individual nodes via Preboot Execution Environment (PXE). Region Controller immediately receives and stores the node's hardware information, such as its architecture and MAC address, in the database. The MAAS configuration page will indicate a successfully registered node, followed by the option to manually choose the node for commissioning. Installing the program to test whether the MAAS was functioning properly was the final step.

C. HCDM as Cloud Computing with IaaS

According to the findings of this study, HCDM plays a crucial role as a server provisioning system that simplifies the online deployment of local cloud computing applications. Regarding Figures 3 and 4, it can be seen that HCDM as cloud computing acted as a private cloud, consisting of two (2) internet-connected modules, Region Controller and Cluster Controller. The Region Controller is responsible for node and user management, network communications, and inter-Clusters Controller interface. Cluster Controller, on the other

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 10, October-2022

hand, is responsible for monitoring nodes, deploying operating systems, and managing images and power states. Multiple Cluster Controllers can be assigned to a Region Controller.

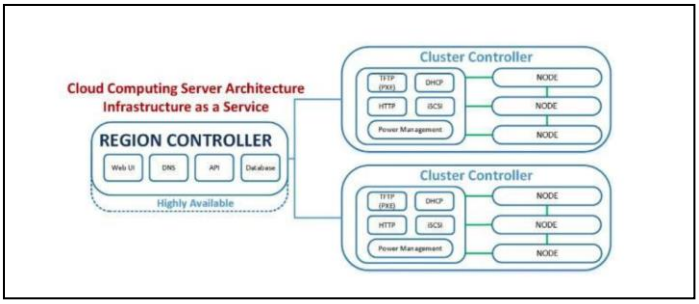

Fig. 2. The design of Private Cloud Model

Fig. 3. The design of Hybrid Cloud Deployment Model

Several sub-applications, including Web UI, Domain Name System (DNS), Application Programming Interface (API), and Database, were included into the Region Controller. Web UI is a web-based gateway for self-service interactions with MaaS Engine. The DNS task at the region controller forwards internet requests from the Cluster Controller to the forwarder. The API queries and controls the MaaS Engine via HTTP requests. While the database task monitors node availability and MaaS engine status.

In addition, in order to evaluate the performance of HCDM, a simulation of the data transmission rate was done. Client data was uploaded into HCDM and Public Cloud under conditions of minimal internet traffic; tests revealed that HCDM had a speed of 11,453 KB/s and Public Cloud had a speed of 106 KB/sec. This indicates that, in terms of data transfer speed, HCDM is one hundred times quicker than Public Cloud. HCDM has two advantages, according to our research: it is more secure and can transfer data faster than public cloud.

The benefits of cloud computing include the resources, such as data, images, videos, and applications, that can be accessed and exploited at any time and place. While the downsides of cloud computing tend to neglect the security component due to a lack of knowledge about it, cloud computing's security is a major concern. This disadvantage could be mitigated by the integration of private cloud and internet to form HCDM, which will maximally increase cloud computing security. In our future research, it may be able to apply HCDM further to IaaS.

IV. CONCLUSION

The design and implementation of HCDM were carried out satisfactorily in this study. In order to evaluate HCDM, preliminary security and data transfer speed analyses have been conducted. Compared to Public Cloud, which has a QUIC Protocol and is within the Public IP Address range, we discovered that HCDM has an SSH protocol and is within the Private IP Address range; hence, HCDM provides a more secure connection. In addition, we examine the data transfer speed between the client and HCDM and the client and the public cloud. Notably, HCDM is capable of 100 times faster data transfer speeds than public cloud. This finding, to the best of our knowledge, expands our understanding of cloud computing. It may serve as a foundation for future research on the Hybrid Cloud Deployment approach, which may be applicable to resolving significant IT startup security challenges.

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
[6] Publishing, Inc., Indianapolis, Indiana)
[7] 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
[8] Chandrasekaran K 2015 Essentials of Cloud Computing (CRC Press Taylor & Francis Group) 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 20-29 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. 31020-1027
[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