CLOUD COMPUTING FUNDAMENTALS

Introduction

Cloud computing is a group of IT services which have been presented to a person on the network with a leased basis current ability to scale up or down their service requirements. Usually Cloud Computing services are delivered by way of an alternative party provider - the master of the infrastructure. IBM defines cloud computing as being simply “the cloud,” is the delivery of on-demand computing resources—everything from applications to data centres—online using a pay-for-use basis (IBM, 2018). Webopedia's defines cloud computing as being usually typically a kind of computing that utilizes sharing computing resources as opposed to having local servers or personal devices to handle applications (Webopedia, 2018). In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the web," therefore the phrase cloud computing means "a form of Internet-based computing," where different services — such as servers, storage and applications — are shipped to an organization's computers and devices over the Internet. Cloud Computing is similar to grid computing, a form of computing where unused processing cycles off computers in the network are harnessed, to fix problems too intensive for virtually stand-alone machines.

Deployment Models

Within a Cloud Deployment model, networking, platform, storage and software infrastructure are considered as services which can be further scale up or down as per the consumer demands. The Cloud Computing model has four main deployment models:

a. **Private Cloud:** Private cloud is the phrase utilized to describe a cloud computing platform that is implemented inside the corporate firewall, under the power over the IT department. An exclusive cloud is designed to provide the same product or service benefits of public cloud systems, but numerous objections on the cloud computing model are removed including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance (Webopedia, 2018). Only the organization and designated stakeholders may have access to operate on a concrete Private cloud (Dooley,

2010). One of the best examples of a private cloud is Eucalyptus Systems (Nurmi *et al*., 2009).

b. **Public Cloud:** A type of cloud computing where a company relies on a third-party cloud company for services including servers, data storage and applications, which are shipped to the corporation through the Internet. A public cloud can free companies from the potentially expensive costs of needing to purchase, manage and gaze after on-premises hardware and software infrastructure. Public clouds could also typically be deployed faster with more scalability and accessibility than on-premises infrastructure due to the population cloud provider's expertise and existing infrastructure. Public cloud subscribers may pay pay-as-you-go fees or fixed monthly fees for public cloud services they utilize. Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-accommodation substratum over the Internet, via web applications/web accommodations, from an off-site third-party provider who apportions resources and bills on a fine-grained utility computing substratum. It is basically a pay-per-use model, similar to a prepaid electricity metering system which is user-flexible to cater the demand for cloud optimization (Platform Computing, 2010). Security of public clouds are more vulnerable than the other cloud models because the measures to prevent malicious attacks on public clouds are technically more difficult and of course expensive to handle. Examples of a public cloud include Microsoft Azure, Google App Engine.

c. **Hybrid Cloud:** A combined way of private clouds and public clouds in which some critical data resides within the enterprise's private cloud while other results are held in and accessible at a public cloud. Hybrid clouds seek to offer the advantages of scalability, reliability, rapid deployment and potential personal savings of public clouds with all the security and increased control and management of private clouds. An example of a Hybrid Cloud includes Amazon Web Accommodations (AWS) (Global Netoptex Inc., 2018).

d. **Community Cloud:** Infrastructure shared by a few organizations for just a shared cause and may be managed by them or even a third party service provider and rarely offer cloud

model. These clouds tend to be based on an agreement between related business organizations, for instance, banking or educational organizations. A cloud environment operating as outlined by this model may exist locally or remotely. One particular community cloud includes Facebook.

Entities of Cloud Computing

Cloud providers and consumers are the two main entities available on the market. Service brokers and Service resellers are also classified as two newly emerging service level entities in the Cloud computing environments.

These entities are explained below:

1. **Cloud Providers:** Cloud Providers includes Internet service providers (ISPs), telecommunication organizations, and large BPOs that include media (Internet connections) or infrastructure (hosted data centres). This enables end-users to gain access to cloud services. Companies also can include systems integrators that build and support data centres to host private clouds and they can offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to their consumers or to the service brokers, resellers, etc.

2. **Cloud Service Brokers:** Cloud Service Brokers includes technology consultants, business organizations, registered brokers, agents, service agencies and promoters which guide consumers within the selection of cloud computing services. Service brokers give full attention to the negotiation from the relationships between consumers and providers without owning or handling the whole cloud infrastructure. Also, they add extra services together with Cloud providers.

3. **Cloud Resellers:** Resellers can be a key point through the Cloud market if the Cloud providers will further grow their business across continents. Cloud providers may also choose local IT consultancy companies or resellers in their existing products to act as new resellers to promote their Cloud-based products inside of a particular region.

4. **Cloud Consumers:** Customers participate in the sounding Cloud consumers. However, also Cloud service brokers and resellers can participate in this category as soon as there are customers of another Cloud provider, broker or reseller.

CLOUD COMPUTING ARCHITECTURE

There are basically 3 layers in cloud computing. Companies use it differently based on their needs. The 3 layers are application, platform and lastly infrastructure. These layers are usually presented in the form of a pyramid with infrastructure at the bottom; platform in the middle; and application at the top of the pyramid.

The Bottom Layer

The bottom layer which is infrastructure is also known as 'infrastructure as a service' (IaaS). This is where the things start and where people begin to build. This is the layer where the cloud hosting lives. The examples of company that provides Cloud infrastructure are Amazon Web Services, GoGrid, and the Rackspace Cloud. Cloud infrastructure is also known to work as a deliver computer infrastructure. Most companies, in this part will operate their own infrastructure. It will allow them to give more services and features and also give more control than other layers in Cloud Pyramid. There are pros and cons in the characteristic of Cloud Infrastructure. The pros are that it can give the company full access or control of the company infrastructure while the cons are that sometimes it come with premium price. It can be very complex to maintain, manage and also to build.

The Middle Layer

The middle layer which is platform is also known as 'platform as a service' (PaaS). The examples of company and product of Cloud Platform are Google App Engine, Heroku, Mosso (now the Rackspace CloudSites offering), Engine Yard, Joyent or force.com. In contrast to the Cloud Application, this layer is where the users build up the increase of flexibility and control. Unfortunately, it still somehow limits what can user do or not. There are strengths and weakness of characteristic in this Cloud Platform. The strength of Cloud Platform is that it has more control than cloud Application and it also good for developers with a certain position target. Meanwhile the weakness is that sometimes it depends more on Cloud Infrastructure Providers and sometimes it also sticks to the platform ability only. For example, building an app, involves downloading and installing Android SDK (4GB) and other related libraries like maven, Google APIs and so on.

Instead, users can use an instance from an already setup platform to start building the app. However, users will be limited to libraries and version of SDK preinstalled.

The Top Layer

The top layer which is application is also known as 'software as a service' (SaaS). In this layer, the users are really limited to what the application can do. The part of company that is involved is the public email providers such as Gmail, Hotmail, Yahoo Mail, etc. Most companies use services in this particular Cloud layer. Usually, users can only get the pre-defined functions and cannot access more than that. Therefore, users can use the application as it appears; and they have no knowledge or any control to the application. The advantages however are that it is free, easy to use and it offers a lot of different services including Google Docs, Sheet, Presentation, CRM, SalesForce and so on.

CLOUD SERVICE MODELS

Service Models

In line with the different types of services offered, cloud computing can be considered to incorporate three layers: software being a service (SAAS), platform being a Service (PAAS), and infrastructure like a Service (IAAS) (Iyer & Henderson, 2010; Han, 2010, Mell & Grance, 2010). Infrastructure as a Service (IaaS) is the lowest layer that delivers basic infrastructure support service. The middle layer, Platform as a Service (PaaS), provides environment for hosting end-user's applications. Software like a Service (SaaS) may be the topmost layer which comes with a complete application offered as service at will.

Software as a Service (SaaS)

Software as a Service (SaaS) (Lin, 2012) is described as software which is deployed over the internet. With SaaS, a provider licenses a credit application to customers either to be a service at the moment, by having a subscription, in the-pay-as-you-go model, or (increasingly) at no cost if there is opportunity to generate revenue from different streams, like from advertisement or user list sales.

Similar to the fundamental concept of cloud computing, SaaS is generally a model whereby the customer licenses applications and provisions those to the end-users at will. The skills operate on the provider's infrastructure and are also accessed by way of a public network connection. Applications could possibly be offered through Internet as browser applications or they are often downloaded and synchronized with user devices. SaaS offers compelling benefits. It simplifies licensing. In fact, the consumer does not need to get a software license in the least. This is the task on the provider. There is also no requirement to calculate maximum capacity. It outsources the tiresome task of application, preservation and upgrades and ties consumer costs to handling, which lowers flat charge and principal investment. It does so with the expense of restricting customer flexibility with regards to configuration options increase schedule. This rapid growth suggests that SaaS has decided to become a commonplace within every organization and therefore it is significant to be aware of what SaaS is, where it works and security issues. The core technology of SaaS is dedicated to its multi-tenant architecture. Chong and Carraro (2006) characterized SaaS as –Software deployed being a hosted service and accessed online. So as to provide proficient and successful services to SaaS consumers, the SaaS providers have got to design their application architecture as –multi-tenant, scalable, efficient, and configurable (Chong & Carraro, 2006).

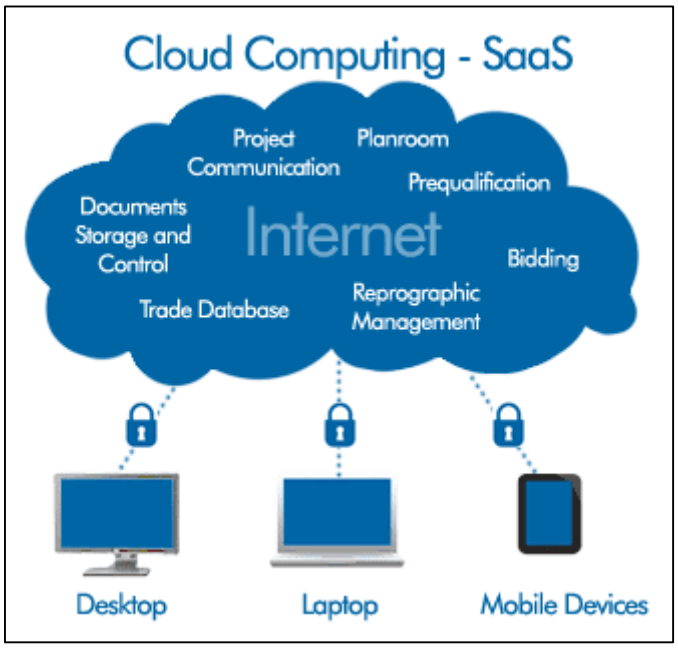

Figure 4 – SaaS (Mirza, 2016)

Threats in SaaS

Software-as-a-service keeps growing in popularity although not all IT decision-makers are taking the leap. "*Security will be the No. 1 reason preventing firms motionless to SaaS,*" Forrester analyst Liz Herbert writes in a recent set of software-as-a-service adoption (Herbert, 2010). There are numerous security risks associated with adopting software-as-a service. Listed below are four problems to think about:

- Undeveloped Identity Management
- Weak Cloud Standards
- Secrecy in Security and data centres
- Risk in universally Accessibility

Platform as a Service (PaaS)

Platform as a service (PaaS) (Beri, 2015) may be the delivery of a computing platform and solution stack like a service. It facilitates deployment of applications without worrying about cost and complexity of purchasing and managing the underlying hardware and software layers, that would be providing every facilities required to offer the complete life cycle to create and deliver web applications and services entirely available from the web itself. That is no software downloads or installation for developers, IT managers or end-users. Cloud platforms become run-time environments which support a couple of programming languages. They will offer additional services such as reusable components and libraries that you can get as objects and application programming interfaces. Ideally, system will offer plug-ins into common development environments, for instance Eclipse, to facilitate development, testing and deployment. Platforms will also be escalating to real-world incorporation platform services together with business process integration, and guaranteed system-to-system communication.

Figure 5 – PaaS (Dhiman, 2017)

Threats in PaaS

- Default Application Configurations
- SSL Protocol based attacks
- Insecure permission on cloud data

Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) (Lin, 2012) can be a method of delivering Cloud Computing infrastructure – servers, storage, network and operating systems – being an on-demand service. Rather than purchasing servers, software, data centre space or network equipment, clients instead buy those resources being a fully outsourced service at will. Cloud consumers directly use IT infrastructures provided from the IaaS cloud. Virtualization is expansively used in IaaS cloud so that users can integrate/decompose physical property within an ad-hoc manner to meet increasing or shrinking resource demand from cloud customers. It is surely an evolution of VPS offerings and merely supplies a mechanism to consider advantage of hardware along with other physical resources without capital investment or physical administrative requirements. The benefits of services at this stage are that there are not many restrictions for the consumer. There might be challenges including dedicated hardware but any software program can run within the IaaS context.

Threats in IaaS

The most significant risk that can be expected when working with an IaaS contribution is coping with vulnerabilities in operating systems (OS's) and its services. Linux and Windows are used in more than 90% of the clusters on the cloud. Both OSs and services will continue to have vulnerabilities. OS and service vulnerabilities are made public through many outlets, and in many instances, exploits are publically available.

VIRTUALISATION AND RESOURCE MANAGEMENT

Virtualisation is the process of simulating hardware, so that several operating systems could be run on a single machine. Most servers are used only about 10 – 20 % if dedicated to a single client. In order to maximise the usage of servers in the cloud, VMs (a VM - Virtual Machine – is the simulation of hardware to create an environment similar to that of physical hardware. Popular examples include VMWare, VirtualBox) are used. One server could be hosting several VMs as shown in Figure 6 and each VM is dedicated to one client only. VMs could then be migrated to others servers based on resource management (CPU, Memory or Storage usage) or Locality (Content Delivery Network). The main aim of virtualisation is to provide strong isolation, security, performance and simplicity.

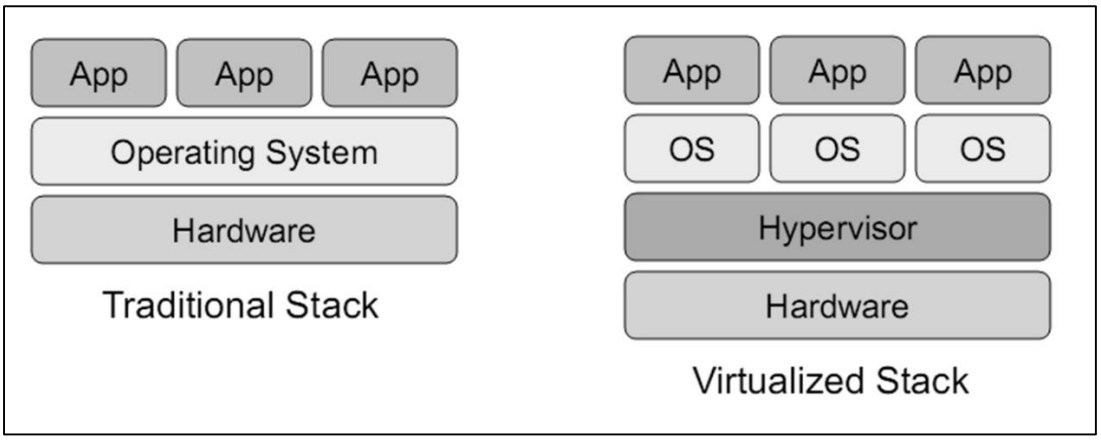

Figure 6 – Traditional VS Virtualised Stack

Types of Virtualisation Technology

1. **Hardware Partition**

   In this approach, hardware (CPU, Memory and storage) is partitioned by using a Partition Controller. Each partition has their own CPU/Memory and independent Operating System installed. However the disadvantage of this method is the lack of flexibility for the management of the resources in real-time. Once the system is set-up, and a user finds that there is need, for example, of more memory, the system cannot be reconfigured.

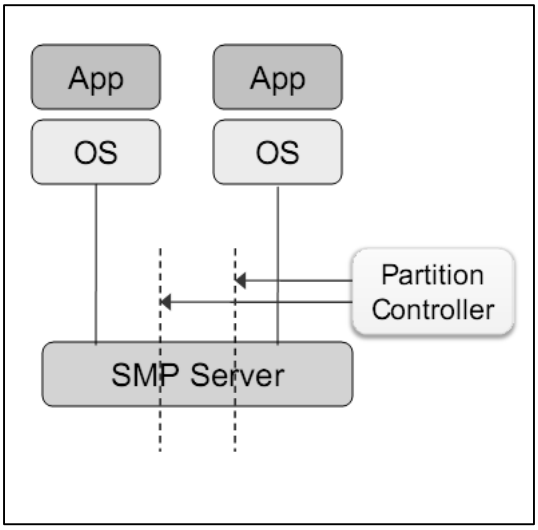

Figure 7 – Hardware Partitioning

2. Virtual Machine Monitoring (VMM)

In this approach, an application known as VMM is installed on the Host OS, and which allows to create several VM having each their own OS. In this type of virtualisation, the kernel of host OS is not modified, as compared to Hardware partition. Another advantage of this method is that it allows each VM to have an OS independent of the host OS as shown in Figure 8. However, the downsides of this type is the low efficiency and high cost of hardware instruction translation.

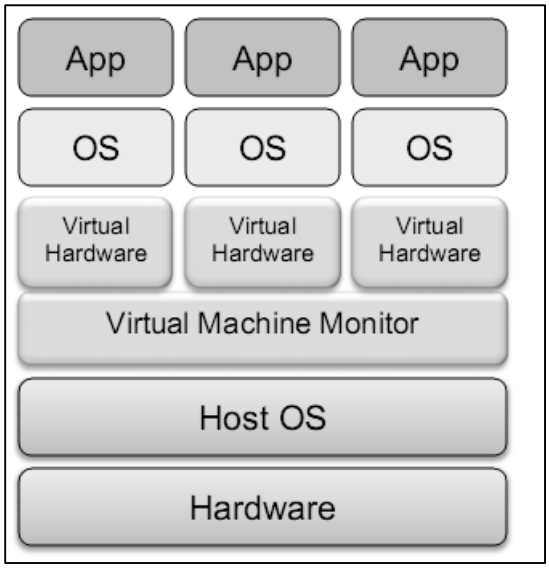

Figure 8 – Virtual Machine Monitor

3. Para-Virtualisation

In this approach, there is no host OS as such. Instead a modified OS kernel together with a Xenhypervisor is used. The Xenhypervisor allows multiple guest OS to run, and it manages resources allocation. Most modern Processor now have Virtualisation (VT) support embedded. The efficiency of the overall system is greatly improved compared to VMM. In VMM, there is an OS which is installed and on top of it, the VMM system will run. This process will consume Memory and CPU compared to Xenhypervisor which replaces the OS and VMM in one single layer.

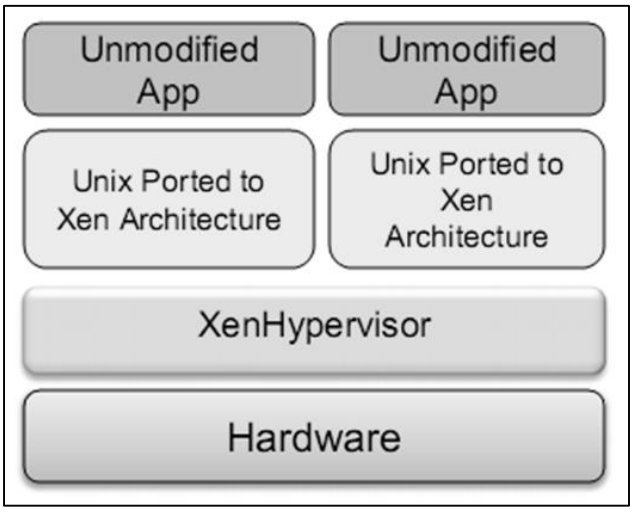

Figure 9 – Para-Virtualisation

4. OS Virtualisation

In this approach, one OS instance is installed on a single host. A virtualisation platform is installed on top of the host OS. The virtualisation platform then offers the possibility to create containers to host virtual OS as shown in Figure 10. The benefits of this deployment is the low cost and possibility of running hundreds of VPS (Virtual Private Server) on a single server.

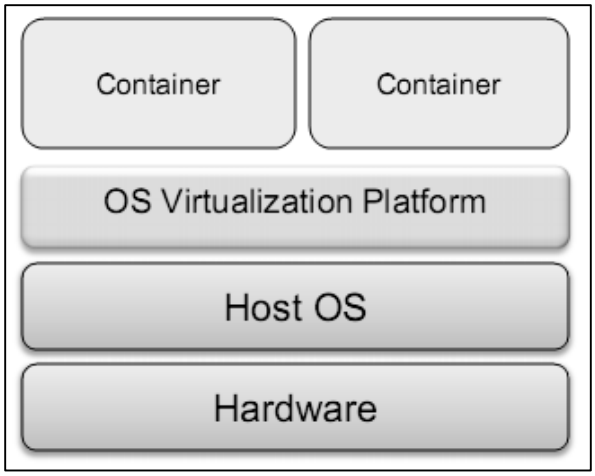

Figure 10 – OS Virtualisation

Vendors of Virtualisation Software

Virtualisation is now a well-established technology and major vendors include VMware, HyperV (Windows Server 2008), oVirt, VirtualBox (Oracle).

NOTE:

Parts of this module has been adapted from "*Cloud computing: An overview. Book Chapter of Cloud Computing: Reviews, Surveys, Tools, Techniques and Applications*" - Nazir, M., Tiwari, P., Tiwari, S.D. and Mishra, R.G., 2015 - An Open-Access eBook published by HCTL Open.