Research Journal of Applied Sciences 9 (4): 181-186, 2014
ISSN: 1815-932X

Analysis of Trend, Service and Deployment Models in Cloud Computing with Focus on Hybrid Cloud and its Implementation

[1]D. Praveena and [2]P. Rangarajan
[1]Department of Information Technology,
[2]Department of Electrical and Electronics Engineering,
R.M.D. Engineering College, 601206 Kavaraipettai, Tamil Nadu, India

Abstract: The emergence of cloud computing has significantly changed the industry's perception of infrastructure, service delivery and development models. The business use of cloud based services is expanding and as a result there is a requirement for analysis and research on secured use of cloud computing. The enhanced requirement of enterprises lead to the evolution of combinatorial approach of cloud model called 'Hybrid Cloud' which is mix up of public and private cloud. This transition towards hybrid architecture has stimulated the concerns on a critical issues and challenges associated with effective implementation of security model. As a result the main objective of this study is of two sets; firstly to analyze the trend, service models, deployment models in cloud computing and focus shift towards hybrid cloud and secondly to analyze the security issues associated with hybrid cloud coupled with IaaS and possible solutions to mitigate. This review article also discusses the introduction of Virtual Private Network (VPN) tunnel and data encryption approach as solution to mitigate the security issues associated with Hybrid Cloud Model. The VPN approach and data encryption operating in IaaS service model ensures the authentication, integrity and confidentiality of involved data and communications between the cloud and enterprises.

Key words: Cloud computing, hybrid cloud, IaaS, virtual private network, VPN, VPN tunnel, data encryption, cloud security

INTRODUCTION

Cloud computing has become one of the most important buzzwords in the corporate world because of its innovative model of computing as a utility. It ensures increased flexibility, expansion/scalability and reliability while decreasing operational and support costs. Despite of all benefits, majority of potential cloud users are not interested to move to cloud computing on a large scale due to the inbound and unaddressed security issues present in cloud computing. In this study, the cloud computing trends has been analyzed across deployment and service models with focus towards hybrid cloud and addresses the issues in hybrid cloud coupled with Iaas with solutions.

MARKET ANALYSIS

Cloud computing has become the hot trend of the corporate world today. There is continued growth in all types of public, private and hybrid clouds. Some of the key market trends provided by market analysts are given as:

Demand for private clouds is expected to double as many organizations look for ways to gain greater flexibility from their computing resources while still maintaining control of their data. Forrester predicts the private cloud market to rise from $7.8 Billion in 2011 to >$15 Billion in 2020 (IBM, 2011)

The global public cloud services market will more than triple in size over the next 5 years to reach revenues of $66 billion in 2016 (Ovum, 2011)

Public cloud services will grow five times faster than overall IT enterprise spending (19% annually through 2015) (Gartner, 2011a, b)

Hybrid cloud computing which brings together external public cloud services and internal private cloud services as well as the capabilities to secure, manage and govern the entire cloud spectrum will be a major focus for 2012 (Gartner, 2012)

Cloud computing domain has grown beyond the anticipation. It is a highly disruptive trend that fetches new opportunities. According to IDC, "Cloud services are

Corresponding Author: D. Praveena, Department of Information Technology, R.M.D. Engineering College, 601206 Kavaraipettai, Tamil Nadu, India

interconnected with and accelerated by other disruptive technologies including mobile devices, wireless networks, big data analytics and social networking. As during the mainframe and PC eras, the new platform promises to radically expand the users and uses of information technology, leading to a wide and entirely new variety of intelligent industry solutions" (IDC, 2011).

CLOUD COMPUTING-TREND OVERVIEW

Cloud computing provides individuals and organizations with new options on how they acquire or deliver IT services with reduced emphasis on the constraints of traditional software and hardware licensing models (Chamberlin, 2013).

Drivers: Clouds offer substantiate cost savings and pay as you go model with enabled speed of delivery of new services and new capabilities. Hybrid cloud models allow organizations to host part of their data into the public cloud and other IT-resources in a private cloud or on-site.

Challenges: Customers are concerned about the security risks of cloud models and reliability of some public clouds. Many users are not interested in storage of their data by a third party or where potential access available to other users.

Implications: The key factor in modeling cloud computing is the requirement of anytime, on-the-go accessibility. The users expect to see continued development of delivery models (IaaS, PaaS and SaaS) as customers expect deployment of cloud applications. New companies, companies with complex supply chain operations and companies going through reorganizations or business process transformations are good candidates for clouds. Meanwhile, large enterprises are focusing on the strategy to migrate their apps to the cloud.

SERVICE MODELS OF CLOUD COMPUTING

Cloud computing as defined by National Institute of Standards and Technology (Mell and Grance, 2011) is a model for enabling always-on, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., storage, applications, services, etc.) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In this new model, computing resources will utilize existing technologies with a datacenter that uses virtualization to isolate instances of applications or services being hosted on the "cloud". The datacenter enables cloud users to rent computing resources based on their requirements.

The Cloud Service Providers (CSP) are the organization using the cloud to host applications and the cloud providers are the organization offering the datacenter management services.

The three main service models defined by NIST for cloud computing (Mell and Grance, 2011).

Software as a Service (SaaS): The cloud provider allows the cloud consumer to deploy an application on a cloud infrastructure. The customers rent software hosted by the vendor.

Platform as a Service (PaaS): The cloud provider offers the cloud consumer with the facility to develop and deploy applications on a cloud infrastructure using tools and services supported by the cloud service provider. In simple words, customers rent infrastructure and programming tools hosted by the vendor to create their own applications.

Infrastructure as a Service (IaaS): The cloud provider provides the cloud consumer a virtual machine. The cloud consumer can utilize the setup for processing, storage, networks and to deploy and run arbitrary software supported by the operating system of virtual machine. In simple words, customers rent processing, storage, networking and other fundamental computing resources for all purposes.

DEPLOYMENT MODELS OF CLOUD COMPUTING

The four deployment models for cloud computing are public, private, hybrid and community clouds.

Public cloud: The cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group. This is also called as External Clouds.

Private cloud: The cloud infrastructure is owned or leased by a single organization and is operated solely for that organization. This is also called as 'Internal/In-house Clouds'.

Hybrid cloud: The cloud infrastructure is a combination of two or more clouds (internal, community or public) that remain unique entities but are bound together by standardized or proprietary technology.

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., standards, mission, policy and compliance and security requirements).

The main advantage of cloud computing is its pay for use model of computing as a resource. This innovative model of computing helps organizations and its businesses to purchase as many computing resources as they need without huge investment on IT infrastructure. Other advantages of cloud computing are increased flexibility and immense scalability for a relatively constant price. For example, a cloud user can rider 1000 h of computational power on a single cloud order for the same price as 1 h of computational power on 1000 cloud orders (Armbrust *et al*., 2009). The benefits can be summarized as:

- Delivery of service (faster time to value and time to market)
- Reduction of cost (CapEx vs. OpEx tradeoff and costs that are more competitive)
- IT department transformation (focus on innovation vs. maintenance and implementation)
- No upfront capital investments on on-premise infrastructure (servers, applications, network, licenses, maintenance, facilities, hardware, etc.)

Despite of its advantages, many large enterprises are reluctant to adopt cloud computing because of security concerns. A survey conducted by IDC IT group in 2009 depicts that over 87% of respondents cited security as the number one issue preventing adoption of the cloud (Ramgovind *et al*., 2010). This result paves the way for the analysis of security issues associated with cloud computing and addressing for adoption of cloud computing.

PARADIGM SHIFT ON REQUIREMENT OF CLOUD

At the stage of huge propaganda of cloud computing, entire industry focus shifted from 'what does cloud mean' in 2010 to securing and managing cloud. The business use of cloud based services is expanding and as a result there is a requirement for analysis and research on secured use of cloud and cloud based security approaches.

Cloud computing has the potential to significantly change the way enterprises and their 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.

FOCUS TOWARDS HYBRID CLOUD

Gartner (2012)'s recent survey indicates the typical stages that enterprises will go through, from data center virtualization, to private cloud, to hybrid cloud use, where 'cloud busting' to external cloud resources expands local data center/private cloud capacity.

PROGRESS TOWARDS VIRTUALIZATION

Figure 1 indicates that data center managers, close to half believe they will be using hybrid cloud by 2015. As the majority believes in hybrid, IT architectures, processes and security capabilities will need to change and extend. In another case study provided by Gartner case study, securing the cloud describes that the security features that enabled a high-value application run on internal data centers to be 'cloud busted' to a public IaaS provider to support business demands for global, elastic service delivery.

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 (2010). 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 2 years.

For delivering IT infrastructure services, cloud providers rely on virtualization mechanisms so that it helps in delivering resources to customers in less time. In spite of these significant advantages, migrating IT infrastructure from enterprises to the public cloud involves many challenges (Golden, 2009). 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 (Golden, 2009). 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.

BENEFITS OF HYBRID MODEL

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 (Fig. 2).

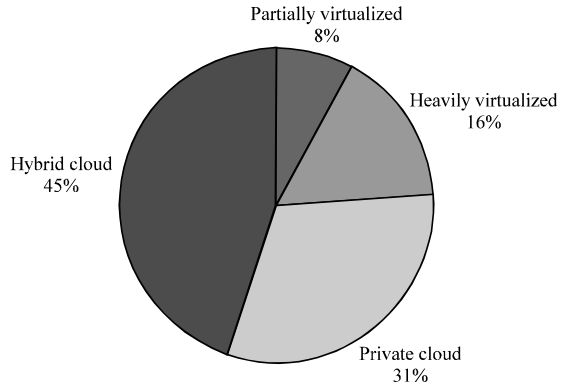

Fig. 1: Progress towards virtualization (Gartner, 2012)

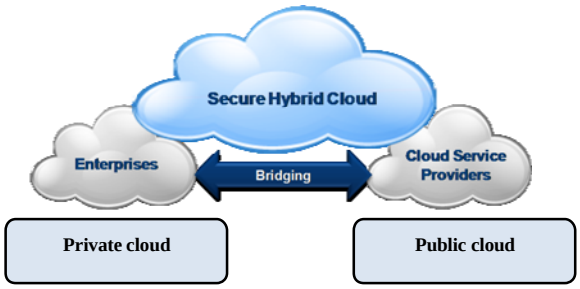

Fig. 2: Benefits of Hybrid Model (Sequeira, 2010)

ISSUES IN HYBRID MODEL COUPLED WITH IaaS

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. 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 Corporation (2010) 83% of enterprises rated security as important criteria to be considered in hybrid clouds. The 79% said backup and recovery and 76% rated continuous data protection as one of their top initiatives.

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 on Cloud Computing (CircleID, 2009), 5:1 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. The major concern for most of them is breach 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.

Reconfiguration issues: Many issues are generated due to migration of components from the internal cloud to the public cloud. Researchers discuss several challenges that can be created as a result of reconfiguring components in hybrid cloud (Hajjat *et al*., 2010). The subsets of this issue include component placement, addressing and firewall.

Component placement: Identifying the components to be migrated 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, transaction delays, communication costs associated with migration (Hajjat *et al*., 2010). Taking all these factors into consideration a solution must be designed.

Addressing: In recent times, majority of 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. The challenges prove to be critical limitation for cloud in providing dynamic deployment and agility (Considine, 2010).

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 continuous changing requirements of current enterprises firewall does not provide a good solution because firewall rules should be modified for each trivial update in enterprises (Wood *et al*., 2009).

SHARED TECHNOLOGY ISSUES

IaaS provider might offer multiple clients partitioned Virtual Machine (VM) access to the same physical server. Multitenant 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 (Shah, 2010). Apart from this anyone with privileged access to the VM's can read or manipulate a customer's data. A guaranteed technical solution is required to ensure confidentiality and integrity of computation, in a way that is verifiable by the customers of the service (Santos *et al*., 2009).

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.

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 data from attackers.

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. The major solution providers of VPN approach are Amazon VPC, Open VPN and Open Bridge Citrix.

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 (Rubin, 2009). 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 (Rubin, 2009).

CONCLUSION

Most of the enterprises IT organizations are planning to deploy cloud models in their daily IT operations to seek the benefits provided by cloud computing models. The enterprises have to choose from the available cloud deployment and resource models which suits their needs. 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 access control rules are some of the solutions.

RECOMMENDATIONS

In this study, the focus is mainly on the hybrid cloud and its effective implementation to secure transmission between the cloud and the enterprises. The other important aspects to be analyzed pertaining to cloud security are communication from internet to the cloud, communication between applications within the cloud and finally communication between two different clouds. In future, a detailed research work can be done to explore the new borne issues with implementation of hybrid cloud coupled with IaaS.

REFERENCES

Armbrust, M., A. Fox, R. Griffith, A.D. Joseph and R.H. Katz *et al*., 2009. Above the clouds: A Berkeley view of cloud computing. Technical Report No. UCB/EECS-2009-28, February 10, 2009. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html.

Chamberlin, B., 2013. Cloud computing: A horizon watching trend report. http://www.slideshare.net/orizonWatching/cloud-computing-a-horizon-watching-trend-report-05feb2013.

CircleID, 2009. Survey: Cloud computing No Hype, but fear of security and control slowing adoption. February 26, 2009. http://www.circleid.com/posts/20090226_cloud_computing_hype_security/.

Considine, J., 2010. Networking in federated clouds-The L2/L3 debate. http://www.cloudswitch.com/page/networking-in-federated-clouds-the-l2-l3-debate.

Gartner, 2011a. Gartner says worldwide enterprise IT spending to reach $2.7 Trillion in 2012. Orlando, Fla., October 17, 2011. http://www.gartner.com/newsroom/d/1824919.

Gartner, 2011b. Gartner identifies the top 10 strategic technologies for 2012. Orlando, Fla., October 18, 2011. http://www.gartner.com/newsroom/id/1826214.

Gartner, 2012. Securing and managing cloud computing. https://www.gartner.com/doc/2007315/securing-managing-cloud-computing#-7587926.

Golden, B., 2009. The case against cloud computing, part one. January 22, 2009. http://www.cio.com/article/477473/The_Case_Against_Cloud_Computing_Part_One.

Hajjat, M., X. Sun, Y. Sung, D. Maltz, S. Rao, K. Sripanidkulchai and M. Tawarmalani, 2010. Cloudward bound: Planning for beneficial migration of enterprise applications to the cloud. Proceedings of the ACM SIGCOMM 2010 Conference, August 30-September 3, 2010, ACM, New Delhi, India, pp: 243-254.

IBM, 2011. IBM introduces new portfolio of private cloud offerings. http://www-03.ibm.com/press/us/en/pressrelease/35596.wss.

IDC, 2011. Public IT cloud services spending to reach $72.9 billion in 2015, capturing nearly half of net new spending growth in five key product segments, according to IDC. http://www.idgglobalsolutions.com/news/public-it-cloud-services-spending-to-reach-729-billion-in-2015-capturing-nearly-half-of-net-new.

Mell, P. and T. Grance, 2011. The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology. Special Publication 800-145. National Institute of Standard and Technology, U.S. Department of Commerce, September 2011, Gaithersburg, MD., USA. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Ovum, 2011. Public cloud services market to hit revenues of $66 billion. http://ovum.com/press_releases/public-cloud-services-market-to-hit-revenues-of-66-billion/.

Ramgovind, S., M.M. Eloff and E. Smith, 2010. The management of security in Cloud computing. Proceedings of the Information Security for South Africa, August 2-4, 2010, Sandton, Johannesburg, pp: 1-7.

Rubin, E., 2009. Making cloud computing secure for the enterprise. http://www.cloudswitch.com/page/making-cloud-computing-secure-for-the-enterprise.

Santos, N., K.P. Gummadi and R. Rodrigues, 2009. Towards trusted cloud computing. Proceedings of the Conference on Hot Topics in Cloud Computing, June 14-19, 2009, Berkeley, CA, USA .

Sequeira, A., 2010. Great dialogue with CIOs at InfoWeek 500, 2010. VMware Community, Security and Networking, September 17, 2010. http://cto.vmware.com/great-dialogue-with-cios-at-infoweek-500-2010/.

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

Symantec Corporation, 2010. Symantec state of the data center report 2010: Global data. January, 2010, pp: 1-83.

Wood, T., A. Gerber, K.K. Ramakrishnan, P. Shenoy and J. Van der Merwe, 2009. The case for enterprise-ready virtual private clouds. Proceedings of the Conference on Hot Topics in Cloud Computing, June 14-19, 2009, Berkeley, CA., USA., pp: 1-5.

Yankee Group, 2010. Yankee group survey finds infrastructure as-a-service adoption growing. www.yankeegroup.com/about_us/press_releases/2010-08-23.html.