IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 2, February 2018

Concepts of Cloud Computing

Poornima.K.M[1], Sneha Ganesan[2], Sherinvergle Chinnappan[3], Princy Angelin.J[4]

Assistant Professor, Depart., of BCA & M Sc.S.S, Sri Krishna Arts and Science College, Kuniyamuthur, Coimbatore[1]

BCA, Second year, Sri Krishna Arts and Science College, Kuniyamuthur, Coimbatore[2,3,4]

Abstract: Cloud computing-Virtual Technology-Pay per as you go-User’s flexibility-Utilization and efficiency-resource pooling-Reliability and Scalability-Rapid elasticity.

Keywords: Characteristics;Arichitecture;Service models;Deployment models;Security and Privacy.

I. INTRODUCTION

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud providers typically use a "pay-as-you-go" model, which is a reason for sudden operating expenses if administrators are not familiarized with cloud-pricing models.

II. CHARACTERISTICS

A. *Characteristics of cloud computing:*

- Increase in flexibility for organizations may be improved, as cloud computing may increase users' agility with re-provisioning, adding, or expanding technological infrastructure resources.

- Cloud providers render reduced cost. The capital expenditures are converted by public-cloud delivery model. This purportedly lowers barriers to entry, as infrastructure is actually given by a third party and need not be bought one-time or infrequent intensive computing tasks. As well, less IT skills are required for implementation of projects that use cloud computing. Most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

- Device and location independence enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect to it from anywhere.

- Maintenance of cloud computing applications is easier and no need to install (e.g., different work locations, while travelling, etc.).

- Multitenancy enables sharing of resources and costs across a large pool of users thus allowing for:

- Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

- Peak-load capacity increases (users need not engineer and pay for the resources and equipment to meet their highest possible load-levels)

- Utilization and efficiency improvements for systems that are often only 10–20% utilized.

- Performance is monitored by IT experts from the service provider, and consistent and loosely coupled architectures are constructed using web services as the system interface.

- Resource pooling is the provider’s computing resources are commingle to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to user demand. There is a sense of location independence in that the consumer generally have no control or knowledge over the exact location of the provided resource.

- Productivity may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are

DOI 10.17148/IARJSET.2018.5215

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

matched, nor do users need to install application software upgrades to their computer.

- Reliability improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

- Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time (Note, the VM startup time varies by VM type, location, OS and cloud providers), without users having to engineer for peak loads This gives the ability to scale up when the usage need increases or down if resources are not being used.

- Security can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because service providers are able to devote resources to solving security issues that many customers cannot afford to tackle or which they lack the technical skills to address. However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":

- On-demand self-service: A consumer can unilaterally provision 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 thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

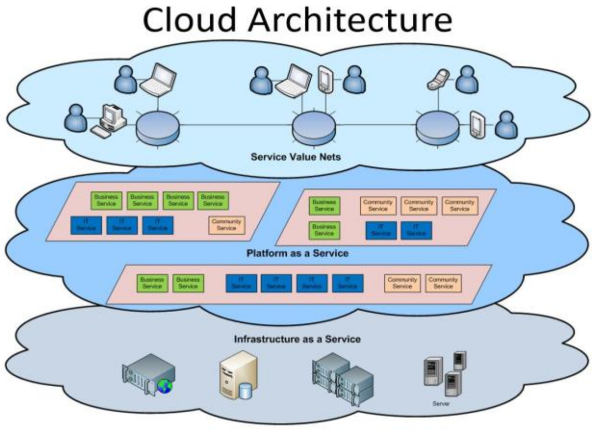
- Resource pooling: The provider's computing resources are pooled to serve multiple consumers by a multi-tenant model, with different physical and virtual resources dynamically assigned and has been reassigned according to consumer demand.

- Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

- 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.

B. Architecture:

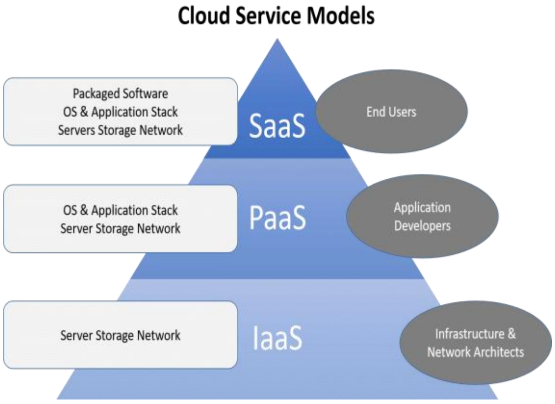
Cloud architecture the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue. Elastic provision implies intelligence in the use of tight or loose coupling as applied to mechanisms such as these and others.



DOI 10.17148/IARJSET.2018.5215

III. TYPES OF CLOUD COMPUTING

A. Server models
B. Deployment models



Though service-oriented architecture advocates "everything as a service" (with the acronyms EaaS or XaaS, or simply aas), cloud-computing providers offer their "services" according to different models, of which the three standard models per NIST are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These models offer increasing abstraction; they are thus often portrayed as a layers in a stack: infrastructure-, platform- and software-as-a-service, but these need not be related. For example, one can provide SaaS implemented on physical machines (bare metal), without using underlying PaaS or IaaS layers, and conversely one can run a program on IaaS and access it directly, without wrapping it as SaaS.
Infrastructure as a service (IaaS):
Infrastructure as a service (IaaS):

I. SERVER MODELS

Infrastructure as a Service (IaaS):

"Infrastructure as a service" (IaaS) refers to online services that provide high-level APIs used to dereference various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. A hypervisor, such as Xen, Oracle Virtual Box, Oracle VM, KVM, VMware ESX/ESXi, or Hyper-V, LXD, runs the virtual machines as guests. Pools of hypervisors within the cloud operational system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements. Linux containers run in isolated partitions of a single Linux kernel running directly on the physical hardware. Linux c groups and namespaces are the underlying Linux kernel technologies used to isolate, secure and manage the containers. Containerization offers higher performance than virtualization, because there is no hypervisor overhead. Also, container capacity auto-scales dynamically with computing load, which eliminates the problem of over-provisioning and enables usage-based billing. IaaS clouds often offer additional resources such as a virtual-machine disk-image library, raw block storage, file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles.

Platform as a Service (PaaS):

PaaS vendors offer a development environment to application developers. The provider typically develops toolkit and standards for development and channels for distribution and payment. In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming-language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers like Microsoft Azure, Oracle Cloud Platform and Google App Engine, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually. The latter has also been proposed by an architecture aiming to facilitate real-time in cloud environments.[need quotation to verify] Even more specific application types can be provided via PaaS, such as media encoding as provided by services like bitcodin.com or media.io.

Software as a Service (SaaS):

In the software as a service (SaaS) model, users gets access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis or using a subscription fee. In the SaaS model, cloud providers

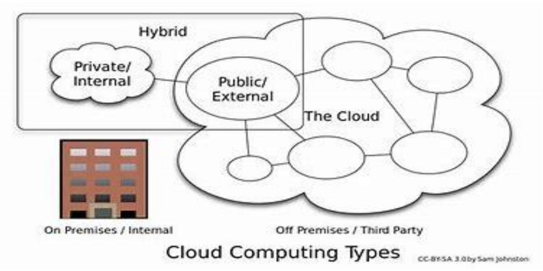
DOI 10.17148/IARJSET.2018.5215

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 2, February 2018

install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud user's own computers, which simplifies maintenance and support. Cloud applications differ from other applications in their scalability—which can be achieved by cloning tasks onto multiple virtual machines at run-time to meet changing work demand. Load balancers distribute the work over the set of virtual machines. This process is transparent to the cloud user, who sees only a single access-point. To accommodate a large number of cloud users, cloud applications can be multitenant, meaning that any machine may serve more than one cloud-user organization.

Mobile "Backend" as a service (MBaaS):
This model is also called backend as a service (BaaS), web app and mobile app developers are provided with a way to link their applications to cloud storage and cloud computing services with application programming interfaces (APIs) exposed to their applications and custom software development kits (SDKs) The services provided are user management, push notifications, integration with social networking services and more. This model is a very recent model in cloud computing, with most BaaS startups dating from 2011 or later but trends indicate that these services are gaining significant mainstream traction with enterprise consumers.

Deployment models:



Cloud Computing Types

Private Cloud:

This model is operated for only one organization. It is managed either by a single institution or an external or an internal host. Undertaking a private cloud requires business environment to reevaluate decision about existing resources. This improves business but raises security issues. Automatic-run data centers are capital intensive. They have a significant physical footprint, requiring allocations of space, hardware, and environmental controls. These assets have to be refreshed periodically, resulting in additional capital expenditures. They have attracted criticism because users "still have to buy, build, and manage them" and does not benefit from less hands-on management, essentially "[lacking] the economic model that makes cloud computing such as intriguing concept".

Public Cloud:

A network that is open for public use is called a “public cloud”. Public cloud services are free. But, technically there may be little or no difference between public and private cloud architecture, security consideration may be extensibly different for services like applications, storage, and other resources that are made available by a service provider for a public audience and when communication is effected over a non-trusted network. Generally, public cloud service providers like Amazon Web Services (AWS), Oracle, Microsoft and Google own and operate the infrastructure at their data center and access is generally via the Internet. AWS, Oracle and Microsoft also offer direct connect services called "AWS Direct Connect", "Oracle Fast Connect" and "Azure ExpressRoute" respectively, such connections require customers to purchase or lease a private connection to a peering point offered by the cloud provider.

Hybrid Cloud:

Hybrid cloud is a combination of two or more clouds (private, community or public) that has to be distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources. Gartner defines a hybrid cloud service as a cloud computing service that is composed of some composition of private, public and community cloud services, from different service providers. Hybrid cloud service crosses isolation and provider boundaries so that it can't be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service varied use cases for hybrid cloud composition exist. For example, an organization may store sensitive client data in house on a private cloud application, but interconnect that application to a business intelligence application provided on a public cloud as a software service. This example of hybrid cloud extends the capabilities of the enterprise to deliver a specific business service through the addition of externally available public cloud services. Hybrid cloud adoption

DOI 10.17148/IARJSET.2018.5215

depends on number of factors such as data security and compliance requirements, level of control needed over data, and the applications an organization uses.

Security And Privacy:

Cloud computing provide privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies, which users must agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access. According to the Cloud Security Alliance, the top three threats in the cloud are Insecure Interfaces and API's, Data Loss & Leakage, and Hardware Failure—which accounted for 29%, 25% and 10% of all cloud security outages respectively. Together, these form shared technology vulnerabilities. In a cloud provider platform being shared by different users there may be a possibility that information belonging to different customers resides on same data server. Additionally, Eugene Schultz, chief technology officer at Emagined Security, said that hackers are spending substantial time and effort looking for ways to penetrate the cloud. "There are some real Achilles' heels in the cloud infrastructure that are making big holes for the bad guys to get into". Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack—a process he called "hyper jacking". Some examples of this include the Dropbox security breach, and iCloud 2014 leak. Dropbox had been breached in October 2014, having over 7 million of its user’s passwords stolen by hackers in an effort to get monetary value from it by Bitcoins (BTC). By having these passwords, they are able to read private data as well as have this data be indexed by search engines (making the information public).

There is the problem of legal ownership of the data (If a user stores some data in the cloud, can the cloud provider profit from it?). Many Terms of Service agreements are silent on the question of ownership. Physical control of the computer equipment (private cloud) is more secure than having the equipment off site and under someone else's control (public cloud). This delivers great incentive to public cloud computing service providers to prioritize building and maintaining strong management of secure services. Some small businesses that don't have expertise in IT security could find that it's more secure for them to use a public cloud. There is the risk that end users do not understand the issues involved when signing on to a cloud service (persons sometimes don't read the many pages of the terms of service agreement, and just click "Accept" without reading). This is important now that cloud computing is becoming popular and required for some services to work, for example for an intelligent personal assistant (Apple's Siri or Google Now). Fundamentally, private cloud is seen as more secure with higher levels of control for the owner, however public cloud is seen to be more flexible and requires less time and money investment from the user.

Limitations and disadvantages:

According to Bruce Schneier, "The downside is that you will have limited customization capacity. Cloud computing is less cost because of economics of scale, and — like any outsourced task — you tend to get what you get. A restaurant with a limited menu is less cost than a personal chef who can cook anything you want. Fewer options at a much cheaper price: it's a feature, not a bug." He also suggests that "the cloud provider might not meet your legal needs" and that businesses need to weigh the benefits of cloud computing against the risks. In cloud computing, the control of the back end infrastructure is limited to the cloud vendor only. Cloud providers often decide on the management policies, which moderates what the cloud users are able to do with their deployment. Cloud users are also limited to the control and management of their applications, data and services. This includes data caps, which are placed on cloud users by the cloud vendor allocating certain amount of bandwidth for each customer and are often shared among other cloud users.

Privacy and confidentiality are big concerns in some activities. For instance, sworn translators working under the stipulations of an NDA, might face problems regarding sensitive data that are not encrypted. Cloud computing is beneficial to many enterprises; it lowers costs and allows them to focus on competence instead of on matters of IT and infrastructure. Nevertheless, cloud computing has proven to have some limitations and disadvantages, especially for smaller business operations, particularly regarding security and downtime. Technical outages are inevitable and occur sometimes when cloud service providers become overwhelmed in the process of serving their clients. This may result to temporary business suspension. Since this technology's systems rely on the internet, an individual cannot be able to access their applications, server or data from the cloud during an outage.

REFERENCES

[1] Cloud Computing, Black Book by, Kailash Jayaswal, Jagannath Kallakruchi, Donald J. Houde, Dr.Devan Shah.
[2] Cloud Computing Design, Thomas Erl, Robert Cope, Amin Naserpour.