Key infrastructure elements for cloud computing

S.J.Mohana[1], M.Saroja[2], M.Venkatachalam[3]
[1,2,3,] of Computer Applications, Erode Arts and Science college,Erode, India)

Abstract

Clouds consist of a collection of virtualized resources, which include both computational and storage facilities that can be provisioned on demand, depending on the users' needs. users are charged on a pay-per-use basis. This paper gives a quick overview of cloud and describes the key infrastructure elements for cloud computing. This paper is a brief survey based of readings on "cloud" computing and it tries to address, related research topics and challenges ahead.

Keywords – cloud computing, middleware, hypervisor, security,management, virtualization.

1. Introduction

Cloud computing has been the most prevalent technology in the past few years. Cloud computing is a model for enabling ubiquitous, 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]. Cloud providers should satisfy customers' various workload requirements. When cost of operating cloud resource is considered, then the makespan also becomes an important issue. The Cloud is drawing the attention from the Information and Communication Technology community because of the set of services with common characteristics, provided by important industry players. However, existing technologies of cloud computing such as virtualization, utility computing and distributed computing are not new.

2. Types Of Cloud

Clouds can be classified as public, private, community or hybrid depending on the model of deployment. A private cloud is the cloud infrastructure owned or leased by a single organization and is operated solely for that organization. A public cloud is owned by an organization selling cloud services to the general public or to a large industry group. A Community cloud is shared by several organizations and supports a specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance considerations). A hybrid cloud is a composition of two or more clouds (private, community, or public) that are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting).

3. Key Characteristics

On-demand self-service*: Without human intervention, cloud user should be able to use* computing apabilities, such as server time and network storage, as and when needed.

Pay per use: cloud users are charged for what they use. The pricing model depends on the quality and uantity of services consumed [2] . Some of the factors considered for billing includes measuring storage, andwidth and consumption of computing resources.

Ubiquitous network access *:* Ubiquitous network access allows all users to access any kind of information at anytime, and from anywhere.

Location independent resource pooling: The provider's computing resources are pooled to serve all consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand[3]. Location of the cloud resources are abstracted from the consumers. Some of the cloud resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity: cloud computing has the ability to scale resources up and down as needed. For the consumers, the cloud resources available for rent appear to be infinite and can be purchased in any quantity at any time.

4. Architectural Blocks

The key infrastructural elements of cloud are hardware& networking, hypervisor , middleware, security &management

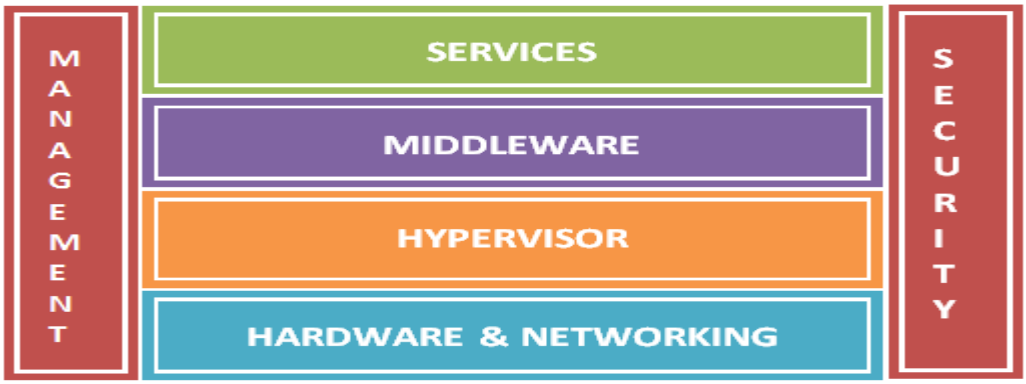

Figure 1: cloud architectural blocks

4.1 Hardware and Networking

The lower layer of cloud infrastructure has hardware and networking devices. It includes storage devices, ervers, cooling units, power units , other hardware and networking components.

4.2 Hypervisor

A hypervisor can also be termed as virtual machine manager. It is a software that allows more than one operating systems to share a single hardware host. Each operating system appears to have the host machines resources all to itself.However, the virtual machine manager is actually controlling and allocating the host machine's resources to each operating system. Hypervisor also makes sure that virtual machines cannot disrupt each other.

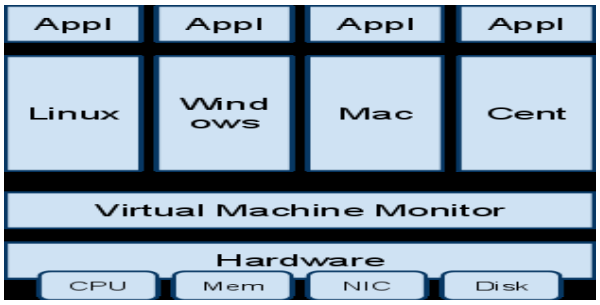

Figure 2 : virtual machines

Basically, there are two kinds of server virtualization techniques: full virtualization and para virtualization. In full virtualization Virtual machine talks to hypervisor which communicates with the hardware platform. CPU understands the unmodified instructions generated by Virtualized OS. Advantages of full virtualization are complete decoupling of the software from the hardware and complete isolation of different applications. Disadvantages are VMM should provide additionally virtual bios, virtual memory space and virtual devices and also hypervisor creates and maintains data structures like shadow memory page table . VMware's virtualization products and Microsoft Virtual Server are examples of full virtualization. In para virtualization guest OS uses specialized API that talks to the VMM which sends the virtualization requests to the hardware. VMM does not need a resource intensive translation of instructions .Advantages of para virtualization are near native performance and migration .Disadvantage is that it is not applicable for Windows OS .Xen is a virtual machine monitor (hypervisor) for IA-32 (x86, x86-64), IA-64 architectures. It allows several guest operating systems to be executed on the same computer hardware concurrently.

4.3 Cloud Middleware

Software that integrates applications, services and content available on the cloud is called cloud middleware. Middleware is a software that glues various elements of cloud computing. Middleware is an important component of

cloud computing as it helps complex applications on a cloud to contact each other constantly to work in unison. Applications and web components hosted anywhere on the cloud can be re-used with this middleware technology. Some key characteristics possessed by Cloud Middleware are data management , user interfaces and portals , identity / security management , billing & metering and management & monitoring .Various Cloud Middleware's include Eucalyptus - University of California ,Nimbus - Globus alliance ,Open Nebula - DSA Research, Reservoir - European Union FP7 (associated with OpenNebula) and UEC - Ubuntu Enterprise Cloud- Ubuntu + Eucalyptus .

4.4 Cloud Services

Cloud computing provides three different kind of services :Platform as a Service(PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). In PaaS, platform for developing and deploying an application is provided as a service to developers over the Web. Examples include Google AppEngine, Azure services and Amazon web services[4].In IaaS, hardware (server, storage and network), and associated software (operating systems virtualization technology, file system) are delivered as a service to cloud users. Examples include VMware, Amazon EC2.Software as a Service hosts and manages a given application in their own data center and makes it available to multiple tenants and users over the Web. Some SaaS providers use another cloud provider's PaaS or IaaS to offer their service s. Some of SaaS providers include Oracle CRM On Demand, Salesforce.com, and Netsuite.

4.5 Security And Management

when cloud services are used security policies should be deployed to protect data, applications, and the associated infrastructure. Cloud users must trust the cloud providers with their environment and data.Identification & authentication: Priorities and permissions may be granted to specified users to access cloud resources. Every user must be verified and validated using various security mechanisms. uthorization : Authorization policy in cloud computing will determine the type of services, resources or activities the user is permitted. The cloud users must be authorized before performing certain activities. onfidentiality: Confidentiality plays an important role in cloud computing. Organization's data is distributed in cloud across multiple remote servers. Protecting data in cloud computing, allows for information security protocols to be enforced at various layers of cloud applications.

Integrity: lthough outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it's lacking of offering strong assurance of data integrity and availability may impede its wide adoption by both enterprise and individual cloud users [5]. Therefore cloud's data should be robustly imposed with ACID (atomicity, consistency, isolation and durability) properties .

Non-repudiation: A sender or receiver of a message cannot deny having sent or received the message . Using the traditional e-commerce security protocols and token provisioning to data transmission, cloud providers can assure non-repudiation in Cloud computing . Availability: Availability is one of the most critical information security requirements in Cloud computing because it is a key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models. The service level agreement is the most important document which highlights the trepidation of availability in cloud services and resources between the cloud provider and client.

5. Future of the Cloud

Industry analysts including Gartner expects 90 percent of organizations surveyed expect to grow with cloud citing cost-effectiveness and ease/speed of deployment as primary reasons for adoption. Organizations will make use of several trends such as shared, virtualized and automated IT architectures. Businesses of all sizes will adopt cloud due to the introduction of cloud-enabled application platforms .

6. Conclusion

Cloud computing model has immense potential as it offers significant performance gains as regards to response time and cost saving under dynamic workload scenarios[6]. This article discusses the concept of cloud computing, implementation mechanism, architecture and several forms and characteristics of cloud computing.There exists lot of opportunities in cloud computing to explore further for researchers as well as industrial developers.

Key open issues that needs further investigation includes Security, Privacy and Trust, Cloud Interoperability, Dynamic Pricing of Cloud Services, Dynamic Negotiation and SLA Management, Energy Efficient Resource Allocation and User QOS and Regulatory and Legal Issues.

References

[1]. www.nist.gov › ITL › Computer Security Division
[2]. 2.Cloud Computing PMO .Cloud Computing Initiative:May 6, 2009 Summit Briefing Book
[3]. . Web Information Systems and Technologies: 7th International Conference WEBIST 2011, Noordwijkerhout,
[4]. The Netherlands, May 6-9, 2011, Revised Selected Papers
[5]. Amazon simple storage service. Web Page
[6]. http://www.amazon.com/gp/browse.html?node=16427261
[7]. Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Towards Secure and Dependable Storage Services in
[8]. Cloud Computing," IEEE transactions on Services Computing, 06 May 2011
[9]. Rajkumar Buyya, Anton Beloglazov, and Jemal Abawajy. "Energy-Efficient Management of Data Center
[10]. Resources for Cloud Computing: A Vision, Architectural Elements, and Open Challenges" .Elsevier journal,
[11]. june 2009
[12]. Sankaran Sivathanu, Ling Liu, Mei Yiduo, and Xing Pu." Storage Management in Virtualized
[13]. Cloud Environment" cloud computing, 2010 IEEE international conference.
[14]. http://www.vmware.com/virtualization/
[15]. Toby Velte , Anthony Velte , Robert Elsenpeter . Cloud Computing, A Practical Approach. Edition 2010.