Security Challenges in Hybrid Cloud Infrastructures

Koushik Annapureddy
Aalto University - School of Science and Technology
koushik.annapureddy@tkk.fi

Abstract

Cloud computing has the potential to significantly change the way enterprises and their IT (Information Technology) systems run, but in order to achieve this the current cloud computing model needs to be changed according to the enterprise requirements. These modifications lead to the evolution of the hybrid cloud, which is a mix of both public and private clouds. Here, we consider hybrid cloud deployment and Infrastructure as a Service (IaaS) consumption model in detail since these provide the greatest flexibility for the enterprise users. In order to succeed with hybrid cloud approach, there are a few challenges that must be addressed such as application complexity and security. In this paper, we focus on the challenges and security issues which may arise in the enterprises due to migration of their IT infrastructure towards the hybrid model and finally analyze some of the solutions which helps in providing secure connectivity between the public cloud and the enterprise internal network.

1 Introduction

Cloud computing is a solution in which computing resources such as hardware, software, network's and storage are provided to users on demand. The main principle behind designing this type of solution is to provide the users and enterprises with the computation and storage resources they require, while allowing the customers to pay only for the amount they use.

Enterprises, by deploying cloud solutions into their IT infrastructure, are able to achieve efficiency, cost reduction, elasticity and agility. Choosing an appropriate cloud deployment model for their IT operations is one of the important decisions for enterprises. Consider a recent survey of large enterprises worldwide conducted by Yankee Group [10]. Over 24% of the enterprises informed that they are already using IaaS, and an additional 37% of them expect to adopt IaaS during the next two years. In large enterprises, the IT infrastructure [16] can be broadly divided into three elements, namely Equipment (Enterprise servers, storage, network and security devices), Facilities (Data centers, power cooling system)and Monitoring/Management systems and most of them spend a lot of time and money on evaluating, buying, configuring and managing all software and hardware required for their operations. All these issues can be solved by delivering IT infrastructure from the cloud model. Cloud infrastructure services, or IaaS, delivers computer infrastructure, typically a platform virtualization environment, as a service to the customers. Instead of purchasing servers, software, data center space or network equipment, customers can buy those resources as a fully outsourced service from cloud provider. For delivering I.T infrastructure services, cloud providers rely on virtualization mechanisms so that it helps in delivering resources to customers in less time[9].

In spite of these significant advantages, migrating IT infrastructure from enterprises to the public cloud involves many challenges[12]. The complex nature of current enterprise applications pose problems such as performance issues, delay in response time and network latency when deployed in the cloud. Apart from this, industry-specific regulations and national privacy laws restrict on what type of data an enterprise can migrate to the cloud [12]. Because of these issues, there has been a lot of interest among enterprises in hybrid architectures where enterprise applications are partly hosted on-premises and partly in the cloud. Public and private cloud/Internal Network together provide resources to the enterprises. Hybrid architectures offer enterprises security along with cost savings, flexibility, scalability, high performance while meeting business and technical needs.

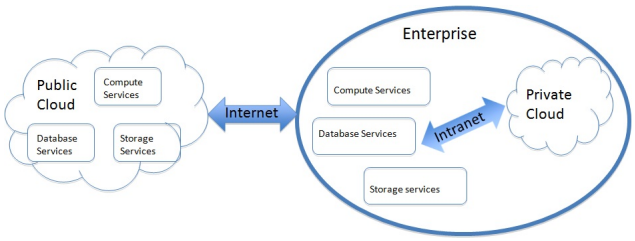

Figure 1: Hybrid Cloud[3]

Even though by providing IaaS through the hybrid model, enables a flexible, on-demand approach for satisfying computing requirements for enterprises, there are many issues to be addressed. The main barrier to enterprise adoption of IaaS is security. 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. Apart from this complexity, there are many security issues such as managing the communication link between both sites during delivery of IT infrastructure from cloud to enterprises, defining firewall with optimal rules to allow only approved traffic from cloud, incompatible network policies. 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 challenges involved while deploying hybrid cloud architecture for enterprise needs, Section 4 describes the solutions

which help in enterprises to operate efficiently and securely in hybrid environment. Section 5 discusses on differences in the mentioned solutions. We conclude and give future work in Section 5 and Section 4 respectively.

2 Background

Due to emergence of virtualization as an efficient method for sharing the resources, cloud computing gained popularity over the last few years. Before migrating IT infrastructure into the cloud, it is the responsibility of the enterprises to analyze the different security threats possible in each cloud and service models. In this section, we provide an overview study of all the models used in cloud.

2.1 Understanding Different Service Models

The services offered by cloud computing models range from web based word processors and email clients to application development platforms such as WaveMaker, Engine Yard to Virtual Infrastructure providers which lease full virtual machines. In this section, we present various types of delivery models used in cloud.

2.1.1 Software as a Service (SaaS)

In this model, software is delivered or offered to customers as a service. SaaS [11] is a software application delivery model in which enterprises hosts and operates their application over the internet so that customers can access it. Earlier, companies have run software on their own internal infrastructures and computer networks, but now most of them have migrated to the SaaS model. One benefit of this model is customers do not need to buy any software licences or any additional equipment for hosting the application. Instead, they pay for using the software application. Users checking mail using Gmail, Yahoo mail, managing appointments with google calendar are some of the SaaS applications users encounter in their daily life.

2.1.2 Platform as a Service (PaaS)

This model provides a platform for building and running custom applications. There is a lot of complexity and cost involved in building and running applications within the enterprise like support from hardware, a database, middleware, an operating system and other software. Enterprises should have team of network, database and system experts for setting up the configuration suitable for development. With continuous evolving business requirements, the application needs to be changed every time thus causing long development cycles due to redeployment. With PaaS, enterprises can build applications without installing any tools on their local systems and can deploy them without many difficulties. By using PaaS as a development platform web applications can be built almost five times faster than using conventional Java or .Net methods[7].

2.1.3 Infrastructure as a Service (IaaS)

In organizations, maintaining their internal IT related tasks like installing, configuring servers, routers, firewalls and other devices is a cumbersome process and it requires dedicated personnel for carrying out these tasks. Apart from this there are many challenges the enterprise has to tackle while managing their infrastructure. IaaS [15] provides a solution by migrating the IT infrastructure to the cloud and it is the responsibility of the cloud provider to tackle the issues of IT infrastructure management. Virtualization techniques are most commonly used in this model. VMWare, Amazon EC2, IBM BlueHouse, Microsoft Azure, Sun ParaScale Cloud Storage,etc are some of the infrastructure services.

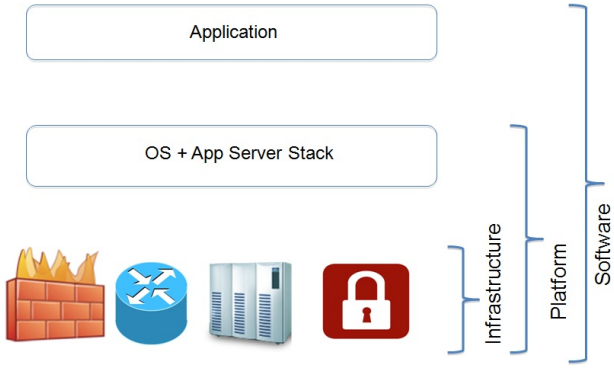

Figure 2: Cloud Resource Consumption Models[2]

2.2 Cloud Models

Irrespective of the service model delivered by cloud provider there are four different deployment models used according to the enterprise requirements. Below we provide a detailed explanation about all the deployment models.

Public cloud: In this model, a cloud service provider provides cloud infrastructure, such as applications and storage, available to the general public or large organization over the internet. These services can be offered for free or on a pay-per-usage model. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform [8].

Private cloud: This model is similar to the public cloud on basis of operation except the fact that the resources (applications and storage) are operated for a single organization. The service provider can be the same organization or a third party. This models suits better for private organizations where they provide hosted services to limited number of people behind a firewall. Organization that needs or wants more control over their data than they can get by using a third-party hosted service such as Amazon EC2 or Simple Storage Service (S3).

Community cloud: Some organizations has concerns over privacy, efficiency, security, compliance considerations because of dependence on major cloud vendors like Google, Amazon and Microsoft. This models suits for these types of organizations where cloud infrastructure is shared by several organizations which have common requirements [17]

Hybrid cloud - This model evolves by combining two or more clouds (private, community, or public). It combines the resources available within premises with the cloud functionality. Retaining control over valuable data by enterprises is the main reason behind evolution of this model. Enterprises have the privilege of storing their valuable data within their internal network and migrate remaining functionality and unimportant data to cloud.

3 Challenges and Insights

Today, most of the enterprise applications are multi tiered in nature and typically consist of multiple components. Hybrid architecture allows the enterprises to place their applications partly on premises and partly in the cloud. Since data is the life blood of many enterprises, monitoring the access permissions and protecting it is very important. Any compromise in the data security will not be acceptable and many solutions are created to protect such data and information. Apart from this, the enterprises must comply with many of the regulations that require data governance. By moving the data into the cloud, enterprises will lose some capabilities to govern its own data set. Indeed, it has to rely on the service providers to guarantee the safety of their data. According to the recent survey conducted by symantec [5] 83% of enterprises rated security as important criteria to be considered in hybrid clouds. 79% said backup and recovery and 76% rated continuous data protection as one of their top initiatives. Let us examine the challenges that appear when the enterprise decides to move their components to a hybrid cloud.

3.1 Confidentiality and Integrity

Even though companies can greatly reduce IT costs by migrating data and computation to the hybrid cloud, most of them have security concerns. According to the recent survey [4] where more than 500 global C-level executives and IT managers in 17 countries were interviewed, and found that inspite of the benefits that cloud provides, "By a 5-to-1 ratio, executives report that they trust existing internal systems over cloud-based systems due to fear about security threats and loss of control of data and systems"[4]. The major concern for most of them is violation of confidentiality and integrity of data. A company's data present in cloud can be leaked or tampered, intentionally or accidentally. Such actions result in damage to reputation and finances of a company.

3.2 Reconfiguration Issues

Many issues are generated due to migration of components from the internal cloud to the public cloud. Here, we discuss several challenges that can be created as a result of reconfiguring components in hybrid cloud [18] .

3.2.1 Component Placement

Planning which components to migrate to the cloud is a complex problem. Several factors must be taken into account during migration planning. Today, most of the enterprise applications consist of large number of components with complex interactions and inter-dependencies. Before migrating, component's many factors must be taken into account such as enterprise policies, cost savings from migration, increased transaction delays, wide area communication costs that may result from a migration[18]. Taking all these factors into consideration a solution must be designed.

3.2.2 Addressing

Nowadays, most of the enterprises are looking towards the cloud for dynamic applications and deployment like easily creating a set of virtual machines within the cloud to run the application, but there are difficulties when trying to link the different application components in and out of the cloud. Assume a scenario in which enterprise components are partly hosted within enterprise and partly in cloud. Suppose if there is a requirement where the internal enterprise components IP address have been changed and they operate from different location then for each new modification, cloud providers had to get alter the core networking and edge devices. This challenges prove to be critical limitation for cloud in providing dynamic deployment and agility [14].

3.2.3 Firewall

In order to safeguard the components moved to the cloud, it is the responsibility of the enterprise to create a firewall within the cloud and at the gateway of its own network. While firewalls rules are carefully designed reflecting the complex application interdependencies so only the application components that need to talk to each other are permitted to do so, they pose some limitations like exposing security holes at time of misconfiguration, vulnerable to dynamic cloud computing environments. Due to continuos changing requirements of current enterprises firewall does not provide a good solution because firewall rules should be modified for each trivial update in enterprises[22].

3.3 Shared Technology Issues

IaaS provider might offer multiple clients partitioned Virtual Machine (VM) access to the same physical server. Multi-tenant systems that store multiple clients data in one logical and physical database are more prone to this kind of error than those that store each tenant's data in separate logical databases with different schemas for each client. There is a chance of accessing data in one VM from another VM on the same physical server [21]. Apart from this anyone with privileged access to the VM's can read or manipulate a customer's data. Thus, there is a need for a technical solution that guarantees the confidentiality and integrity of computation, in a way that is verifiable by the customers of the service [20]

3.4 Application Security

Most of the IaaS providers publish RESTful APIs to accommodate all types of enterprise customers. Cloud consumers, for example enterprises, usually make outbound

calls into an IaaS provider using a REST-based or SOAP-based API for provisioning and managing server instances. Such standards-based API calls provide significant flexibility and ease for automating cloud resource management. However, this flexibility also opens the door to security risks that should be addressed [8]. It is the responsibility of the cloud provider to implement application security and at the same time enterprises have to make sure that their API calls directed towards cloud are secure and clean. Denial of Service attack on cloud management APIs can be caused by sending poor SOAP or REST requests from enterprise.

4 Solutions

In IaaS, since the cloud provides the whole computing and storage power as a service to the enterprises and end-users there is a need to explore the solution which helps in providing secure transfer of IT infrastructure services from cloud to enterprise internal network. Providing secure transfer through tunneling and encryption are the important methods for protecting corporate's data from attackers.

4.1 Virtual Private Network / Secure Tunnel

VPN (Virtual Private Network) provides secure access between enterprise and cloud. Solution developed based on VPN allows enterprises to have complete control over their data. Most of the third party companies like citrix, cohesive FT, etc have provided security solutions based on VPN.

4.1.1 Amazon VPC

Since this solution is developed by Amazon the public cloud is assumed as Amazon Web Services. With Amazon Virtual Private Cloud (VPC), enterprises can create their own virtual cloud inside amazon public cloud such that their IT infrastructure is hosted within a specific subnet. VPC provides a VPN connection between enterprise IT infrastructure and the enterprise virtual cloud (present inside public cloud). The VPN connection uses IPsec tunnel mode to protect the data from eaves dropping and tampering. All the security policies which were implemented within enterprise can be extended to virtual cloud. From the figure three presented below it is clear that the enterprise has created its own virtual cloud called VPC inside a amazon public cloud. With the help of the VPN gateway and the customer gateway, a VPN connection is established over the internet, between enterprise network and amazon public cloud.

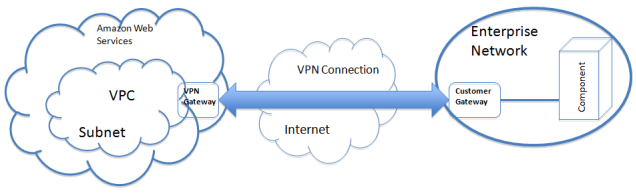

Figure 3: Amazon Virtual Private Cloud[6]

4.1.2 Open VPN

This is an open source VPN solution for providing secure data exchange between networks. Here, OpenSSL-based encryption is used for securing the data. Open VPN establishes a secure tunnel for data exchange between enterprise IT infrastructure and cloud. For encrypting the communication in tunnel it uses OpenSSH protocol. OpenVPN provides a secure network using standard SSL/TLS protocol. It supports multiple ways of authenticating the cloud and enterprise before establishing a secure connection such as verifying certificates, using smart cards, based on username/password credentials, using firewall access control policies etc[13].

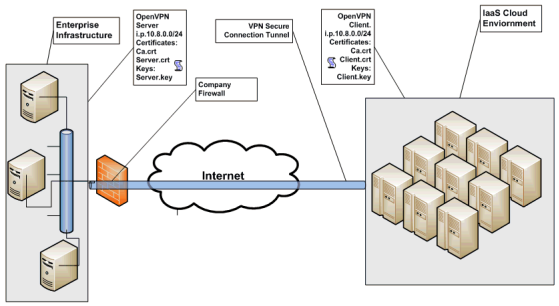

Figure 4: Open VPN[13]

In the figure 5, the authentication between the enterprise and IaaS cloud provider is based on certificates. Before establishing a tunnel certificate validation is done. The certificates and key are generated at one end (cloud) and sent to the other end (Enterprise IT infrastructure). While establishing tunnel the validity of certificates is verified at both sides and enterprises with valid certificates will be able to communicate with cloud. This feature provides enterprise level security[13].

4.1.3 Open Bridge Citrix

Cloud bridge solution provides transparent network and seamless connectivity between enterprise and the public cloud. In order to provide seamless hybrid cloud they must be securely connected and should behave as single integrated network. OpenCloud Bridge, extends the enterprise demilitarized zone (DMZ) into the cloud securely and transparently. By using cloud bridge solution, enterprises no longer need to worry about modifying the network, changing the security and access configurations since it allows the enterprises and cloud to appear as a single network[1].

In order to provide a seamless communication experience to enterprise users while accessing cloud they should be able to access data as if they are using local machines. Optimizing the Wide Area Network (WAN) performance is very much important for improving the communication speed. WAN optimization, caching, Wide-area file services are some methods which are used by cloud bridge in improving the communication speed between enterprise and cloud[1].

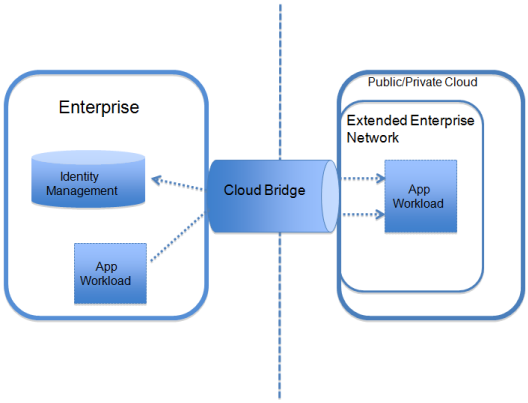

Figure 5: Citrix Cloud bridge[1]

4.2 Data Encryption

Encryption is a widely used solution for addressing the threats based on confidentiality and integrity issues. Enterprises need to encrypt their data and communications in order to protect from malicious attackers present in the internet. But managing the encryption mechanism in cloud requires management and configuration overhead for secure key change from both cloud and enterprise perspective. All the data present in the cloud will be in encrypted format and it requires key from the enterprises to decrypt the data[19]. But if in case of poor configuration there is a probability of key exposure which may result in compromise of enterprise data confidentiality and integrity. With the help of encryption mechanism, data which is in transit through the internet is protected. The data present within enterprises can be protected by providing access control or role based access. While data is in public cloud it is present under encrypted mode such that it could not be accessed by cloud provider or unauthorized user[19].

5 Future Work

In this paper we mainly focused on the ways to secure communication between the enterprises and the cloud. Apart from this there are other important scenarios where security may be a big concern such as communication from internet to the cloud, communication between applications within the cloud (In case of Amazon assume communication between EC2 and S3) and finally communication between two different clouds. Other than threats on data, which is in transit or present within enterprise and cloud, there are possibilities of threats from cloud providers and competitors on running the virtual images. In future, a lot of research work can be done in providing a trusted platform by IaaS providers while running virtual images.

6 Conclusion

Most of the enterprise IT organizations are planning to deploy cloud models in their daily IT operations to seek the benefits provided by cloud computing models. It is upto the enterprises to choose from the available cloud deployment and resource models. Hybrid model is designed in such a way that it matches with the enterprise requirements, allowing them to place data partly within the local network and in the cloud. But there are some potential threats from outside attackers to the valuable enterprise's data. Various companies have come up with solutions like creating a secure tunnel between enterprise and cloud, encrypting the data and storing it in cloud and setting up firewall with basic ACL rules are some of the solutions discussed here.

References

[1] Extending your existing datacenter to the cloud. Technical report. www.citrix.com/site/resources/dynamic/citrix_opencloud_bridge.pdf.

[2] HIEs, Future PaaS for Healthcare? Technical report. http://chilmarkresearch.com/2009/11/02/hies-future-paas-for-healthcare/.

[3] Perform The Hybrid Cloud Dance Easily With newScale,rPath and Eucalyptus. Technical report. http://www.cloudave.com/category/technology/platforms/.

[4] Survey: Cloud Computing 'No Hype', But Fear of Security and Control Slowing Adoption. Technical report. http://www.circleid.com/posts/20090226_cloud_computing_hype_security/.

[5] Symantec 2010 State of the Data Center Global Data. Technical report. http://www.symantec.com/content/en/us/about/media/pdfs/Symantec_DataCenter10_Report_Global.pdf.

[6] Was ist Amazon Virtual Privat Cloud? Technical report. http://clouduser.org/2010/01/20/was-ist-amazon-virtual-privat-cloud/.

[7] Platform as a Service (PaaS) - Powering On-Demand SaaS Development. Technical report, SalesForce, April 2009. http://wwww.sales.com.

[8] Security Guidance for Critical Areas of Focus in Cloud Computing. Technical report, Cloud Security Alliance, April 2009. www.cloudsecurityalliance.org/csaguide.pdf.

[9] Extend your IT Infrastructure with Amazon Virtual Private Cloud. Technical report, Amazon web services, January 2010. http://aws.amazon.com/vpc.

[10] Yankee Group Survey Finds Infrastructure-as-a-Service Adoption Growing. Technical report, Yankee Group, August 2010. http://www.yankeegroup.com/about_us/press_releases/2010-08-23.html.

[11] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the Clouds: A Berkeley View of Cloud Computing. Technical report, Electrical Engineering and Computer Science University of California at Berkeley, February 2009. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html.

[12] Bernard Golden. The Case Against Cloud Computing. Technical report, January 2009. http://www.cio.com/article/477473/The_Case_Against_Cloud_Computing_Part_One.

[13] R. Bhose and K. C. Nair. Integrating Composite Applications on the Cloud Using SCA. Technical report, March 2010. http://www.ddj.com/cpp/223800269.

[14] J. Considine. Networking in Federated Clouds - The L2/L3 Debate. Technical report, October 2010. http://www.cloudswitch.com/blog/category/HybridCloud.

[15] Dustin Amrhein and Scott Quint . Cloud computing for the enterprise. Technical report, IBM, April 2009. http://www.ibm.com/developerworks/websphere/techjournal/0904_amrhein/0904_amrhein.html.

[16] Jim Leach. The Rise of Service Oriented IT and the Birth of Infrastructure as a Service. Technical report, March 2008. http://advice.cio.com/jim_leach/the_rise_of_service_oriented_it_and_the_birth_of_infrastructure_as_a_service.

[17] A. Marinos and G. Briscoe. Community cloud computing. In M. Jaatun, G. Zhao, and C. Rong, editors, *Cloud Computing*, volume 5931 of *Lecture Notes in Computer Science*, pages 472–484. Springer Berlin / Heidelberg, 2009.

[18] Mohammad Hajjat,Xin Sun,Yu-Wei Eric Sung,David MAltz,Sanjay Rao,Kunwadee Sripandikulchai and Mohit Tawarmalani. Cloudward Bound: Planning for Beneficial Migration of Enterprise Applications to the Cloud. In *SIGCOMM'10*, August 30 - September 3 2010.

[19] E. Rubin. Making Cloud Computing Secure for the Enterprise. Technical report, December 2009. http://www.cloudswitch.com/section/enterprise-cloud-computing-white-papers.

[20] N. Santos, K. P. Gummadi, and R. Rodrigues. Towards trusted cloud computing. In *HOTCLOUD*. USENIX, 2009.

[21] S. N. Shah. Cloud computing by government agencies- Meeting the business and security challenges in the cloud. Technical report, August 2010. http://www.ibm.com/developerworks/industry/library/ind-govcloud/.

[22] Timothy Wood and Prashant Shenoy and Alexandre Gerber and K.K.Ramakrishnan and Jacobus Van der Merwe. The case for enterprise-ready virtual private clouds. In *HotCloud'09: Proceedings of the 2009 conference on Hot topics in cloud computing*, pages 4–4, Berkeley, CA, USA, 2009. USENIX Association.