INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN MANAGEMENT & COMPUTER APPLICATIONS

VOL. 1, ISSUE 1, OCT. 2012 ISSN NO: 2319-7463

Network Virtualization via Cloud Computing and its Security Issues

Nikhil Pandya
Department of Information Technology, Jaipur Engineering College & Research Center, Jaipur
nikhil.pandya09@gmail.com

ABSTRACT

Cloud is a concept of updating of resources without affecting the infrastructure to reduce the need of backup system and encourage the continuous execution of application. Cloud provides potential "Reliability" and "Scalability" for the applications either deployed or running on cloud. Cloud computing is offering utility oriented IT services to users worldwide. It will speed up the development of intelligent, proactive "nextgen" documents that will improve the productivity of knowledge workers around the world, but several challenges lie in the way before the cloud becomes a widely accepted paradigm for computing. There are concerns about security and there is considerable confusion about the relative merits of public, private and hybrid clouds. It enables hosting of applications from consumer, scientific and business domains. In this paper, we discuses a Cloud Computing approach for context-aware navigation by exploiting the computational power of resources made available by Cloud Computing.

Keywords: Cloud computing, system architecture.

INTRODUCTION

Cloud computing is redefining IT operations by eliminating routine infrastructure deployment, configuration and maintenance. Once only a dream, today dynamic provisioning, paying for usage, and automatic recovery from hardware failures are all a reality. Cloud computing is an enabler for new projects. Getting applications to market faster, and with lower capital expense, creates new opportunities. At the same time, cloud computing assures that as demand increases and businesses grow, resources can be added on demand [1].

Metaphor of the Cloud

In an attempt to demystify some of the confusion surrounding this popular topic, the National Institute of Standards and Technology offers this definition of cloud computing: "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."[2]

VOL. 1, ISSUE 1, OCT. 2012 ISSN NO: 2319-7463

Cloud Computing is a model that can be rapidly provisioned and released with minimal management effort or service provider interaction in order to enable convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). Cloud computing security also known as "cloud security" is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, controls and techniques deployed to protect data, applications and the associated infrastructure of cloud computing. Cloud security is not to be confused with security software offerings that are "cloud-based" also known as security-as-a-service. Many commercial software vendors have offerings such as cloud-based anti-virus or vulnerability management.

A simple cloud Catalogue

If you think about the email example above, you can quickly understand one of the fundamental distinctions involved in cloud computing. If your email server is located in an outsourcing partner's carefully controlled data centre, its part of a private cloud. If you use an Internet-based email program like Microsoft Hotmail, Yahoo Mail or Google's Gmail, on the other hand, the server that holds all of your email is part of a "public cloud" that can be accessed and used by anyone equipped with a computer and web browser. There are other kinds of clouds out there in IT-land, including hybrid clouds, which combine public and private clouds in a customized configuration. Hybrid clouds are a sensible solution for a growing number of business applications. All of these clouds offer advantages in terms of scalability, multitasking capabilities and multitenancy. And users can share a single application, database or other resources, which dramatically reduces the need for organizations to keep investing in their own computing resources. Obviously, all of these variations on the cloud theme have different features, advantages and applications. But they all have the potential to improve the traditional paradigm for enterprise computing [3].

Cloud Power

Let's go back to the basics. Cloud computing provides an entirely new model for enterprise computing, because it converts a fixed-cost infrastructure into a new paradigm based on transactional, "pay as you go" fee-based services. These services are divided into four basic categories:

a) Software as a Service (SaaS)

b) Enabling platform as a service (ePaaS) providers

c) Application platform as a service (aPaaS) provider

d) Infrastructure as a Service (IaaS)

In essence, then, the cloud is a remarkably effective platform for outsourcing, because it turns so many fixed cost scenarios into services. As a result, you can tap into the cloud for your computing infrastructure, your software applications and a wide range of sophisticated business process services[4]. Here are some of the benefits:

1) Unlimited storage for documents and data

2) Unlimited processing power.

3) Dynamic flexibility and scalability

4) Economies of scale

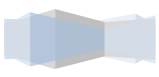
5) Streamlined implementations.

6) More outsourcing options for small businesses.

7) More capabilities for real-time and online collaboration

8) A sensible solution for a mobile workforce

9) A greener approach to everyday business



VOL. 1, ISSUE 1, OCT. 2012 ISSN NO: 2319-7463

A Brief chronicles about cloud computing

The underlying concept of cloud computing dates back to the 1960s, when John McCarthy opined that "computation may someday be organized as a public utility." Almost all the modern-day characteristics of cloud computing (elastic provision, provided as a utility, online, illusion of infinite supply), the comparison to the electricity industry and the use of's 1966 book, The Challenge of the Computer Utility. The actual term "cloud" borrows from telephony in that telecommunications companies, who until the 1990s offered primarily dedicated point-to-point data circuits, began offering Virtual Private Network (VPN) services with comparable quality of service but at a much lower cost. By switching traffic to balance utilization as they saw fit, they were able to utilize their overall network bandwidth more effectively. The cloud symbol was used to denote the demarcation point between that which was the responsibility of the provider and that which was the responsibility of the user. Cloud computing extends this boundary to cover servers as well as the network infrastructure. After the dot- combubble, Amazon played a key role in the development of cloud computing by modernizing their datacenters, which, like most computer networks, were using as little as 10% of their capacity at any one time, just to leave room for occasional spikes. Having found that the new cloud architecture resulted in significant internal efficiency improvements whereby small, fast- moving "two-pizza teams" could add new features faster and more easily, Amazon initiated a new product development effort to provide cloud computing to external customers, and launched Amazon Web Service (AWS) on a utility computing basis in 2006.

In early 2008, Eucalyptus became the first open- source, AWS API-compatible platform for deploying private clouds. In early 2008, Open Nebula, enhanced in the RESERVOIR European Commission-funded project, became the first open- source software for deploying focused on providing QoS guarantees (as required by real-time interactive applications) to cloud-based infrastructures, in the framework of the IRMOS European Commission-funded project, resulting to a real-time cloud environment. By mid-2008, Gartner saw an opportunity for cloud computing "to shape the relationship among consumers of IT services, those who use IT services and those who sell them "and observed that "organizations are switching from company-owned hardware and software assets to per-use service-based models" so that the "projected shift to cloud computing will result in dramatic growth in IT products in some areas and significant reductions in other areas."[5]

ARCHITECTURE

The Cloud Computing Architecture of a cloud solution is the structure of the system, which comprises on-premise and cloud resources, services, middleware, and software components, geo-location, the externally visible properties of those, and the relationships between them. The term also refers to documentation of a system's cloud computing architecture. Documenting facilitates communication between stakeholders, documents early decisions about high-level design, and allows reuse of design components and patterns between projects [6].

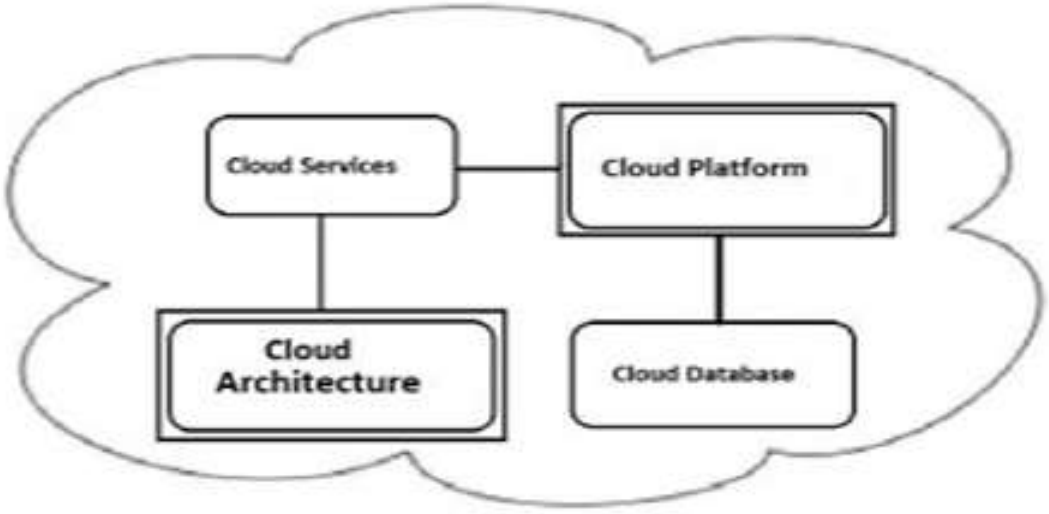


Fig: A Simple cloud computing architecture

VOL. 1, ISSUE 1, OCT. 2012 ISSN NO: 2319-7463

Cloud architecture is based on creation of large data center by defining a n abstraction between the platform and the operational system. Basically systems which use for deploying an application or information storing are used to call “Management Fabric Automated” system. This also an important part of cloud architecture. At the time of the deployment it provisions the hardware, deploy the operating system image on server and deploy services on server. The number of server can be more than one. The set of server can also follow the “Grid Approach”, i.e. can be connected through LAN. The owner of the service can set the “Security Configuration” and other “Access Right” for service. Instead of that the architecture also use to have “Load Balance”, “DNS Server” and “Switches” and “Router”[7].

STACKS IN CLOUD COMPUTING

Infrastructure as a service (IaaS) providers– These players will focus on building and operating large scale data centres providing sophisticated infrastructure management services to optimize utilization of capital intensive computing, storage and network facilities [8].

- Enabling platform as a service (ePaaS) providers– These players will focus on managing service grids that source and aggregate enabling services like security, performance management and data translation. In the ePaaS layer, the services aggregated by the service grid will be largely transparent to end users but critical to the application developers building application services at the next layer. These service grids may be provided by specialized independent businesses orby large user enterprises who offer their enabling services to other enterprises. The service grids 13 will be targeted by domain of expertise; e.g., application security services; or SOX compliance services for financial institutions.

- Specialized software as a service (SaaS) providers – These will be highly specialized developers of enabling and application services that will leverage ePaaS platforms described above. These providers will also include a growing number of “user” enterprises who discover the benefits of “exposing” key elements of their business operations as services to be consumed by other enterprises.[9]

- Application platform as service (aPaaS) providers– These players will focus on managing service grids that source and aggregate application services. These players will specialize in particular application domains, whether defined horizontally (e.g., human resource management, customer relationship management), or defined vertically (e.g., financial services, health care) [8]. Their focus will be on providing aggregation platforms for a vast array of more specialized application service providers, offering specialized services like SLA management and service directories, enhanced by deep domain expertise to help users configure the appropriate bundles of application services. A critical role of these aPaaS providers will be to enable cloud users to create new coarse-grained business services, composed of granular services available through the aPaaS platform. For example, a financial services aPaaS might enable a financial institution to construct a new loan product by aggregating atomic services such as identity verification, credit history checking, credit risk modelling, etc. As a result, through the aPaaS, the financial institution is able to easily construct a new innovative coarse-grained product by piecing together several best-in-class atomic services which it would otherwise need to create or source through in-house resources [9].

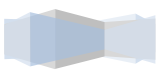
CLOUD COMPUTING SECURITY

Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub- domain of computer security, network security, and, more broadly, information. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Cloud security is not to be confused with security software offerings that are "cloud-based" (a.k.a. security-as-a-service). Many commercial software vendors have offerings such as cloud-based anti- virus or vulnerability management [10].

SECURITY ISSUES

- Data Loss: Important personal data such as contacts, photos, calendar entries, etc may lost due to server failure therefore their privacy maintenance is a basic issue.[11]

- Phishing: It is a way of acquiring sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity. This technique directs user to enter their details in fake page whose look and feel are exactly same as that of the legitimate one.[11].



VOL. 1, ISSUE 1, OCT. 2012 ISSN NO: 2319-7463

- Password Cracking: Well known term, refer to recover password from data that has been stored in or transmitted by computer system. It is used to describe the penetration of a network, system, or resource with or without the use of tools to unlock a resource that has been secured with a password.

- Identity Management: Broad administrative area that deals with identifying individuals in a system and controlling access to the resources in that system by placing restrictions on the established identities of the individuals. Decides the basis to identity humans and authorized them across worldwide spread computer networks.[10]
- Application Security: Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures be in place in the production environment.

- Privacy: It refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data about one's self. It includes whether email can be stored or read by third parties without consent, or whether third parties can track the web sites someone has visited.[12]

Security in the Cloud

Cloud architectures must have well-defined security policies, methods and procedures. There are specific security issues that anyone considering cloud computing must address to ensure that they will still have adequate security policy control over applications and services; as well as meeting customer service level agreements on security while remaining compliant with rules and regulations on data security.

- Integrated Cloud Security: IT teams can also leverage a virtual infrastructure aware IPS solution, integrated with the hypervisor, to provide the needed visibility and security to prevent communication directly between hosted partitions within the virtual server. These directly integrated solutions employ hypervisor-based APIs, and can also be used to ensure that even offline virtual machines are protected and can stay up to date with patches, AV/IDS signatures filters and rules while they are in an offline or mobile state.[13].

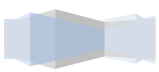
- Cloud Burst Security: One of the primary advantages of cloud computing is that enterprise can move applications that consist of several virtual machines to the cloud provider when the physical environment requires additional processor or compute resources. These bursting virtual machines need security policies and baseline histories to move with them. When a virtual machines moves, if the security policy does not accompany it, that virtual machines becomes vulnerable. In addition, when virtual machines move, they lose their performance histories and administrators must re-evaluate the virtual machine performance baselines.[10]

- Compliance Concerns: The auditing community is aware that current practices for auditing cloud environments are inadequate. As compliance grows in importance, enterprise implementing clouds need to satisfy their auditors' concerns; especially since creating an identity for an individual virtual machine and tracking that virtual machine from creation to deletion creates challenges for even the most mature virtualized environments. Virtual machine sprawl--when the number of virtual machines being created is growing more quickly than an enterprise's ability to manage them-- adds complexity. [14]

- Isolate networks: The first responsibility of the cloud provider is to provide a level of isolation between all of the different networks that are a part of the virtualization infrastructure. These networks include management networks, VMware VMotion or Live Migration networks, IP storage networks, and individual customer networks. All of these networks should be segmented from each other. Administrators can use a couple primary methods to achieve isolation.[15]

- Secure customer access to cloud-based resources: Customers will need to have a way to access their resources that are located within the cloud and be able to manage those resources in a secure manner. Therefore, it is incumbent upon the cloud provider to supply the customer with a management portal that is encrypted. SSL Encryption would be the most common tool for this task.[10]

- Strong authentication, authorization and auditing mechanisms: It is very important in this type of shared environment to properly and securely authenticate system users and administrators and provide them with access to only the resources



VOL. 1, ISSUE 1, OCT. 2012 ISSN NO: 2319-7463

they need to do their jobs or the resources that they own within the system. It is also very important in a cloud environment to know who is doing what within the system, when they did it, and what exactly they did.[16]

CONCLUSION

Cloud computing is the most popular notion in IT today; even an academic report from UC Berkeley says "Cloud Computing is likely to have the same impact on software that foundries have had on the hardware industry." Cloud computing as we see it emerging today is somewhat amorphously defined, making it difficult to form a point of view about the capabilities of currently available cloud computing instances to manage next century platforms. While it is clear that they can manage today's common platforms, we see architectural challenges for the future that we believe will be difficult to address using current cloud architectures and architecture styles. We identify technical challenges including architecture style, user and access control management, the need to have externally managed business and infrastructure policies through interaction Containers, and the need for Utility Computing capabilities that must be addressed to meet future architecture requirements. Adding architecture components like the interaction container and externalized policy engine will improve cloud capabilities, but until these become fundamental components in cloud architecture, it is unlikely that a cloud will be able to manage the concerns of a service grid. It is interesting to note, however, that the construct of a service grid enables it to manage the concerns of a cloud. A service grid, as an autonomic architecture that is hardened to be both a service-oriented technology platform and a business platform, can be expected to scale both downward to support enterprise architectures and upward and outward to support the types of architectures likely to be pervasive in twenty-first-century computing.

ACKNOWLEDGMENT

This work was supported by Jaipur Engineering College and Research Centre (JECRC). We are thankful to Mr. Arpit Agarwal (Director, JECRC) for valuable suggestions, kind support and encouragement. Further, also want to convey thanks to Dr. Ekta Menghani (Biotechnology Department, MGIAS,) Associate Professor Manish Tiwari (E&C Department, JECRC) and Ms. Neha Gupta (H.O.D., I.T. JECRC) for their time to time suggestions and technical support.

REFERENCES

[1]. http://www.3tera.com/download/AppLogicCloudatasheet.pdf

[2]. http://www.nist.gov/

[3] http://www.xerox.com/downloads/usa/en/xgs/whitepapers/xgs_whitepaper_cloud_computing.pdf

[4] http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%20services.pdf

[5] Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, by Tim Mather, Subra Kumaraswamy, and Shahed Latif; O'Reilly Media Inc, 2009

[6] http://www.sei.cmu.edu/library/assets/presentations/Cloud%20Computing%20Architecture%20-%20Gerald%20Kaefer.pdf

[7] http://www.johnhagel.com/cloudperspectives.pdf

[8] http://www.xerox.com/downloads/usa/en/xgs/whitepapers/Cloud-Computing-PDF-Free-Download.pdf

[9] http://webobjects.cdw.com/webobjects/media/pdf/Sun_CloudComputing.pdf

[10] Cloud Computing: Implementation Management, and Security, by John Rittenhouse and James Ransome; CRC Press 2010

[11] http://blogs.iss.net/archive/papers/VirtualizationSecurity.pdf

[12] http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

[13] http://www.vmware.com/files/pdf/cloud/VMware-Savvis-Cloud-WP-en.pdf

[14] http://www.clavister.com/documents/resources/whitepapers/clavister-whp-security-in-the-cloud-gb.pdf

[15] https://www.owasp.org/images/1/12/Cloudy_with_a_chance_of_0_day_-_Jon_Rose-Tom_Leavey.pdf

[16] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf