ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 3; Issue 1; Page No. 28-33

Hybrid Cloud Computing: Overview and its Challenges

*[1]Swati Pawar, [2]Akshita Sharma, [3]Puja Kumari

[1,2,3] M. Tech. Scholar, Department of Computer Science and Engineering, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India

ABSTRACT
Cloud Computing has taken the IT industry by storm over the past few years. It promises to provide a flexible IT architecture, accessible through internet from lightweight portable devices. It offers users a scalable, elastic, and cost-effective computing environment. It is important for an organization that begins to use cloud services to consider which type of cloud service best meets their business requirements. In order to build and deploy applications more quickly, more cost effectively and with more control, hybrid cloud environment delivers the ultimate choice, flexibility and speed. It provides virtual IT solutions through a mix of both public and private clouds. This paper discusses the concept of Hybrid cloud computing and its issues and security challenges. It also discusses some tips for tackling these issues and problems.

Key words: Cloud Computing, Hybrid Cloud, Security issues

INTRODUCTION:

Cloud computing is a computing paradigm that allow centralized data storage and provides on-demand access to a shared pool of computing resources over the Internet [3]. Gartner defines cloud computing as ''a style of computing where massively scalable IT- enabled capabilities are delivered 'as a service' to external customers using Internet technologies'' [1]. The cloud services are location independent and cost effective. The customers can access the resources from anywhere and pay only for the amount they use. The cloud offers several benefits like pay-for-use, improved performance, lower IT infrastructure costs, fewer maintenance issues, instant software updates, unlimited storage capacity, increased computing power and real time detection of system tampering. The main advantage for the cloud users is the reduction of infrastructure costs and its maintenance.

Many Small and Medium Business companies are adopting cloud services at a rapid pace. Big worldwide companies such as Google, IBM, Microsoft, Amazon etc. also adopted the Cloud Computing. According to the recent IDC cloud research, "worldwide spending on public IT cloud services is expected to be more than $107 billion in 2017" [2].

One of the important decisions for enterprises is to choose an appropriate cloud deployment model. They can choose to deploy applications on Public, Private or Hybrid clouds. A Public cloud is a type of deployment model in which service provider delivers resources like applications, storage and infrastructure to the customers, on-demand, and with payment based on usage. Although the public cloud services are cost-effective, they are not considered as secure as private clouds. Private cloud provides greater levels of operational control and transparency than public cloud. But they are also costly because the enterprise will have to purchase/rent and maintain all the necessary software and hardware. Today many companies started using a mix of these clouds to gain the maximum advantage of both which is also referred to as a Hybrid Cloud.

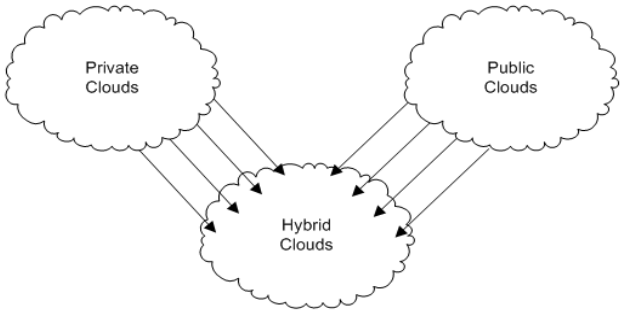

Figure 1: Hybrid Clouds

While a hybrid approach promises flexibility and control, there are many challenges such as security and application portability. The rest of the paper is organized as follows. In Section 2, we provide an overview on the different service models being used and cloud architectures which can be deployed according to the enterprise requirements. Section 3 presents the overview and benefits of hybrid cloud computing. Section 4 presents the challenges involved while deploying hybrid

cloud architecture for enterprise needs, Section 5 describes the solutions which help in enterprises to operate efficiently and securely in hybrid environment. We conclude and give future work in Section 6.

1. BACKGROUND

Although there are many benefits of using cloud computing, there are many factors to take into account when deciding which is right for your business. It is the responsibility of the enterprises to analyze each service models and deployment models. In this section, we provide an overview study of all the models used in cloud.

1.1. Service Models

There are three service models in cloud computing by which different types of services are delivered to the end user.

1.1.1. Infrastructure-as-a-Service (IaaS)

It provides the infrastructure (computing platform), resources and tools (servers, storage, network, etc.) to build an application environment. It is the responsibility of the cloud provider to tackle the issues of IT infrastructure management such as installing, configuring servers, routers, firewalls and other devices. Virtualization techniques are used in this model. Physical resources are abstracted by virtualization, which means they can be shared by several operating systems and end user environments. Instead of purchasing, housing, and managing the basic hardware and software infrastructure components, users can obtain those resources as virtualized objects controllable via a service interface. VMWare, Amazon EC2, IBM Blue House, Microsoft Azure, Sun Para Scale Cloud Storage, etc. are some of the infrastructure services.

1.1.2. Platform-as-a-Service (PaaS)

This model is mainly used by developers who want to develop and run a cloud application for a particular platform. It facilitates the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers [4]. It provides platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services. Google Apps is one of the major PaaS providers.

1.1.3. Software-as-a-Service (SaaS)

It provides the computing platform and applications to customers for use. One benefit of this model is customers do not need to buy any software licenses or any additional equipment for hosting the application. Instead, they pay for using the software application [5]. Some examples are Facebook, Twitter, and various web-based email systems such as those offered by Google.

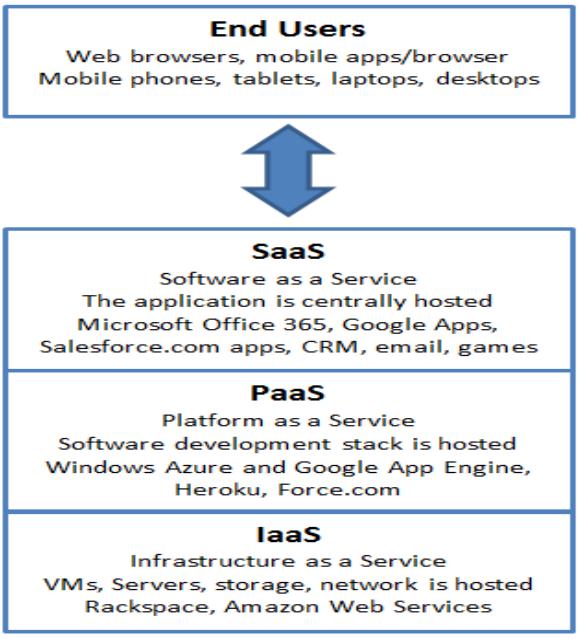

Figure 2: Service Models

1.2. Cloud Deployment Models

There are four types of cloud deployment models that are used for different services according to the enterprise requirements.It is essential to examine your current IT infrastructure, usage and needs to determine which type of cloud computing can help you best achieve your goals.

1.2.1. *Public Cloud*

In this model, the service provider provides resources like infrastructure, applications and storage, available to the customers or large organization over the internet [1]. These services can be offered for free such as Gmail or on a pay-per-usage model. The customer has no visibility and control over where the cloud services are being hosted. This is the most cost effective model but there are many security issues in this model. Examples of public clouds include Google App Engine, Amazon Elastic Compute Cloud (EC2) and Windows Azure Services Platform.

1.2.2. *Private Cloud*

In this model, the resources (applications and storage) are only accessible by a single organization. But it is more costly than public cloud services because we need to buy, build and manage them. A private cloud is suitable for organizations that have certain security and performance monitoring tools that the public cloud provider doesn't use. Private cloud services use a private network to restrict access to information, providing greater control and security.

1.2.3. *Hybrid Cloud*

Hybrid cloud refers to a combination of two or more clouds (private, community, or public). It is usually a

combination of on-and off-premise where some data resides in the private cloud environment and some resides in the public cloud environment. It gives more secure control over the data and also other parties to access data. One of the disadvantages of these services is that we have to manage different security platforms together.

1.2.4. *Community Cloud*

In this model infrastructure is shared between several organizations which have common requirements (security, compliance, jurisdiction, etc.) from a specific community [11]. Community clouds can be either on-premise or off-premise. Since all data is housed at one location, one must be careful in storing data in community cloud because it might be accessible by others.

2. HYBRID CLOUD COMPUTING

Many IT companies discover that public cloud computing does not meet security requirements. They prefer to store sensitive data on their own private servers. Private cloud provides more security and better performance, but it is not cost efficient. Therefore, a mix of these clouds can be used to gain maximum advantages of both these clouds.A hybrid cloud allows companies to use public cloud for non-sensitive operations, reducing storage and maintenance costs while using a private network for sensitive or mission-critical operations to maximize security. Hybrid cloud offers security along with agility, cost savings, high availability of services and scalability. Microsoft is now offering the hybrid cloud infrastructure to many of its clients. According to Frank Gens, an IDC chief analyst, "Virtually every customer, at least from the midmarket up, will have a mix of both [Public and Private Clouds]."

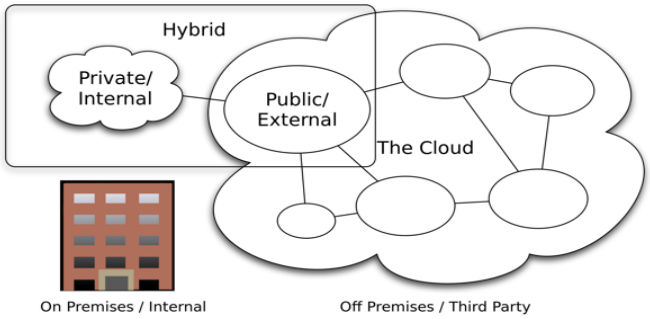

Figure 3: Hybrid cloud [6]

According to Research and Market's "Global Hybrid Cloud Market 2014 - 2018" findings, the global hybrid cloud market is expected to grow at a five year compound annual growth rate of 30% from 2014 to 2018 [7]. One of the key drivers for hybrid cloud adoption was the need for companies to reduce IT spending. Enterprises are charged on a per-use basis which is more economical for them.

3.1 Avanade Survey results

Avanade's recent global study "Hybrid Cloud: From Hype to Reality," of 1,000 C-level executives, business unit leaders and IT decision-makers, shows that businesses of all sizes, in all geographies, claim interest in adoption of hybrid cloud [8]. About 69 percent of respondents believing that it should be one of the biggest areas of focus for their company in 2015.

Some of the key results are:

- Most businesses are investing in hybrid cloud at a faster rate than private or public clouds. Companies have strong interest in, and adoption plans for, hybrid cloud in the next one to three years.
- There are many challenges involved in the hybrid cloud including security concerns, costs and skills needed to implement.
- While many businesses are prioritizing hybrid cloud adoption, some are confused about what exactly hybrid cloudmeans. More than half (55 percent) of C-level executives, business unit leaders and IT decision-makers were unable to identify all the basic attributes of hybrid cloud.
- Security and privacy concerns are the biggest barriers to adoption and implementation of cloud solutions today. More than half (53 percent) of respondents see security as a barrier to implementation of hybrid cloud.
- About 39 percent respondents indicate that customization and flexibility were advantages of hybrid cloud over public-only cloud. Improved security (38 percent) and improved user experience (29 percent) were also acknowledged as significant advantages of hybrid cloud over public-only models.

3.2 Benefits of Hybrid Cloud Computing

There are many benefits of deploying hybrid cloud model. Some of the key benefits are:

3.2.1 The ability to leverage both private and public cloud

Companies are able to leverage the best of what both have to offer by intermixing private and public cloud infrastructures, making a more flexible IT environment. A hybrid model allows businesses to rely on the cost-effective public cloud for non-sensitive operations and on the private cloud for sensitive and critical operations.

3.2.2 Optimized costs

One of the main benefits of the hybrid cloud is reduced costs. With this model companies can enjoy seamless

scaling by allocating resources for immediate projects at a much lower cost. In addition, it includes a pay-for-your-payment feature as part of its public cloud services.

3.2.3 Enhanced agility

Hybrid cloud provides companies enhanced agility to move seamlessly between the two model, rather than being pigeonholed into one model or the other. It has emerged as a new, powerful, more disruptive and economical way of delivering IT services than the traditional premise-bound, hardware bound model.

3.2.4 Enhanced security

One of the main concerns of a public cloud is data integrity and security. Hybrid clouds offer extra security to your data. Enterprises have the privilege of storing their valuable data within their internal network and migrate unimportant data to cloud.

3.2.5 Improved performance and scalability

By employing a hybrid cloud model, an enterprise can quickly deploy new applications and add resources as needed by bursting out of the private enterprise to a public cloud processing and storage capacity. Flexibility to respond quickly to business needs is the key benefits associated with a hybrid model.

4. CHALLENGES IN HYBRID CLOUD

Today many organizations started using hybrid cloud computing to get benefits offered by both private and public clouds – agility, cost efficiencies, and high availability of services. By integrating the public cloud with the private cloud, businesses get the flexibility to isolate sensitive data while still benefiting from the many advantages offered by the cloud. To many organizations, allowing information to be transported across a network that can be subject to third-party interference is an unnecessary and reckless security risk. Protecting the data and monitoring its access permission is very important. According to Avanade's recent global study "Hybrid Cloud: From Hype to Reality," 53 percent of companies identified security and privacy issues as the top concerns to hybrid cloud implementation [8]. Also a commissioned study is conducted by Forrester Consulting on behalf of Juniper Networks in January 2014 [12]. In this survey half of respondents (50 percent) stated that network security when connecting to cloud services has the biggest impact on creating a hybrid cloud, followed by network bandwidth (42 percent), network performance (42 percent), and network reliability (39 percent). Let us examine the key challenges that appear while deploying hybrid cloud in enterprises.

4.1. Security challenges

Secure communication and data sharing between two environments is one of the biggest concerns for IT and business leaders in moving to a hybrid cloud model. The three key areas of concern related to security and privacy of data in the hybrid cloud are

- ✓ Location of data
- ✓ Control of data
- ✓ Secure transport of data

The confidentiality of a company's data will be violated as the data present in the cloud can be leaked or tampered, intentionally or accidentally. The tiniest of holes in the security are unacceptable because it could result in vulnerabilities for all subscribers. Many enterprises refuse to commit to it because they trust existing internal security measures over the ones employed by cloud service providers. Ensuring the consistency of security policies between the on-premises environment and the service provider is also a significant challenge/barrier for enterprises.

4.2. Issue of money

Organizations that have a small IT budget probably can't afford a rollout of a hybrid cloud solution. The upfront cost of the servers on the private end of the spectrum is very costly and the needs of smaller businesses can likely be served adequately using the services of a public cloud provider. Therefore they prefer public cloud over hybrid cloud.

4.3. Reprogramming and Adjustments

Many issues are generated due to migration of components from on-site to the public cloud. Before migrating, many factors must be taken into account such as enterprise policies and cost savings from migration. The enterprise also have to create firewall within the cloud and at the gateway of its own network. Current enterprises firewalls does not provide a good solution because firewalls rules should be modified for each trivial update in enterprises. The potential need for re-architecting applications to operate in the shared environment is also a major concern.

4.4. Seamless integration between the data center and public cloud provider

Creating seamless integration between the data center and public cloud provider is one of the major considerations while adopting a hybrid cloud model, so that the virtual machines can be moved on demand between sites. While migrating resources of an enterprise to the hybrid clouds the complexity of software and configuration increases, due to separation of resources into multiple clouds. It is difficult to manage and integrate on-premises infrastructure with cloud services. The enterprises have to manage the communication link between both sites during delivery of IT infrastructure from cloud to the data center. The public cloud services

are generally at remote locations so there are also latency and bandwidth related issues associated with any remote application.

5. SOLUTIONS

5.1. Choosing the right public cloud provider

Choosing the right public cloud provider is essential before deploying hybrid cloud in the enterprise. The organization must ask about the technology they use in their data centers and how they handle replication, backup and disaster recovery.

5.2. Using Virtual Private Network (VPN) tunnel

A Virtual Private Network (VPN) create a secure network connection across a public network through the use of encryption. In order to achieve high security the enterprises create their own virtual private cloud within the public environment and connect it to their private environment through VPN.

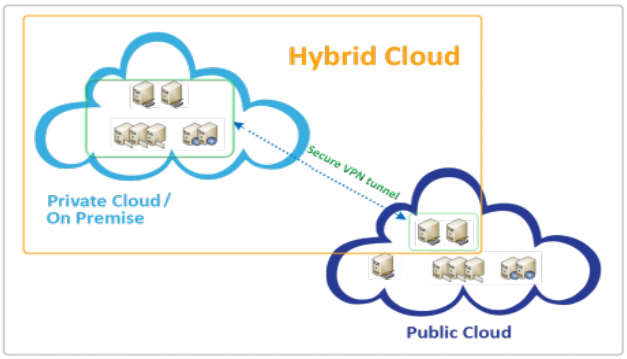

Figure 4: A secure VPN tunnel in Hybrid cloud

For VPN connections, the principle of tunneling is employed. In tunneling, a secure point-to-point connection, a tunnel, is created through which the data transfers. VPN security depends on security of both the company's private network and the public cloud. The key building blocks for providing VPN security are:

- ✓ Firewalls
- ✓ Encryption

A firewall act as a strong barrier between any private network and the public Internet. The remote user will establish an authenticated connection with the firewall. Firewalls are used to restrict what type of packets can passed through and which protocols are allowed through. Encryption is also an important component of a secure VPN. In encryption, all the data sent from one computer are encrypted in such a way that only the computer it is sending to can decrypt the data. Two types of encryption are commonly used. One is public-key encryption in which a system uses two keys, a public key which is known to everyone and a private key which is known only to the recipient of the message. Second is symmetric-key encryption system in which the sender and receiver both share a single, common key that is used to encrypt and decrypt the message.

Most of the third party companies like Amazon, Citrix etc. have provided security solutions based on VPN [10].

5.2.1. Citrix Open Cloud Bridge

Citrix Open Cloud Bridge solution provides transparent network and establish secure and optimized bridges to public cloud services such as Amazon Web Services and Microsoft Windows Azure as well as to their own datacenters and branches [9]. Open Cloud Bridge eliminates the need to modify network, changing the security and access configurations because it makes the service provider environment and enterprises to appear as a single network. Open Cloud Bridge securely extends the enterprise demilitarized zone (DMZ) into the cloud. Cloud Bridge merges WAN optimization and in-depth application visibility in a unified platform that delivers maximum functionality.

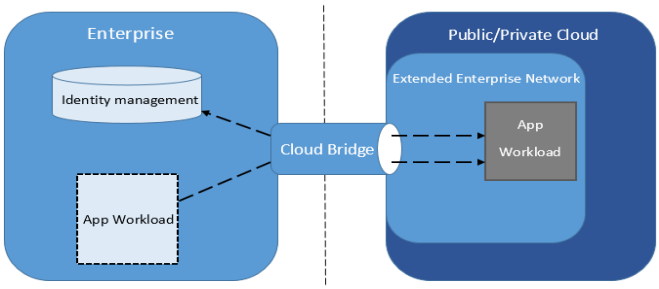

Figure 5: Citrix Cloud Bridge

5.3. AAA Servers

An AAA (authentication, authorization and accounting) servers is a sever program that handles user requests in the enterprise and provides authentication, authorization, and accounting (AAA) services. It is used for more secure access in a remote-access VPN environment. Authentication is used to identify a user, by having the user enter a valid user name and valid password before access is granted. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials not match, authentication fails and network access is denied. Authorization implements policies that determine which resources and services a valid user may access. Accounting keeps track of the amount of system time or the amount of data a user has sent and/or received during a session.

6. FUTURE WORK

In this paper we have provided the overview of hybrid cloud computing and its various challenges. We also

presented some ways to secure communication between cloud and enterprise. The hybrid cloud computing will definitely be one of the biggest areas of focus for the companies in next coming years. Because hybrid cloud is flexible and customizable to an organization's requirements, it may better mitigate security concerns and other issues than other cloud models. Today many businesses are prioritizing hybrid cloud adoption but there are also confusion about the true potential of hybrid cloud and its strategic value to the business. In future, a hybrid cloud strategy will need to be developed by organizations to realize the true benefits of hybrid cloud solutions.

7. CONCLUSION

Over the last few years, cloud computing has become one of the fast growing segments of the IT industry. Many businesses are adopting cloud services at a rapid pace. Therefore, what kind of cloud an organization needs now is perhaps the most strategic decision IT leaders will need to make right now. Hybrid cloud seamlessly combines internal resources and public cloud platforms into a single platform, providing ultimate flexibility and control. But there are also some concerns remain about the integration and security of data in hybrid cloud infrastructures. Various solutions to secure the data such as using a VPN, data encryption and firewalls have been discussed in this paper.

8. REFERENCES

1. Gartner. Predicts 2014: Cloud Computing Affects All Aspects of IT Technical report. http://www.gartner.com/technology/topics/cloud-computing.jsp
2. IDC Forecasts about Cloud Computing. Technical Report, IDC (International Data Corporation), September 2013. http://www.idc.com/getdoc.jsp?containerId=prUS24298013
3. Michael Glas and Paul Andres, "An Oracle white paper in enterprise architecture - achieving the cloud computing vision", CA - U.S.A, Oct 2010.
4. Intel White Paper, What Is PaaS?, July 2014. http://www.intel.com/content/www/us/en/cloud-computing/cloud-computing-what-is-paas-cloud-demand-paper.html
5. S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 34 (1) (2011), pp. 1–11.
6. Wikipedia, Cloud Computing http://en.wikipedia.org/wiki/ Cloud_computing
7. Research and Markets: Global Hybrid Cloud Market 2014-2018, Technical Report, April 2014. http: // www. researchandmarkets.com /research/ 6l5bz9/ global _hybrid
8. Avanade Survey - Hybrid Cloud: From Hype to Reality, December 2014. http://www.avanade.com/ Documents/ Resources/hybrid-cloud-global-study.pdf
9. Open Cloud Bridge: Extending your existing datacenter to the cloud, Citrix Whitepaper. http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-open-cloud-bridge-extending-your-existing-datacenter-to-the-cloud.pdf
10. Amazon Virtual Private Cloud Connectivity Options, Whitepaper, July 2014. http://aws.amazon.com/vpc/
11. Community cloud computing benefits and drawbacks. http://www.computerweekly.com/news/1510117/Community-cloud-computing-benefits-and-drawbacks
12. Commissioned study conducted by Forrester Consulting on behalf of Juniper Networks. Technical Report, January 2014. http://www.juniper.net /assets /us/en/local/pdf/additional-resources/forrester-tap-report.pdf