Journal of Engineering and Applied Sciences 12 (11): 3008-3013, 2017
ISSN: 1816-949X

Challenges and Issues in Cloud Environment

Nitin Gahlawat, Ayush Aggarwal, Yash Devgan and Poonam Nandal
Department of Computer Science and Engineering, Faculty of Engineering and Technology,
Manav Rachna International University, Fariabad, India

Abstract: Cloud computing refers to the services that are provided to users in pay as you use style. Cloud computing has various benefits such as flexibility, easy management, easy to expand, cost saver, etc. Cloud computing reduces initial investments as there is no need to invest in devices like hard disks and I/O devices as all the care is taken by the cloud provider. Cloud is a relatively new technology, the development and the use of cloud is still in its early stage. Industries are still hesitant in shifting to cloud in a permanent manner due to various issues and challenges that occurs when shifting to cloud environment. In this study, we will discuss the cloud architecture and the key challenges, issues a user and industry faces inside a cloud environment.

Key words: Cloud, network, service provider, public, private, hybrid

INTRODUCTION

Cloud computing refers to process of storing data on remote servers rather than storing on your personal computer. Cloud computing is a relatively new technology and is expected to rule the future of IT sector (Ren *et al*., 2012). On-demand computing or the term cloud computing generally refers to Software as a Service (SaaS), Platform as a Service (Paas), Infrastructure as a Service (Iaas) from computation point of view.

The computing activity of today's corporate world is shifting from the personal desktop or the organization server infrastructure to the cloud environment. This shift will definitely have a major impact on the computational system of the overall corporate world involving every person in IT industry, hardware manufacturer and software developers.

The emerging field of cloud computing involves the major services provided over the internet across the world. This domain is also the major concern and interest of many business owners, organization owners as it provides the resources as platform, software, infrastructure as a service to all of them. Although, the domain of cloud computing is of interest but as it is an emerging field for all the IT industry, there are many issues which still needs to be considered. These issues like data security in cloud which is the need of the era, load balancing which is to be done appropriately so that all the resources are to be utilized efficiently by providing the good throughput and response time.

Cloud has the ability to reduce the cost by optimizing and expanding efficiencies (Takabi *et al*., 2010). In a cloud technology, resources such as memory, processers are made available to the general public that can be used and released by users with the help of in and demand style. After the popularity of Web 2.0 cloud computing has now become the popular catchphrase. However, the cloud computing is not the new word and does not have any new concept but it is having a strong relation with the grid computing, distributed systems, cluster computing, utility computing.

In cloud computing, the service providers like Microsoft, Amazon, Google, GoGrid, etc. are using the technologies based on virtualization in association with the abilities of the computational resources used over the internet across the world. From the point of view of virtualization technology, all the cloud service providers also known as CSP, various virtual systems from different corporate needs to be again located on the similar server physically for the maximum utilization of virtualization to give the effective response time. The CSP must associate with the MSP Model which is the managed service provider for the data security of all the customers to retain them in their organization as the data security is the major concern in cloud environment. However, maximum IT industry are shifting toward the cloud environment for their benefits gained by expanding their own infrastructure but no one can compromise in terms of security of data and respective applications.

In cloud, role of a CSP (Cloud Service Provider) is divided into two parts (Zhang *et al*., 2010). Infrastructure provider: it is responsible for management of cloud and renting resources to its users on prices based on usage

Corresponding Author: Nitin Gahlawat, Department of Computer Science and Engineering,
Faculty of Engineering and Technology, Manav Rachna International University, Fariabad, India

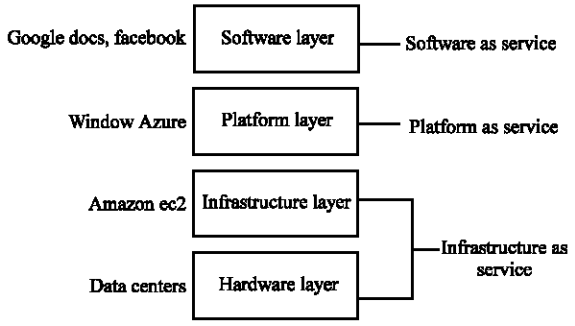

Fig. 1: Three tier cloud architecture

model. Service provider: it rents resources from various infrastructure providers so that they can be used by the users (Zhang *et al*., 2010).

Layers in cloud: In this study, we will look at the different layers present in cloud. The architecture of cloud is usually partitioned in four different layers which are: hardware layer, infrastructure layer, platform layer and the last layer which is application layer.

Hardware layer: This layer of cloud is implemented in datacenter as it consists of physical devices like routers, servers, switches, power and cooling systems. It deals with problems like fault tolerance, management of traffic and configuration of hardware (Zhang *et al*., 2010).

Infrastructure layer: Infrastructure layer in a cloud is commonly known as virtualization layer. This layer is placed above hardware layer and below platform layer in a cloud (Zhang *et al*., 2010). This layer provides a group of virtual machines which provides a platform for user to run applications. End user programs remain inside the virtual machines itself.

Platform layer: This layer is placed above infrastructure layer. This layer provides an Integrated Development Environment (IDE) for a user to build its applications without having any clue of background processing. This layer basically consists of operating system and frameworks (Zhang *et al*., 2010). This layer provides an environment and can help in limiting the access to the system according to the user.

Application layer: This is the layer which actually provides on demand services and functions. It consists of actual applications such as google and Facebook where cloud is actually used. In this layer applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet (Zhang *et al*., 2010).

Figure 1 shows the typical three tier cloud architecture. Infrastructure layer and hardware together work as Infrastructure as a Service (IaaS) model, platform layer works as a Platform as a Service (PaaS) Model and software layer acts a Software as a Service (SaaS) Model. Hardware layer is the first layer followed by infrastructure layer. Platform layer is between infrastructure layer and software layer. On the top of the cloud architecture is the software layer which consist of actual applications such as Google docs, Facebook, Hotmail, etc.

MATERIALS AND METHODS

Types of cloud: In this study, we will be looking at different cloud models that are available for a user to opt from. A user can select any of the following cloud deployment models according to their requirements. There are three types of clouds deployment models available. Each cloud model has its own particular limitations and features.

Public cloud: In this cloud environment, cloud services are made available to the public. In setting up public cloud, no initial capital is required. These cloud services are cheaper however they are not recommended for business corporations as the user lack complete control over its data. These clouds are publicly available to the masses. Most of the services in case of public clouds are available on pay as you use basis. However, public cloud lacks the security in comparison to private clouds as data can be attacked by external attacks and viruses (Kuyoro, 2011).

Private cloud: Private cloud is relatively new cloud technology in which cloud services are implemented inside a company's data storage centers (Mell and Grance, 2011). In this type of cloud, entire control over the data lies in the hand of a particular organization. These clouds are more secure and reliable in comparison to public clouds. These clouds are designed in such a way so as meet up with the requirements of one particular organization or company. Private clouds are an improved version of clouds and they have high security features as compared to other clouds as it restricts unauthorized access to working and operations of a cloud (Mell and Grance, 2011).

Hybrid cloud: Hybrid cloud is a type of cloud which is private and it is connected to various other clouds that can be seen as a single unit and can be managed in a central manner. This type of cloud employs features of both public and private clouds. These clouds are highly flexible. In hybrid cloud, some part of the services are stored on private cloud while other services are stored on public cloud. User in case of hybrid cloud has the option

Table 1: Different cloud commercial products

Names	IBM Bluecloud	IBM Ensembles	Google app Engine	Google Docs	Sales force.com gifttag	Amazon EC2	Windows Azure
Level	Platform level	Infrastructure level	Platform level	Software level	Software level	Infrastructure level	Platform level
Services	Rational application development	Web 2.0	MapReduce	big table	record security	amazon web services	hotmail
Security features	Power VM	Websphere2	HW secured in data centers	HW secured in data centers	Metadat API	Public key Infrastructure	Replicated data

of storing general purpose applications on public class as it is cheaper and can store confidential and personal information on private clouds for security reasons.

Commercial products: In this study, we will discuss and compare various cloud computing products available. There are various cloud commercial products available in the market. Different commercial products work on different layers depending upon their actual usage. Amazon EC2 and Windows Azure are the two commonly used products.

Amazon EC2: Amazon EC2 is the most commonly used cloud commercial product. Amazon EC2Works at infrastructure layer. For a 32 bit architecture amazon Ec2 1.7 GB of memory is required and price is $0.10 for 1 h (Juve *et al*., 2009). It has the option of storing various instances at different places (Fox *et al*., 2009). It is a high speed product and its average rate of transmission is around 1000 kbps.

Windows Azure: This cloud product is implemented at platform level. It provides a Window like interface where a user can run its programs and store the required data. Windows Azure works in point to point fashion. User is required to defined http and TCP protocols (Hill *et al*., 2011). Languages such as C++ and C# are supported in windows Azure. Table 1 compares different cloud commercial products and the level at which they work.

Salesforce.com Gifttag: This is developed at software level. Salesforce.com provides various reported services like Apex, record security, visualforce. The security features given are metadata API and administrative security.

Google app Engine: This cloud product is implemented at platform level. It helps the user to use its own language, frameworks, runtimes and third party libraries. This is completely managed cloud product which is not related to infrastructure so the user can only focus on the code.

Google Docs: This cloud product is developed at the software level. The services provided by them are big table and it is hardware secured in data centers.

IBM Bluecloud: This cloud product is implemented at platform level. Its main focus is to provide distributed computing among various data centers. It uses the techniques like parallel workload scheduling and virtualized linux images. This enhances the use of open source software and standards.

IBM Ensembles: This cloud product is developed at infrastructure level. This type of product is mainly used for the design and development of various applications which are connected together. It is also very common for integration platform.

RESULTS AND DISCUSSION

Key challenges in cloud environment: Cloud computing has numerous benefits and advantages but still it has some various barriers which prevents permanent adoption of cloud computing. There are various issues in cloud that needs to be taken care of. In this study, we will look at the some of the key challenges in cloud environment.

Energy administration: It is assumed that more than 50% of the total operational cost is spent on power and cooling techniques. The main aim is to cut the energy cost as well as meet government and environmental standards. Large amount of capital is invested in power and cooling techniques used in data centers in order to save energy. However, designing of energy efficient devices slows down the processing rate of CPU and partially turns off various hardware devices which in turn effects performance. There should be a good balance between power saving and performance. To provide good balance between power usage and performance various researchers are trying to find optimal solution to this problem (Kumar *et al*., 2009). This problem is yet to be addressed and still remains a key issue.

Certainty in data deletion: Another issue in cloud system is lack of backup facility. In case data gets deleted from hard disks stored in data centers due to device failure user data will definitely get deleted unless user has local copy of the data. A cloud can also face trust issues as it too can suffer from downtime problem like our traditional servers (Jadeja and Modi, 2012).

Cost: Though cloud can help in cutting down the initial costs as there is no requirement of hard disks and other storage devices on the user side but the cost will significantly rise when a user shifts from traditional system to the cloud system as the cost of migration of data is quite high. The cost factor will further rise if a user chooses to opt for hybrid cloud instead of public or private cloud as the data is distributed within various clouds (Dillon *et al*., 2010).

Security of data: Even after various advancements, security of the data stored in the cloud still remains a major concern. As services providers have no knowledge regarding security of data centers they are completely dependent on infrastructure provider in order to attain maximum security as user no longer actually possess the data, its integrity may be at risk. Encrypting the data before placing it on cloud can somehow help in dealing with privacy issues but encryption of data is not a practical solution as it slows down the searching process. Moreover downloading our data and decrypting it consumes large bandwidth and as result cost factor also increases. Botnet attacks and loss of data are the other issues concerned with the security of cloud. Cloud provides an easy environment for the hackers to spread spam and malwares. Novel techniques are required to deal with cloud issues. Phishing is another major concern when security of cloud is concerned (Dillon *et al*., 2010). In case of cloud environment, remote attestation can be used to tackle with security problems however virtual machines tend to transfer from one location to another, remote attestation alone is not enough. Transfer of virtual machines should only be there when you trust both source and destination. Researchers are constantly committed on creation of secure protocols (Wood *et al*., 2007).

Payment model: Analysis of cost in case of clouds is a tiresome task as compared to traditional systems. Mostly the usage cost is calculated depending on the use of virtual machine instead of the actual underlying physical hardware. Different cloud providers employ different methods for the calculation of user usage. Most cloud providers charge on the basis of resources consumed by users. For example, Amazon EC2 cloud services charge user on the basis of time they spent while Google charges users according to the cycle they consume. Since, the cloud infrastructure is not transparent there is no practical method to relate resource consumption with the user cost. As various resources in a cloud are shared between different users, a cloud provider may impose unexpected charges on user whereas the real reason for this may be network load or hardware bugs caused by other users. Pooling of various resources through virtualization has made cost calculation a tedious task. Researchers are still working for creation of efficiency payment models which are scalable and flexible.

Lack of interoperability: Interoperability is required as it allows user to maximize resources at different layers each cloud service provider uses its own techniques and methods to interact with the user and provide its services. This prevents the simultaneous usage of various clouds and users are forced to stick with only one particular cloud services provider and this further leads to vendor locking. Interoperability is crucial to provide smooth flow of data within various clouds but clouds as of now lacks the interoperability capabilities. As cloud is still at an early stage, interoperability related issues are yet to be resolved (Jensen *et al*., 2009).

Management of traffic: Various applications these days are dependent on data traffic in order to provide better functionality and performance. Measuring the data traffic in a cloud environment is a hard task as there are several links in the datacenter (Choo, 2010). It is assumed that the traffic in a cloud environment follows a fixed pattern however various IDE's and applications used in data centers changes this fixed pattern and makes calculation of data traffic a difficult task. Dean and Ghemawat (2008) discussed the traffic of data centers by studying the path from routers. However, there is not much work regarding analysis of data traffic and this issue is yet to be tackled.

Combining servers: Since, usage of energy also plays a crucial role in cloud environment, combining various servers together to perform one particular task can help in expanding usage of services and simultaneously reducing the usage of energy. In case of combining servers, servers that are underutilized are treated as single unit and other servers can go into power saving state thus saving power consumption. However, combining server halts the behavior of programs that use cloud. Sharing of resources leads to congestion of resources and as a result behavior of the application gets affected. Moreover the working of cloud servers is not transparent and sometimes it may give unexpected results. As discussed by Wood *et al*. (2007), it is necessary to keep record of virtual machine fluctuations to deal with resource congestion and to provide effective combining of servers.

Relocation of virtual machines: Virtualization basically refers to the creation of an abstraction layer above the actual physical hardware layer. Virtualization plays a key

role in a cloud environment as there can't be any cloud in absence of virtualization. Virtualization is mostly used to discover hotspots. However, detection of hotspots in clouds is a tedious task and relocation of virtual machines lacks the ability to quickly respond to change in demands. Clark *et al.* (2005) discussed that transferring complete operating system and all of its programs and treating them as a single unit helps to tackle the issues faced at process level migration and researched about various benefits of transfer of virtual machines.

Privacy: Privacy is one of the major issues in cloud environment. Various communities aren't willing to store information on devices set outside their corporations as they worry non public information could be in danger and unauthorized individuals would possibly access their data. Cloud operations must be transparent enough to the user and transparent about privacy assurance (Hawang and Li, 2010).

CONCLUSION

Cloud computing is a new technology and the introduction of cloud, has changed the scenario of traditional computing. As we know the consumption of data is increasing day by day and it is not possible to carry out that on hardware device. So, the entry of this cloud technology has helped us to overcome this problem but the development of cloud techniques is still at fresh state. There are still some key issues in cloud environment like energy administration, inappropriate payment model, vendor locking, security and privacy issues. These issues still remain key issues in cloud and are yet waiting to be resolved. In this study, key issues and challenges related to cloud environment have been highlighted.

ACKNOWLEDGEMENTS

Researchers would like to express the gratitude to Dr. Kiran Khatter, Research Mentor, Accendere Knowledge Management Services Pvt. Ltd. and other Research Mentors from Accendere KMS Pvt. Ltd. For their comments on earlier versions of the manuscript. Although, any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERNCES

Choo, 2010. Cloud computing: Challenges and future directions. Trends Issues Crime Criminal Justice, Vol. 400.

Clark, C., K. Fraser, S. Hand, J.G. Hansen and E. Jul *et al.*, 2005. Live migration of virtual machines. Proceedings of the 2nd Conference on Networked Systems Design & Implementation Vol. 2, May 02-04, 2005, USENIX Association, Berkeley, California, pp: 273-286.

Dean, J. and S. Ghemawat, 2008. MapReduce: Simplified data processing on large clusters. Commun. ACM, 51: 107-113.

Dillon, T., C. Wu and E. Chang, 2010. Cloud computing: Issues and challenges. Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), April 20-23, 2010, IEEE, Perth, Australia, ISBN:978-1-4244-6695-5, pp: 27-33.

Fox, A., R. Griffith, A. Joseph, R. Katz and A. Konwinski *et al.*, 2009. Above the clouds: A Berkeley view of cloud computing. Master Thesis, University of California, Berkeley, Berkeley, California.

Hawang, K. and D. Li, 2010. Trusted cloud computing with secure resources and data coloring. IEEE Comput. Soc., 14-22.

Hill, Z., J. Li, M. Mao, A.R. Alvarez and M. Humphrey, 2011. Early observations on the performance of windows azure. Sci. Program., 19: 121-132.

Jadeja, Y. and K. Modi, 2012. Cloud computing-concepts, architecture and challenges. Proceedings of the 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), March 21-22, 2012, IEEE, New York, USA., ISBN:978-1-4673-0211-1, pp: 877-880.

Jensen, M., J. Schwenk, N. Gruschka and L.L. Iacono, 2009. On technical security issues in cloud computing. Proceedings of the IEEE International Conference on Cloud Computing, September 21-25, 2009, Bangalore, India, pp: 109-116.

Juve, G., E. Deelman, K. Vahi, G. Mehta, B. Berriman, B.P. Berman and P. Maechling, 2009. Scientific workflow applications on Amazon EC2. Proceedings of the 5th IEEE International Conference on E-Science Workshops, December 9-11, 2009, Oxford, UK, pp: 59-66.

Kumar, S., V. Talwar, V. Kumar, P. Ranganathan and K. Schwan, 2009. vManage: Loosely coupled platform and virtualization management in data centers. Proceedings of the 6th ACM International Conference on Autonomic Computing, June 15-19, 2009, ACM, Barcelona, Spain, ISBN:978-1-60558-564-2, pp: 127-136.

Kuyoro, S., 2011. Cloud computing security issues and challenges. Int. J. Comput. Networks, 3: 247-255.

Mell, P. and T. Grance, 2011. The NIST definition of cloud computing recommendations of the national institute of standards and technology. Nist Spec. Publ., 145: 1-7.

Ren, K., C. Wang and Q. Wang, 2012. Security challenges for the public cloud. IEEE Internet Comput., 16: 69-73.

Takabi, H., J.B. Joshi and G.J. Ahn, 2010. Security and privacy challenges in cloud computing environments. IEEE Secur. Privacy, 8: 24-31.

Wood, T., P. Shenoy, A. Venkataramani and M. Yousif, 2007. Black-box and gray-box strategies for virtual machine migration. Proceedings of the 4th USENIX Conference on Networked Systems Design and Implementation, April 11-13, 2007, Cambridge, Massachusetts, USA., pp: 17-17.

Zhang, Q., L. Cheng and R. Boutaba, 2010. Cloud computing: State-of-the-art and research challenges. J. Internet Serv. Applic., 1: 7-18