ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

Cloud Computing: An Introspection

Rohit Kumar[1]

M. Tech. Scholar, Department of Information Technology,

ABV-Indian Institute of Information Technology and Management, Gwalior, Madhya Pradesh, India

Abstract: Cloud Computing has proven its importance in IT era. Now a days, we want a technology that suits our growing needs and that also on very reasonable cost. Cloud computing shows itself as a best example of. Since every technology faces some issues regarding functioning and behaviour, the fact remains true with Cloud Computing also. It faces some serious security issues regarding access control, authentication, multi-tenancy, elasticity, etc. This Paper tries to give you a basic understanding of cloud computing, related simulators and explores the cloud computing aspects and then puts forward the issues related to its security.

Keywords: Cloud Computing, Access Control, Authentication, Multi-tenancy, Cloud Modeling and Simulation

I. INTRODUCTION

Cloud computing is considered as a new generation IT paradigm. It introduces its own features that make it beautiful. While incurring low cost, you may get benefits of fast data accessing. It is like a Pay For Your Fraction(PFYP) concept, since you are required only to pay for the fraction of resources that you actually use. Cloud computing has different working models and you can easily choose a specific one according to your need. Cloud Computing analogy is taken from real clouds since in its philosophy, resources are like clouds that may increase or decrease in number as per demand. Multiple users can use the resources at the same time, thus supporting the concept of parallelism and providing maximum resource utilization.

You can access and use your cloud resources from anywhere at anytime. But all these features come up with some "extra cost". This extra cost may be dictated in terms of Security Risks, involved in cloud computing usage and this fact hinders the popularity of cloud computing. Various measures are taken to audit and limit theses risks. This paper tries to explore the cloud computing aspects and put forward the related security risks issues.

II. CLOUD COMPUTING HISTORY

Cloud computing, or the cloud, is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet[1]. The concepts behind cloud computing dates back
to 1950s. At that time, large-scale mainframe computers became available in academia and corporations. These were accessed via thin clients/terminal computers, often referred to as "dumb terminals", called so because they were used for communications but had no internal processing capacities. To make a better use of costly mainframes, a practice was developed that allowed multiple users to share both the physical access to the computer from multiple terminals as well as to share the CPU time. This eliminated periods of inactivity on the mainframe and allowed for a greater return on the investment. The sharing of CPU time on a mainframe was known in industry as time-sharing. The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, autonomic, and utility computing have led to a growth in cloud computing[1].

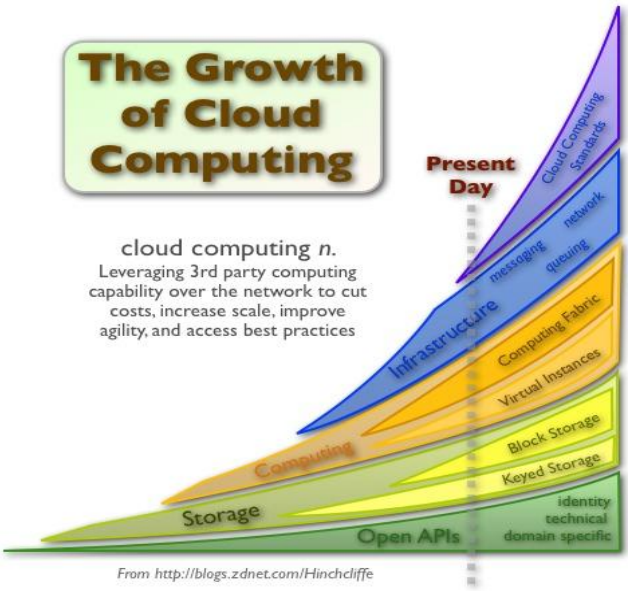


Fig 1. Cloud development Issues [19]

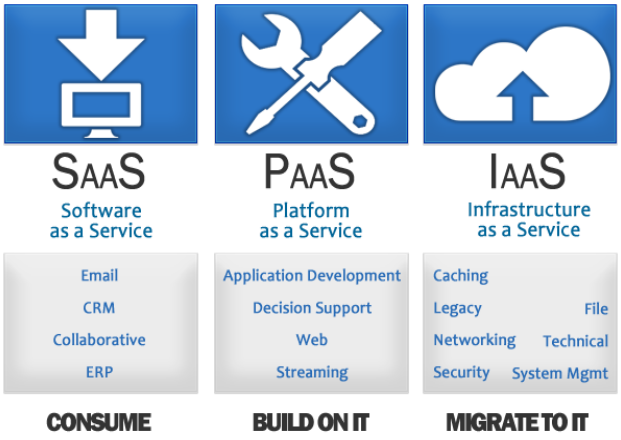
III. CLOUD COMPUTING ASPECTS

Cloud computing is a new technology and has several related aspects that make it different. To have a better understanding of cloud computing, one must have the basic views of these aspects. Some common cloud aspects are given below:

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

Fig 2. Cloud-based Service Models [20]



A. *Service Delivery Model*

Depending on your need, you can choose the proper cloud service delivery model. The three basic service delivery models are as follows [2] -

- Infrastructure-as-a-service(IaaS): Cloud providers deliver computation, storage and network resources.
- Platform-as-a-service(PaaS): Cloud providers deliver platform, tools and business services to develop, deploy and manage their applications.
- Software-as-a-Service(SaaS): Cloud providers give applications hosted on the cloud infrastructure for application implementation.

B. *Deployment Model*

A cloud architecture is created according to intended needs. According to different needs, the cloud environments are categorized, basically in three categories.

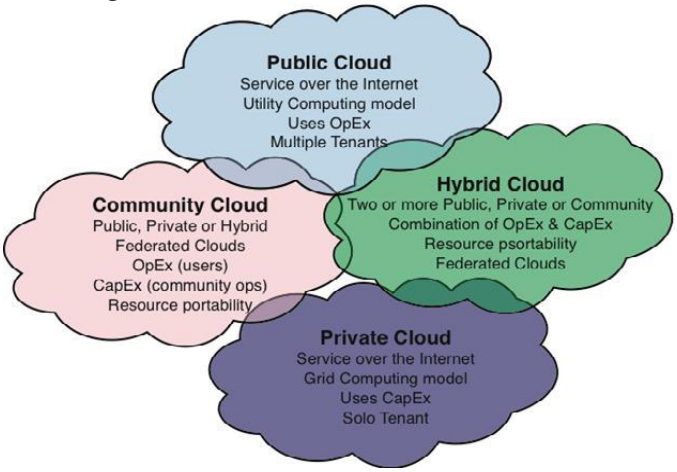


Fig 3. Cloud-based Deployment Models [21]

Thus, the three general deployment model are as follows[2]:

- Private cloud: A cloud platform dedicated for specific organization.
- Public cloud: A cloud platform available to public users to register and use the available infrastructure.
- Hybrid cloud: A private cloud that can extend to use resources in public clouds.
- Community cloud: A cloud environment accessible only by organizations with similar interests.

C. *Stakeholders*

In cloud computing different stakeholders are involved. Each stakeholder has their own security management systems/processes and each one has their own expectations (requirements) and capabilities (delivered) from/to other stakeholders[18]. The cloud computing model has following involved stakeholders[3]:

- Cloud provider (an entity that deliver infrastructure to the cloud consumers)
- Service provider (an entity that uses the cloud infrastructure to deliver applications/services to end users)
- Service consumer (an entity that uses services hosted on the cloud infrastructure).

D. *Single Cloud/ Multi-Cloud*

When cloud user have their services only from a single cloud provider. The scenario comes under Single Cloud category. But dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multi-clouds", "intercloud" or "cloud-of-clouds"[4]. In this cloud users access services from more than one cloud.

IV. MODELING AND SIMULATION

Currently, modeling and simulation technology has become a useful and powerful tool in cloud computing research community to deal with related issues[5]. As the experimentation in a real environment is expensive, time costly, and not repeatable, it is often hard to analyze the performance and security issues on actual cloud environments.

Therefore, modeling and simulation technology becomes increasingly popular in the cloud industry and academy[5]. We summarize cloud computing simulators proposed in the literature which are aimed to evaluate the performance and security of cloud computing systems, and describe the main features of these simulators :

A. *Cloudsim*

It provides a generalized, and extensible simulation framework that enables seamless modeling, simulation, and experimentation of emerging Cloud computing infrastructures and application services. Researchers and industry-based developers can focus on specific system design issues that they want to investigate, using CloudSim. They are not required to concern about the low level details of Cloud-based infrastructures and services[7].

B. CloudAnalyst

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

In 2009, a new simulation tool CloudAnalyst was proposed that was directly based on CloudSim and extends some of the capabilities of CloudSim. This simulator can be applied to study the behavior of large scaled Internet application in cloud environment and separates the simulation experimentation exercise from a programming exercise. It also enables a modeler to repeatedly perform simulations and to conduct a series of simulation experiments with slight parameters variations in a quick and easy manner[8].

C. SPECI

SPECI stands for Simulation Program for Elastic Cloud Infrastructures. It is a simulation tool which allows exploration of aspects of scaling as well as performance properties of future Dcs. There is a rapid increase in the size of data centres (DCs) used to provide cloud computing services. Not all properties in the middleware that manages Dcs scale linearly with the number of components. Further, "normal failure" also complicates the assessment of the per-formance of a DC. Unlike other engineering domains, there are no well established tools that allow the prediction of the performance and behaviour of future generations of Dcs [9].

D. GreenCloud

Greencloud is a sophisticated packet-level simulator for energy-aware cloud computing data centers with a focus on cloud communications. It offers a detailed fine-grained modeling of the energy consumed by the data center IT equipment, such as computing servers, network switches, and communication links[6].

E. Open Cloud Testbed (OCT)

OCT is a wide area testbed and with its four data centers that are connected with a high performance 10Gb/s network, it can address the requirements of extremely large data streams that challenge other types of distributed infrastructure. Several utilities are developed to support the development of cloud computing systems and services, including novel node and network provisioning services, a monitoring system, and a RPC system[10].

F. Open Cirrus

Unlike existing alternatives, Open Cirrus(a cloud computing testbed) federates distributed data centers. It aims to stimulate innovation in systems and applications research and catalyze development of an open source service stack for the cloud[11].

G. GroudSim

GroundSim is an event-based simulator that needs just one simulation thread for scientific applications on grid and cloud environments. It is mainly dedicated for the IaaS, but it is easily extendable to support additional models[12].

H. NetworkCloudSim

Simulation tools allow researchers to rapidly evaluate the reliability and performance of their new algorithms on a large heterogeneous Cloud infrastructure. However, most of the solutions lack either advanced application models such as message passing applications and work-flows or scalable network model of data center. To fill this gap, a popular Cloud simulator(CloudSim) is extended with a scalable network and generalized application model, which permits a much precise evaluation of scheduling and resource provisioning policies to optimize the performance of a Cloud infrastructure[13].

I.EMUSIM

EMUSIM combines emulation (AEF) and simulation(CloudSim) to enable more accurate models of software artefacts (obtained via profiling during emulation) to be used during simulations. This is quite useful when the tester has no idea on the performance of the software under different levels of concurrency and parallelism, which hinders the utilization of simulation. These can replace in situ(back-side) experiments when such experiments would require a scale that is either unavailable for the tester or too expensive to run in a public Cloud[14]. The architecture automatically extracts information from application behavior via emulation and then uses this information to generate the corresponding simulation model[15].

J. DCSim

DCSim (Data Centre Simulator) is an extensible data centre simulator implemented in Java, designed to provide an easy framework for developing and experimenting withdata centre management techniques and algorithms. It is anevent-driven simulator, simulating a data centre offering IaaS to multiple clients. It focuses on modelling transactional, continuous workloads (such as a web server), but can be extended to model other workloads as well[16].

K. iCanCloud

iCanCloud has been designed to obtain a good trade-off between flexibility, accuracy, performance and scalability, which makes it a powerful simulation platform for designing, testingand analyzing both actual and non-existent architectures. In fact, complete high performance computing systems can be modeled using this simulation platform. The best feature of iCanCloud is its ability to model and simulate large environments (thousands of nodes) with a customizable level of detail. Distributed applications can be simulated using this framework[17].

V. CLOUD COMPUTING SECURITY RELATED ISSUES

There are many cloud areas that must be security-conscious. Since cloud computing uses the virtualization concept, thus it is necessary to give proper attention to all possible security related areas. Some common security related issues are[2][18]:

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

A. Multitenancy

It means that multiple tenants(clients) use the common resource(server). Cloud Computing uses Multi-tenancy as a basic principle, since it believes in the better utilization of resources. But it may cause to severe security problems since while allowing multiple tenants, you have to maintain proper
security policies and access control mechanisms.

B. Elasticity

It is a way to convey the message that the user should be able to increase/decrease its assigned resources according to need. But before releasing a resource, user should make it confirm that the resource doesn't have any related information
anymore.

C. Availability of Information

Information availability refers to proper access to data. But in cloud, since we work in a virtual environment then the information is stored far from your direct reach. Now there may be a possibility of server failures, cloud crash, etc. then the user will be in a condition of non-availability of information. Although high security measures are implemented but still there is a information security risk.

D. Secure Information Management

Cloud Management Layer(CML) is the microkernel that can be extended to incorporate and co-ordinate different components such as service monitoring, billing, services registry and securuty management of cloud. Any breach of this layer can cause malicious activities. Security Management should include security requirements and policies specifications derived from tenant organizations which are reviewed and applied in tenant's specific environment.

E. Information Integrity and Privacy

In a cloud environment, various organizations port their data to cloud but due to some flaws if the securiy of cloud
infrastructure is breached then information privacy, integrity and authentication issues come up.

F. Cloud Secure Federation

When users use services that depend on services from different clouds then there is a need to maintain security policies on both clouds and in between. Thus whenever two or more clouds integrate together to offer their combined services then their security requirements must be federated and enforced physically as well as logically.

G. Multiple Stakeholders

Different stakeholders have their different security management policies and these policies may conflict with each other since different stakeholders may have different backgrounds. Besides this, different tenants may have different trust levels with service provider and some tenants may itself be attackers. Thus complex trust issues are generated.

H. Third-Party Control

In cloud computing the owner of data has no control over its data processing. It means that the cloud user has to give up control over its IT assets. But to make this thing easy, cloud provider make the management and maintenance of cloud
services more transparent and audit-able by the customers. This should include recording logs and complete administrative sessions affecting the part of the cloud infrastructure used by the customer. And if customer demands it then it should be accessible. On the other side, cloud providers are not able to deliver efficient and effective security controls because they are not aware of the hosted service's architectures. Furthermore, cloud providers are faced with a lot of changes to security requirements while having a
variety of security controls deployed that need to be updated. This further complicates the cloud provider's security administrator's tasks.

VI. SECURITY ENABLERS FOR THE CLOUD

Maintaining a secure cloud environment is the today's necessity. By having following points in your mind, you can have a much secure cloud environment :

A. *Identity and Access Management*

Identity is the base of access control. To identify any entity you have to be in touch of an personal identity. Identity should identify the entity properly and uniquely but must not
disclose any private information. Cloud platforms should deliver or support a robust and consistent Identity management system. Identity information privacy, identity mapping, authentication, single sign on, authorization, etc. should be a part of this system.

B. *Key Management*

Proper key management should be done to keep the information confidential and the system consistent. Suitable encryption/decryption mechanisms should be employed.

C. *Security Management*

Due to huge no of stakeholders and deep dependency stack, maintaining security protocols and providing a consistent system becomes a challenge. Security management needs to properly identify the security requirements and having proper
feedback from environment at regular interval.

D. *Secure Software Development Life-cycle:*

While developing softwares for a cloud environment, the process should be slightly modified to include the security aspect. SDLC should involve proper security measure at each step like calculating risk factor etc. to make a consistent software.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

E. *Security Performance and Optimization*

Adopted Security Measures affect the performance of underlying services adversely. So while implementing security measures we should have a constant sight on the system performance parameter also. So we should try to make a proper balance between both.

F. *Federation of security between clouds*

In case of multi-cloud services, a user is required to have a federated account of security requirements, since it avails the facilities from more than one cloud platform and it has to confront with all involved cloud platform issues.

VII. CONCLUSION

As we have discussed about the cloud computing basics, concepts, related issues, simulation environments, key security areas and other things, so now we can say that the cloud computing has potential to deal with future needs and it will be a milestone of future computation architectures. But we need to work on some areas to improve its performance index and to make it a more suitable candidate for future needs. Cloud is a revolutionary technology and with its proper development, it can change the face of almost all computational models.

VIII. ACKNOWLEDGMENT

We are grateful to our director Prof. S.G Deshmukh for his motivation for research oriented works. Thanks and appreciation to the helpful people at ABV-IIITM Gwalior.

REFERENCES

[1] http://en.wikipedia.org/wiki/Cloud_computing
[2] Akhil Behl, Kanika Behl "An Analysis of Cloud Computing Security Issues" 2012 IEEE
[3] Anas BOUAYAD, Asmae BLILAT, Nour el houda MEJHED, Mohammed EL GHAZ "Cloud computing : security challenges" 2012 IEEE
[4] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom "Cloud Computing Security: From Single to Multi-Clouds" 2012 45th Hawaii International Conference on System Sciences
[5] Wei Zhao, Yong Peng, Feng Xie, Zhonghua Dai "Modeling and Simulation of Cloud Computing: A Review" 2012 IEEE Asia Pacific Cloud Computing Congress (APCloudCC)
[6] http://greencloud.gforge.uni.lu/
[7] http://www.cloudbus.org/cloudsim/
[8] Wei Zhao, Yong Peng, Feng Xie, Zhonghua Dai "Modeling and Simulation of Cloud Computing:A Review" 2012 IEEE Asia Pacific Cloud Computing Congress (APCloudCC)
[9] Iango Sriram "SPECI, a simulation tool exploring cloud scale data centres" CloudCom 2009, LNCS 5931, pp. 381-392
[10] Robert Grossman, Yunhong Gu, Michal Sabala, Collin Benner, Jonathan Seidman and Joe Mambratti "The Open Cloud Testbed: A Wide Area Testbed for Cloud Computing Utilizing High Performance Network Services. "
[11] http://www.cs.cmu.edu/~droh/papers/opencirrus ieeecomputer.pdf
[12] http://students.cec.wustl.edu/~azinoujani/
[13] Saurabh Kumar Garg and Rajkumar Buyya "NetworkCloudSim: Modelling Parallel Applications in Cloud Simulations" 2011 Fourth IEEE International Conference on Utility and Cloud Computing.
[14] http://www.cloudbus.org/cloudsim/emusim/
[15] Rodrigo N. Calheiros, Marco A. S. Netto, Cesar A. F. De Rose, Rajkumar Buyya "EMUSIM: An Integrated Emulation and Simulation Environmentfor Modeling, Evaluation, and Validation of Performance of Cloud Computing Applications" 2012
[16] Michael Tighe, Gaston Keller, Michael Bauer, Hanan Lutfiyya "DCSim: A Data Centre Simulation Tool for Evaluating Dynamic Virtualized Resource Management" 2012 IFIP
[17] Gabriel G. Castane, Alberto Nunez, Jesus Carretero "iCanCloud: A brief architecture overview" 2012 10th IEEE International Symposium on Parallel and Distributed Processing with Applications
[18] Huaglory Tianfield "Security Issues In Cloud Computing" 2012 IEEE International Conference on Systems, Man, and Cybernetics
[19] http://storagenerve.com/2009/09/17/cloud-the-quest-for-standards/
[20] http://www.azureadvantage.co.uk/aboutazure/cloudcomputing/Pages /default.aspx
[21] http://cavdar.net/cloud-computing/