International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

CONFRONT AND ISSUES IN CLOUD COMPUTING PLATFORMS AND APPLICATIONS

Dr. Rupak Sharma[1], Dr. Rajeev Sharma

[1,2]*Asst. Professor Dept. of Computer Applications*

SRM University NCR campus Modinagar-201204 (India)

ABSTRACT

Cloud computing represents both the hardware and the software delivered as services over the Internet .The cloud Computing is an innovative notion that defines the use of computing as a utility, that has recently attracted significant attention. Cloud computing is a relatively recent term, builds on decades of research in virtualization, distributed computing, utility computing, and more recently networking, web and software services. Cloud computing is an emerging model of business computing. In this paper, we explore the concept of cloud architecture and compares cloud computing with grid computing. We also address the characteristics and applications of several popular cloud computing platforms the concept of virtualization needs to be understand and implement in the cloud computing systems, which enables the user as well as the owners for the better and robust management and usage of the cloud. This paper discusses the concept of "cloud" computing, some of the issues it tries to address, related research topics, and a "cloud" implementation available today. We identified several challenges from the cloud computing adoption perspective and we also highlighted the cloud interoperability issue that deserves substantial further research and development. However, security and privacy issues present a strong barrier for users to adapt into cloud computing systems.

***Keywords*— Cloud computing, architecture, challenges, cloud platforms, research issues, Virtualization**

Definition

A cloud is a pool of virtualized computer resources. A cloud can:

Host a variety of different workloads, including batch-style back-end jobs and interactive, user-facing applications. Allow workloads to be deployed and scaled-out quickly through the rapid provisioning of virtual machines or physical machines.

Support redundant, self-recovering, highly scalable programming models that allow workloads to recover from many unavoidable hardware/software failures .Monitor resource use in real time to enable rebalancing of allocations when needed.

I.INTRODUCTION

Cloud computing is the next natural step in the evolution of on demand information technology services and products. It is the development of parallel computing, distributed computing grid computing, and is the combination and evolution of Virtualization, Utility computing, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). Cloud is a metaphor to describe web as a space where computing has been pre installed and exist as a service; data, operating systems, applications, storage and processing power exist on the web ready to be shared. To users, cloud computing is a Pay-per-Use-On-Demand mode that can conveniently access shared IT resources through the Internet. Where the IT resources include network, server, storage, application, service and so on and they can be deployed with much quick and easy manner and least management and also interactions with service providers. Cloud computing can much improve the availability of IT resources and owns many advantages over other computing techniques. Users can use the IT infrastructure with Pay-per-Use-On-Demand mode; this would benefit and save the cost to buy the physical resources that may be vacant.

II.COMPARISION BETWEEN CLOUD AND GRID COMPUTING

A comparison [6] can be summaries as follows:

a. Construction of the grid is to complete a specified task, such as biology grid, Geography grid, national educational grid, while Cloud computing is designed to meet general application and there are not grid for a special field.
b. Grid emphasizes the “resource sharing” to form a virtual organization. Cloud is often owned by a single physical organization (except the community Cloud, in this case, it is owned by the community), who allocates resources to different running instances.
c. Grid aims to provide the maximum computing capacity for a huge task through resource sharing. Cloud aims to suffice as many small-to-medium tasks as possible based on users’ real-time requirements. Therefore, multi-tenancy is a very important concept for Cloud computing.

d. Grid trades re-usability for (scientific) high performance computing. Cloud computing is directly pulled by immediate user needs driven by various business requirements.
e. Grid strives to achieve maximum computing. Cloud is after on-demand computing – Scale up and down, in and out at the same time optimizing the overall computing capacity.

II.VIRTUALIZATION

Virtualization is another very useful concept. It allows abstraction and isolation of lower level functionalities and underlying hardware. This enables portability of higher level functions and sharing and/or aggregation of the physical re-sources.

The virtualization concept has been around in some form since 1960s (e.g., in IBM main-frame systems). Since then, the concept has matured considerably and it has been applied to all aspects of computing – memory, storage, processors, software, networks, as well as ser-vices that IT offers. It is the combination of the growing needs and the recent advances in the IT architectures and solutions that is now bringing the virtualization to the true commod-ity level. Virtualization, through its economy of scale, and its ability to offer very advanced and complex IT services at a reasonable cost, is poised to become, along with wireless and highly distributed and pervasive computing de-vices, such as sensors and personal cell-based access devices, the driving technology behind the next waive in IT growth [44].

Not surprisingly, there are dozens of virtualiza-tion products, and a number of small and large companies that make them. Some examples in the operating systems and software applica-tions space are VMware[1], Xen – an open source

Linux-based product developed by XenSource[2],and Microsoft virtualization products[3], to men-tion a few. Major IT players have also shown a renewed interest in the technology (e.g., IBM, Hewllet-Packard, Intel, Sun, RedHat). Classi-cal storage players such as EMC, NetApp, IBM and Hitachi have not been standing still either. In addition, the network virtualization market is teeming with activity.

III.CLOUD SERVICE MODELS

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

Cloud service models are commonly divided into SaaS, PaaS, and IaaS that exhibited by a given cloud infrastructure. It's helpful to add more structure to the service model stacks: Fig. 2 shows a cloud Service model [13] that makes the most important security-relevant cloud components explicit and provides an abstract overview of cloud computing for security issue analysis.

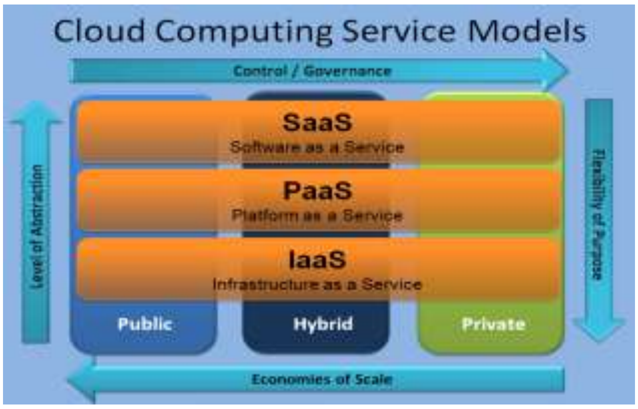

Fig. 2. The cloud Service model.

Software as a Service (SaaS)

Software-as–a-Service (SaaS) model allows to provide software application as a service to the end users. It refers to a software that is deployed on a host service and is accessible via Internet. There are several SaaS applications like Billing and invoicing system, Customer Relationship Management (CRM) applications, Help desk applications, Human Resource (HR) solutions. Some of the SaaS applications are not customizable such as Microsoft Office Suite. But SaaS provides us Application Programming Interface (API),which allows the developer to develop a customized application.

Platform as a Service (PaaS)

Platform-as-a-Service offers the runtime environment for applications. It also offers development and deployment tools required to develop applications. PaaS has a feature of point-and-click tools that enables non-developers to create web applications. App Engine of Google and Force.com are examples of PaaS offering vendors. Developer may log on to these websites and use the built-in API to create web-based applications. But the disadvantage of using PaaS is that, the developer locks-in with a particular vendor. For example, an application written in Python against API of Google, and using App Engine of Google is likely to work only in that environment.

Infrastructure as a Service (IaaS)

Cloud consumers directly use IT infrastructures (processing, storage, networks and other fundamental computing resources) provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers. The basic strategy of virtualization is to set up independent virtual machines (VM) that are isolated from both the underlying hardware and other VMs. Notice that this strategy is different from the multi-tenancy model, which aims to transform the application software architecture so that multiple instances (from multiple cloud consumers) can run on a single application (i.e. the same logic machine). An example of IaaS is Amazon's EC2.

Data as a Service (DaaS)

The delivery of virtualized storage on demand becomes a separate Cloud service - data storage service. Notice that DaaS could be seen as a special type IaaS. The motivation is that on-premise enterprise database systems are often tied in a prohibitive upfront cost in dedicated server, software license, post-delivery services and in-house IT maintenance. DaaS allows consumers to pay for what they are actually using rather than the site license for the entire database. In addition to traditional storage interfaces such as RDBMS and file systems, some DaaS offerings provide table-style abstractions that are designed to scale out to store and retrieve a huge amount of data within a very compressed timeframe, often too large, too expensive or too slow for most commercial RDBMS to cope with. Examples of this kind of DaaS include Amazon S3, Google BigTable, and Apache HBase, etc.

Network as a Service (NaaS):

Network-as-a-Service allows us to access to network infrastructure directly and securely. NaaS makes it possible to deploy **custom routing protocols.** NaaS uses **virtualized network infrastructure** to provide network services to the customer. It is the responsibility of NaaS provider to maintain and manage the network resources.

Having a provider working for a customer decreases the workload of the customer. Moreover, NaaS offers **network as a utility.** NaaS is also based on **pay-per-use model.**

IV.CLOUD COMPUTING PLATFORMS

i. AbiCloud

Abicloud [5] is a cloud computing platform, It can be used to build, integrate and manage public as well as private cloud in the homogeneous environments. Using Abicloud, user can easily and automatically deploy and manage the server, storage system, network, virtual devices and applications and so on. The main difference between Abicloud and other cloud computing platforms is its powerful web-based management function and its core encapsulation manner. Using the Abicloud, user can finish deploying a new service by just dragging a virtual machine with mouse. This is much easier and flexible than other cloud computing platforms that deploy new services through command lines.

Abicloud can be used to deploy and implement private cloud as well as hybrid cloud according to the cloud providers' request and configuration. It can also manage EC2 according to the rules of protocol. Besides, apply the Abicloud, a whole cloud platform based on Abicloud can be packed and redeployed at any other Abicloud platform. This is much helpful for the transformation of the working environment and will make the cloud deployment process much easier and flexible.

ii.Eucalyptus

Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems) [5] mainly was used to build open-source private cloud platform. Eucalyptus is an elastic computing structure that can be used to connect the users' programs to the useful systems, it is an open-source infrastructure using clusters or workstation implementation of elastic, utility, cloud computing and a popular computing standard based on a service level protocol that permit users lease network for computing capability.

Currently, Eucalyptus is compatible with EC2 from Amazon, and may support more other kinds of clients with minimum modification and extension.

iii.Nimbus

Nimbus [5] is an open tool set and also a cloud computing solution providing IaaS. It permits users lease remote resources and build the required computing environment through the deployment of virtual machines.

Generally, all these functional components can be classified as three kinds. One kind is client- supported modules which are used to support all kinds of cloud clients. Context client module, cloud client module, reference client module and EC2 client module are all belonging to this kind of component. The second kind of component is mainly service-supported modules of cloud platform, providing all kinds of cloud services. It includes a context agent module, web service resource framework module, EC2 WSDL module and a remote interface module. The third kind of component is the background resource management modules which are mainly used to manage all kinds of physical resources on the cloud computing platform, including work service management module, IaaS gateway module, EC2 and other cloud platform support module, workspace pilot module, workspace resource management module and workspace controller.

iv.OpenNebula

OpenNebula [5] is also an open source cloud service framework. It allows user deploy and manage virtual machines on physical resources and it can set user's data centers or clusters to flexible virtual infrastructure that can automatically adapt to the change of the service load. The main difference of OpenNebula and nimbus is that nimbus implements remote interface based on EC2 or WSRF through which user can process all security related issues, while OpenNebula does not. OpenNebula is also an open and flexible virtual infrastructure management tool, which can use to synchronize the storage, network and virtual techniques and let users dynamically deploy services on the distributed infrastructure according to the allocation strategies for data center and remote cloud resources. Through the interior interfaces and OpenNebula data center environment, users can easily deploy any types of clouds.

V.APPLICATIONS

There are a few applications of cloud computing [4] as follows:

1) Cloud computing provides dependable and secure data storage center. Cloud computing can realize data sharing between different equipments.

2) The cloud provides nearly infinite possibility for users to use the internet.

3) Cloud computing does not need high quality equipment for the user and it is easy to use.

VI.ISSUES IN CLOUD COMPUTING

More and more information on individuals and companies is placed in the cloud; concerns are beginning to grow about just how safe an environment it is? Issues of cloud computing can summarize as follows:

i.Privacy

Cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data centers rather than stay in the same physical location, users may leak hidden information when they are accessed cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

ii.Reliability

The cloud servers also experience downtimes and slowdowns as our local server.

iii.Legal Issues

Worries stick with safety measures and confidentiality of individual all the way through legislative levels.

iv.Compliance

Numerous regulations pertain to the storage and use of data requires regular reporting and audit trails. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements.

v.Freedom

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers.

vi.Long- Term Viability

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company.

VII.ISSUES IN CLOUD INTEROPERABILITY

a. Intermediary Layer

A number of recent works address the interoperability issue by providing an intermediary layer between the cloud consumers and the cloud-specific resources (e.g. VM).

b. Open Standard

Standardization appears to be a good solution to address the interoperability issue. However, as cloud computing just starts to take off, the interoperability problem has not appeared on the pressing agenda of major industry cloud vendors.

c. Open API

SUN has recently launched the Sun Open Cloud Platform under the Creative Commons license. A major contribution of this platform is the proposed (in-progress) the cloud API. It defines a set of clear and easy-to-understand RESTful Web services interfaces, through which cloud consumers are able to create and manage cloud resources, including compute, storage, and networking components in a unified way.

d. SaaS and PaaS Interoperability

While the aforementioned solutions generally tackle with IaaS interoperability problems, SaaS interoperability often involves different application domains such as ERP, CRM, etc. A group of experts in the field of data mining raises the issue of establishing a data mining standard on the cloud, with a particular focus on “the practical use of statistical algorithms, reliable production deployment of models and the integration of predictive analytics” across different data mining-based SaaS clouds. PaaS interoperability not yet discovered Since PaaS involves the entire software development life-cycle on the cloud, it would be more difficult to reach the uniformity with regards to the way consumers develop and deploy cloud applications.

VIII.SECURITY AND PRIVACY ISSUE

The security and privacy-related challenges in cloud computing. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing leads to several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure.

Finally, data mining techniques may be applicable for malware detection in the clouds As shown in Figure 2, there are six specific areas of the cloud computing environment where equipment and software require substantial security attention (Trusted Computing Group’s White Paper, 2010). These six areas are: (1) security of data at rest, (2) security of data in transit, (3) authentication of users/applications/ processes, (4) robust separation between data belonging to different customers, (5) cloud legal and regulatory issues, and (6) incident response. For securing data at rest, cryptographic encryption mechanisms are certainly the best options. The hard drive manufacturers are now shipping self-encrypting drives that implement trusted storage standards of the trusted computing group (Trusted Computing Group’s White Paper, 2010).

These self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Although software encryption can also be used for protecting data, it makes the process slower and less secure since it may be possible for an adversary to steal the encryption key from the machine without being detected. 8 Encryption is the best option for securing data in transit as well. In addition, authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit. Strong authentication is a mandatory requirement for any cloud deployment. User authentication is the primary basis for access control. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. The trusted computing group’s (TCG’s) IF-MAP standard allows for real-time communication between a cloud service provider and the customer about authorized users and other security issues. When a user’s access privilege is revoked or reassigned, the customer’s identity management system can notify the cloud provider in real-time so that the user's cloud access can be modified or revoked within a very short span of time.

One of the more obvious cloud concerns is separation between a cloud provider's users (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers. Technologies are currently available that can provide significant security improvements for VMs and virtual network separation.

IX.CHALLENGES ON CLOUD ADOPTION PERSPECTIVE

Based on a survey conducted by IDC in 2008[1]

A. Security

Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to an organization's data and software. The multi - tenancy model and the pooled computing resources on cloud computing has introduced new security challenges such as shared resources (hard disk, data, VM) on the same physical machine invites unexpected side channels between a malicious resource and a regular resource. And, the issue of "reputation fate-sharing" will severely damage the reputation of many good Cloud "citizens" who happen to, unfortunately, share the computing resources with their fellow tenant - a notorious user with a criminal mind. Since they may share the same network address, any bad conduct will be attributed to all the users without differentiating real sub verters from normal users.

B. Costing Model

Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication.

C. Charging Model

From a cloud provider's perspective, the elastic resource pool (through either virtualization or multi-tenancy) has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions on static computing.

D. Service Level Agreement

It is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers.

X.CONCLUSION

This paper discussed the architecture and popular platforms of cloud computing. It also addressed challenges and issues of cloud computing in detail. In spite of the several limitations and the need for better methodologies processes, cloud computing is becoming a hugely attractive paradigm, especially for large enterprises.

Cloud Computing initiatives could affect the enterprises within Five to Six years as it has the potential to significantly change IT.

REFERENCES

[1] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," *2010 24th IEEE International Conference on Advanced Information Networking and Applications(AINA)*, pp. 27-33, DOI= 20-23 April 2010

[2] M. Q. Zhou, R. Zhang, W. Xie, W. N. Qian, and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," *2010 Sixth International Conference on Semantics, Knowledge and Grids(SKG)*, pp.105-112, DOI= 1-3 Nov. 2010

[3] J. F. Yang and Z. B. Chen, "Cloud Computing Research and Security Issues," *2010 IEEE International Conference on Computational Intelligence and Software Engineering (CiSE)*, Wuhan pp. 1-3, DOI= 10-12 Dec. 2010.

[4] S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "Cloud Computing Research and Development Trend," In *Proceedings of the 2010 Second International Conference on Future Networks* (ICFN '10). IEEE Computer Society, Washington, DC, USA, pp. 93-97. DOI=10.1109/ICFN.2010. 58.

[5] J. J. Peng, X. J. Zhang, Z. Lei, B. F. Zhang, W. Zhang, and Q. Li, "Comparison of Several Cloud Computing Platforms," *2009 Second International Symposium on Information Science and Engineering (ISISE '09)*. IEEE Computer Society, Washington, DC, USA, pp. 23-27, DOI=10.1109/ISISE.2009.94.

[6] S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "The Comparison between Cloud Computing and Grid Computing," *2010 International Conference on Computer Application and System Modeling (ICCASM)*, pp. V11-72 - V11-75, DOI= 22-24 Oct. 2010.

[7] M. M. Alabbadi, "Cloud Computing for Education and Learning: Education and Learning as a Service (ELaaS)," *2011 14th International Conference on Interactive Collaborative Learning (ICL)*, pp. 589 – 594, DOI=21-23 Sept. 2011.

[8] P. Kalagiakos "Cloud Computing Learning," *2011 5th International Conference on Application of Information and Communication Technologies (AICT)*, Baku pp. 1 - 4, DOI=12-14 Oct. 2011.

[9] P. Mell and T. Grance, "Draft nist working definition of cloud computing -vol. 21, Aug 2009, 2009.

[10] "Sun Microsystems Unveils Open Cloud Platform," [Online]. Available: http://www.sun.com/aboutsun/pr/2009-03/sunflash.20090318.2.xml,2 009.

[11] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a Service Security: Challenges and Solutions," *2010 7th International Conference on Informatics and System*, pp. 1-8, March 2010.

[12] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," *2009 8th IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2009, pp. 711-716.

[13] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," *2011 IEEE Security and Privacy*, pp. 50-57, DOI= March/April 2011.

[14] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," *Proceedings of the 44th Hawaii International Conference on System Sciences*, 2011.