Journal of Advances and Scholarly Researches in Allied Education
Vol. 15, Issue No. 12, December-2018, ISSN 2230-7540

An Analysis on Some Issues and Implications of Cloud Computing: A Secure Tool

Ankit Bansal[1]* Dr. Vijay Athavale[2]

[1] Assistant Professor, Gulzar Group of Institutes, Ludhiana

[2] Professor and Director, ABES Engineering College, Ghaziabad, Uttar Pradesh

Abstract – There is always a strong pressure on Information Technology (IT) to do more with fewer resources. Over the decades, this pressure to rationalize IT costs spurred a number of paradigms, technologies and buzzwords. Some of them failed to meet their promises, while others became successfully embed in IT practices and infrastructures, providing sizeable benefits. The paradigm of cloud computing is currently riding this wave, promising to be the next great revolution in IT. Cloud computing appears to have the right technological and market ingredients to become widely successful. However, there are some key areas where cloud computing is still underperforming – such as security. Availability, security, privacy and integrity of information are some of the biggest concerns in the process of designing, implementing and running IT services based on cloud computing, Cloud computing is a rapidly developing and excellent promising technology. It has aroused the concern of the computer society of whole world. Cloud computing is Internet-based computing, whereby shared information, resources, and software, are provided to terminals and portable devices on-demand, like the energy grid. Cloud computing is the product of the combination of grid computing, distributed computing, parallel computing, and ubiquitous computing. It aims to build and forecast sophisticated service environment with powerful computing capabilities through an array of relatively low-cost computing entity, and using the advanced deployment models like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service),HaaS (Hardware as a Service) to distribute the powerful computing capacity to end-users. This paper will explore the background and service models and also presents the existing research issues and implications in cloud computing such as security, reliability, privacy, and so on.

----------X----------

INTRODUCTION

Cloud computing represents the response to the new requirement in the IT. In fact, it can be said that cloud computing is an evolution of the concept "grid computing". The most important difference between them is in the method of management. In grid computing, the user must manage the entire system (server, network element, operating system, software…). But, in cloud computing, the system is offered like a service. So, the user deals only with what he needs and doesn't be concerned with other services/issues. It means that cloud computing can be used friendly. In fact, the cloud computing adopts the concept of utility computing. So, most people can use it without any specific knowledge of how the system operates or the need to manage anything. The grid computing is generally oriented to scientific researchers who have an important knowledge in computer sciences. Many projects are developed or under construction to respond to the increasing demand. Amazon with Elastic Compute cloud (EC2) was the leader in this domain. Then every actor-major in the IT follows and presents his own system like Microsoft and her system Azure, Google and App Engine, IBM and Blue Cloud.

Innovations are the necessity to ride the inevitable tide of change. Rapid development in technology has profoundly influenced human lifestyle by bringing risk as well as sophistication in the day to day activities. Recent technology provides services in a plug and plays fashion. Computing is being transformed into a model that can provide customized as well as commoditized services. These services are delivered in a manner similar to the typical utilities like water, electricity, and telephones. Distributed computing has spawned many familiar technologies such as grid, utility, and cloud computing to support such computing paradigm. These techniques have aimed at allowing access to a large amount of computing power in a fully virtualized manner.

Cloud computing has emerged as a popular paradigm by offering computing, storage, and software as a service in last few decades. In fact, grid computing has evolved before cloud computing

and become a basis for cloud computing. Cloud computing essentially represents the increasing trend towards the external deployment of IT resources, such as computational power, storage, and business applications as services.

There are many similarities between cloud computing and grid computing. Some people say cloud and grid computing have same operational principle while according to other cloud computing is an extension of grid computing. However Foster et al. have differentiated cloud computing from grid computing as: "Cloud computing not only overlaps with grid computing but it is evolved out of grid computing. Cloud relies on grid computing as its backbone and infrastructure support."

Similarly the technical differences between cloud computing and grid computing presented by Katarina Stanoevska-Slabeva and Thomas Wozniak as, "Cloud computing differs from grid computing in terms of virtualization. Cloud computing leverages virtualization to maximize the computing power. The purpose of virtual computing environment is to improve resource utilization by providing a unified integrated operating platform for users and applications based on the aggregation of heterogeneous and autonomous resources. Virtualization at all levels (system, storage, and network) became famous again as a way to improve system security, reliability, availability, reduce costs, and provide greater flexibility. While grid computing achieves high utilization by the allocation of multiple servers onto a single task or job.

The virtualization of servers in cloud computing makes high utilization by allowing one server to compute several tasks concurrently. Grid is usually used for job execution while clouds are more frequently used to support long-running services."

Cloud Computing started as a mean for interpersonal computing but now it is widely used for accessing software online, online storage without worrying about infrastructure cost and processing power. Organizations can offload their IT infrastructure in the cloud and gain from fast scalability. These organizations, not only include small businesses but also some parts of American government IT infrastructure is moved to cloud as well.

It is important to understand the risks and threats in a cloud environment, so that an efficient security policy can be prepared for defense purposes. Preparation begins with understanding where awareness comes in. To adopt cloud computing it is important that organizations have an acceptable level of trust in it. Information security enhancement or success does not mean tossing technical solution to all the problems but it can also be accomplished with awareness like training and education.

The need to address some security issues related to cloud and virtualization as well as people's perceptions to analyze, the level of awareness is needed. There has been a lot of research work that covers the technical side of these technologies but a lot of work has to be done on people's perception of cloud computing and its security issues.

In IT sector the most discussed and revolutionary topic is cloud computing. Immense research is being conducted in the academia and industry on cloud computing. This study shows that cloud computing is comprised of different core technologies and cloud can be used as a tool in SWAF, which will help them in monitoring and managing their networks.

Cloud computing is not a new concept; it is originated from the earlier large-scale distributed computing technology. However, it will be a subversion technology and cloud computing will be the rapid revolution in the Computer Science and Information Technology field. Which represent the development trend in the IT industry from hardware to software, software to services, and distributed service to centralized service. Cloud computing is also a new mode of business computing is virtualization. It will be widely used in the near future. The core concept of cloud computing is reducing the processing burden on the users. Eventually users use a wide variety of devices, including PCs, Laptops, Smart Phones, and PDAs to access different kinds of utility programs, storage, and application development platforms over the Internet. All these services offered by cloud computing providers. An advantage of the cloud computing technology includes cost savings, high availability, and easy scalability. However, still there exist many problems in cloud computing today, the current researchers or practitioners pointing that data security and privacy risks have become the primary concern for people to transfer or migrate to cloud computing.

CLOUD COMPUTING ARCHITECTURE

In this section, we describe cloud computing in term of composition model, business model and deployment model.

Cloud computing composition model-

Generally, cloud computing is divided into 4 layers: the hardware layer, the infrastructure layer, the platform layer and finally the application layer. This layer architecture allows developing the system easily. In fact, every layer can be updated and/or changed without any knowledge and/or modification in other layers. This layer division is compared to OSI model of the network protocol. So, with such architecture, the deployment of new software or the installation of a new hardware component does not affect other element of the system.

The layer architecture is composed of:

The hardware layer: This layer regroups all the hardware components of the cloud computing system. It concerns the management of the physical server, network component, power and controlling system. In this layer, we speak about the supervision of the data center. Usually, a cloud computing provider manages several data centers.

The infrastructure layer: It represents the virtualization layer. It allows creating the virtual resource that will be used by the upper layer. The most used virtualization technologies are Xen1, KVM2 and VMware3.

The platform layer: This layer is dedicated to the operating system and application frameworks. It depends on the virtual machine created in the lower layer.

The application layer: This layer is the highest level of the hierarchy. All the cloud applications are combined in this layer. It represents the front office of the cloud computing system.

The business model of cloud computing is based on this layer architecture. Each offer in the business model corresponds to one or two layers in the architecture model.

Cloud computing business Model-

As we have seen in the introduction, cloud computing represents a response to the new requirement in the Information Technologies. The businesses model combines the offer of cloud computing to the consumers. The authors try to describe the possible offers. They conclude that everything is a service represented as XaaS like SaaS (Software as a Service), PaaS (Platform as a Service), HaaS (Hardware as a Service), DaaS ([Development, Database, Desktop] as a Service), IaaS (Infrastructure as a Service)… More examples can be found in.The three services most used in this model are IaaS, PaaS, and SaaS.

IaaS (Infrastructure as a Service): consumers use directly the IT infrastructure (computing power, networks, storage …). These resources are provided over virtualization technologies. The physical resources are integrated or decomposed to respond to the consumers demand. The virtualization strategy consists on creating virtual machines as many as the need. So in this service, the provider manages only the resources and it is up to the consumers to define the operating system and the application that will be used.

PaaS (Platform as a service): This service provides the software resource including operating system, development frameworks… So, in this type of service, the consumer has to develop and manage only his application. The service provider offers all the necessary tools to the consumer to allow him to run his application.

SaaS (Software as a service): It refers to provide on-demand application over the internet. So all the system, from the hardware layer to the final application is administered and controlled by the service provider. The consumer uses the application only when he needs and has nothing to manage or to create to perform his need.

Cloud computing deployment model-

The deployment model is composed essentially of 4 types defined in the cloud community: Public Cloud infrastructure: The provider of this kind of system offers a set of resources (hardware or/and software) as a service to general public. The public clouds present many advantages like no initial capital investment on infrastructure. In exchange in this infrastructure, there is a lower control of the system by the user which hampers the efficiency in many business scenarios.

Private Cloud infrastructure: This type of deployment is operated for one user (organization). The management of this system can be performed by the organization itself or a third part. In private cloud, the user has more control in the system. That's why the use of this type is preferred in business especially at the first integration of cloud technology.

Hybrid cloud infrastructure: In this system, we have a combination of the other type of cloud computing deployment. It appropriates the business: the private cloud for the essential use and the public cloud when there is an increase of the need. So, hybrid cloud can be used in order to optimize users' resources depending on the actual activities.

CLOUD COMPUTING ISSUES AND IMPLICATIONS

The new paradigm of cloud computing provides sophisticated benefits and advantages over the previous computing paradigms and many organizations are customizing, migrating and adopting it. In the last few years, cloud computing has grown from being a promising logic; business is virtualization concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud and gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. However, there are still a number of issues, challenges and implications are identified, which are currently addressed by researchers, academicians and BI (business intelligence) practitioners.

1. Security

Clouds provide companies are still concerned about security when using cloud computing. Users are also worried about the vulnerability to attacks, when information and critical IT resources are outside the firewall. Where is the data more secure, on local hard drive or on high security servers in the cloud? However, in the cloud, the data will be distributed over the network through individual computers regardless of where the repository of data is ultimately stored. Industrious hackers can invade virtually at any server, and there are the statistics show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider stealing.

2. Reliability

Clouds computing still always offer round the clock reliability. There were few cases where cloud computing services suffered few hours' outages. In the present and future days to expect more cloud computing providers, richer services, established standards and best practices. Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the taxonomy of cloud computing. Once you choose a particular provider, you may be locked-in, thus bring a potential business secure risk.

3. Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users personal data may be scattered in various virtual data center rather than stay in the same hard drive physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

4. Open Standard

Open standards are critical to the growth of cloud computing. Most cloud provider's interpretation with APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs and there are a number of open standards under development, including the OGF's Open Cloud Computing Interface. The Open Cloud Consortium (OCC) is working to develop consensus on early cloud computing standards and practices.

5. Performance

The major issue in performance can be for some intensive transaction-oriented and other data intensive applications, in which cloud computing may lack adequate performance. Also, users who are at a long distance from cloud providers may experience high latency and delay.

6. Bandwidth Cost

Cloud computing offered companies, can save money on hardware and software; however they could incur higher network bandwidth charges. Bandwidth cost may be low for smaller Internet-based applications, which are not data intensive, but could significantly, grow for data-intensive applications.

7. Long-term Feasibility

Users may be sure that the cloud data or information put into the cloud storage will never become invalid even particular cloud computing service provider go broke or get acquired and swallowed up by a larger company. "The cloud potential providers how to would get the data back, and it would be in any format that it is import into a replacement application"-Gartner.

8. Legal Issues

In the same way that the electricity one uses may have been generated in another country where costs are lower, the computer processing power or storage one buys via a Cloud service may be based in another country, or indeed may be divided between multiple countries. But as well as the cost and efficiency advantages brought in this arrangement, this also raises vexing legal issues in the case of Cloud Computing arising out of exporting customers data abroad; also, the Cloud Services Provider has to contend with the Legal Systems under different Jurisdictions with not so much of visibility as to where the Data resides and how it is routed to the End User while passing through different Legal Jurisdictions. Again, vexing Legal Issues relating to ownership of data and liability for its loss or misuse have to be dealt with by the Cloud Service Providers. The legal issues differ from those arising from conventional outsourcing or hosting.

THE SECURITY CHALLENGES INTRODUCED BY CLOUD COMPUTING

As already mentioned, security, privacy and integrity are some of the biggest concerns in the implementation and use of the cloud computing services. However, data encryption, compliance with standards and service level agreements can be used to minimize security concerns.

From a technical point of view, the majority of security risks associated with cloud computing are already present in traditional data centres. Possibly, apart from very specific risks induced by server virtualization (which also exist, to some extent, in traditional data centres using server consolidation), most of the security risks are shared by both paradigms – for instance SQL injection, cross-site scripting, zero-day exploits of applications and operating systems, etc.

Virtualization does increase the impact of some of these risks, since successful attacks on the hosting machine (where the hypervisor is located) may potentially compromise every hosted virtual machine.

However, such events can be reasonably avoided and/or controlled using appropriate protection mechanisms for the hosting machines. Faults on the virtualization platforms themselves are also an obvious risk, but up to now, there are very few examples of such faults (and even fewer of negative consequences of such faults).

In simple terms, availability means that an organization has its full set of computing resources accessible and usable at all times. Availability is also a major concern, even though there are no fundamental differences, from a strictly technical point of view, between traditional services and cloud-based services – except for the possible addition of more network links to the core of critical system components.

The majority of problems, therefore, are not inherently technical. They relate with the implicit need to trust external parties to maintain critical information and provide critical IT services. This need was already present in traditional IT services – whenever new equipment or new applications were deployed in the data centre, there was an implicit need to trust the associated providers. Nonetheless, there is a fundamental difference: in cloud computing it is much more difficult to manage the chain of trust, since there is no clear view – for the client institution – on the way the service is provided. The client only knows the service provider, and the whole web of subcontracted service components is usually opaque or, at most, not verifiable by third parties.

Under the cloud-computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the service provider. In order to maintain its systems protected, the customer needs to gather detailed information about the security-oriented requirements of its IT services, applications and data. This knowledge will be useful when migrating to cloud computing paradigms, since it allows comparing and evaluating traditional services with their cloud-based counterparts.

Before the customer can solve/mitigate the issues on security, he needs to perform a risk assessment to properly identify and evaluate the assets, threats and the possible countermeasures to implement.

Identify and evaluate assets-In traditional data centres, the customer assets encompass information, applications, hardware, network, installations and IT workers. However, the cloud-computing paradigm moves some of the responsibilities from the customer to the cloud provider. For instance, the cloud provider becomes responsible for hardware (in the case of IaaS) or applications and hardware (in the case of SaaS). Therefore, the customer should determine in advance, for the assets to move to the cloud, how valuable they are and what happens if, for instance, information becomes stolen or simply inaccessible.

CLOUD COMPUTING SERVICE MODELS

Cloud service models describe how cloud services are made available to clients. Most fundamental service models include a combination of IaaS (infrastructure as a service), PaaS (platform as a service), and SaaS (software as a service). These service models may have synergies between each other and be interdependent – for example, PaaS is dependent on IaaS because application platforms require physical infrastructure.

The **IaaS (Infrastructure as a Service)** model provides infrastructure components to clients. Components may include virtual machines, storage, networks, firewalls, load balancers, and so on. With IaaS, clients have direct access to the lowest-level software in the stack – that is, to the operating system on virtual machines, or to the management dashboard of a firewall or load balancer. Amazon Web Services is one of largest IaaS providers.

The **PaaS (Platform as a Service)** model delivers a pre-built application platform to the client; clients needn't spend time building underlying infrastructure for their applications. On the backend, PaaS automatically scales and provisions required infrastructure components depending on application requirements. Typically, PaaS solutions provide an API that includes a set of functions for programmatic platform management and solution development. Google AppEngine is a popular PaaS provider, and Amazon Web Services also provides some PaaS solutions in addition to IaaS offerings.

SaaS (Software as a Service) provides ready online software solutions. The SaaS software provider has complete control of application software. SaaS application examples include online mail, project-management systems, CRMs, and social media platforms.

The main difference between SaaS and PaaS is that PaaS normally represents a platform for application development, while SaaS provides online applications that are already developed.

CONCLUSION

Cloud computing encompasses various technologies, such as computing networks, virtualization, operating systems, used in the traditional data centres leading to that it may suffer some security problems associated with such technologies. While in the IT departments and datacentres the manager may install multiple firewalls and intrusion detection systems from different vendors (serially laid out) in order to protect the information in the cloud computing environment the customer must trust in the providers the security of his information and applications. In this paper, to analyze and discussed an emerging technology: Cloud Computing. The evolving is one of the core platform for Computer Science (academics) and Information Technology (industry) in the professional world. It describes cloud background, evolution, definition, service models, deployment models and some existing issues. There is no doubt that the cloud computing is the emerging development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, on-demand service and so on, also challenges at security, reliability, and privacy, legal issues and so on. Because of this, it has been attracted by everyone including the attackers. The paper is expected to be a right path or URL for those who works or does research in cloud computing. We acknowledge the cloud computing era, to solving and prevent the existing issues and implications for maximum necessity is required.

REFERENCES

1. A. Snigh and M. Malhotra (2012). Agent based framework for scalability in cloud computing, International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 3, No. 4, April 2012.

2. B. Sonisky, Chapitre L. (2011). Cloud Computing Bible, Wiley Publishing Inc. 2011

3. Cochran and Witman, Cochran, M. and Witman, P. (2011). Governance and service level agreement issues in a cloud computing environment. *Journal of Information Technology Management*, 22(2): p. 41.

4. Dhar, S. (2011). From outsourcing to cloud computing: Evolution of it services. In *Technology Management Conference (ITMC), 2011 IEEE International*, pages 434 –438.

5. Foster, Y. Zhao, I. Raicu and S. Lu (2008). "Cloud Computing and Grid Computing 360 Degree Compared," Grid Computing Environments Workshop (GCE '08).

6. Grobauer et. al., Grobauer, B., Walloschek, T., and Stocker, E. (2010). Understanding cloud-computing vulnerabilities. *Security Privacy, IEEE*, PP(99): pp. 1–1.

7. M. Rajendra Prasad, Dr. Jayadev Gyani, Dr. P. R. K. Murti (2012). "Mobile Cloud Computing Implications and Challenges", IISTE Journal of Informational Engineering and Applications (JIEA); http://iiste.org; pp.7-15, Vol.2, No.7.

8. P.Gupta, A. Seetharaman, and J. R. Raj (2013). "The usage and adoption of cloud computing by small and medium businesses," International Journal of Information Management, vol. 33, no. 5, pp. 861–874.

9. Patel et. al., Patel, P., Ranabahu, A., and Sheth, A. (2009). Service Level Agreement in Cloud Computing. *Cloud Workshops at OOPSLA09*, 1: pp. 1–10.

10. Ramgovind et. al., Ramgovind, S., Eloff, M., and Smith, E. (2010). The management of security in cloud computing. In *Information Security for South Africa (ISSA), 2010*, pages 1 –7.

11. S. Rajan and A. Jairath (2011). "Cloud computing: The 5th generation of computing," in Proceedings of the International Conference on Communication Systems and Network Technologies. IEEE, pp. 665–667.

12. Tharam Dillon, Chen Wu, Elizabeth Chang, 2010 24th IEEE International Conference on Advanced Information Networking and Applications, "Cloud computing: Issues and Challenges".

13. V. Chang, R. J. Walters, and G. Wills (2014). Review of Cloud Computing and existing Frameworks for Cloud adoption. Nova Publishers.

14. Y. Sahu and R. Pateriya (2013). "Cloud computing overview with load balancing techniques," International Journal of Computer Applications, vol. 65, no. 24, pp. 40–44.

15. Zhang et. al., Zhang, S., Zhang, S., Chen, X., and Huo, X. (2010b). Cloud computing research and development trend. *Future Networks, 2010. ICFN" 10. Second International Conference on*, 0: pp. 93–97.

Corresponding Author

Ankit Bansal*

Assistant Professor, Gulzar Group of Institutes, Ludhiana

erankitbansal@gmail.com