BAOU
Education for All

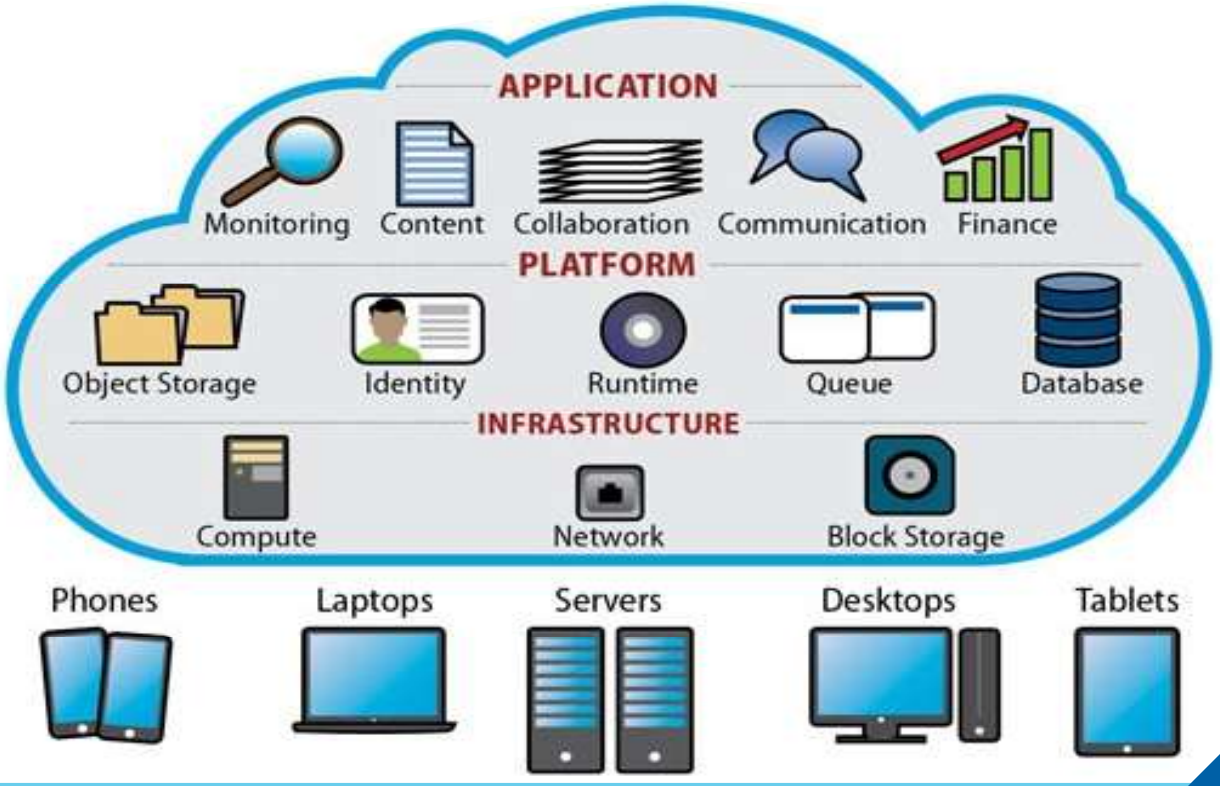
Dr.Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCS-202

Cloud Infrastructure and Services

Cloud Infrastructure and Services



Post Graduate Diploma in Cyber Security (PGDCS)

2021

Cloud Infrastructure and Services

Dr. Babasaheb Ambedkar Open University

Cloud Infrastructure and Services

Course Writer

Dr. Jitendra Bhatia — Assistant Professor
Computer Engineering Department,
Vishwakarma Government Engineering college,
Ahmedabad

Dr. Chirag Patel — Assistant Professor
Information Technology Department,
Vishwakarma Government Engineering college,
Ahmedabad

Content Reviewer and Editor

Prof. (Dr.) M. T. Savliya — Professor and Head,
Computer Engineering Department,
Vishwakarma Government Engineering college,
Ahmedabad

ISBN:

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

Dr.Babasaheb Ambedkar Open University

PGDCS-202

Cloud Infrastructure and Services

Block-1: Introduction to Cloud Computing

Block-2: Cloud Computing Services

Block-3: Application Architecture for Cloud and Cloud Deployment Techniques

Block-4: Risk, Security, Consequences and Cost of Cloud Computing

Block-1

Introduction to Cloud Computing

Unit 1:Introduction to Cloud

1

Unit Structure

1.1 LEARNING OBJECTIVE

After studying this unit, student should be able to:

- `Understand the basics of cloud computing
- Know the other similar configurations
- Understand the difference between applications oriented versus service oriented architecture.

1.2INTRODUCTION TO CLOUD

Cloud computing was formally put forward in IT industry by IBM who announced its plan of cloud computing in the end of 2007. Due to the growth of IT industry, the need of computing and storage has increased manifolds. Cloud Computing is the emerging technology for online allotment of computing resources and storage for user's data on the pay-as-you-go basis following utility computing model. Although computer experts and manufacturers have different views about cloud computing, it is an indisputable fact that cloud computing has brought opportunities and challenges to IT industry. IT professionals actively promote the development of cloud computing from their own products and technical theory. Cloud computing has become the largest hearing field in IT by 2010. Not only IT industry, but also other industries are actively discussing the vague "cloud" world. At present, what kind of cloud is being applied? What kind of services and business are provided by cloud computing? What is the impact of cloud computing in IT industry?

Cloud computing is defined as a large – scale distributed computing paradigm. Whereas the cloud providers or users are having their own private infrastructure, where the several types of services are provided to clients using virtual machines which are hosted by providers.

The most acceptable definition of cloud computing was introduced by National Institute of Standards and Technology (NIST): "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."

Cloud computing uses the storage, resources, and services of remote host across internet instead of physical servers or pcs. It includes some utilization techniques which improves the efficiency of the system. Some are the Network Utility, Network Activity, Disk I/O utility, CPU utilization of a system and available memory for perform the operation. It is a breakthrough that contracts with various services over the internet. Cloud computing avoids the up-front infrastructure cost and enables to focus on the primary goals.

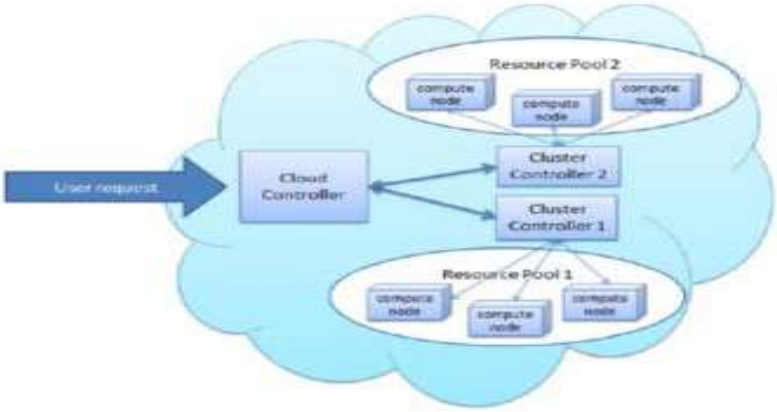


Figure: Cloud architectural view

It primarily focuses on scalability, high performance, high availability, fault-tolerant, consistent and easy to use, manage, monitor, and efficiency provisioning. Cloud Computing can be visualized into three steps that are Cloud application, Cloud Platform and Cloud infrastructure. The three main services that are associated with cloud computing are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) which are accessible to the user as public, private or hybrid cloud. The user can reserve and release resources on demand, allowed by the Elasticity characteristic of cloud computing, which helps to reduce the cost by making them pay as per use.

Most of us use cloud computing all day long without realizing it. When you sit at your PC and type a query into Google, the computer on your desk isn't playing much part in finding the answers you need: it's no more than a messenger. The words you type are swiftly shuttled over the Net to one of Google's hundreds of thousands ofclustered PCs, which dig out your results and send them promptly back to you. When you do a

Google search, the real work in finding your answers might be done by a computer sitting in California, Dublin, Tokyo, or Beijing; you don't know—and most likely you don't care!

The same applies to Web-based email. Once upon a time, email was something you could only send and receive using a program running on your PC (sometimes called a mail client). But then Web-based services such as Hotmail came along and carried email off into the cloud. Now we're all used to the idea that emails can be stored and processed through a server in some remote part of the world, easily accessible from a Web browser, wherever we happen to be. Pushing email off into the cloud makes it supremely convenient for busy people, constantly on the move.

Preparing documents over the Net is a newer example of cloud computing. Simply log on to a web-based service such as Google Documents and you can create a document, spreadsheet, presentation, or whatever you like using Web-based software. Instead of typing your words into a program like Microsoft Word or OpenOffice, running on your computer, you're using similar software running on a PC at one of Google's world-wide data centers. Like an email drafted on Hotmail, the document you produce is stored remotely, on a Web server, so you can access it from any Internet-connected computer, anywhere in the world, any time you like. Do you know where it's stored? No! Do you care where it's stored? Again, no! Using a Web-based service like this means you're "contracting out" or "outsourcing" some of your computing needs to a company such as Google: they pay the cost of developing the software and keeping it up-to-date and they earn back the money to do this through advertising and other paid-for services.

1.3CHARACTERISTICS OF CLOUD COMPUTING

On-demand self-service: Resources should be always available when you need them, and you have control over turning them on or off to ensure there’s no lack of resource or wastage happen.

Scalable: You should be able to scale (increase or decrease the resource) when necessary. The cloud providers should have sufficient capacity to meet customer’s needs.

Multi-tenant: Sometimes you may be sharing the same resource (e.g. hardware) with another tenant. But of course, this is transparent to the customer. Cloud provider shall responsible for the security aspect, ensuring that one tenant won't be able to access other's data.

Self-service computation and storage resource: Related processes including billing, resource provisioning, and deployment should be self-service and automated, involving much less manual processing. If a machine where our service is hosted fails, the cloud provider should be able to failover our service immediately.

Reliability: Cloud provider should be able to provide customer reliability service, committing to uptimes of their service.

Road network access: All the cloud computing services are accessible over the network, supporting various client platforms.

Resource Pooling: The computing resources of a provider are pooled together to serve multiple users using multi-tenant model, with dynamic provisioning of different physical and virtual resources on user demand.

Rapid elasticity: It is the seamless scaling out and scaling in of the cloud resources. Services are provisioned and released as per the need of the user. They seems as infinite to a user.

Measured service: It reflects the pay-as-you-go model of utility computing. Provides accounting service of a resource involving monitoring, measuring and billing transparently based on utilization.

More efficient resource utilization

Reduced time to market

1.4OTHER SIMILAR CONFIGURATIONS

System Administrators often used to talk about servers as a whole unit that includes the hardware, the OS, the storage, and the applications. Servers are often referred to by their function i.e., the Exchange server, the SQL server, the File server, etc.

What if Server fails?

If the File server fills up, or the Exchange server becomes overtaxed, then the System Administrator must add in a new server. Unless there are multiple servers, if

a service experiences a hardware failure, then the service is down. System Administrators can implement clusters of servers to make them more faults tolerant. However, even clusters have limits on their scalability, and not all applications work in a clustered environment. This raised issues on server maintenance and thus originating the concept of Virtual server.

Virtual Server

Virtual server concept separates the server software away from the hardware. Virtualization is what creates a cloud. This includes the OS, the applications, and the storage for that server. Servers end up as mere files stored on a physical box, or in enterprise storage. A virtual server can be serviced by one or more hosts, and one host may house more than one virtual server. Virtual servers can still be referred to by their function i.e. email server, database server, etc. If the environment is built correctly, virtual servers will not be affected by the loss of a host. Hosts may be removed and introduced almost at will to accommodate maintenance. Virtual servers can be scaled out easily. If the administrators find that the resources supporting a virtual server are being taxed too much, they can adjust the amount of resources allocated to that virtual server. Server templates can be created in a virtual environment to be used to create multiple, identical virtual servers. Virtual servers themselves can be migrated from host to host almost at will.

Service Oriented Architecture

Service-oriented architecture (SOA) is a style of software design where services are provided to the other components by application components, through a communication protocol over a network. The basic principles of service-oriented architecture are independent of vendors, products and technologies.A service is a discrete unit of functionality that can be accessed remotely and acted upon and updated independently, such as retrieving a credit card statement on line.

A service has four properties according to one of many definitions of SOA:

1. It logically represents a business activity with a specified outcome.
2. It is self-contained.
3. It is a black box for its consumers.
4. It may consist of other underlying services.[3]

Different services can be used in conjunction to provide the functionality of a large software application, a principle SOA shares with modular programming. Service-oriented architecture integrates distributed, separately maintained and deployed software components. It is enabled by technologies and standards that facilitate components' communication and cooperation over a network, especially over an IP network.

Service-oriented architecture (SOA) is a software development model for distributed application components that incorporates discovery, access control, data mapping and security features.

For decades, software development required the use of modular functional elements that perform a specific job in multiple places within an application. As application integration and component-sharing operations became linked to pools of hosting resources and distributed databases, enterprises needed a way to adapt their procedure-based development model to the use of remote, distributed components. Simple models like the remote procedure call (RPC) were a start in the right direction, but RPC lacked the security and data-independent features needed for truly open and distributed operations**.**

The solution to this problem was to redefine the old operation model into a broader and more clearly architected collection of services that could be provided to an application using fully distributed software components. The architecture that wrapped these services in mechanisms to support open use under full security and governance was called the service-oriented architecture, or SOA. SOA was introduced in the late 1990s as a set of principles or requirements; within a decade, there were several suitable implementations.

Differences between Cloud Computing and SOA:

Despite the similarities between Cloud Computing and SOA, they are not the same. Following are some of the differences between them:

- **Outcome vs. Technology** – In Cloud Computing, we are paying for the outcome but in SOA we are paying for technology.
- **External vs. External and/or Internal Point-of-View** – In Cloud Computing, the

services that organizations get are from external organization but in SOA these services can be either from external organizations (e.g., Yahoo! Pipes) and/or internally (e.g., system-to-system integration between two or more systems).

- **IaaS, PaaS, SaaS vs. Software Components** – In Cloud Computing, the services provided can go up and down the stack but in SOA the services are software components.

Grid Computing

Grid computing and cloud computing are conceptually similar that can be easily confused. The concepts are quite similar and both share the same vision of providing services to the users through sharing resources among a large pool of users.

Both are based on network technology and are capable of multitasking meaning users can access a single or multiple application instances to perform different tasks.

While grid computing involves virtualizing computing resources to store massive amounts of data, whereas cloud computing is where an application doesn't access resources directly, rather it accesses them through a service over the internet.

In grid computing, resources are distributed over grids, whereas in cloud computing, resources are managed centrally.

Grid computing is a network based computational model that has the ability to process large volumes of data with the help of a group of networked computers that coordinate to solve a problem together.
Basically, it's a vast network of interconnected computers working towards a common problem by dividing it into several small units called grids. It's based on a distributed architecture which means tasks are managed and scheduled in a distributed way with no time dependency.

The group of computers acts as a virtual supercomputer to provide scalable and seamless access to wide-area computing resources which are geographically distributed and present them as a single, unified resource to perform large-scale applications such as analyzing huge sets of data.

Both grid computing and cloud computing are network-based computing technologies that involve resource pooling, but cloud computing eliminates the complexity of buying hardware and software for building applications by allocating

resources that are placed over multiple servers in clusters. Grid computing, on the contrary, is a computing technology that combines computing resources from various domains to reach a common goal.

The computers on the network work on a task together and every computer can access the resources of every other computer within the network. In simple terms, grid computing is a group of interconnected computers that work together to handle huge volumes of data.

Cluster Computing

More than one computer combine to form a cluster. It exhibits very high performance but from the end users perspective, they feel like working on a standalone system. Cluster computing follows distributed systems as its principle. LAN acts as the connection unit here. The clustering methods encompass HPC IAAS, HPC PAAS, which are further luxurious and hard to set up and preserve than a single computer. A computer cluster helps to largely reduce the unavailability of these systems and provides larger storage to other desktop workstation or computer.

Some of the most widely used Cluster Computers are Petroleum Reservoir Simulation, Google Search Engine, Earthquake Simulation, Weather Forecasting.

1.5LET'S SUM UP

Points to ponder

- SOA is a framework that allows business processes to be highlighted to deliver interoperability and rapid delivery of functionality
- Cloud computing decreases the hardware and software demand from the user's side.
- Grid computing is a network based computational model that has the ability to process large volumes of data.
- Grid is a application oriented while cloud is a service oriented.
- The cloud servers are owned by infrastructure providers and are placed in physically disparate locations.

1.6CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1.7FURTHER READING

1. Here is an article about the various Linux commands:
   https://www.guru99.com/cloud-computing-for-beginners.html

1.8ASSIGNMENTS

1) Discuss in detail, the advantages of cloud computing.
2) How grid computing differs from the cloud computing?
3) What do you mean by virtualization?

1.9ACTIVITIES

Q1. Multiple Choice Questions:

1) All cloud computing applications suffer from the inherent _____ that is intrinsic in their WAN connectivity.
   - A. propagation
   - B. latency
   - C. noise
   - D. All of the mentioned

2) Cloud computing is a _____ system and it is necessarily unidirectional in nature.
   - A. stateless
   - B.stateful
   - C. reliable
   - D. 4

3) Which of the following is related to service provided by Cloud ?
   - A. Sourcing
   - B. Ownership
   - C. Reliability
   - D.AaaS

1.10CASE STUDIES

Prepare a list of services provided by giant cloud service providers like Amazon, IBM, Microsof Azure etc.

Unit 2: Cloud and Other Architectures

2

Unit Structure

1.1 LEARNING OBJECTIVE

After studying this unit, student should be able to:

- understand the basic layered architecture of cloud
- explore various other architectures
- exploit the advantages of virtualization

1.2 CLOUD LAYERED ARCHITECTURE

The term cloud computing is a wide umbrella encompassing many different things; lately it has become a buzzword that is easily misused to revamp existing technologies and ideas for the public. Cloud computing can be viewed as a collection of services, which can be presented as a layered cloud computing architecture, as shown in Fig.

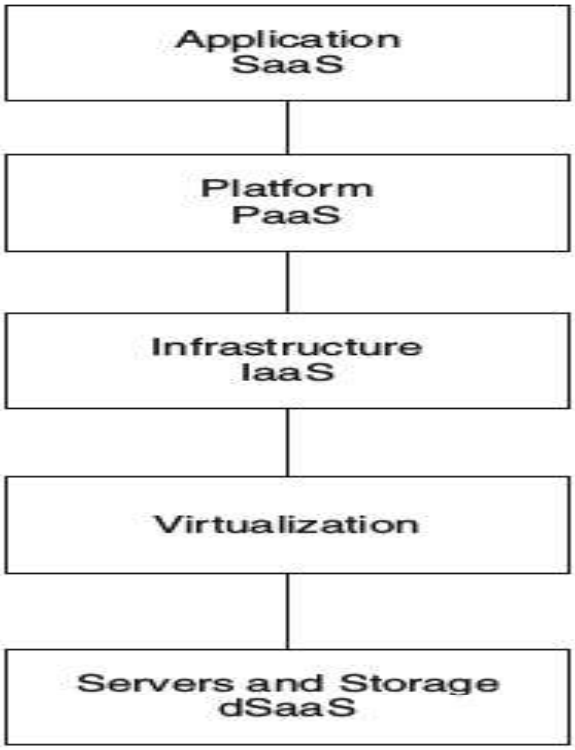


Fig: Layered Architecture of Cloud Computing

The services offered through cloud computing usually include IT services referred as to SaaS (Software-as-a-Service), which is shown on top of the stack. SaaS allows users to run applications remotely from the cloud. Infrastructure-as-a-service (IaaS) refers to computing resources as a service. This includes virtualized computers with guaranteed processing power and reserved bandwidth for storage and Internet access. Platform-as-a-Service (PaaS) is similar to IaaS, but also includes operating systems and required services for a particular application. In other words, PaaS is IaaS with a custom software stack for the given application. The data-Storage-as-a-Service (dSaaS) provides storage that the consumer is used including bandwidth requirements for the storage.

1.3 CLOUDVERSUS PEER TO PEER ARCHITECTURE

A peer-to-peer architecture is a network of hosts in which resource sharing, processing, and communications control are completely decentralized. Each host acts as a server or provider of certain services. However, it relies on other nodes within the network for other services. All clients on the network are equal in terms of providing and using resources and users are authenticated by each individual workstation. In peer-to-peer networking, users are allowed to access the resources available on the network on their own. This makes the security factor very risky.

There are important benefit-related dissimilarities between cloud and peer-to-peer deployments. Distinctive benefits of cloud computing are that it can be easily scaled to meet growth demands, enables access to any type of hosted applications, does not burden user-end devices, and needs to be configured with the highest levels of security. On the other hand, peer-to-peer deployments are relatively inexpensive and simple to set up and manage.

The shortcomings of cloud computing include high initial capital investment and good technology expertise to establish and managed it. The downside of peer-to-peer architecture is that it is limited in extensibility, tends to overburden user workstations by making them work as servers for other users, has lax security, and is typically unable to provide any type of system-wide service. But, these downsides of peer-to-

peer implementations can be overcome by using servers that are dedicated to computing, storage, management, and monitoring.

1.4 CLOUD COMPUTING VS CLIENT-SERVERARCHITECTURE

In client/server architecture, one logs on to a server, authenticating their identification against credentials saved on the server and not on the local computer. Whereas cloud access usually occurs without the need for manual user-provided credentials, after the user has logged on to the computer, or other devices, utilizing locally-saved credentials.

Both of them provide storage of the user computer for necessary files. Some would claim that cloud storage is more transparent to the user, which is absolutely true.

Client/server architectures are normally deployed in organizations where control of the user computer and computer access, such as centrally-stored user credentials, operating system updates, or updating user applications are centrally administered and directed.

The primary difference in cloud computing and traditional networking or hosting is the implementation, and in one word that is “virtualization.” Virtualization allows for extensive scalability, giving clients virtually limitless resources.

In a traditional networking setup, the server is settled in hardware and if you want to scale up to more users than the current hardware can support, you would need to allocate more money for upgrades and there would still be a limit. But with cloud computing infrastructure, multiple servers are already in place at the start, they then use virtualization to render only the resources that a specific user needs which give it great scalability from the small needs of resources of personal businesses to heavy corporate resource needs. A Cloud provider is able to scale resources without issues and the client will only need to pay for what they use. In traditional networking, you need to pay for everything; the hardware, the installation, maintenance, or even just rent it for a monthly fixed price, even if you only need a small bit of resource.

In summary, cloud architecture is or can be just another kind of a client/server architecture where the user is cunningly insulated from the client/server aspects of its implementation. It all depends on who controls what cloud and which cloud that we are talking about. Expect that in the near future, all client/server architectures look more like the cloud than networks of old, but it is still pretty much the same thing. Remote storage of user data that is modified locally and accessible to the user regardless of which platform they use to access it.

1.5 CLOUD COMPUTING VS GRID COMPUTING

Grid computing is a network-based computational model that can process a large amount of data with the help of a group of interconnected computers that coordinate to solve the problem together. The computing is done by dividing the problems into several small problems called grids. These grids are then deployed on the computers on the network. The group of computers acts as a virtual supercomputer that provides scalable and seamless access to wide area computing resources which are distributed on computers and are not present on the internet.

1.6 DIFFERENCES BETWEEN CLOUD COMPUTING AND GRID COMPUTING

Grid computing is a distributed architecture-based computing where each task is divided into smaller tasks deployed on computer networks. Cloud computing, on the other hand, is based on network technology where every user of the cloud has its own private resource that is provided by the specific provider.

Both the technologies having similar characteristics of resource pooling; however, they differ in their architectures, business model, interoperability and certain different features. Grid computing is a collection of distributed resources where resources are distributed over different computing units present over different locations. Whereas, cloud computing is a form of computing where resources are centrally managed which are located over multiple servers in clusters.

The main function of grid computing is task scheduling since the task is divided into grids that are being distributed on several computers connected to the network. After all the grids(sub-tasks) gets completed, they are sent back to the main machine which integrates the small task into a summed up one. Whereas, cloud computing does the process computing based on the resource pooling i.e. the resources are grouped according to process requirements.

The cloud manages data, security requirements, job queues, etc. by eliminating the needs and complexity of buying hardware and software needed to build applications which are to be delivered as a service over the cloud. Grid computing is mostly used by academic research and is able to handle large sets of limited duration jobs that involve huge volumes of data.

Conclusively it can be said the grid computing is a network that is connected to different computing units that hold the required resources for computation. While cloud computing is a network that contains all the resources distributed over different servers in the form of cluster, which can be used by certain computers for different computations.

1.7 SERVER VIRTUALIZATION VS CLOUD COMPUTING

Virtualization technology is one of the fundamental components of cloud computing, especially in regard to infrastructure-based services. Virtualization allows the creation of a secure, customizable, and isolated execution environment for running applications, even if they are untrusted, without affecting other users' applications. The basis of this technology is the ability of a computer program—or a combination of software and hardware—to emulate an executing environment separate from the one that hosts such programs. For example, we can run Windows OS on top of a virtual machine, which itself is running on Linux OS. Virtualization provides a great opportunity to build elastically scalable systems that can provision additional capability with minimum costs. Therefore, virtualization is widely used to deliver customizable computing environments on demand.

Virtualization is a large umbrella of technologies and concepts that are meant to provide an abstract environment—whether virtual hardware or an operating system—to run applications. The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing. In fact, virtualization technologies have a long trail in the history of computer science and have been available in many flavors by providing virtual environments at the operating system level, the programming language level, and the application level. Moreover, virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking. Since its inception, virtualization has been sporadically explored and adopted, but in the last few years there has been a consistent and growing trend to leverage this technology. Virtualization technologies have gained renewed interested recently due to the confluence of several phenomena.

The advantage of cloud computing is the ability to virtualize and share resources among different applications with the objective for better server utilization. In non-cloud computing three independent platforms exist for three different applications running on its own server. In the cloud, servers can be shared, or virtualized, for operating systems and applications resulting in fewer servers (in specific example two servers).

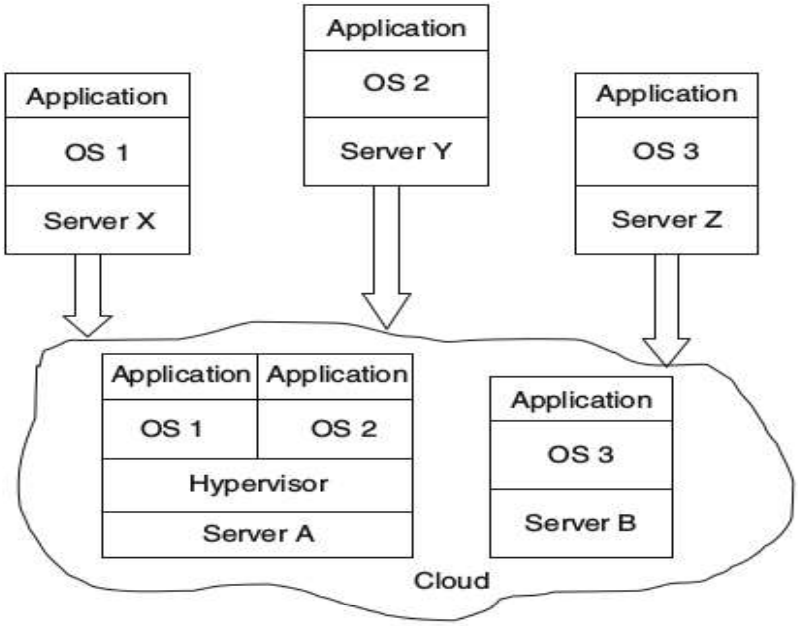


Figure: An example of Fig: An example of virtualization: in non-cloud computing there is a need for three servers; in the cloud computing, two servers are used (adapted from Jones)

Virtualization technologies include virtual machine techniques such as Vmware and Xen, and virtual networks, such as VPN. Virtual machines provide virtualized IT-infrastructures on-demand, while virtual networks support users with a customized network environment to access cloud resources.

1.8 VIRTUALIZATION AND CLOUD COMPUTING

Virtualization plays an important role in cloud computing since it allows for the appropriate degree of customization, security, isolation, and manageability that are fundamental for delivering IT ser-vices on demand. Virtualization technologies are primarily used to offer configurable computing environments and storage. Network virtualization is less popular and, in most cases, is a complementary feature, which is naturally needed in build virtual computing systems. Particularly important is the role of virtual computing environment and execution virtualization techniques. Among these, hardware and programming language virtualization are the techniques adopted in cloud computing systems. Hardware virtualization is an enabling factor for solutions in the Infrastructure-as-a-Service (IaaS) market segment, while programming language virtualization is a technology leveraged in Platform-as-a-Service (PaaS) offerings. In both cases, the capability of offering a customizable and sandboxed environment constituted an attractive business opportunity for companies featuring a large computing infrastructure that was able to sustain and process huge workloads. Moreover, virtualization also allows isolation and a finer control, thus simplifying the leasing of services and their accountability on the vendor side. Besides being an enabler for computation on demand, virtualization also gives the opportunity to design more efficient computing systems by means of consolidation, which is performed transparently to cloud computing service users. Since virtualization allows us to create isolated and controllable environments, it is possible

to serve these environments with the same resource without them interfering with each other. If the underlying resources are capable enough, there will be no evidence of such sharing. This opportunity is particularly attractive when resources are underutilized, because it allows reducing the number of active resources by aggregating virtual machines over a smaller number of resources that become fully utilized. This practice is also known as server consolidation, while the movement of virtual machine instances is called virtual machine migration.

1.9 LET'S SUM UP

Points to ponder

- A peer-to-peer architecture is a network of hosts in which resource sharing, processing, and communications control are completely decentralized.
- Grid computing is a distributed architecture-based computing where each task is divided into smaller tasks deployed on computer networks.
- Virtualization allows for extensive scalability, giving clients virtually limitless resources.
- Peer-to-peer deployments are relatively inexpensive and simple to set up and manage.

1.10 FURTHER READING

1. Here is an article about the various Linux commands: https://techdifferences.com/difference-between-cloud-computing-and-grid-computing.html

1.11 ASSIGNMENTS

1) What is virtualization and what are its benefits?
2) What are the characteristics of virtualized environments?
3) State the difference between client server and peer to peer architectures.
4) Compare and contrast grid versus cloud computing.

1.8 CASE STUDIES

1.8 Case Studies (Optional)

Prepare a documentation of various hypervisor for virtualization.

Unit 3: Cloud Computing in a nutshell

3

Unit Structure

1.1 LEARNING OBJECTIVE

After studying this unit, student should be able to:

- understand the basics of system models for distributed systems and cloud
- understand the basic principles and desired features of cloud computing
- assess risks and challenges involved in adopting cloud computing

1.2 SYSTEM MODELS: DISTRIBUTED AND CLOUD

The fundamentals of distributed and cloud computing systems are they are built over a huge number of autonomous computer nodes. And these computer nodes are interconnected in LANs, MANs, WANs in a coexisting manner. Massive systems are considered highly scalable and can reach web-scale connectivity, either physically or logically. massive systems are classified into four groups: clusters, P2P networks, computing grids, and Internet clouds over huge data centers.

1) A cluster of Cooperative computers: A computing cluster consists of interconnected stand-alone computers which work cooperatively as a single integrated computing resource. In the past, clustered computer systems have demonstrated impressive results in handling heavy workloads with large data sets.

2) Grid Computing Infrastructures: As an electric utility power grid, a computing grid offers an infrastructure that couples computers, software/middleware, special instruments, and people and sensors together. The grid is often constructed across LAN, WAN, or Internet backbone networks at a regional, national, or global scale. Enterprises or organizations present grids as integrated computing resources. They can also be viewed as virtual platforms to support virtual organizations. The computers used in a grid are primarily workstations, servers, clusters, and supercomputers. Personal computers, laptops, and PDAs can be used as access devices to a grid system.

3) Peer-to-Peer Network Families: An example of a well-established distributed system is client-server architecture. In this scenario, client machines (PCs and workstations) are connected to a central server for computing, e-mail, file access, and database applications. P2P architecture offers a distributed model of networked systems. First, a P2P network is client-oriented instead of server-oriented.

4) Internet Cloud: a cloud allows workloads to be deployed and scaled-out quickly through rapid provisioning of virtual or physical machines. The cloud supports redundant, self-recovering, highly scalable programming models that allow workloads to recover from many unavoidable hardware/software failures. Finally, the cloud system should be able to monitor resource use in real time to enable rebalancing of allocations when needed. Cloud computing applies a virtualized platform with elastic resources on demand by provisioning hardware, software, and data sets dynamically. The idea is to move desktop computing to a service-oriented platform using server clusters and huge databases at data centers.

1.3 CLOUD COMPUTING LAYERS:

I. Infrastructure as a Service (IAAS): IAAS providers give low-level abstractions of physical devices. Amazon Web Services (AWS) is an example of IAAS. AWS provides EC2 for computing, S3 buckets for storage, etc. Mainly the resources in this layer are hardware like memory, processor speed, network bandwidth, etc.

II. Platform as a Service (PAAS): PAAS providers offer managed services like Rails, Django, etc. One good example of PAAS is Google App Engineer. These are the environments in which developers can develop sophisticated software with ease. Developers just focus on developing software, whereas scaling and performance are handled by PAAS provider.

III. Software as a Service (SAAS): SAAS provider offers an actual working software application to clients. Salesforce and Github are two good examples of SAAS. They hide the underlying details of the software and just provide an interface to work on the system. Behind the scenes, the version of Software can be easily changed.

1.4 BASIC PRINCIPLES OF CLOUD COMPUTING

The six principles - detailed in the recently published ISACA publication Guiding Principles for Cloud Computing Adoption and Use - include enablement, cost/benefit, enterprise risk, capability, accountability, and trust. Here's how ISACA defines each of those principles:

1) Enablement: Plan for cloud computing as a strategic enabler, rather than as an outsourcing arrangement or technical platform.
2) Cost/benefit: Evaluate the benefits of cloud acquisition based on a full understanding of the costs of cloud compared with the costs of other technology platform business solutions.
3) Enterprise risk: Take an enterprise risk management perspective to manage the adoption and use of the cloud.
4) Capability: Integrate the full extent of capabilities that cloud providers offer with internal resources to provide comprehensive technical support and delivery solution.
5) Accountability: Manage accountabilities by clearly defining internal and provider responsibilities.
6) Trust: Make trust an essential part of cloud solutions, building trust into all business processes that depend on cloud computing.

1.5 DESIRED FEATURES OF CLOUD

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 using a multi-tenant model, with different physical and virtual resources

dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacenter). Examples of resources include storage, processing, memory and network bandwidth.

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 to be 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 the provider and consumer.

1.6 CHALLENGES AND RISKS IN CLOUD COMPUTING

Cloud Migration: Cloud migration is the process of moving data, applications, and other important information of an organization from its on-premises either desktops or servers to the cloud infrastructure, and this can also involve in moving data between different cloud setups.

Cloud migration enables all the computing capabilities those were performed earlier by devices installed on-premises. Cloud migration is a big challenge as many companies when they require to migrate from on-premises to cloud or from one cloud to another, they partner with experienced cloud service provider.

Incompatibility: During moving workloads from on-premises to the cloud, the common issue the incompatibility between on-premises infrastructure and the services which are companies going to buy from the public cloud providers. In last current years, most CSPs tried to create “connectors of sort” to make practices more standardize and homogenous.

Data Security: CSPs are responsible to provide clouds' security, but they're not responsible for your apps, servers, and security of data. As per CDW 2013 State of the Cloud Report, "46 percent of respondents face security of data or applications as a significant challenge."

When your CSP ensure you about the complete compliance and regulation, don't consider it as 100% compliant and yielding. You still require to encrypt and secure your own data and should invest in buying suite of tools from your CSP to protect your data from cyber-attacks.

Lack of Expertise: With the quick advancements and improvements in cloud technologies, more and more organizations are clouds to place their workloads. However, they face difficulties to keep up with the tools which require particular expertise. Organizations can deal with this challenge by providing cloud technologies training to their sys admins along with development staff.

Downtime: Businesses suppose complete data accessibility and availability when their data is stored on cloud anytime from anywhere. The main challenge most organizations face is they can access their data from cloud only through internet connection. So, poor internet connection can disrupt cloud services and higher risks of data accessibility.

Bandwidth Cost: Though organizations and businesses can save money on hardware using cloud, but they have to pay extra for the bandwidth they use to access their workloads. However, it doesn't charge much for smaller apps, but data-intensive apps need more bandwidth which can costs higher.

1.7 LET'S SUM UP

Points to ponder

- P2P architecture offers a distributed model of networked systems.
- Cloud computing applies a virtualized platform with elastic resources on demand by provisioning hardware, software, and data sets dynamically.
- IAAS providers give low-level abstractions of physical devices.
- SAAS provider offers an actual working software application to clients.

1.8 FURTHER READING

1. Here is an article about the various Linux commands:

https://cloudacademy.com/blog/cloud-migration-benefits-risks/

1.9 LEARNING OBJECTIVE

1) Discuss in detail, various other desirable features of cloud computing.
2) Explain how down time violate the service level agreement.
3) What do you mean by virtualization?

1.10 ACTIVITIES

Q1. Multiple Choice Questions:

1) Which of the following benefit is related to creates resources that are pooled together in a system that supports multi-tenant usage?
   a) On-demand self-service
   b) Broad network access
   c) Resource pooling
   d) All of the mentioned
2) Which of the following is the most important area of concern in cloud computing?
   a) Security
   b) Storage
   c) Scalability
   d) All of the mentioned
3) Which of the following is best known service model?
   a) SaaS
   b) IaaS
   c) PaaS
   d) All of the mentioned

Unit 4: Cloud Types and Models 4

Unit Structure

1.1 LEARNING OBJECTIVE

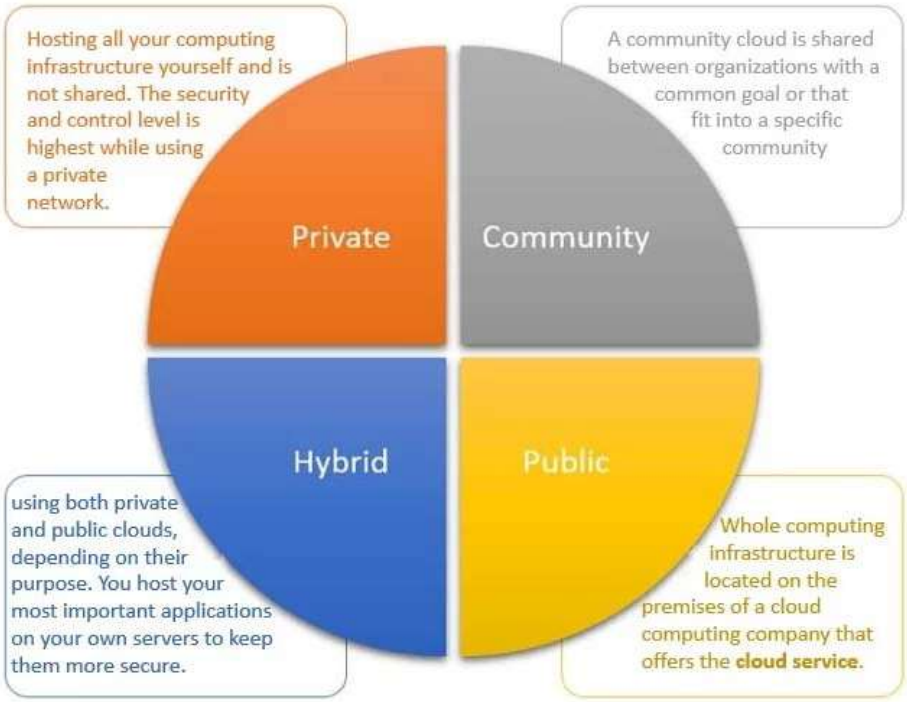
After studying this unit, student should be able to:

- understand the various types of cloud and services
- identify the various uses of cloud computing.

1.2 CLOUD TYPES

To be precise, cloud computing is the delivery of computing services like servers, storages and more over the Internet. The companies that offer these computing services are called cloud providers. They charge for cloud computing services based on usage.

Cloud computing is usually classified on the basis of location, or on the service that the cloud is offering. Based on a cloud location, we can classify cloud as: Public, Private, Hybrid, and Community. Depending on the type of data we are working with, we have to compare public, private, and hybrid clouds in terms of the different levels of security and management required.



Public Cloud

Public clouds are the most common way of deploying cloud computing. The cloud resources (like servers and storage) are owned and operated by a third-partycloud service provider and delivered over the Internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software and other supporting infrastructure are owned and managed by the cloud provider. In a public cloud, you share the same hardware, storage and network devices with other organisations or cloud “tenants”. You access services and manage your account using a web browser. Public cloud deployments are frequently used to provide web-based email, online office applications, storage, and testing and development environments.

Advantages

- Lower costs – no need to purchase hardware or software, and you only pay for the service you use.
- No maintenance – your service provider provides the maintenance.
- Near-unlimited scalability – on-demand resources are available to meet your business needs.
- High reliability – a vast network of servers ensures against failure.

Limitations

- The total cost of ownership (TCO) can rise exponentially for large-scale usage, specifically for midsize to large enterprises.
- Not the most viable solution for security and availability sensitive mission-critical IT workloads.
- Public clouds often cannot meet many security regulatory compliance requirements since different servers reside in multiple countries with various security regulations.
- Low visibility and control into the infrastructure, which may not suffice to meet regulatory compliance.
- Network issues can occur during peaks in online traffic.

Private Cloud

A private cloud consists of computing resources used exclusively by one business or organisation. The private cloud can be physically located at your organisation's on-site data centre, or it can be hosted by a third-party service provider. But in a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organisation. In this way, a private cloud can make it easier for an organisation to customise its resources to meet specific IT requirements. Private clouds are often used by government agencies, financial institutions and any other medium to large-sized organisations with business-critical operations seeking enhanced control over their environment.

Advantages

- More flexibility – your organisation can customise its cloud environment to meet specific business needs.
- Improved security – resources are not shared with others, so higher levels of control and security are possible.
- High scalability – private clouds still afford the scalability and efficiency of a public cloud.

Limitations

- Expensive solution with a relatively high total cost of ownership as compared to public cloud alternatives for short-term use cases.
- Mobile users may have limited access to the private cloud considering the high security measures in place.
- The infrastructure may not offer high scalability to meet unpredictable demands if the cloud data center is limited to on-premise computing resources.
- The heightened security of a private cloud can make it difficult to access from remote locations too.

Hybrid Cloud

Often called "the best of both worlds", hybrid clouds combine on-premises infrastructure, or private clouds, with public clouds so that organisations can reap the advantages of both. In a hybrid cloud, data and applications can move between

private and public clouds for greater flexibility and more deployment options. For instance, we can use the public cloud for high-volume, lower-security needs such as web-based email, and the private cloud (or other on-premises infrastructure) for sensitive, business-critical operations like financial reporting. In a hybrid cloud, “cloud bursting” is also an option. This is when an application or resource runs in the private cloud until there is a spike in demand (such as a seasonal event like online shopping or tax filing), at which point the organisation can “burst through” to the public cloud to tap into additional computing resources.

Advantages

- Control – your organisation can maintain a private infrastructure for sensitive assets.
- Flexibility – you can take advantage of additional resources in the public cloud when you need them.
- Cost-effectiveness – with the ability to scale to the public cloud, you pay for extra computing power only when needed.
- Ease – transitioning to the cloud doesn’t have to be overwhelming because you can migrate gradually – phasing in workloads over time.

Limitations

- It can get expensive.
- A difficulty with a hybrid cloud is it can be hard to maintain and secure on account of being more complex.
- Integration can be a challenge since a hybrid cloud is a combination of different clouds, data and applications.
- Strong compatibility and integration is required between cloud infrastructure spanning different locations and categories. This is a limitation with public cloud deployments, for which organizations lack direct control over the infrastructure.
- Major compatibility issues can arise across the infrastructure when developing a hybrid cloud as well.
- Additional infrastructure complexity is introduced as organizations operate and manage an evolving mix of private and public cloud architecture.

Community cloud:

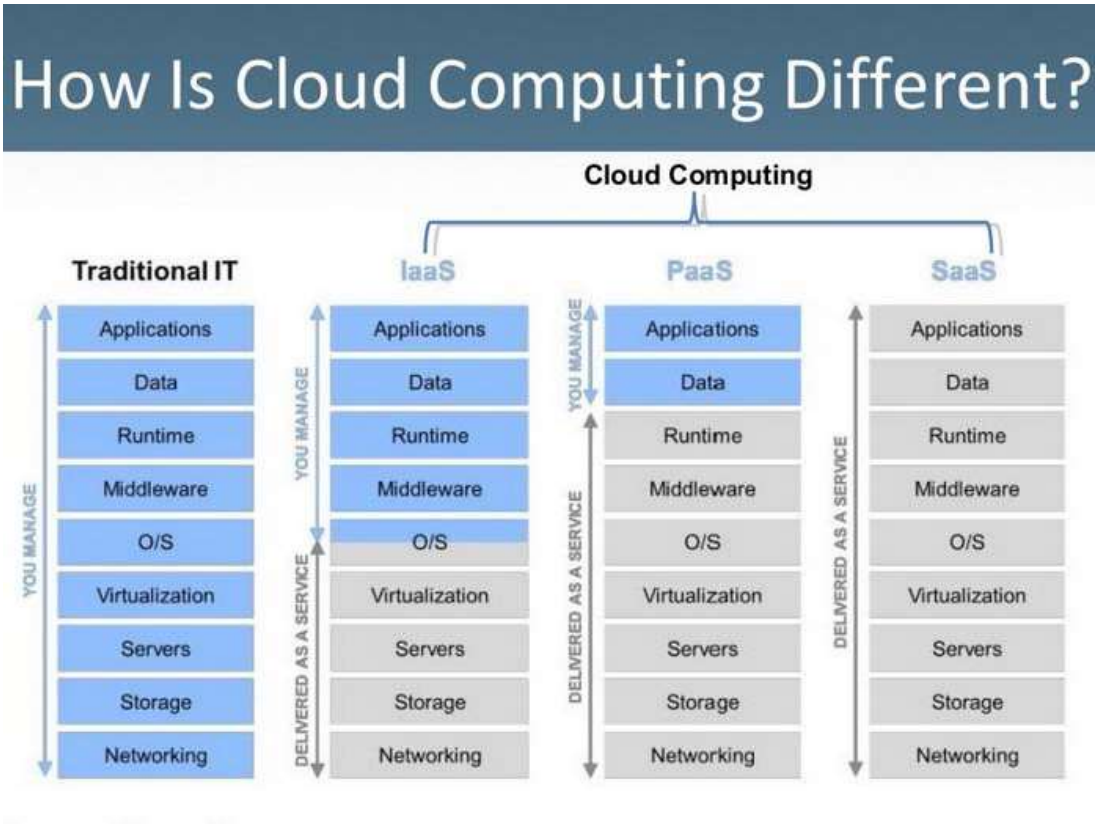
Community clouds are distributed systems created by integrating the services of different clouds to address the specific needs of an industry, a community, or a business sector. In community cloud, the infrastructure is shared between organization which have shared concerns or tasks. The cloud may be managed by an organization or a third party.

Sectors that use community clouds are:

1. Media Industry: Media companies are looking for quick, simple, low-cost way for increasing efficiency of content generation.Most media productions involve an extended ecosystem of partners. In particular, the creation of digital content is the outcome of a collaborative process that includes movement of large data, massive compute-intensive rendering tasks, and complex workflow executions.
2. Healthcare Industry: In healthcare industry community clouds are used to share information and knowledge on the global level with sensitive data in the private infrastructure.
3. Energy and Core Industry: In these sectors, the community cloud is used to cluster set of solution which collectively addresses management, deployment, and orchestration of services and operations.
4. Scientific Research: In this organization with common interests of science share large distributed infrastructure for scientific computing.

1.3 TYPES OF CLOUD SERVICES

Cloud computing services fall into 4 categories: infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS) and FaaS (functions as a service). These are sometimes called the cloud computing stack, because they build on top of one another.



Infrastructure as a service (IaaS): IaaS is the most basic category of cloud computing services that allows you rent IT infrastructure (servers or VM's) from a cloud provider on a pay-as-you-go basis.

Platform as a service (PaaS): Platform-as-a-service (PaaS) refers to the supply an on-demand environment for developing, testing, delivering and managing software applications. It is designed to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and databases needed for development.

Software as a service (SaaS): Software-as-a-service (SaaS) is a method for delivering software applications over the Internet as per the demand and on a subscription basis. SaaS helps you host and manage the software application and underlying infrastructure and handle any maintenance (software upgrades and security patching).

Functions as a service (FaaS)

FaaS adds another layer of abstraction to PaaS, so that developers are completely insulated from everything in the stack below their code. Instead of handling the

hassles of virtual servers, containers, and application runtimes, they upload narrowly functional blocks of code, and set them to be triggered by a certain event. FaaS applications consume no IaaS resources until an event occurs, reducing pay-per-use fees.

1.4 USE OF CLOUD COMPUTING

Although we do not realize we are probably usingcloud computing right now, most of us use an online service to send email, edit documents, watch movies, etc. It is likely that cloud computing is making it all possible behind the scenes. Today a variety of organisations ranging from tiny startups to government agencies are embracing this technology for the following:

- Create new apps and services as well as store, back up and recover data
- Host websites and blogs
- Stream audio and video
- Deliver on demand software services
- Analyze data for patterns
- Make predictions

1.5 LET'S SUM UP

Points to ponder

- A fundamental characteristic of public clouds is multi tenancy.
- Private clouds are distributed systems that work on a private infrastructure and providing the users with dynamic provisioning of computing resources.
- Hybrid cloud is a heterogeneous distributed system resulted by combining facilities of public cloud and private cloud.
- A major drawback of private deployments is the inability to scale on demand and to efficiently address peak loads.
- In community cloud, the infrastructure is shared between organization which have shared concerns or tasks.

1.6 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1.7 FURTHER READING

- Here is an article about the various Linux commands:
  https://www.vxchnge.com/blog/different-types-of-cloud-computing
  https://www.geeksforgeeks.org/types-of-cloud/

1.8 ASSIGNMENTS

- Compare and contrast public versus private cloud.

1.9 ACTIVITIES

Q1. Multiple Choice Questions:

1) Which of the following is owned by an organization selling cloud services?
   a) Public
   b) Private
   c) Community
   d) Hybrid

2) _____ provides virtual machines, virtual storage, virtual infrastructure, and other hardware assets.
   a) IaaS
   b) SaaS
   c) PaaS
   d) All of the mentioned

3) Which of the following provides development frameworks and control structures?
   a) IaaS
   b) SaaS
   c) PaaS
   d) All of the mentioned

4) _____ is a complete operating environment with applications, management, and user interface.

a) IaaS

b) SaaS

c) PaaS

d) All of the mentioned

5) Which of the following is one of the unique attributes of Cloud Computing?

a) utility type of delivery

b) elasticity

c) low barrier to entry

d) all of the mentioned

6) Point out the correct statement.

a) Service Level Agreements (SLAs) is small aspect of cloud computing

b) Cloud computing does not have impact on software licensing

c) Cloud computing presents new opportunities to users and developers

d) All of the mentioned

7) A service that concentrates on hardware follows the _____ as a Service model.

a) IaaS

b) CaaS

c) PaaS

d) All of the mentioned

8) _____ is a pay-as-you-go model matches resources to need on an ongoing basis.

a) Utility

b) Elasticity

c) Low barrier to entry

d) All of the mentioned

Block-2

Cloud Computing Services

Unit 1:Infrastructure as a Service & Platform as a Service

1

Unit Structure

1.1 LEARNING OBJECTIVE

This chapter discusses about,

- Service Models in Cloud Environment
- Services offered under IaaS and PaaS
- Pricing models for IaaS and PaaS related services
- Major Public Cloud Service Providers and their services
- Case Study of Amazon IaaS
- Case Study of Google App Engine

1.2CLOUD SERVICE MODELS

In the last chapter, we have discussed about different cloud deployment models like: private cloud, public cloud and hybrid cloud. These deployment models are classified based upon the location of hardware resources. The Cloud computing paradigm offers different resources in the form of services. In this unit, we will discuss about different service models: Infrastructure as a Service, Platform as a Service and Software as a Service etc. These services are related with each other. The figure below shows the layered view of these services.

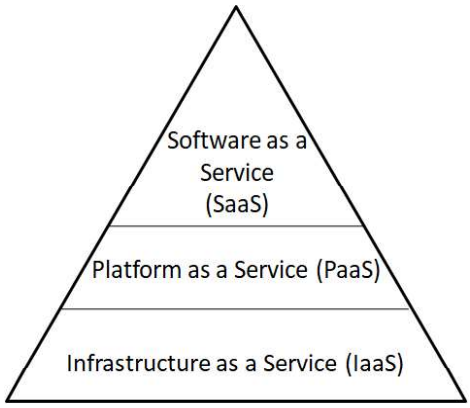


Figure-1 Layered view of Cloud Services

There are mainly two roles in cloud computing environment: Cloud Service Provider and Cloud Service User. The responsibilities of service providers and users depend upon the type of service. The figure 2 summarizes responsibilities. In case of in house on premise data centre each and every resources are managed by the

user. If user moves to cloud based service model, some of the tasks are carried out by service providers. The IaaS service provider manages all low level resources like network, physical servers, operating system etc. The users have to concentrate on their applications, run time environments, middleware and the data. If the user moves to PaaS, he or she has to just focus on application and data everything else is managed by PaaS service provider. The SaaS provides highest level of freedom in which, users just make use of services all other things in background are managed by SaaS provider. Some of the most common IaaS, PaaS and SaaS public service providers are listed in table 1

Type of the Service	Major Service Providers
IaaS	Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE), DigitalOcean, Linode, Rackspace
PaaS	Google App Engine, Apache Stratos, AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, OpenShift
SaaS	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting

Table-1 Major Public Service Providers

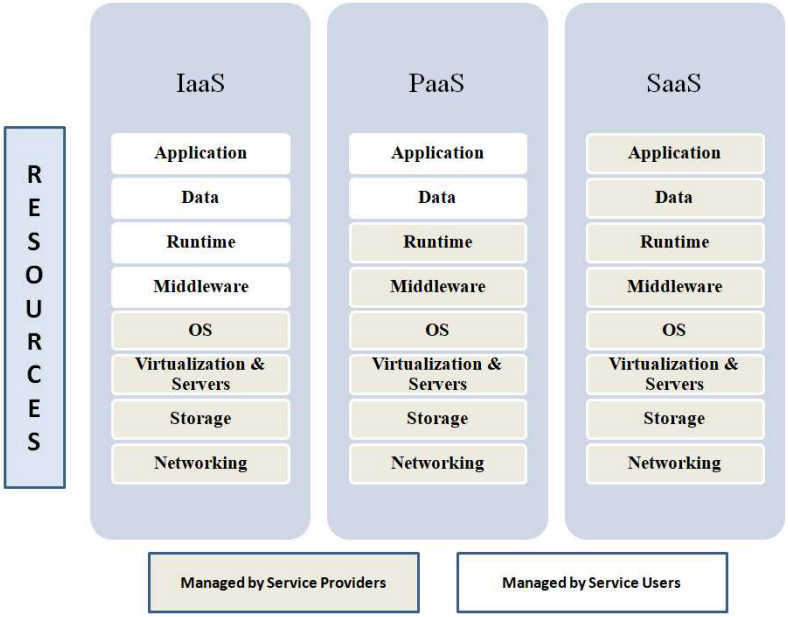


Figure-2 Responsibilities of service providers and users

1.3 INFRASTRUCTURE AS A SERVICE(IaaS)

Traditionally, companies spend huge amount to own and manage the IT related hardware infrastructure (physical resources). The infrastructure is maintained as “On premise & In-house” data centre. Instead of owning the IT resources, the cloud computing paradigm offers access to IT infrastructure in the form of services i.e. less cost of ownership. These services are called Infrastructure as a Service (IaaS). Various services offered via IaaS are:

- Storage Service
- Compute Service
- Network Service
- Cloud Management Service

➢ **Characteristics of IaaS**

- Access through rich user interface

  IaaS providers offer different interfaces to access their services. Some of the most common interfaces are Web Interface, Programming API and Command Line Interface (CLI) etc.

- Pay as you Go model

  There are various pricing models for accessing IaaS. One of the most common models is Pay as you Go. In this model, users are charged based on the amount to time the service is used and the type of service.

- Self service based on demand provisioning

  Users of IaaS can choose their desired service from rich set of available offerings. Cloud service providers offer different services via online platforms.

- Higher availability

  Infrastructure related services are offered over the Internet. Users can access their infrastructure from any part of the world via any device. This feature makes services highly available.

- Highly Reliable

  IaaS providers have huge amount of hardware resources pooled in their data centres across different locations. In case of any failure of any service, they switch over user services on some other physical hardware in a very amount of time. This kind of feature makes IaaS very reliable.

- Scalable

  Scalability is one of the inhering characteristics of cloud computing. Generally, cloud users are not aware about the workload. They may hire infrastructure related resources by considering some initial workload. In case of higher workload, this may lead to the performance degradation. IaaS providers offer the feature of auto scaling. This enables the users to scale up or down (increase or decrease) their hired resources.

- **When to use IaaS?**

  - When the demand of computing resources is volatile.
  - When new organizations want to reduce the capital cost incurred on the purchase of hardware resources.
  - When specific, trial or temporary access of hardware resources is needed.

- **When not to use IaaS?**

  - When we want the higher level of performance. The on-premise or dedicated hosted infrastructure gives better performance than IaaS.
  - When the regulatory compliance restricts the off-shoring or outsourcing of the data storage and processing.

- **Different services offered by IaaS Providers**

  1. **Storage Services**

     It allows users to store data on the data storage devices owned by cloud service providers. The data stored on cloud can be accessed at any time and from any place. In background, the storage service providers manage several distributed storage devices. They also maintain redundancy and consistency of data to provide reliable services. These internal complexities of storage service providers are kept hidden from users.

Some of the issues with storage service are: Dependency of Internet, Network Latency and data security. The pricing of storage service depends upon various factors like:

- Storage capacity
- Amount of data transferred to cloud
- Amount of data retrieved from cloud
- Nature of reliability and security

2. Compute Services

Generally, the IaaS providers offer compute services in the form of virtual machine instances. This service refers to the provision of various computing resources like, RAM, CPU and I/O. IaaS providers offer different configurations of compute resources in form of many instances types. Users can easily choose the type of instance from set of available options.

The price of particular instance (service) depends upon factors like: Amount of resources, Type of hardware resources, Type and version of operating system, Mode and duration of service etc. Some of the most popular pricing models are,

- On-Demand

  This type of service offers flexibility to users such that they can occupy desired compute service at any time. The users are charged on hourly basis. Users can occupy and free resources on the fly without any long term commitments. This mode is suitable for the users, who do not know their compute related requirements in advance.

- Prepaid

  It is also called the reservation based model. In this, users have to pay in advance for the specific time during which they want to access the service. IaaS services under this mode are cheaper than the on-demand mode because, service providers know the resource requirements in advance and they can do better management of their infrastructure. This mode is suitable for the users who know their compute related requirements in advance.

- Auctioned

  This model allows users to bid for required resources. The bid price is controlled by service providers on the basis of supply & demand of resources. This mode helps service providers to improve utilization of their unutilized infrastructure. Similarly, this model is useful to users because they can get desired compute resources at cheaper rate. This mode is suitable when the resource requirement is not immediate. This model is useful for non-production environments.

3. Network Related Services

IaaS providers also offer network related services. Two most widely used IaaS network services are: Load Balancing and DNS. The Load balancing service provides a single access point to several servers owned by a particular organization. The load balancer distributes requests among several servers. Some of the most common load balancing approaches are: simple round robin, weighted round robin, dynamic round robin, least connections, fastest server etc.

DNS is hierarchical system used for resolution of names and IP addresses. A cloud provider's DNS services offer to store IP/domain-name mapping for both internal and external servers. Some of the main features under DNS service are listed below.

- Store IP/domain-name mapping for both internal and external servers. DNS management API for developers is used to automate DNS related operations such as authentication and domain-zone creation
- Extended security and access control
- Geo location-based DNS routing

4. Cloud Management Services

Cloud Management Service providers help the customers to simplify Cloud management related operations. Cloud management services (CMS) help to fill gaps between cloud management tools. CMS providers work directly with specific cloud service providers to integrate their services with a

customer's existing cloud, or to create extra value added services on top of the provider's existing infrastructure.

- Cloud Value Added Management Services

  The Value Added Management Services enhance existing cloud provider services by building additional features on top of it. The value added management service help customers to save time and resources by automating regular tasks which are manually performed.

- Cloud Integration Service (CIS)

  CIS provides a ways to have integration between private and public clouds. CIS offers an abstraction layer which enables transparent multi-cloud support. A CIS can automate administrative tasks like: provisioning, scaling, monitoring and configuration. CIS provides multi-cloud governance tools to allow customers to monitor logs, security events, and resource utilization from a single dashboard.

- Cloud Service Brokerages (CSB)

  The CSB aggregate the services offered by different cloud providers. It organizes these services into a easily-searchable service catalogue. CSB services can be considered as a marketplace for cloud services from where, customers can quickly identify and purchase required services.

1.4PLATFORM AS A SERVICE(PaaS)

Platform as a Service (PaaS) is a cloud service model which provides a configurable application platform. PaaS can be considered as an abstraction layer above the hardware, operating system, and virtualization stack.

The PaaS model helps companies to reduce complexity of infrastructure and application maintenance. It allows companies to focus on core software development process and improve productivity. The figure 3 gives overview of services offered under PaaS model.

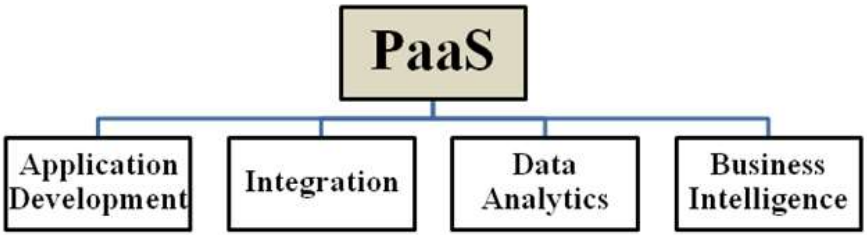


Figure-3 Services offered under PaaS Model

- **Benefits of PaaS**

PaaS provides means to simplify tasks like,

- Write, build and deployment tools for rapid application development and deployment
- Application integration with other components such as web services and databases
- Multi-tenancy, platform service that can be used by many concurrent users
- Easy Management of API
- Logging, reporting, and code instrumentation
- Security, Scalability, redundancy and auto-provisioning infrastructure to applications

- **Services offered under PaaS Model**

1. **Integration Services**

The Integration service helps companies to integrate data from multiple sources. Data may be available from different sources like: on-premise private cloud databases, public cloud databases, vendor databases, CRM systems, Messaging systems etc. The integration task becomes very challenging because of data quality, compatibility and standards.

Dell Boomi is a leader in cloud data integration. It integrates over 40 different technologies and protocols like Oracle, SAP, Siebel, Salesforce, Hadoop, QuickBooks etc. The data integration can be achieved either by writing our custom code or by using integration service.

The data integration done via custom written code approach has several drawbacks like:

- Large internal resource requirements
- Frequent changes are not supported
- Lack of business agility
- Higher maintenance cost
- Manual backups
- Custom security

Against the custom written code based approach, the integration service has several advantages like:

- Small requirements of IT infrastructure
- Easy to use
- Cost effectiveness
- Automatic update
- Built-in security
- Supports large variety of technologies and standards

2. Application Development and Deployment Services

PaaS application development and QA services help companies to improve the code quality. It also helps to accelerate software development process and better collaboration among development team.

In today's world, development teams prefer to use agile software development model instead of conventional waterfall model. The agile development method needs higher level of team collaboration and an intense continuous delivery cycle with frequent code releases, tests, and deployments. The development teams are geographically distributed across different locations. In all these situations, companies can benefit from PaaS tools that simplify and streamline team collaboration and create a faster time-to-market cycle.

PaaS development platforms like Google AppEngine and Amazon Beanstalk take a continuous delivery approach (agile development approach) to the next level by giving more support for developers through automating build, test, release, deployment, and operation processes.

In PaaS environment, users don't need to be an expert of operating system or networking tasks to manage the operations related to infrastructure. The PaaS based cloud platform performs all these tasks. In addition to routine infrastructure operations, PaaS also does auto scaling of infrastructure based on certain application performance conditions.

3. Data Analysis and Business Intelligence Services

These services help companies to simplify data analysis related operations and apply statistical analysis methods to support business decision making and information retrieval. The need for data analysts and statisticians is very high. It is very expensive for companies to hire data scientists, and it also takes a long time to develop internal expertise. PaaS platforms cannot completely solve this issue, but they can certainly hide some complexity and simplify data analysis related tasks. These services are more suitable for companies which satisfies bellow conditions,

a. Data are already hosted in the cloud
b. Limitations of service are acceptable
c. Data analysis related workload is not predictable and in this case will benefit from cloud elasticity
d. Don't have sufficient financial resources to build an internal data analysis platform
e. SLA requirements are satisfied by service provider.

Data analysis and statistical modelling related tasks require massive computational capacity which can be easily hired by IaaS model. This idea makes data analysis task cost effective.

Some of the issues with this kind of service are as below.

1. Lack of Control

   Companies do not have full control on public cloud data related operations such as storage, backup, network transfer and security (access control & encryption).

2. Lack of Customization

   Public cloud services have many customers. These services cannot fully satisfy the need of each and every customer. Typically, service providers try to offer “good-enough” solutions and sets of features that are usable by a majority of customers. If additional features are required, there is no guarantee that the provider can add them.

3. Lack of Maturity

   Many public cloud services under this category are offered and built by relatively new companies. Sometimes, these solutions may not provide the same rich set of features found in on-premise solutions like Oracle, Teradata, or SAP.

1.5CASE STUDIES

- **Case Study 1**
  Amazon (IaaS Platform)
- **Case Study 2**
  Google App Engine (PaaS Platform)

Unit-2 Software as a Service and Database as a Service

2

Unit Structure

2.1 LEARNING OBJECTIVE

This chapter discusses about,

- Software as a Service Model
- Database as a Service Model
- Case Study about Software as a Service (SalesForce.com)
- Case Study about Database as a Service (https://aws.amazon.com/rds/Oracle DBaaS / Amazon RDBMS aaS)

2.2 SOFTWARE AS A SERVICE (SaaS)

Software as a Service (SaaS) is a cloud computing based services delivery model in which software are provided online and on-demand basis. Two major key events which increased the popularity of the SaaS based approach are:

1. The Internet became a commercial platform.
2. For companies it was costly, complex and difficult to install, run, upgrade and manage Software.

SaaS refers to the software which is deployed on a hosted service and is accessible over the Internet. Just like other cloud delivery models as described in previous chapter, the SaaS allows companies to reduce expenses on purchase and management of software application resources.

SaaS is one of the most widely used cloud delivery model. Almost every software vendor tries to offer software over SaaS model. Currently, there are SaaS offerings in every category of software products. Some of the most widely adopted categories of application software under SaaS model are:

- Billing and Inventory Systems
- Customer Relationship Management (CRM) software
- Help desk related applications
- HR management applications
- Security related software
- Social service related software

- **Desired Characteristics of SaaS software**

Some of the desired characteristics which make the SaaS software commercially feasible are listed as below.

- The SaaS application should be generalized so that customers will be interested in the application.
- The SaaS application should be modular and service oriented.
- An SaaS application should include measuring and monitoring features so customers can be charged based on actual usage
- SaaS applications should have sophisticated navigation mechanism to provide ease of use
- The SaaS application must have a built-in billing service.
- SaaS applications must ensure integrity, reliability and security of customer's data
- SaaS applications should constantly provide faster releases of new features and new capabilities. This must be provided without affecting existing customers.

- **Features of SaaS based application software**

Some of the important features of SaaS based application software are:

a. SaaS makes the software available over the Internet.
b. SaaS allows usage or subscription based licensing.
c. SaaS applications are cost effective since they do not require any maintenance at end user side.
d. SaaS based applications are available on demand and they can be scaled up or down on demand.
e. The Software is maintained by the vendor rather than where they are running.
f. They are automatically upgraded and updated.
g. All users are running same version of the software.

- **Benefits of SaaS based Approach**

A. Minimal Software Tools

The SaaS based approach needs minimal or no software installation at client site which gives benefits like:

- No complex software package installation at client side
- Very less configurations at client side
- Software distribution cost is less
- Software management and update task becomes easy

B. Centralized Management of Data

Generally, in SaaS based application software the data is stored on Cloud. Service providers take care about reliability, security and access control of data by features like replication and encryption.

C. Multitenant Solutions

Multiple users can share a single instance of data and application by virtual isolation. Users can customize their applications based on requirements without affecting basic functionality.

D. Efficient usage of software licence

Users can have single license for multiple computers running at different locations which reduces the cost of licensing. Users do not require license servers because the software runs in the provider's infrastructure

E. Reduced Cost

SaaS platforms use multi-tenant architectures in which the same hardware platform and software is shared among multiple customers. This helps the SaaS service providers to provide services at lower costs.

- **SaaS Delivery Models**

SaaS based software can be broadly classified and delivered into three categories. These categories are discussed in this section.

- **Packaged software services**

  This is the biggest area in the SaaS market. This comes in many different options like Customer Relationship Management, Supply Chain Management and Finance Management etc. Applications in this category focus on a particular business process such as, Employee Management Process which includes functions like managing employees' benefits, salaries, leaves, and annual performance reviews etc. Some of the Companies working in the packaged software market are following:

  - Netsuite, like Salesforce.com, offers a CRM foundation. Netsuite provides several modules for enterprise resource planning (ERP) application to provide financial, e-commerce, and business intelligence services.
  - RightNow offers a CRM suite of products for marketing, sales, and other industry solutions.
  - Constant Contact is a marketing automation platform. They partners with CRM platforms like salesforce.com. They provide solutions to automate the process of sending emails and other marketing efforts.
  - Intuit provides a Financial Services Suite of products to provide accounting related services for small- and medium-sized businesses.

- **Collaborative software services**

  In current scenario the teams are located at different locations across the world which needs to collaborate. This kind of collaboration is possible due to the ubiquitous availability of the Internet. Some of the most common software which need collaborative efforts are web conferencing, document collaboration, project planning, instant messaging etc. Some of the companies working under collaborative software based approach are:

  - MicrosoftLive is one of the first collaboration as a service platform. Microsoft offers live meetings and messaging services. They also provide email server as a service.
  - GoogleApps from Google supports various collaborative applications like e-mail, document management, and instant messaging. It also publishes APIs so third party software developers can integrate with the platform.

- Zoho is an open-source collaboration platform to provide email, document management, project management, and invoice management related services. It also supports APIs to its environment to support collaborative development.
- Cisco Webex Collaboration platform offers SaaS based unified communications as a service.

- **Enabling and management services**

  Software in this category provides support for development and the deployment of SaaS applications. They provide development tools which are needed by developers to extend SaaS applications. They also provide facilities like testing, monitoring, and measuring of applications. Major services under this category of SaaS are as described below.

  a. Testing as a service

  Testing is one of the biggest uses for cloud computing. Development companies use this service to do different types of testing like functional testing, unit testing, stress testing, performance testing etc. Many vendors offer testing as a service including HP, IBM, Sogeti etc.

  b. Monitoring and management as a service

  Sometimes, companies using SaaS need to monitor their services to check whether their desired service levels have been satisfied by SaaS providers or not. In collaborative environments, companies may need to monitor service levels of different SaaS based applications.

  c. Development as a service

  This delivery model of development infrastructure is created through one of the Platform as a Service. Some vendors like Amazon offer support service for developers.

  d. Security as a service

  Many vendors, who provide antivirus software, offer their products as a service. Some of these vendors are Symantec, McAfee, CA, and Kapersky Labs etc. Identity management is an important aspect of on premise as well as cloud services.

e. Compliance and governance as a service

Compliance and governance related tasks are time consuming and complicated. This kind of services provide features like patch management, business continuity planning, discovery of records and messages, governance requirements such as SOX (Sarbanes-Oxley) in the United States and SaS 70 (Statement of Audit Standard) controls for data.

- **Limitations of SaaS Applications**
  - Not suitable for real time systems

    SaaS based applications run in cloud infrastructure. These applications are accessed by users over the Internet. The network delay makes SaaS based applications less suitable for real time systems.

  - Internet Dependency

    The Internet connectivity is must to work with these applications. The availability and speed of Internet may limit the access of these applications.

  - Data security and compliance

    Customer data is stored on cloud. It may cause security and compliance issues.

  - Lack of Interoperability and integration and Vendor locking

    SaaS based applications lack the flexibility of interoperability and integrations. These features are only possible if supported by vendors. This may lead to the vendor locking situations.

  - Less customization

    SaaS based applications are designed and developed by considering the common requirements of customers. This kind of generalized design may not provide some specific requirements of particular customer. In this case, if customization support is available than only these features can be developed.

- Limited range of applications

  SaaS based approach is relatively new and in growing phase. All the desktop based applications which are currently in use do not have SaaS based option.

2.3 DATABASE AS A SERVICE (DBaaS)

Database as a Service (DBaaS) is an architectural approach that enables IT providers to deliver database related functionality as a service to one or more consumers. The DBaaS allows customers to host their database related infrastructure in cloud and get freedom from many low level database related operations. Customers can focus more on their actual application development work.

DBaaS providers host database in cloud infrastructure and they also manage all hardware and networking related tasks. They also offer extra services like scaling, failover, backup, restore etc. Currently, DBaaS related services are available for every modern relational database like MySql, Oracle etc.

- **Why DBaaS?**

A conventional approach for database needs to allocate hardware and software resources. This requires budget and time for managing and deploying database systems. These tasks are to be repeated for development, testing and production environments.

These issues of conventional database can be overcome by DBaaS. In the case of DBaaS, the cloud-based automation provides the centralized database management application which reduces DBA related overhead. All intense and dedicated tasks like configuration, optimization, provisioning, backup, security, monitoring, networking, automation, upgrades, maintenance, etc. are performed by the DBaaS service provider's automated database management system. The figure 4 shows the usefulness of DBaaS approach over DBA. DBaaS relieves users from,

- Costly hardware/software purchases

- Compatibility checks

- Dependencies resolutions

- Backup and Cron jobs

- Hardware or OS failures

- System upgrade

- Management of Firewall rules

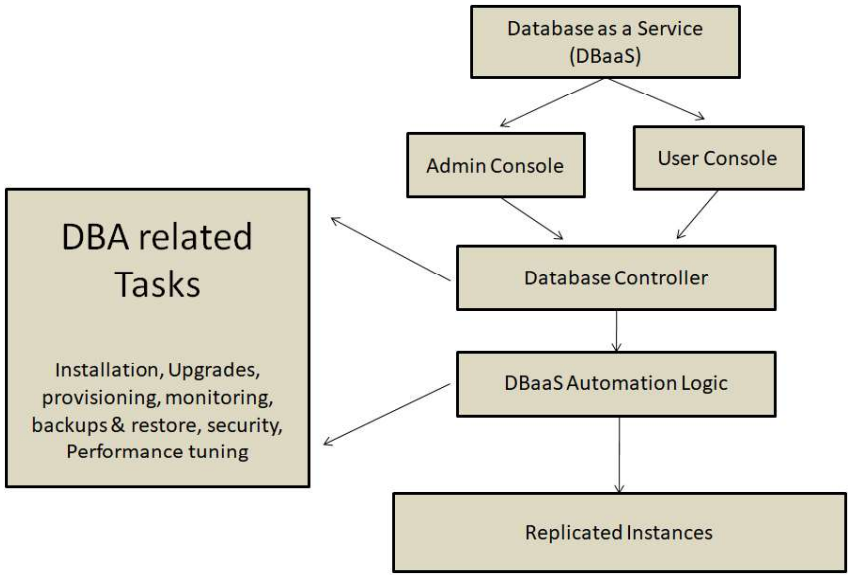


Figure- 4 DBaaS Services

(http://www.informit.com/articles/article.aspx?p=2521584&seqNum=3**)**

The services offered by the DBaaS vendor to the end user fall into three main categories: Provisioning services, Administrative services, and Reporting services. Some of these services are optional, and others are mandatory

Provisioning Services: Some of the provisioning related services are,

- The ability to request new databases
- Choose database options as per requirements (partitioning, advanced security, Real Application Cluster)
- Add or remove computing resources (storage, CPU, network bandwidth, etc.) to existing databases.
- Database backup capability

Administrative Services: Admin services offered by DBaaS include,

- Perform on-demand database restores and recoveries
- Perform database cloning from existing database backups
- Database performance monitoring and alerting capabilities

Reporting Services: Reporting services include,

- Database performance management and performance tuning via GUI
- Resource consumption and usage reports to facilitate scaling related operations
- The ability to track provider compliance to the SLAs

- **Selection of correct DBaaS Vendor**

The selection of DBaaS vendor by particular organization depends on several parameters. These parameters are described in this section.

1. Location of Database

Generally organizations hire cloud based application servers to deploy their applications and database servers for data storage. Ideally, these both categories of servers should be located nearby to each other may be within same datacentre. If they are located away from each other, there will be two major problems. First one is the latency. Due to distance between application server and database server, there will be latency which will degrade overall performance of system. The other issue is security. Due to different location of application and database servers, they require network for communications. This kind of network based data transfer may cause security issues.

2. Fault Tolerance, Availability and Redundancy

If the organization is running a production level application, the database should always be available, even during the hardware failure or maintenance. Generally, DBaaS vendors provide fault tolerance and higher availability via multi node based clusters.

Before choosing DBaaS vendor, one should check the approach used by vendors for fault tolerance. The cluster nodes might be created within a same datacentre or in different datacentres at different geographic locations.

Management of the cluster nodes at different geographic locations provides better protection against failures. Other parameters to consider are

- The mode of failure recovery: whether it is automatic or requires human interaction?
- Does the vender offer availability related SLA?
- How faulty components are replaced? Automatic or with human intervention.

3. Data durability via backup and restore

DBaaS vendor must have robust and reliable mechanism for backups and durability. The important things to consider are:

- Does the vendor use tools for managing backups?
- Does the vendor support point-in-time restore facility?
- Does vendor perform automatic backups and can we create custom schedule to create backups?
- Can we easily and quickly restore backups?

4. Performance Monitoring, analysis and Alerts

The Monitoring, performance analysis and alert features provide us the capabilities to check the health of database and its performance. Some of the important parameters to consider are:

- Does the vendor provide easy access to database related log files?
- Does the automatic alerts about failure are supported?
- Does the custom alerts are supported?
- Does the vendor provide real time and historical information about database performance metrics?

5. Performance and Scaling

The DBaaS vendor should provide a platform that performs well for normal workload. The similar kind of performance should be provided in case if the data volume becomes huge. The performance requirements of application should be assessed against the actual workload by simulating different kind of application workloads. Customers should not rely only on the benchmark workloads because it may not give correct picture about actual

workloads. To support performance requirements, scaling operations (horizontal / vertical) are performed be vendors. In the vertical scaling, resources (RAM, CPU, Disks) are added as data volume grows. The horizontal scaling adds more nodes to the system to handle the growth in data volume.

6. Security

Data is the most important asset for any organization. The DBaaS vendor must have expertise in security and should provide tools to ensure data security against the unauthorized access. Some of the important things to consider are:

- Is the database access logged?
- Does vendor support encryption of data?
- Does SSL certificated validation based data access is supported?
- Is authentication required to connect to database?
- Can firewall be configured to limit the database access?
- Does the vendor perform security audits?
- Does the vendor follow best security practices and standards?
- Does the vendor own any security compliance certificate?

7. Support

The faster and helpful vendor support is very much important for smooth execution of database and application. DBaaS vendor must provide advises and must respond in case of any emergency. Some of the points to consider are:

- Does the support is a part of DBaaS or additional cost is required?
- Does the provider offer a SLA regarding support and response times?
- Does the provider have a good reputation for outstanding support?

- **DBaaS Conceptual Architecture**

The figure 5 [Ref oracle document] shows the conceptual architecture of DBaaS, various components of DBaaS and relationship among them. The DBaaS

conceptual model shows the core capabilities which are required for the delivery of database related services.

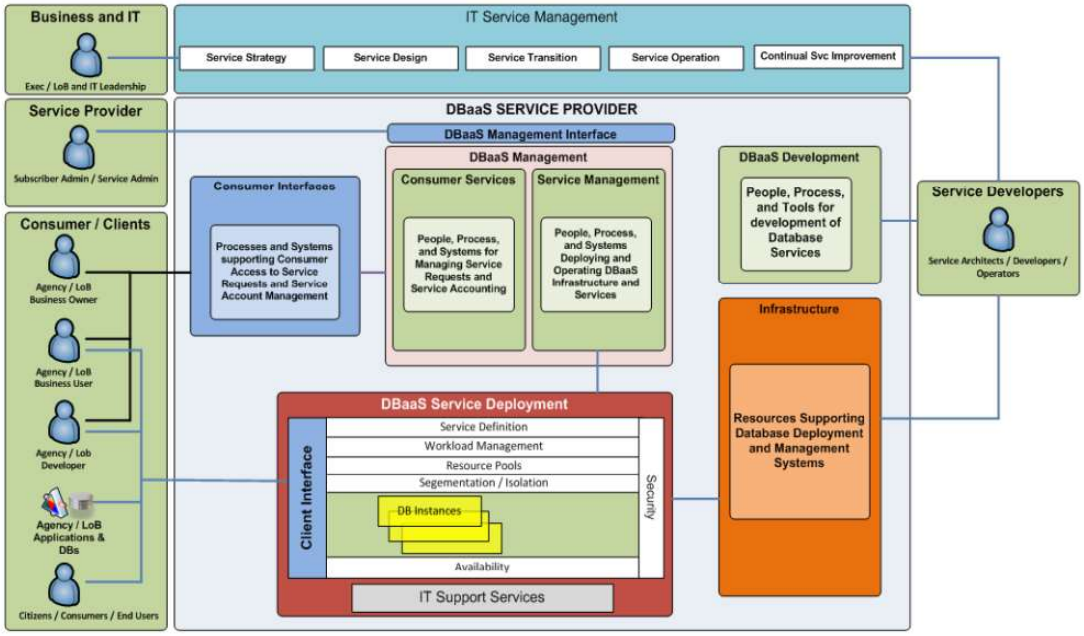


Figure-5 Conceptual architecture of DBaaS

1. DBaaS Development

DBaaS Development is required for defining the service offerings and for the management of the service catalogue. The DBaaS development is concerned with,

- The people, process and tools which are used to build the DBaaS service
- The design of the infrastructure required to provide the DBaaS
- The design and development of the system

2. DBaaS Management

It does the management of people, process and systems which are involved in organization's ability to request, manage, operate, and account for database services and their utilization. DBaaS Management has mainly two sub-capabilities:

- Subscriber Services- Supports the interactions between the subscriber and delivery of database services

- Service Management - Implements database services and manages the resources and systems supporting their delivery

3. DBaaS Service Deployment

This component deals with physical resources and their configuration to support the DBaaS. It also provides the interfaces required to manage the deployment, monitoring, and management of the services. It also deals with server configuration, networking and software which support the specific database deployment models.

4. Infrastructure

This component deals with the actual physical server resources required for systems and services for the management and deployment of the DBaaS architecture. The infrastructure includes servers, networking, software and other facilities.

5. IT Service Management

This component is used for service definition, design, operational practices and policies. The Service Management provides capabilities for defining and managing the services required for policies for design, change management, service operation & structure, the improvement framework.

6. Subscriber Interfaces

This interface provides systems and procedures to interact with the DBaaS management capabilities and subscribed database service instances.

Unit 3: Security as a Service 3

Unit Structure

3.1 LEARNING OBJECTIVE

This chapter discusses about security in cloud computing model.

- Introduction to Security as a Service (SECaaS)
- Cloud Security Risk Analysis
- SECaaS Categories defined by CSA
- Cloud Security Control Mechanisms
- Benefits of SECaaS
- Evaluation of Cloud Security Issues
- Cloud Security Standards
- Case Study: SECaaS

3.2 INTRODUCTION TO SECURITY AS A SERVICE

Cloud computing paradigm offers various benefits like on-demand scalability, pay as you go, accessibility to the data and application from anywhere in the world etc. With all these benefits, one of the major issues in cloud environment is security. Though the cloud offers many benefits, the security related issues make customers reluctant about migration towards cloud.

Different types of cloud computing service models provide different levels of security services. You get the least amount of built in security with an IaaS and highest level of security with SaaS. Proxy and brokerage services can be used to separate clients from direct access to shared cloud storage. Logging, auditing, and regulatory compliance are all features that require planning in cloud computing systems.

To provide security assurance in cloud, vendors offer security related solutions in the form of services. These are called Security as a Service also known as SeCaaS. The SECaaS is a service model in which, the cloud vendors offer security solutions subscription basis. The major goal of SeCaaS is to provide security to information systems along with business objectives of the organizations. The SeCaaS mainly focuses on three pillars of information security namely: Confidentiality, Integrity and Availability. Another reason behind popularity of

SeCaaS is the lack of expertise in cyber security field. Many companies cannot find security professionals.

3.3 CLOUD SECURITY RISK ANALYSIS

Before moving to the cloud based approach, any organization should do the risk analysis. The following steps will help any organization in risk analysis.

1. Determine which resources are to be moved to cloud

   The organization should clearly identify set of functionalities (data, services, or applications) those will be shifted in cloud.

2. Determine the risk sensitivity of each resource.

   Risks regarding loss of privacy, unauthorized access, data loss, lack of availability etc. should be evaluated.

3. Determine the risk associated with the particular cloud deployment model

   Cloud types can be public, private (both external and internal), hybrid, and shared community types. With each of this type, we should consider where data and functionality will be maintained.

4. Identify, which service model will be used?

   For each different service model (IaaS, SaaS, and PaaS), the customers are responsible for security at different levels.

5. Evaluate vendor security system

   If you have selected a particular cloud service provider, you should evaluate its system and also understand how data is transferred, where it is stored, and how to move data both in and out of the cloud.

3.4SECAAS CATEGORIES

The Cloud Security Alliance (CSA) has classified SECaaS services into different categories. The figure 6[REF] shows the CSA cloud reference model with security boundaries.

Identity and Access Management

This category involves managing access to various enterprise resources by verifying the identity of the entities and granting the correct level of access to the entity on the basis of authorization.

Data Loss Prevention

This category includes protecting the data in the cloud in every state, i.e. data at rest and in motion

Web Security

This category involves providing real-time protection by redirecting the web-traffic to the cloud provider and then forwarding the clean traffic to the customer.

Email Security

This category provides control over outbound and inbound emails, thus protecting the customer from phishing and malicious attachments in email.

Security Assessments

These are the audits performed by third party for cloud services or assessment of the on-premises systems via cloud-provided systems.

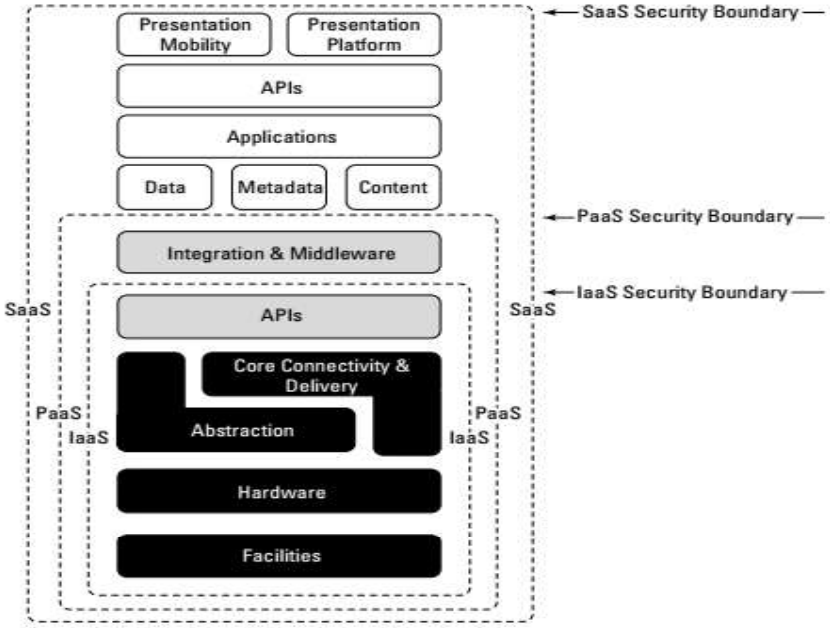


Figure-6 CSA cloud reference model

Intrusion Management

This category includes the process of intrusion detection by prevention via anomaly based approach to respond to unusual events.

Security Information and Event Management (SIEM)

SIEM analyses and correlates the event logs related to security issues and provides real-time report and alert on the security issues that may require urgent attention.

Encryption

It is the process of providing private and public cryptographic algorithms for the security of data at rest, in motion, etc.

Business Continuity and Disaster Recovery

It is the process of ensuring the business objectives are in continuity in the event of any failures.

Network Security

It includes security provisions that allocate access and protect the underlying the network resource services.

- **Control Mechanisms for Cloud Security**

1. Detective Control

Detect and react promptly & appropriately to any security violation incident.

2. Preventive Control

Strengthen the system against security violation incident or attack by actually removing the vulnerabilities.

3. Deterrent Control

Reduce attack on cloud system; it reduces the threat level by giving a warning sign.

4. Corrective Control

Reduce the consequences of any security violation incident by controlling/limiting the damage.

3.5BENEFITS OF SECURITY AS A SERVICE

1. The latest and most updated security tools available.

   The conventional anti-virus tools are effective and useful only if they are updated with the latest virus definitions. SeCaaS gives latest and updated tools to handle the latest threats.

2. You get access to the best security people

   Generally, there is a shortage of expert security professionals. It is very difficult to manage in-house security professional team. The SeCaaS vendors hire best security professionals. Using these services gives us access to their expertise.

3. Faster provisioning.

   The beauty of as-a-service offerings is that you can give your users access to these tools instantly. SECaaS offerings are provided on demand, so you can scale up or down as the need arises, and you can do so with speed and agility.

4. You get to focus on what's more important for your organization.

   Using a web interface or having access to a management dashboard can make it easier for your own IT team to administer and control security processes within the organization.

5. Makes in-house management simpler.

   If you have protected data, it is not enough to just keep it secure. You should know when a user accesses this data when he or she does not have any legitimate business reason to access it.

6. Save on costs

   You do not have to buy hardware or pay for software licenses. Instead, you can replace the upfront capital with variable operating expense, usually at a discounted rate compared to the upfront costs.

3.6EVALUATION OF CLOUD SECURITY ISSUES

1. Authenticate all people who access the network.
2. Set access permissions for users to have access of the applications and data.
3. Authenticate all software and services running on any computer. Automate and authenticate software patches and configuration changes.
4. Formalize the process of requesting permission to access data or applications.
5. Monitor network activities and log unusual activity. The intruder detection system can be utilized.
6. Log all user activity and program activity and analyze it for unexpected behaviour.
7. Encrypt, up to the point of use, all valuable data that needs extra protection.
8. Periodically verify the network related vulnerabilities in all software and services.

3.7CLOUD SECURITY STANDARDS

The processes and practices required for the implementation of security in cloud are defined by standards. These standards are used to ensure secure and trusted environment with privacy and security of data in cloud.

A basic for security is to create layers of defence aka "*defence in depth*". This approach has an advantage - the security can be maintained even during the failure of any layer e.g. Use of Firewall system in combination with IDS (Intrusion Detection System). This type of layered security is desired in cloud computing environment. Traditionally, security was implemented at the endpoints. Organizations were using firewalls, IDSs, and antivirus software inside private network. Today, with managed security services offered by cloud providers, additional security can be provided inside the cloud. In this section SAML, OAuth, OpenID and SSL/TLS standards are discussed.

3.7.1 Security Assertion Mark up Language (SAML)

SAML is a standard for the communication of authentication, authorization and attribute information among online partners. It is based on XML. It provides the facility to securely exchange identity and entitlements related assertions between partner organizations. SAML is built upon existing standards like: SOAP, HTTP, and XML. SAML uses HTTP as its communications protocol along with SOAP. SAML assertions and protocols are specified using XML schema. SAML uses digital signatures for authentication and message integrity. The SAML use XML-based assertions and protocols, bindings, and profiles. The SAML defines XML-based assertions, protocols, bindings, and profiles.

The SAML Core provides general syntax and semantics for SAML assertions. It also describes the protocol used to request and transmit assertions. SAML protocol refers to what is transmitted, not how it is transmitted. A SAML binding determines how SAML requests and responses map to standard messaging protocols.

The SAML has two parties involved: Asserting Party (SAML authority) and Relying party (Consumer/Requester). The asserting party is a platform or an application who relay security information. The relying party (consumer or requester) is a partner site that receives the security information. The exchanged information contains information like: subject's authentication status, access authorization etc. A subject is any entity in a particular system/domain.

SAML assertions

These are usually transferred from identity providers to service providers. The statements in assertion are used by service providers to make access control related decisions. Sample SAML assertion is below:

<saml:Assertion A...>

<Authentication>

...

</Authentication>

<Attribute>

...

</Attribute>

<Authorization>

...

</Authorization>

</saml:Assertion A>

The above assertion can be interpreted as:

Assertion A, issued at time T by issuer I, regarding subject S, provided conditions C are valid.

SAML Protocols

A SAML protocol describes the method of packaging SAML assertions into SAML request and response elements. It also provides processing rules for SAML entities. Generally, a SAML protocol is a simple request–response based protocol. The most important type of SAML protocol request is a query. A service provider makes a query directly to an identity provider over a secure channel.

SAML Queries

There are mainly three types of SAML queries namely: Authentication query, Attribute query, and the authorization decision query. The attribute type query is mainly used. The response of an attribute query is a SAML response which contains assertion having attribute statement.

3.7.2 Open Authentication (OAuth)

OAuth provides simple and standard format for secure web application related API authorization. OAuth is a method used for publishing and interacting with protected data. For developers, OAuth provides users access to their data while protecting account credentials. The OAuth provides facility to users so that they can grant access to their information. After granting access, provider and consumers can share information without sharing the identity.

OAuth does not have features like automated discovery of endpoints, language support, XML-RPC and SOAP, OpenID integration, signing algorithms etc. It considers only fundamental aspects of the protocol,

- Establish a mechanism for exchanging a user name and password for a token

- Provide tools to protect the token

The Security and privacy are not provided by the protocol but SSL can help to get privacy.

3.7.3 Open ID

It is an open standard which provides digital identity for user authentication and access control based on single-sign-on (SSO) mechanism. The conventional log-in process (i.e., a log-in name and a password) can be replaced by allowing users to log in once and gain access to all participating systems. The OpenID is a kind of unique URL and is authenticated by the entity which has the OpenID URL. This protocol does not require any central authority to authenticate a user. The OpenID allows the parallel use of different kind of authentication methods like smart cards, biometrics, or ordinary passwords.

Sample usage of OpenID protocol:

- A user visits a web site where an OpenID based log-in form is displayed.
- The form contains only one field for the OpenID identifier (OpenID URL).
- This form is attached to OpenID client implementation library.
- User will have previously registered an OpenID URL.
- The user types this OpenID identifier into the OpenID log-in form and authentication process is completed.

The relying party requests the webpage at particular URL and reads HTML link tag to discover identity provider. There are two modes by which the relying party can communicate with the identity provider:

1. checkid_immediate

   The relying party requests that the provider does not interact with the user. The communication is relayed through the user's browser without explicitly notifying the user.

2. checkid_setup

The user communicates with the provider server directly using the same web browser as is used to access the relying party site. This option is widely used on the web.

Steps to create a new OpenID session

- The relying party and the identity provider generate a shared secret handle, and the handle is stored by relying party.

- The checkid_setup process redirects relying party's user browser to the identity provider where, the user can authenticate with the provider.

- There can be different methods for authentication. Typical case can be like: The OpenID identity provider prompts the user for a password and asks whether the user trusts the relying party web site or not.

- If the user declines the identity provider's request to trust the relying party web site, the browser is redirected to the relying party with a message indicating that authentication was rejected. The site in turn refuses to authenticate the user.

- If the user accepts the identity provider's request to trust the relying party web site, the browser is redirected to specific page on the relying party web site along with the user's credentials.

- The relying party must confirm that the credentials really came from the identity provider.

The relying party can be state full or stateless. The state full relying party stores the shared secret which can be used for any further communications. In case of stateless relying party, a background request using check_authentication is done for authenticating user. Once the OpenID based authentication is done, the user is considered as logged in at relying party's system.

3.7.4 SSL / TLS

Transport Layer Security (TLS) is the successor of Secure Sockets Layer (SSL). They both are cryptographically secure protocols used to provide security and data integrity during TCP/IP based communication. These protocols perform encryption at transport layer. The TLS protocol allows client server based

communication across a network and provides protection against attacks like: eavesdropping, tampering, and message forgery.

TLS uses cryptography based mechanism at endpoints for authentication and data confidentiality. TLS uses one way authentication i.e. only the server is authenticated, because the client already knows the server's identity. In this case, the client remains unauthenticated. The browser validates server's certificate and also checks the digital signatures of the server certificate's issuing authority.

The validation process may not identify the server to the end user. For the correct identification, the end user must verify the identity related information stored in the server's certificate. The user must verify the URL, name and address details in server's certificate. Malicious web sites cannot use the valid certificate of another web site. Because, they cannot encrypt the data over transmission so that it can be decrypted using valid certificate. Only a trusted Certificate Authority (CA) can include URL in the certificate to ensure that the URL specified in the certificate is an acceptable or not.

TLS can support two directional security in which, both ends of the connection can be validated to ensure that users are communicating with the one whom they intended. This mode is known as mutual (assured) authentication. The Mutual authentication requires that both client and server must have own TLS certificate.

TLS Steps:

1. Peer negotiation for algorithm support

   The client and server negotiate about encryption, key exchange and authentication related schemes.

2. Key exchange and authentication

   The actual key exchange and authentication is performed using public key mechanisms.

3. Symmetric cipher encryption and message authentication

   The message authentication codes are made up from cryptographic hash functions and after that data transfer begins.

Unit 4:Specialized Cloud Services

4

Unit Structure

4.1 LEARNING OBJECTIVE

In this chapter, we will discuss about some of the solutions provided by cloud in the form of services.

- Identity as a Service (IDaaS)
- Recovery as a Service (RaaS)
- Storage as a Service (SAAS)
- Communications as a Service (CAAS)
- Network as a Service (NAAS)
- Monitoring as a Service (MAAS)

4.2RECOVERY AS A SERVICE (RaaS)

RaaS provides an integrated service or solution to manage backup, archiving, disaster recovery related tasks. RaaS helps companies to recover their servers including OS, applications, and configuration, data, databases and files. In case of any disaster situation, RaaS helps to reduce downtime. Sometimes, RaaS is also known as DRaaS (Disaster Recovery as a Service). Some of the RaaS vendors are: nScaled, Geminare etc.

Advantages of RaaS:

- Loss of critical company data can be avoided
- Protects against the loss or damage of physical infrastructure
- Offers cost effective data recovery
- Accurate and faster recovery is offered
- Offer greater flexibility for backup

4.3IDENTITY AS A SERVICE (IDaaS)

The cloud computing paradigm allows users to access their resources from anywhere and at any time. In this scenario, the role of network is very crucial. In

networked environment, proof of identity is very much important. The identity service stores user's identity related information in digital format such that, it can be further utilized for electronic transactions. Three core functions related to IDaaS are: storage of identity data, query engine and policy engine.

The transactions managed in distributed environment over public network have larger surface area for security attacks compared to private networks. Major security related issues are:

- Network traffic protection

- Resource access management and control

- Authorization based on identity

Among all, the establishment of identity is key issue. The identity provides trusted environment. IDaaS offers mechanisms for digital identity management across multiple systems. The digital identity is a set of attributes that gives reorganization to individual over the networked systems. A digital identity helps systems to identify objects and relationships among them. An identity of a person describes:

1. Biological attributes like age, race, gender, appearance etc.
2. Information about person like: Biography, personal data such as social security numbers etc.
3. Ownership details of a person like: A pattern of blood vessels in eye, fingerprints, accessible bank account, a security key, objects and possessions etc.
4. Relationships with others: Friends and Family, beliefs and values, activities and endeavours, personal selections and choices, habits and practices etc.

The identity over the network can be established by several mechanisms like, single factor, two factor, multifactor etc. In single factor based identity, a user has to provide his/her credentials in the form of user name and password. In two factor authentication mechanism, user needs to provide credentials along with hardware based key. Multi factor authentication requires extra mechanisms like biometric, OTP etc.

Example: Microsoft Office identity profile

The Microsoft maintains identity profile of MS office installation by considering many factors or attributes like:

- A 25-character software product key and product ID
- The uniquely assigned Global Unique Identifier or GUID
- PC manufacturer, CPU type and serial number
- BIOS checksum
- Network adapter and its MAC address, Display adapter
- SCSCI and IDE adapters
- RAM amount, hard drive and volume serial number
- Optical drive
- Region and language settings and user locale

From above attributes, a code is generated and stored into product registration database. If any of the above attribute changes, the reactivation of product is required.

Identity Services in Network

There are several forms of identity services used to validate website, transactions, transaction parties, clients and network related services. Certificate based identity, Ticket or token based identity and other mechanisms are used to manage trust in networked services. The protection of an identity is very challenging and complex task. Identity as a Service (IDaaS) offers different services as listed below:

- Services related to Authentication (identity verification)
- Directory services
- Identity governance
- Identity and profile management
- Policies, roles, and enforcement
- Identity provisioning (external policy administration)

- Registration

- Risk and event monitoring

- Single sign-on services

AZURE AD is example of IDaaS.

4.4STORAGE AS A SERVICE (SAAS)

Cloud storage has a many advantages over traditional data storage. One of the most important advantages is that the user can access stored data from any location with the help of Internet. A cloud storage system maintains one or more data servers connected with the Internet. When a subscriber copies files to the server over the Internet, files are stored in data servers. When a client wants to retrieve the data, he or she can access the data server with a web-based interface, and the server then either sends the files back to the client or allows the client to access and manipulate the data itself.

The Storage as a Service means that a third-party (service provider) rents storage space to end users who do not have budget or capital. Storage as a Service is also useful when, the technical personnel to maintain storage infrastructure are not available. It is also very cost effective.

Block-3

Application Architecture for Cloud and Cloud Deployment Techniques

Unit 1:Introduction of Cloud Application

1

Unit Structure

1.1 LEARNING OBJECTIVE

This chapter discusses about,

- Introduction to Cloud Application
- Cloud application requirements
- architecture for traditional versus cloud application
- assumption for traditional and cloud applications

1.2 INTRODUCTION TO CLOUD APPLICATION

Software application is generally built using many modules. Such modules interact with other modules and also provide interface to external application or services. Application architecture is the design or plan of such software application. It contains the details of software application components, interaction among the components and also interaction of the application with the infrastructure components. application goal is to perform useful business task so application design also considers to automate the business task. This automation of business task helps users to manage, store and share data.

Software application designed using traditional application framework is suitable for stable demand level of the consumer. In such software application some middle-tier software or application framework is used to access database by the web server. Such traditional application framework is not much useful and suitable for application with huge variation in user demand or system load.

It is estimated that in near future all major applications will be migrated to cloud as its easy to scale as per the variation in the demand and other useful features. While migrating application to cloud environment the migration process needs to be planned carefully. After migrating the application to the cloud, software application code needs to be changed to to suit the cloud and also to ensure better user experience.

Many organizations started migrating applications in cloud. After migration to cloud the application can provide better user experience by solving many issues for users. It may also useful to streamline the business tasks in many ways. Even the

application get migrated to cloud but if it is not modified to suit the cloud environment than it will work similar to traditional on premise application.

Time, cost and special skills in cloud-based application architecture is required to rebuild the existing application and to add and use additional features of cloud.

1.3 CLOUD APPLICATION REQUIREMENTS

For developing cloud application proper documentation of design and plan is required in order to gain advantage of cloud environment over the traditional environment. Cloud provides services like cloud-based authentication, security and replication, the newly created application must be capable to coexist with these services.

Requirements and architecture are the two major documents must be written and reviewed carefully first while working with cloud applications.

Application Requirements and Constraints are as below.

- Business needs
- Requirement outcome
- Enterprise vision
- Legal limitations when hosting in the cloud
- Cloud standards
- User of existing templates
- Corporate policy for cloud use.

Again, application requirements can be classified as below.

1) Functional requirement
    - Purpose and objective
    - Business goals
    - User requirements
    - Required features
2) Nonfunctional requirements
    - Performance and response time
    - Security

- Service availability in the cloud
- Backup to other clouds
- Extension to hybrid cloud.
- Localization
- Combability with other cloud platforms
- Support for end user devices

Application requirements are considered for the application architecture. The architecture contains details of each section of the application. It also contains the details of how different sections interact with each other. Application architecture exists at conceptual level and detailed level. Conceptual level deals with business offerings, market products, technology growth etc. detailed level deals with designing, reuse of services and design of user interface.

Certain requirements are difficult to define on public or private cloud where the application will be hosted such as server architecture for IaaS cloud, backup, fault tolerance, data replication technique, security etc . the server architecture covers the hardware design and provide application deployment. Vertical and horizontal scalability is supported by good application server architecture.

1.4ARCHITECTURE FOR TRADITIONAL VERSUS CLOUD APPLICATION

Architecture of the application for cloud is different from the application reside on a traditional, on- premise infrastructure.

In cloud cost is based on resource usage. Resources are available as per demand. Resources are virtualized and at multiple locations which need to be factored in the application architecture. applications must be able to scale the resources either horizontally or vertically to use resources in highly granular manner and be cost effective to operate.

Cloud native application have the following important properties.

- Is a native software architecture pattern where the application is designed to run on cloud and have maximum benefit
    - Distributed , scalable , multi – tanent , platform – independent.

- Different from a cloud enabled or traditional monolithic application
    - Internal components can scale and are inherently distributed
- Light-weight
    - Usage of vms and containers
- Devops/ci based deployment
    - Helps in scaling and faster deployments.

Some important points for cloud native vs traditional application can be summarized as below.

Factors considered	**Cloud native**	**Traditional**
Os	Os abstraction: No need to manage the os	Os dependent: Tradional applications are os dependent.
Predictablity	Predictable: Possible to predict the time to deploy the application.	Un-predictable : Testing cycle is un predictable
Capacity	Right sized capacity: easy to scale as per requirements (scale up or down)	Over sized capacity: Not possible to accurately use the capacity of the machine
Delivery model	Continuous delivery: easy to update software. Easy to drive customer needs.easy to do test driven development.	Waterfall : Waterfall model is used
Scaling	Automated scaling: easy to scale up or scale down resources as per the process requirements.	Manual scaling; Scaling is manual
Recovery	Rapid recovery: inbuilt capability to identify erroneous system and remove that.	Slow recovery : Recovery is slower.

1.5ASSUMPTION FOR TRADITIONAL AND CLOUD APPLICATIONS

The application architect keep using long running assumptions that worked earlier many of these conflict in cloud area. The architect needs to know which assumptions to discard and what new to adopt. The table below shows the old and new paradigms and architecture principles.

	Traditional assumptions	New thoughts or practice
1	Application depends of the similar infrastructure	Applications will be running on highly dynamic and hybrid cloud environment.
2	Applications can have access to device files (unchanged and static)	Application runs on the virtual resources which can move to other resource also amount of resource can vary.
3	Application exists in single location.	Applications are distributed at multiple locations.
4	For data and process integrity database can be used.	Application must be aware of the data integrity and be able to manage the integrity issues.
5	Structured data and predefine format for application.	Different media types and various data types the same field or information for application.
6	Applications will have a fixed format for input and output.	Applications must be designed around social , inter-personal communications.

Unit 2:Cloud Application Requirement

2

Unit Structure

2.1 LEARNING OBJECTIVE

The overall objective of this chapter is to,

- Study about requirements of cloud applications
- Role of Service Oriented Architecture (SOA) in Cloud Applications
- Architecture of parallel cloud applications

2.2 INTRODUCTION

In previous chapters, we have discussed about physical architecture of cloud computing environment. This chapter we will study about cloud application requirements, SOA and parallel cloud applications. The overall environment of cloud is quite different than traditional applications. We should architect cloud applications to leverage the benefits of cloud computing based environment.

2.3 RECOMMENDATIONS ABOUT CLOUD APPLICATION

We know that cloud computing environment is different than traditional environment. This section gives some of the recommendations for cloud application design.

1. Location independent

   Traditional applications are created to run on hardware machines at same physical location with similar,

   - Network configurations
   - Security settings
   - Regulatory domain

   In case of cloud computing environment, the application may run in datacentre of cloud service provider at any location across the globe. Application developer should also provide option of changing cloud service provider where the application is deployed. Sometimes applications are developed and tested over public cloud and finally deployed over private

cloud (infrastructure). The application architect must consider the data as local or remote and the data should be able to access in parallel.

2. Consideration of resource price and utilization

   The pay per use model and scalability are major advantages of cloud based approach. The cloud users are charged according to the usage of resources. In such a scenario, the application architect should try to optimize the hardware usage by application. Similarly, the application scalability should also be considered. In some cases, the cloud service provider price changes according to the time. Some applications tasks like replication, backup, report generation etc. should be scheduled such a way that service provider's costs are lower.

3. Flexible, Dynamic and distributable

   The traditional applications are developed by considering traditional environment in which applications are designed to run on consistent set of computer hardware with stable features and behaviour. This kind of assumption may not work in cloud. The processing data may shift location at any time. Similarly, the available processing capabilities, memory and network bandwidth may very over the period of time. The application design should support heterogeneity in terms of hard resources and runtime environments.

4. Data consistency, integrity and security

   Traditional applications consider that transactions are atomic and atomicity can be achieved by applications or by some middleware software. Many times database software maintains atomicity. In case of cloud, data is distributed at different locations and in different databases. A proper mechanism to manage integrity and consistency should be developed.

   The security of data should be enhanced by automated configuration changes. Application lifecycle management should consider that it may happen that multiple versions of application run in parallel. The cloud based applications rely largely on network. The service provider and consumer have no direct control over latency and delay. Applications must be designed to sustain data integrity related issues. The application should be designed such a way that it can recover from partial failures. It must be fault tolerant i.e. it should have capability to accommodate a wide range of faults.

5. Mobile aware

   It will save effort and time if the application is designed and developed by considering access via smart phones, tablets or any other mobile devices. In future, it may happen that application will be accessed by more and more mobile devices.

6. Applications Should be feature rich

   Traditional applications were designed to accept, preserve and process user inputs (data). It was mainly used for reporting and record keeping. In addition to these basic requirements, cloud applications should have option to communicate with other applications to support business processes. Cloud applications must include human interaction as a part of basic requirement. E.g. if we develop doctor appointment system over cloud, it should have features regarding automated email and SMS when the appointment is booked and even on the day of appointment. A better approach to build relationship between application and society is to use event driven approach.

2.4USE OF CLIENT SERVER MECHANISM FOR CLOUD APPLICATIONS

The application design approach is evolved from monolithic to modular to object oriented to service oriented. The concept of cloud computing and the evolution of powerful mobile devices, has created more options for cloud based applications. The powerful interconnected mobile devices and cloud computing have led to a new approach called Client-Cloud Architecture. In this scenario, developers prepare two applications:

a. Server Application for Cloud

   These applications are architected over private cloud, public cloud or PaaS platforms.

b. Client Application for devices

   These applications include smart phones, tablets and other connected devices and along with different operating systems like IOS, Android, Microsoft etc. The client applications can be distributed online via various app stores. The rich client applications reduces burden on server applications.

As we can see that client cloud approach have many benefits, there are several issues as well.

- Frequently changing client hardware and software configurations
- Less backup facility at client side
- Network delay and security issues
- Different setup and configuration files for type of clients

2.5SERVICE ORIENTED ARCHITECTURE (SOA) BASED CLOUD APPLICATIONS

The overall architecture of cloud based applications differs from traditional application architectures. There is a need for set of separate design principles and design patterns. The design principles and patterns are very much useful to architects and developers. They help to reduce risks, costs and time associated with application building, deploying and managing.

SOA is one of the best architectural guideline for cloud based application developments. This approach focuses on service based application development. Some of the basic characteristics of services are,

- These services are highly interoperable.
- Each service is identified and created to support business process.
- These services work as software modules.
- They can be reused
- They are independent (loosely coupled) so changes become easy
- Self discoverable
- Services can communication with other services using well defined standards and protocols
- Services are self contained.
- Service based application approach gives agility
- Services can be integrated (orchestrated) to achieve desired application feature
- Support cross platform and network based integration

Cloud offers all resource in the form of services. In this scenario, the Service based approach is more suitable for cloud applications. Earlier the SOA based approach was used for distributed application development and for modular application development. Nowadays, SOA is a basic approach for SaaS based software delivery. Various patterns related to SOA are shown in figure 7.

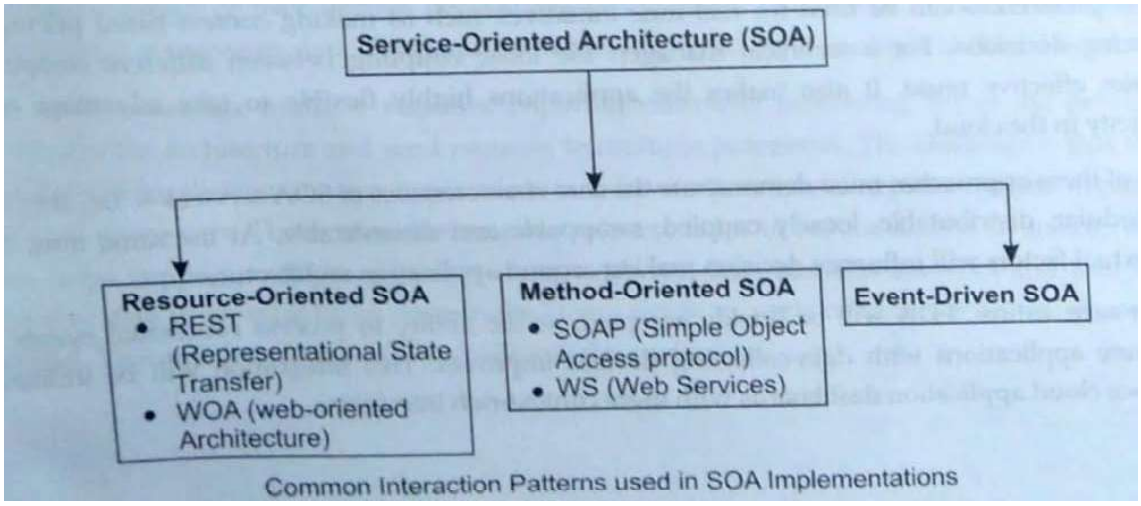


Figure-7 classification of SOA implementation patterns

The figure 7 shows overall classification of SOA implementation patterns.

1. Resource Oriented SOA
   - Uses WWW standards (HTTP)
   - REST (Representational State Transfer) is used for web service implementations
   - This approach is used to support large scale applications over public cloud platforms
2. Method Oriented SOA
   - It uses SOAP (Simple Object Access Protocol) based standard. This protocol is used for data exchange over networks.
   - Support common request – response mechanism
   - WSDL (Web Service Description Language) is used for describing web services.
   - SMTP is used for message transfers
   - XML is used for configuration and exchange of information

3. Event Oriented SOA
   - It is based on asynchronous message exchange approach
   - The cloud application registers as listener and receives a message about an event once the event is generated by source program.
   - The events and messages are displayed over dashboard
   - This approach allows business executives to make transaction related decisions based on up to date information.

All three approaches mentioned above enable SOA based approach to be,

- Modular
- Flexible
- Loosely coupled
- Discoverable
- Swappable and
- Distributable

The overall benefits of SOA based application development can be summarized as,

- More than 60% of SOA based projects have positive effect on organizations
- SOA based approach generate positive returns in short time span
- SOA help to improve agility of organization
- SOA can reduce cost involved in making of IT based systems
- SOA improves developer productivity

2.6PARALLELIZATION WITHIN CLOUD APPLICATIONS

The on-demand availability of large amount of processing capability and memory force architects to use resources effectively. Earlier architectures consider,

- Horizontal scaling for front-end and middleware components
- Vertical scaling for back-end tier

Block-4

Risk, Security, Consequences and Cost of Cloud Computing

Unit 1:Risk in Cloud Computing 1

Unit Structure

1.1 LEARNING OBJECTIVE

Cloud computing provides many benefits to organizations. Along with benefits, various risk factors are related to cloud based environment. In this chapter, we will discuss various risk factors like:

- Vendor Lock-in
- Resource scarcity
- Failure risks
- Network outage related risks
- Legal risks
- Risk about software and application Licensing

1.2 INTRODUCTION

Nowadays, cloud computing is used by various organizations like: banks, brokerage houses, hospitals, manufacturing companies etc. Each type of organization has its own risk level limits. They have to comply with government rules and regulations, security rules and other complacencies.

Cloud computing is multi-tenant and open for all environment which may cause various security challenges. Organizations which use cloud services must test and monitor security related threats. In some cases, it becomes very difficult and incontinent to perform security testing and monitoring. As a cloud service user, organizations need to keep the results of security tests during audit process. Another issue with cloud is about data i.e. user data is stored on remote servers. Sometimes data is replicated for security issues. It is difficult to delete all copies of data when we change service provider.

1.3 CLOUD COMPUTING RISKS AND ISSUES

In this section, various cloud related risks and issues defined by Gartner are described.

1. Regulatory Compliance

   Customers are responsible for security and integrity of their own data even in the case when the data is stored with service provider. Traditionally, service providers perform external audits and certifications. Some cloud service providers do not perform these kinds of audits or certifications whose services can only be used for some trivial functions.

2. Data Location

   Generally, cloud users do not know the physical location of their data. Cloud users ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of customers.

3. Privileged User Access

   The sensitive data stored and processed outside the organization creates a risk about access of data. The outsourced services may overlook the physical, logical or personal controls of data. Cloud users must get information about the people who manage data like, information about hiring of privileged administrators and their controls.

4. Data segregation

   Generally, data in cloud is shared among customers. Cloud users must know the mechanism used to segregate data at rest. Cloud provider should provide details about used encryption algorithm. Faulty encryption may make data unusable and may also affect availability.

5. Recovery

   Cloud service provider should provide details about the data recovery in case of any disaster situation. If service provider does not maintain replicas across multiple sites, the service may not work in case of failure. Cloud users should ask service providers about the complete restoration process and the amount of time required for restoration.

6. Long term visibility

   The cloud service provider may be acquired by larger company in future. Cloud users must make sure that in such cases, data is available. Cloud users should ask service providers that how they would get your data back in the original format in case of any acquisition.

7. Investigative support

   It is very difficult to trace illegal activities in cloud environment. Cloud services are difficult to investigate because logging and data for multiple customers may be located at same place and may also be spread across different locations. Cloud service provider should provide mechanism of investigation in case of any such case.

1.4RISK ASSESSMENT AND RISK MANAGEMENT

Cloud users must do in depth analysis about risks involved in cloud environment. This will help organization to identify possible vulnerabilities and threats. Based on this analysis, one can take measures to avoid risks. The threats may cause issues like financial losses, reduced employ productivity, loss of customer loyalty etc.

Cloud users can use several mechanisms to reduce or mitigate risks. Cloud users should have updated copies of their data backup in their network. Cloud users should have plans to quickly switch between various service providers in case of any outages. The risk management includes:

- Risk identification
- Risk analysis and evaluation
- Identify risk mitigation steps
- Deploy identified steps
- Monitor and evaluate effectiveness of steps taken

➢ **Risk about vendor lock-in**

There are many steps involved when any cloud user migrates from one service provider to another. The risk of migration is always associated with cloud users. Before using any cloud services, cloud users should refer SLA (Service Level

Agreement) documents. Depending upon the type of cloud service, there are several lock-in related issues and mitigation steps.

- Infrastructure as a Service (IaaS)
  Different service providers use different mechanisms for data storage and data access. These differences make migration process difficult. To mitigate this problem, cloud users should take back up of VMs along with data and store them on local devices. Also verify that backed up VMs can be restored later.

- Platform as a Service (PaaS)

  Many times the PaaS environments are unique and proprietary to particular service provider. The standardization process is now well established. Cloud users should make sure that the development environment provided by service provider is supported by other PaaS providers. We should also use standard APIs which make easy migration among different PaaS providers.

- Software as a Service (SaaS)
  SaaS providers offer general purpose environment which can be used to develop user specific tools on particular cloud. It may happen that users data is stored in proprietary format which is not supported by other service provides. To avoid this situation, cloud users should make sure that APIs are compatible with other public clouds. One should be able to export data in standard format which can be further used on other platforms.

➢ **Risk of Not Meeting Regulatory Compliance**

Cloud service providers must certify that their service platforms are complied with regulations. The certificate form audit authorities can be used to provide assurance to cloud users. These certificates will also help cloud user during their own audits. Cloud users must ensure that their providers have obtained acceptable certificates from authorities. Some examples are

- If open source based virtualization platform is used, it may not have compliance about protection or availability.

- If the data is stored outside the country, it may violate the requirements of banks

- **Risk of Loss of Control**

In cloud based environment, infrastructure, network, security and other hardware resources are controlled by service provider. Due to this, SLA may not be much relevant to end users. Similarly, responsibilities of cloud users and service providers are different depending upon the type of service (IaaS, PaaS or SaaS). It may also happen that some of the service providers outsource some part of their datacentre services. In all these situations, the cloud users lose their control over their resources.

- **Risk of resource scarcity or poor provisioning**

One of the major benefits of cloud based environment is on demand provisioning of computing resources. In some situations, the public cloud service users may have to compete for fixed set of available resources like computing, storage or network. Sometimes, the supply of resources is insufficient for the demand. The cloud service provider may have deployed less number of physical resources. Cloud service providers use some algorithms for dynamic resource scheduling which may misbehave in some cases. There are always chances of hardware failures at service provider level. In all these circumstances, there is a risk about scarcity and poor provisioning of cloud resources.

- **Risk in Multi-Tenant Environment**

Cloud computing is multi tenant environment which allows multiple users to access and share same physical resources. The concept of virtualization is utilized for resource sharing. One tenant may access, read, modify or delete the data associated with another tenant. Due to this situation, there is risk associated about data. This may affect the reputation of service provider and cloud users may lose their confidence.

- **Risk of Failure**

A cloud service provider maintains huge amount of hardware resources in the form of datacentre. These resources are pooled and shared among cloud users. The technology of these pooled hardware resources changes time to time. If these physical resources are not updated timely, it may affect the overall service. Along with that, if the older physical resources (infrastructure) are not updated, the risk of failure increases. This situation impacts cloud customers.

- **Risk of failure of supply chain**

Cloud service providers acquire services from other services providers. These acquired services may include network bandwidth, monitoring services, security services etc. The cloud service provider has to follow the rules of third party service providers. Any failure or change in services of third party may adversely affect the services of cloud service provider. The failure at one provider level may cause service degradation or outage of other service providers.

- **Risk of inadequate SLA**

The Service Level Agreement (SLA) provides a mechanism by which the service users and service providers are bound to certain conditions. SLA may include details about service availability, performance, security etc. The SLA should have features so that all conditions regarding user and compliance requirements can be mentioned. The SLA document helps to set responsibilities of both service users and providers. The SLA violation may cause loss to both service provider and service user. In case of violation, the penalty is caused to service provider. Similarly, the violation may cause poor QOS (Quality of Service) to users.

Sometimes, the structure of SLA is inadequate to specify all conditions by service users. In certain situations like if the service provider is acquired by another service provider, than the SLA document should be revised which may lead to risk of incompliance.

- **Risk of malware and Internet attacks**

The cloud computing is an Internet based and self provisioning environment. Anybody can open account form the portal or interface of service provider. This gives chance to malicious users to connect with cloud environment. They may also launch attacks to disable particular service or whole cloud function. One of the most common attacks in cloud environment is:

- Distributed Denial of Service (DDoS) attack

  In basic DOS attack, the malicious user generate dummy workload load (requests) on services such that the performance of service degrades. In some cases, the normal users are not able to use the service. The cloud environment is distributed in which attacker may use DOS attack from different locations to affect several services. It is very difficult to identify the difference between legitimate traffic and dummy traffic.

- **Risk of Cloud Resource Management**

Cloud computing is very dynamic environment in which users enter and exit in very dynamic nature. The efficient and effective management of shared resources will help cloud service providers to enhance QOS along with serving more user requests. The improper management of resources may be caused by:

- Unauthenticated access of cloud resources
- Virus of Malware may lead to heavy network traffic (activity)
- The compute, storage or network related resources may be unnecessarily blocked by cloud users.

- **Risk of physical infrastructure and network outages**

Some of the risks associated with the physical infrastructure of cloud are:

- Theft of physical resources owned by cloud users and kept at provider's datacentre.
- Damage to physical resources by a person who is able to entre datacentre without proper authentications.
- The possibilities of power disruptions or outages.

- The improper air conditioning of datacentre may lead to rise in temperature of servers and other equipments which affects overall functioning of cloud.
- Sometimes, malicious employees or intruders having privileged access may damage physical infrastructure

The outage is a situation in which a specific service is affected temporarily or permanently. In case of network outage, cloud users may not be able to access the latest of copy of data. It may also create inconsistency among replicated data.

- **Software, Application Licensing and Legal (Legislation) Risks**

The licensing of software, applications, development tools, middleware, database and operating systems is a major issue in cloud environment. Generally, licenses are categorized as below:

- User based license: It controls the number of users who can use the software or application. E.g. If we have 20 concurrent user licence with 200 named users means maximum 200 users can use the software or application but concurrently on 20 can access.
- Device based license: In this kind of license mechanism, applications / software are bound with physical hardware. This kind of software can be used by any users who have access to particular hardware machine.
- Organization wide license: This category of license allows all the users of particular organization to access software or application within the organization.

In cloud based environment, license related risks are more because

a. Cloud service provider may add or remove servers dynamically to manage user workloads
b. It is difficult to check the user count over cloud
c. If cloud user obtains license considering peak workload, the license might be unused during most of the times.

Organizations that use cloud platform are from different domains like banking, pharmaceutical, healthcare, automobile etc. Their data resides in cloud datacentre. The data is very sensitive and has to obey certain regulations regarding security,

access, location, recovery, backup etc. Generally, cloud service providers are complied with these regulations. The compliance requirements must be mentioned in SLA documents. Cloud users should also get copy of compliance certificates.

Unit 2:Data Security in the Cloud 2

Unit Structure

2.1 LEARNING OBJECTIVE

Cloud user's data is stored at remote location which is not known to users. This may lead to several data security issues. In this chapter, we will discuss about:

- Data Redundancy
- Data Backup and Recovery
- Data fragmentation and reliability
- Data integrity, confidentiality and migration
- Cloud firewall and virtual firewalls

2.2 INTRODUCTION

The data stored in cloud environment has several threats like:

- Data Security

  Data is stored at remote locations. For better security of data, encryption mechanisms can be used to achieve security.

- Data Availability and Integrity

  The problem in hardware or software at cloud service provider level may lead to unavailability of data. Multiple replicas at different geographical location can be maintained to achieve higher availability in case of any disaster or failure situations. Once, multiple copies are maintained, there is also a risk of data inconsistency is associated.

- Flexibility

  In a multi tenant environment, some applications may have higher utilization which may affect the performance of other users. To avoid this problem, storage access speed should be decided.

- Performance

  In cloud data is stored at remote locations. Due to this, the data access may be affected by network latency. The performance may further degrade due to synchronous operations of read and write. To achieve better performance, providers should employ techniques like data caching (in memory data).

- Price and Complexity

  The price of data storage space impacts the cloud service users. The price should be low. The storage hardware at cloud service provider side may be heterogeneous which makes it very difficult and complex to manage the devices.

2.3 CLOUD DATA CHALLENGES

In this section, various challenges associated with cloud data are discussed along with some of the mitigation steps.

1. Data Redundancy

   Data stored in cloud environment is accessed by multiple users concurrently. The data is stored on heterogeneous hardware environment. The data is stored in multiple copies across different locations in synchronous manner. The data replication system should have knowledge about data location, latency, workload, backup and monitoring of data. To achieve proper data redundancy, following points should be checked.

   - Data must be consistent across all replicas
   - Different steps should be taken to improve data replication and access.
   - Load balancing about data access requests should be considered
   - Data should be recoverable in any circumstances

2. Data backup

   There are certain issues regarding data backup which are listed here:

   - When cloud users take backup of data and stores in local infrastructure, it may cause bandwidth expenses
   - Users need to place backup at safe locations and they should check the media integrity at regular intervals.
   - The backed up data must be protected against malicious users and attacks.
   - The data backup strategy should consider the restoration process before taking backup.

3. Disaster recovery

   Cloud users should consider disaster recovery mechanisms available at service provider before choosing any service provider. The strong disaster recovery mechanism provides benefits like: cost saving, scalability, quick restore, higher availability etc. Certain issues regarding disaster recovery are:

   - Initial data copy- When data size is too large, it is very difficult to make first copy of data over WAN. Cloud users should adopt manual process of data copy using tapes or hard disks.
   - Operating system support- Cloud service providers support most common operating systems like windows, Linux etc. Some of the older operating systems may not be supported by disaster recovery solutions.
   - Less bandwidth- Many disaster recovery service providers create backups using incremental approach instead of taking full backup. This saves the bandwidth, time and cost.
   - Financial Considerations- When data is small in size, it is advantageous to utilize disaster recovery mechanisms offered by cloud service providers. But, if data size is too large, the cloud users should have own mechanisms for disaster recover (it will be cost effective).

4. Data Reliability and Fragmentation

   The reliability of cloud services is very important because,

   - Cloud services are provided over WAN in which multiple vendors are engaged
   - User base is tool large
   - Accessibility and availability of cloud services is very high
   - Cloud services are offered over heterogeneous hardware and software

   As the numbers of cloud users are very high, they all might be working on different parts of data simultaneously. The data may be fragmented and stored over different locations. The data fragmentation forces us to

keep track of different parts of files. The service providers should have mechanisms to reduce data fragmentation and inconsistency.

5. Data Integration

   Some of the factors which make data integration difficult are:

   - Content distribution

     The user data is stored in different files which are distributed and fragmented across several datacentres.

   - Data exchange

     The data stored over cloud is utilized by applications running on other public or private clouds. These may cause compatibility issues among various involved cloud parties.

   - Data change rate

     The data over cloud is accessed by many users concurrently. The user actions may modify the data. The rapid change is in data is challenge for integrity and replication management.

   - Connectivity

     Cloud data can be accessed by users from any location across the world. The basic requirement is Internet connectivity and bandwidth. The connectivity also affects the latency.

   - Control over distribution

     The data control is shared among the cloud service provider and cloud user. This may create integration issues.

6. Data Transformation and Migration

   The data stored over cloud is accessed by many applications. Each application may have its own requirement about the format and structure of data. This may cause data to be converted in different formats as per the requirements of individual application. This kind of data transformation requirements may cause several types of issues.

   - Runtime issues

     Sometimes the stored data and the data required or generate by another cloud application are not compatible with each other.

   - Redundancy issues

The data transformation may create multiples copies of same data in different format. The location tracking and consistency management are major challenges.

- Implementation issues- Data transformation may be complex and expensive. To make it simple process, various standards should be adopted.

Cloud users may need to change service providers or may need to migrate data like user login, profiles and other user data to other cloud service providers. Cloud service providers should have proper format and process to make data migration easy. Some of the data migration challenges in cloud are listed below.

- Concerns about liability
  Cloud providers have maximum data value for damage claims in the SLA. These values may be less than the data value or the efforts required to fix data loss.
- Connectivity issues
  The data in cloud is accessed over the WAN (Internet). There may be faulty network links.
- Compliance issues

  Cloud service providers must comply with various regulations and legal requirements. Some of the examples of compliance are:

  FISMA – Federal Information Security Management Act
  HIPAA- Health Insurance Portability and Accountability

7. Data Security risks
   - Data Confidentiality and Encryption
   - Key Protection and Management
   - Data availability and Integrity
   - Management Interface for Cloud data
   - Cloud Firewall and Virtual Firewall

Unit 3: Application Security in the Cloud

3

Unit Structure

3.1 LEARNING OBJECTIVE

In this chapter, we have discussed about

- Cloud application software lifecycle
- Application security in the cloud
- Application protection

3.2 INTRODUCTION

Cloud uses very strong mechanisms for the data security while data is at rest or at transit. There are two main issues regarding the security of cloud applications.

1. Cloud API and tools for development

   Cloud service providers offer many sets of APIs and application development tools to their customers for application development. Using these cloud users build and integrate their required services. These API and tools should provide protection in virtual environment. Along with this, it should be compatible with other platforms.

2. Application architecture

   Cloud applications greatly depend on other systems and services like identity management, database and encryption systems etc. The main reason behind dependency is the multi-tenancy. The applications hosted in cloud may belong to other cloud providers. The application deployment model is different because it does not follow one server per application approach.

3.3 CLOUD APPLICATION SOFTWARE DEVELOPMENT LIFECYCLE (SDLC)

Security is considered as a one of the important concern during the SDLC. When application is moved in the cloud, the security remains the major challenge. Along with this, cloud applications have several other major issues. Cloud based applications have different environments for development and deployment. Cloud

based application SDLC should have well defined trust model between these two environments. Whereas in conventional application SDLC, the trust can be ensured by isolating hosts and networks from outside infrastructure. The figure 8 shows the SDLC model for traditional internal applications.

The SDLC of cloud based application largely depends on the deployment model.

- **Application Security in IaaS**

The conventional applications ensure data security by several internal controls. The cloud based applications should consider security by different means. In IaaS based service model, service providers create virtual machines (VMs).

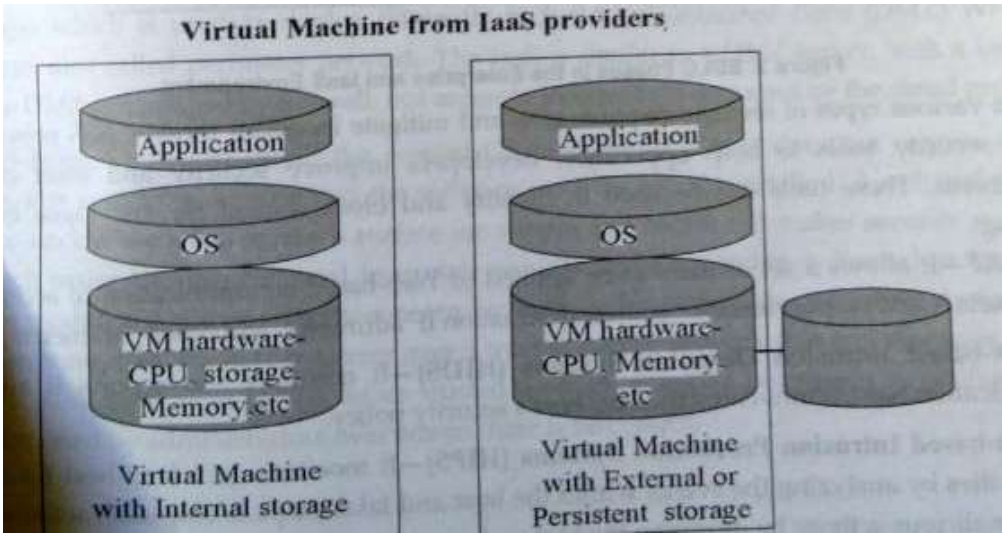


Figure-8SDLC model for traditional internal applications

When application runs under IaaS environment, it may happen that its development and initial testing may be done on internal infrastructure. But, some later SDLC phases like deployment, testing and maintenance are done on cloud infrastructure. The figure 9 show the various SDLC phases.

The cloud service provider (IaaS providers) offer set of tools to deal with security issues. These are discussed below.

- dWAF

  It facilitates to write set of rules which are applied to web applications. Based on these rules, some communication packets can be accepted, dropped by

considering port number, source and destination address, protocol and other parameters.

- HIDS (Host based Intrusion Detection System)
  These systems help us to monitor and report intruders on IaaS host.
- HIPS(Host based Intrusion Prevention System)
  This system monitors each and every host of IaaS for any suspicious activities and takes steps to stop such actions. It drops packets about malicious actions. Sometimes connections are reset or complete traffic is blocked.
- Scanning programs for application security
  These programs are used to record and inspect requests – responses of web based applications. These are reviewed by operators. Using these logs, security experts can detect vulnerabilities in application architecture and code.
- Programs for analysis of source code
  These programs are designed to identify security flaws in source code. These tools are used by experts to analyze compiled codes to identify security risks.

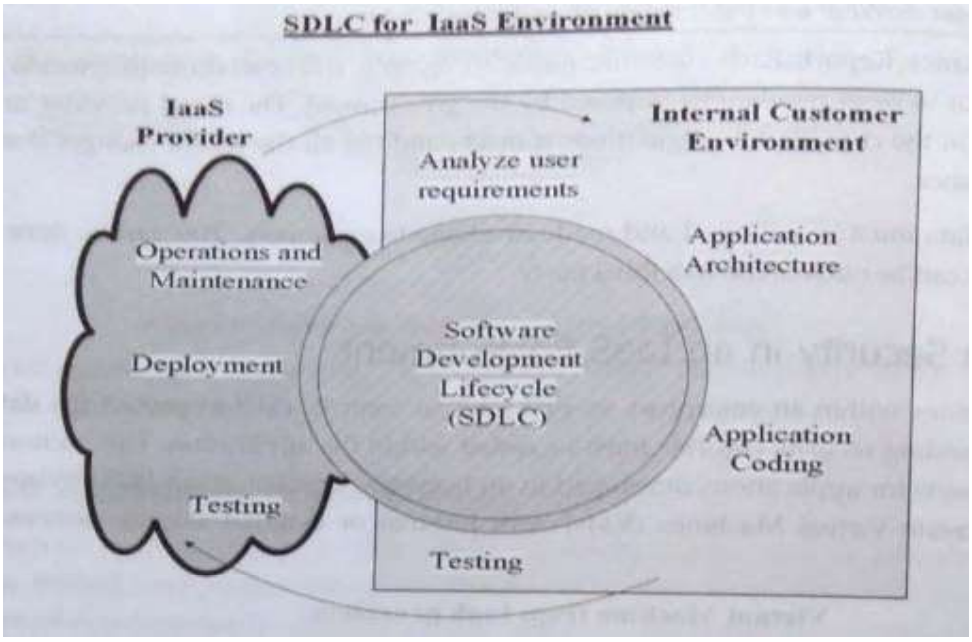


Figure-9SDLC Phases

As from the figure 9 we can observe that, requirement analysis, coding and initial testing are done on internal customer environment. Once these phases are over, application is deployed on cloud where again some test cases are evaluated. Over

IaaS the application must have tight access policy to maintain confidentiality. The security configurations in IaaS environment are similar to the internal architecture. Some security mechanisms which are in-built in intranet environment should be configured explicitly in cloud environment.

The IaaS providers offer services in the form of VMIs (Virtual Machines Images). A virtual machine image is a basic unit of deployment in IaaS environment with its own OS (Operating System) and other configurations. Cloud users make use VM images provided by IaaS providers or by some third parties. In both cases, cloud users should perform more security configurations in VM. For IaaS, users should use hardened OS image which is used to build DMZ (Demilitarized zone) web servers. For IaaS hosts, we should install some other required OS modules. If some OS services are not required by host, these must be removed. A smaller application software stack provides very small attack surface for attackers and viruses. It makes security management very easy and efficient. The need of OS patch updates is also reduced.

Another IaaS application threat is regarding inter host communications. These communications might be done over un-trusted networks which might be used by many other users. In this situation, cloud applications should use digitally signed communication messages. If the message is digitally signed, the application can verify the origin of messages. Digitally signed message are more secure because they can be accepted or rejected based on the origin. The figure 10 shows the mechanism of digitally signed messages.

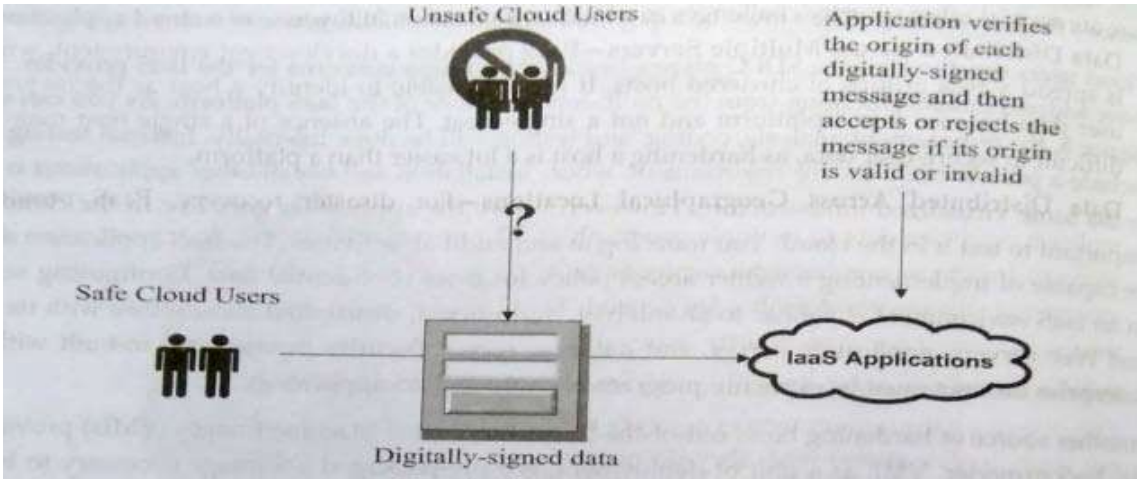


Figure-10Mechanism of digitally signed messages

Another major issue in IaaS application security is about key management. These keys can be used for authentication or encryption. These keys are to be exchanged among various users and hosts.

The data storage is again a big challenge for IaaS applications. The internal applications use the storage provided by other trusted providers. In case of cloud, storage media is shared among customers so encryption is must for data (during rest or transit). IaaS applications must have data filtering and masking mechanisms.

- **Application Security in PaaS environment**

PaaS service providers offer hardware infrastructure, application development blocks, compilers and runtime environments. These can be used similar to the internal application development but in cloud users need to code extra security mechanisms. The security challenges in PaaS are listed below.

- Data distribution on multiple servers

  PaaS providers offer a development environment which may be spread across group of clustered hosts. The data owner cannot correctly identify the host on which data is stored. The absence of single host makes data security difficult task.
- Data distribution over different geographic locations

  PaaS providers store user data on different geographic locations to provide protection against disaster situations. It is challenging to secure data which is spread across different locations. Each datacentre might have separate copy of data and backups.
- Privileged permissions

  Application developers (programmers) have fully privileged environment during development process. During PaaS based development, developers may grant permissions to other persons. They may forget to revoke these permissions back before the actual deployment.
- Risk due to open TCP ports

  PaaS uses distributed file system mechanisms like Hadoop. Along with these, several other frameworks are also used. Each uses different ports for communication. These open ports may provide surface to DOS attackers.

It is very important to consider all above mentioned issues during application development over PaaS platforms. Once the problems or issues are identified, it is the responsibility of user to solve these issues. The PaaS vendor may offer certain security solutions along with platforms.

- **How to protect PaaS platforms**

Some of the most common ways to provide application protection over PaaS platform are,

- Use good tools to identify vulnerabilities in applications. OWSAP is a nonprofit organization to provide tools and best practices over PaaS platforms.
- All application activities should be logged and data should be stored and transferred in encrypted format. The logs should be checked on regular basis to detect security related threats.
- Generally, all API require an application key over PaaS platform. There should be a way to securely maintain these keys and other application credentials.
- One should use secure communication protocols while application development over PaaS. If web services are developed or used, they should also follow secure protocol standards. OASIS (Organization for Advancement of Structured Information Standards) is a nonprofit organization, who establishes secure communication standards. Where ever possible, Cloud applications should use SSL (Secure Socket Layer) based protocols.
- Cloud application developer should be trained about secure application architecture and best coding practices.

The figure 11shows the roles and responsibilities of PaaS service providers and users about applications.

The cloud users should adopt specific security tools and standards to ensure security during SDLC process. All software architects, developers and testers must be aware about the security features offered by PaaS provider. Some PaaS providers give details about best practices and they also give training to users about their platform.

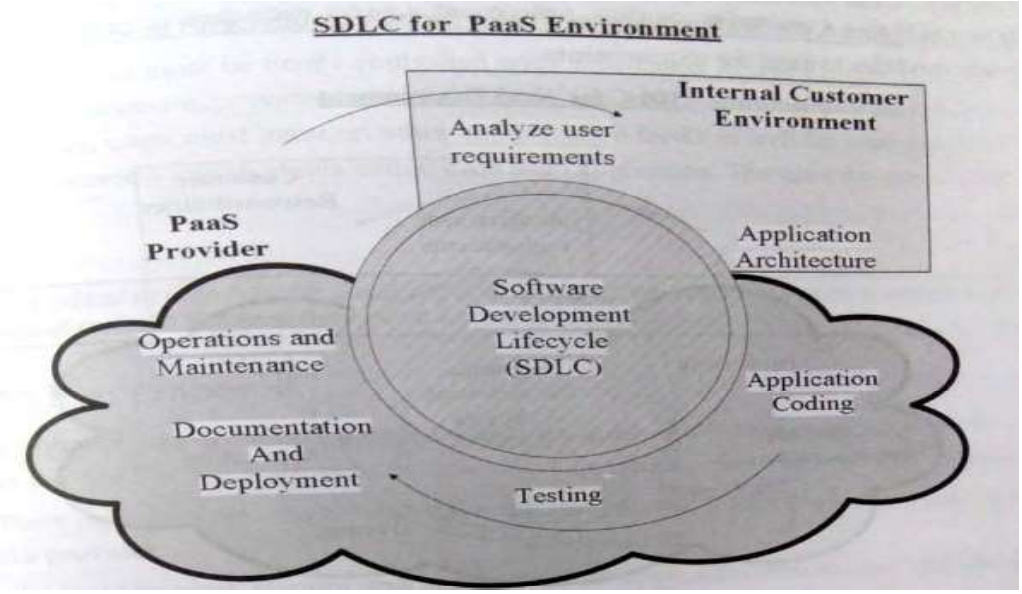


Figure-11Roles and responsibilities of PaaS service providers and users

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

○

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in