AN OVERVIEW OF CLOUD COMPUTING IN DISTRIBUTED SYSTEMS

Usha Divakarla[1] and Geetha Kumari[2]

[1,2]Birla Institute of Technology and Sciences/CSIS, Hyderabad, India

Abstract: Cloud computing is the emerging trend in the field of distributed computing. Cloud computing evolved from grid computing and distributed computing. Cloud plays an important role in huge organizations in maintaining huge data with limited resources. Cloud also helps in resource sharing through some specific virtual machines provided by the cloud service provider. This paper gives an overview of the cloud organization and some of the basic security issues pertaining to the cloud.

Keywords: cloud computing, virtualization, cloud layers, security

I. INTRODUCTION

Cloud computing evolves from grid computing and provides on-demand resource provisioning. Grid computing may or may not be in the cloud depending on what type of users are using it. If the users are systems administrators and integrators, they care how things are maintained in the cloud. They upgrade, install, and virtualize servers and applications. If the users are consumers, they do not care how things are run in the system.

Definition:Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].

II.ESSENTIAL CHARACTERISTICS

On-demand service : A consumer can unilaterally provide computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. ***Broad network access****:* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling*:* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity*:* Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.

Measured Service*:* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Virtualization: Virtualization is a technique of resource sharing that is based on the principle of dividing physical resources(HW) or operating systems(SW)for cost control measures and more efficient utilization of resources.

Types of virtualization

Full virtualization :A technique used to provide a certain kind of virtual machine environment, namely, one that is complete simulation of the underlyinghardware.

Para-virtualization: A technique that presents a software to the virtual machines that is similar but not identical to that of the underlying hardware.

Emulation: hardware emulation is all about using standard virtualization software (also called a Hyper Visor) to form a emulated hardware environment (Called VMM -- Virtual Machine Monitor), for guest operating systems to function on.

OS virtualization: OS allows multiple secure virtual servers to be run. Guest OS is the same as the host OS, but appears isolated.

Application virtualization: Application is gives its own copy of components that are not shared.

III.SERVICE MODELS

Cloud Software as a Service (SaaS)*:* The consumer use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

CP1324, International Conference on Methods and Models in Science and Technology (ICM2ST-10)
edited by R.B.Patel and B.P.Singh

Cloud Platform as a Service (PaaS).The consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the cloud infrastructure , but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS)

The consumer has the capability to provision processing, storage, networks, and other fundamental computing resources. The consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

IV.DEPLOYMENT MODELS

Private cloud:The cloud infrastructure is operated solely for an organization.

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

Public cloud:The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud:The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

V.CLOUD LAYERS

Software-as-a-Service (Saas)
Platform-as-a-Service(Paas) [developers implementation]
Infrastructure-as-a-Service(Iaas) [virtualization, storage Network]
Hardware-as-a-Service

Figure 5 cloud layers[2]

Client: A *cloud client* consists of computer hardware and/or computer software that relies on cloud computing for application delivery, or that is specifically designed for delivery of cloud services.

Application: Cloud application services or "*Software as a Service (SaaS)*" deliver software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers andsimplifying maintenance and support

Platform: Cloud platform services or "*Platform as a Service (PaaS)*" deliver a computing platform and/or solution stack as a service, often consuming *cloud infrastructure* and sustaining *cloud applications*. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers[3].

Infrastructure: Cloud infrastructure services or "*Infrastructure as a Service (IaaS)*" delivers computer infrastructure typically a platform virtualization environment as a service.

Server[Haas]: The *servers* layer consists of computer hardware and/or computer software products that are specifically designed for the delivery of cloud services, including multi-core processors, cloud-specific operating systems and combined offerings.

VI.BASIC CHALLENGES IN CLOUD COMPUTING

Four issues stand out with cloud computing: threshold policy, interoperability issues, hidden costs, and unexpected behavior[2][4].

Threshold policy: To test if the program works, develop, or improve and implement, a threshold policy in a pilot study before moving the program to the production environment. Check how the policy detects sudden increases in the demand and results in the creation of additional instances to fill in the demand. Also check to determine how unused resources are to be de-allocated and turned over to other work.

Interoperability issues: . The problems of achieving interoperability of applications between two cloud computing vendors. Need to reformat data or change the logic in applications.

Hidden costs : Cloud computing does not tell what hidden costs are. In an instance of incurring network costs, companies who are far from the location of cloud providers could experience latency, particularly when there is heavy traffic.

Unexpected behavior : The tests to be made to show unexpected results of validation or releasing unused resources. Need to fix the problem before running the application in the cloud.

Also other issues are[5][6][7][8]:

Cloud providers must work together to ensure that the challenges to cloud adoption are addressed through open collaboration and the appropriate use of standards.

Cloud providers must not use their market position to lock customers into their particular platforms and limiting their choice of providers.

Cloud providers must use and adopt existing standards wherever appropriate. The IT industry has invested heavily in existing standards and standards organizations; there is no need to duplicate or reinvent them.

When new standards (or adjustments to existing standards) are needed, we must be judicious and pragmatic to avoid creating too many standards. We must ensure that standards promote innovation and do not inhibit it.

Any community effort around the open cloud should be driven by customer needs, not merely the technical needs of cloud providers, and should be tested or verified against real customer requirements.

VII. SECURITY ISSUES

Though the above said challenges are existing in cloud computing, security is the major concern. Security in terms of data handling, maintaining, migrating or virtualization in clouds

Security concerns in cloud are not that different from non-cloud service offerings although they are exasperated – because in a single-tenant, non-cloud environment we generally know where information is and how it's being kept. With lots of different customers, that isolation of that data is not appropriately maintained[9][10].

Providers have to manage service and isolation of potentially millions of customers and this presents a challenge as we see infrastructure and applications scale to address consumption at this level.

Every cloud service provider has a different cloud model like: A Saas provider may be relying on other external providers for its backbone, infrastructure and data storage.

Cloud computing places business data into the hands of an outside provider, cloud computing makes regulatory compliance inherently riskier and more complex than it is when systems are maintained in-house. Loss of direct oversight means that client company must verify that service provider is working to ensure that the data security and integrity are ironclad.[11]

Cloud computing compliance is difficult as the customer does not know where the data is stored and how is it manipulated as the service provider is not clearly known.

As there are no specified rules for virtualization cloud providers follow their own rules which later creates challenges for service providers.

VIII. CONCLUSION

Cloud computing though resolves many problems like mass storage area, computing, resource sharing in distributed systems, it still has many problems to solve in it. This paper throws light on some of the technical security issues in cloud computing.

The future work could be to find better SOA for cloud computing, complying better rules for cloud service providers, better data retrieval methods.

REFERENCES

[1] The NIST Definition of Cloud Computing by Peter Mell and Tim Grance

[2] A taxonomy and survey of cloud computing systems by bhaskar Prasad rimol, 978-0-7695-3769-6/09 $26.00 © 2009 IEEE

[3] Google angles for business users with 'platform as a service' by Jack Schofield

[4] Gartner: Seven cloud-computing security risks by By Jon Brodkin

[5] Providing Privacy Preserving in cloud computing by Jian Wang Yan Zhao Shuo Jiang Jiajin Le , 978-1-4244-4700-8/09/$25.00 ©2009 IEEE

[6] A Cloud Computing Platform Based on P2P by KeXu 1, Meina Song 2, Xiaoqi Zhang 3, Junde Song4, 978-1-4244-3930-0/09/$25.00 ©2009 IEEE.

[7] The case of cloud computing by Robert L grossan 1520-9202/09/$25.00 © 2009 IEEE.

[8] On Technical Security Issues in Cloud Computing by Meiko Jensen, *De*, Nils Gruschka, Luigi Lo Iacono, 978-0-7695-3840-2/09 $25.00 ©2009 IEEE

[9] Cloud Computing Could Pose Serious Security Issues by James Zipadelli.

[10] Finding the Intersections of SOA and Cloud Computing by David Linthicum.

[11] Security issues that effect cloud computing data storage by martin Bioh