MODULE 2

Submitted By: Anshika Malsaria

Assistant Professor

Books

Text Books:

1. David S Linthicum, "Cloud Computing and SOA Convergence in your Enterprise A Step by Step Guide", Addison Wesley Information Technology Series.

2.Anthony T Velte, Toby J.Velte, Robert Elsenpeter, "Cloud computing A Practical Approach ", Tata McGraw Hill Publication

3.Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy –

Reference Books:

1. An Enterprise Perspective on Risks and Compliance" , O'Reilly Publications, First Edition
2. Michael Miller, "Cloud Computing – Web-Based Applications that Change the Way You Work and Collaborate Online", Pearson Education, New Delhi, 2009.
3. Cloud Computing Specialist Certification Kit – Virtualization Study Guide

Syllabus

BCO 064B	CLOUD COMPUTING	3-0-0 [3]

OBJECTIVE: At the end of the course, the student should be able to:

1. To understand the architecture of Cloud.
2. To develop an understanding of various aspects of cloud computing.
3. To familiarize the students with fault Tolerance and security measures in cloud.

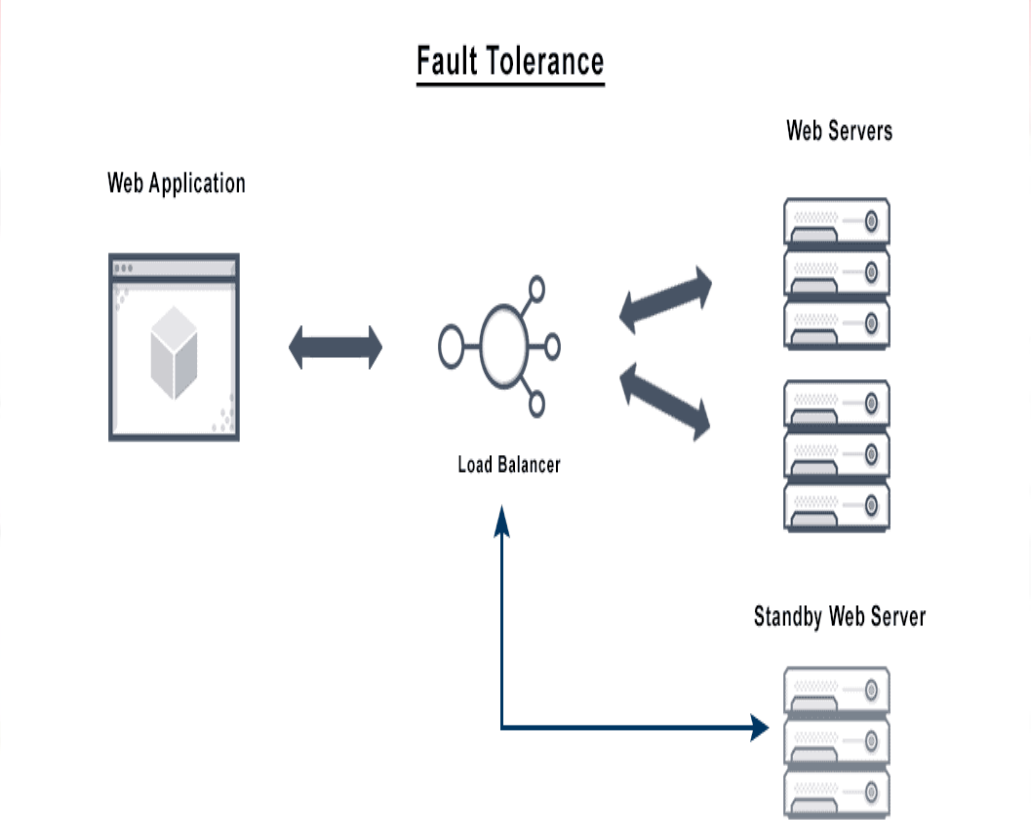
UNIT 1	**Understanding cloud computing:** Introduction to Cloud Computing - Benefits and Drawbacks - Types of Cloud Service Development - Deployment models
UNIT 2	**Cloud Architecture Technology and Architectural Requirements:** The Business Case for Clouds - Hardware and Infrastructure – Accessing the cloud – Cloud Storage – Standards- Software as a Service – Discovering Cloud Services Development tools. Three Layered Architectural Requirement - Provider Requirements - Service Centric Issues - Interoperability – QoS.
UNIT 3	Fault Tolerance - Data Management Storage and Processing - Virtualization Management - Scalability - Load Balancing - Cloud Deployment for Enterprises - User Requirement - Comparative Analysis of Requirement.
UNIT 4	**Security Management in Cloud:** Security Management Standards - Security Management in the Cloud Availability Management - SaaS Availability Management - PaaS Availability Management - IaaS Availability Management - Access Control - Security Vulnerability, Patch, and Configuration Management – Privacy in Cloud- The Key Privacy Concerns in the Cloud - Security in Cloud Computing.
UNIT 5	**Virtualization:** Objectives - Benefits - Virtualization Technologies - Data Storage Virtualization – Storage Virtualization – Improving Availability using Virtualization - Improving Performance using Virtualization- Improving Capacity using Virtualization.

FAULT TOLERANCE

Fault Tolerance

"ability to continue operating uninterrupted despite the failure of one or more of its components"

- In other words, fault tolerance refers to how an operating system (OS) responds to and allows for software or hardware malfunctions and failures.
- An OS's ability to recover and tolerate faults without failing can be handled by hardware, software, or a combined solution leveraging load balancers



- To ensure business continuity and high availability by preventing disruptions arising from a single point of failure.
- Focus most on mission-critical applications or systems.

Levels Of Fault Tolerance

1. **At the lowest level**, the ability to respond to a power failure, for example.

- *A step up*: during a system failure, the ability to use a backup system immediately.
- *Enhanced fault tolerance*: a disk fails, and mirrored disks take over for it immediately.

2.**High level fault tolerant computing**: multiple processors collaborate to scan data and output to detect errors, and then immediately correct them.

- Fault-tolerant systems ensure no break in service by using backup components that take the place of failed components automatically.

- *Hardware systems* with identical or equivalent backup operating systems. For example, mirroring all operations in backup.
- *Software systems* backed up by other instances of software. For example, if you replicate your customer database continuously, operations in the primary database can be automatically redirected to the second database if the first goes down.

High Availability vs Fault Tolerance

Highly available systems are designed to minimize downtime to avoid loss of service.

- Expensive-a totally mirrored system is fault-tolerant; if one mirror fails, the other kicks in and the system keeps working with no downtime at all.
- Less Expensive-A highly available system such as one served by a load balancer allows minimal downtime and related interruption in service without total redundancy when a failure occurs

Components of a Fault-tolerance System

1.Diversity

- If a system's main electricity supply fails.
- The backup not having the same level of capacity as the primary source.

2.Redundancy

- The system is equipped with one or more power supply units (PSUs), which do not need to power the system when the primary PSU functions as normal

3.Replication

- Replication is a more complex approach to achieving fault tolerance.
- It involves using multiple identical versions of systems and subsystems and ensuring their functions always provide identical results. If the results are not identical, then a democratic procedure is used to identify the faulty system.

Elements of Fault-tolerant Systems

1.Hardware Systems

- Redundant array of inexpensive disks (RAID).

2.Software Systems

- Software systems can be made fault-tolerant by backing them up with other software. example backing up a database.

3.Power Sources

- Power sources can also be made fault-tolerant by using alternative sources to support them.EX- uninterruptible power supply (UPS),hardware-heating-ventilation-air conditioning (HVAC)

Factors To Consider in Fault Tolerance

1.Cost

- Organizations must think carefully about the cost elements of a fault-tolerant or highly available system.

2.Quality Degradation

3.Testing and Fault-detection Difficulties

CLOUD DATAMANGMENT

PROCESSING AND STORAGE

What is cloud data management?

"Cloud data management is the practice of storing a company's data on an offsite server that is typically owned and overseen by a vendor who specializes in cloud data hosting".

Capabilities for Data Management in the Cloud

1. Cloud Integration

- Avoiding duplication and resolving conflicts between contradictory records and taking other steps to ensure data accuracy.
- They might want to integrate applications in real time using orchestration, APIs, and messaging, or run extract transform load (ETL) batch integration jobs for their analytics platforms (cloud data warehouses and data lakes) or to keep application data synchronized.

2. Cloud Data Quality and Governance

- An organization must ensure that people across the enterprise are able to easily locate, access, understand, and use data.
- An automated, cloud-based data quality and governance process provides the clean, high-quality data that business and IT users need to quickly realize business value.

3. Cloud Data Privacy and Security

- Integrated cloud data privacy and protection tools
- Automate discovery and classification of sensitive data.
- Map identities for clear ownership and support data access rules.
- Operationalize privacy policies.
- Model and analyze data risk exposure across data stores and locations.
- Orchestrate data protection.

4. Cloud Master Data Management

- 360-degree view of any domain and any relationship in the cloud.
- Cloud master data management (MDM) capabilities synchronize the most critical data across various systems in your organization into a single, validated record, enabling AI and analytics teams to derive deep insights from that data to power your business.

5. Cloud Metadata Management and Data Cataloging

- Hard to find where data resides.
- By leveraging a combination of technical, business, operational, and usage metadata, intelligent data catalogs help build a robust data foundation to support cloud modernization, data governance, and other business priorities.

6. AI-Driven Enhanced Intelligence

- Automatically discover and catalog data across various systems such as ERP, CRM, and so on.
- Automatically discover relationships between customer data and match insights to specific people.
- Automate data integration and data quality tasks, intelligent policy management and enforcement, and more.

Cloud management components

AUTOMATION AND ORCHESTRATION
- Application migration
- VM images/instances
- Configuration management

SECURITY
- IAM
- Encryption
- Mobile/endpoint security

COST MANAGEMENT
- Cloud instance right sizing
- User chargeback and billing

PERFORMANCE MONITORING
- Storage
- Networks
- Applications
- Compute

GOVERNANCE AND COMPLIANCE
- Risk assessment/ threat analysis
- Audits
- Service and resource governance

Benefits of cloud data management

1. **Security**:

- Data management reduces the risk of data loss due to device damage or hardware failure.
- Companies specializing in cloud hosting and data management employ more advanced security measures and practices.

2.Scalability and savings:

- Cloud data management lets users scale services up or down as needed.

3.Governed access:

- With improved security governed data access is allowed.

4.Automated backups and disaster recovery:

- An up-to-date backup speeds up the process of disaster recovery after emergencies.

5.Improved data quality:

- single source of truth. Data remains clean, consistent, and up-to-date.

6.Automated updates:

- When applications need updated, cloud providers run these updates automatically.

7.Sustainability:

- It allows organizations to reduce the carbon footprint created by their own facilities, and to extend telecommuting options to their teams over cloud.

Best practices for a cloud data management strategy

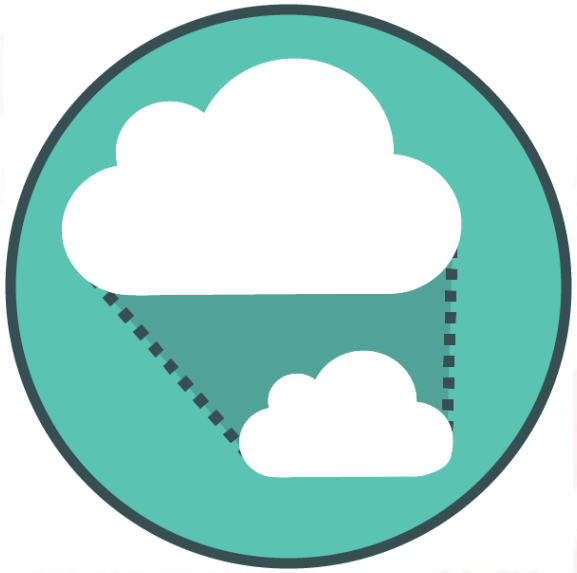
JECRC UNIVERSITY
BUILD YOUR WORLD

1. **Start with a plan.** Will you move all data to the cloud? Or create a hybrid environment? Who needs access to what data? Where should different processing tasks take place? ETL vs. ELT is a good conversation to have now.
2. **Maintain clean data.** Keeping the data "clean" means ensuring that the data entry is accurate and that there are no duplicates or other errors.
3. **Backup the data (often).**
4. **Don't forget about data governance.**

JECRC Foundation

CLOUD

SCALABILITY/ELASTICITY



"Cloud scalability in cloud computing refers to the ability to increase or decrease IT resources as needed to meet changing demand. Scalability is one of the hallmarks of the cloud and the primary driver of its exploding popularity with businesses."

"A similar concept to cloud scalability is cloud elasticity, which is the system's ability to expand and contract based on workload demands."

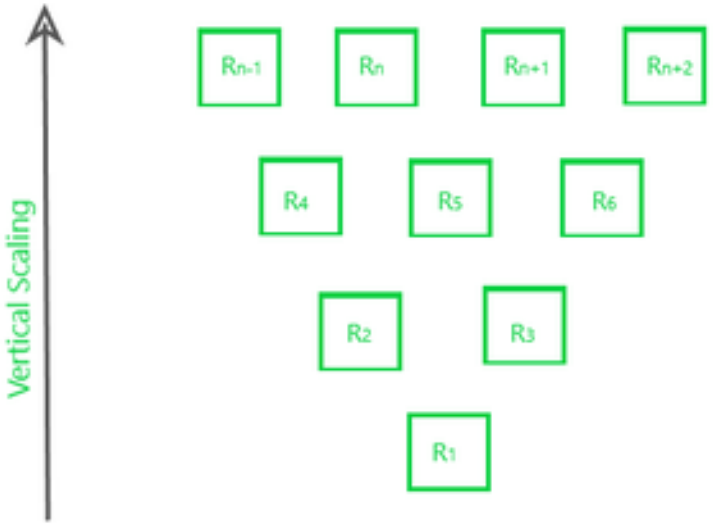
DIFFERENCE-Time

Types of Scalability :

JECRC UNIVERSITY
BUILD YOUR WORLD

1. Vertical Scalability (Scale-up) –

In this type of scalability, we increase the power of existing resources in the working environment in an upward direction. RAM or processing power



JECRC Foundation

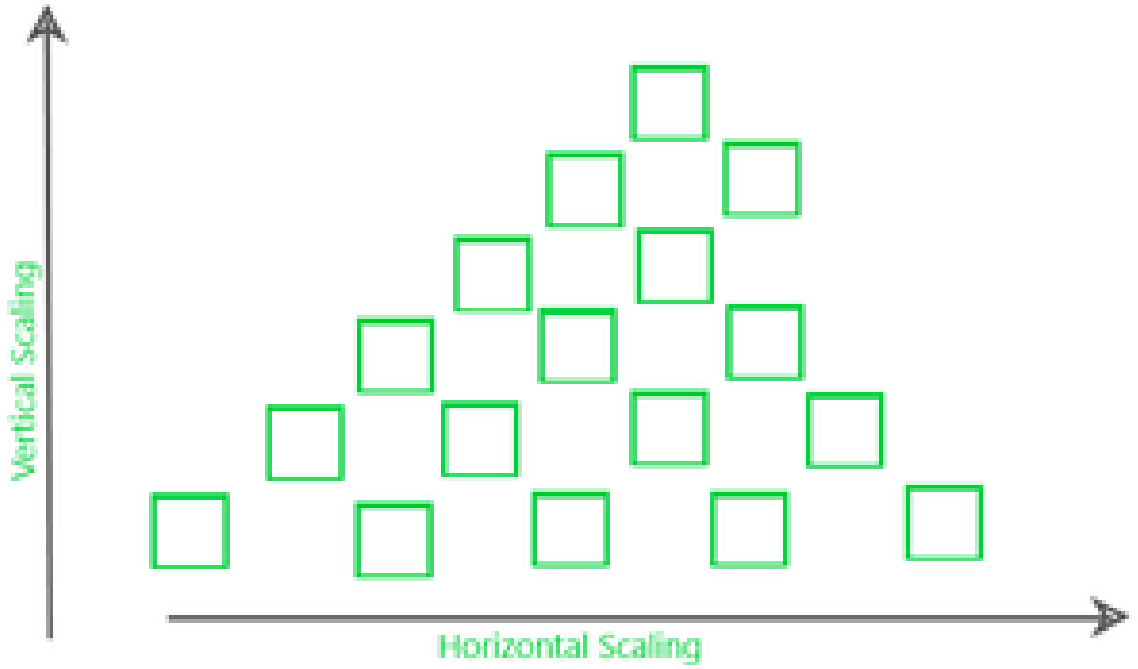
- **2. Horizontal Scalability –**

  In this kind of scaling, the resources are added in a horizontal row.

- Add servers

3. Diagonal Scalability –

It is a mixture of both Horizontal and Vertical scalability where the resources are added both vertically and horizontally.



Difference Between Cloud Elasticity and Scalability :

Cloud Elasticity	Cloud Scalability
Elasticity is used just to meet the sudden up and down in the workload for a small period of time.	Scalability is used to meet the static increase in the workload.
Elasticity is used to meet dynamic changes, where the resources need can increase or decrease.	Scalability is always used to address the increase in workload in an organization.
Elasticity is commonly used by small companies whose workload and demand increases only for a specific period of time.	Scalability is used by giant companies whose customer circle persistently grows in order to do the operations efficiently.
It is a short term planning and adopted just to deal with an unexpected increase in demand or seasonal demands.	Scalability is a long term planning and adopted just to deal with an expected increase in demand.

Benefits of cloud scalability

1.Convenience

2.Flexibility and speed

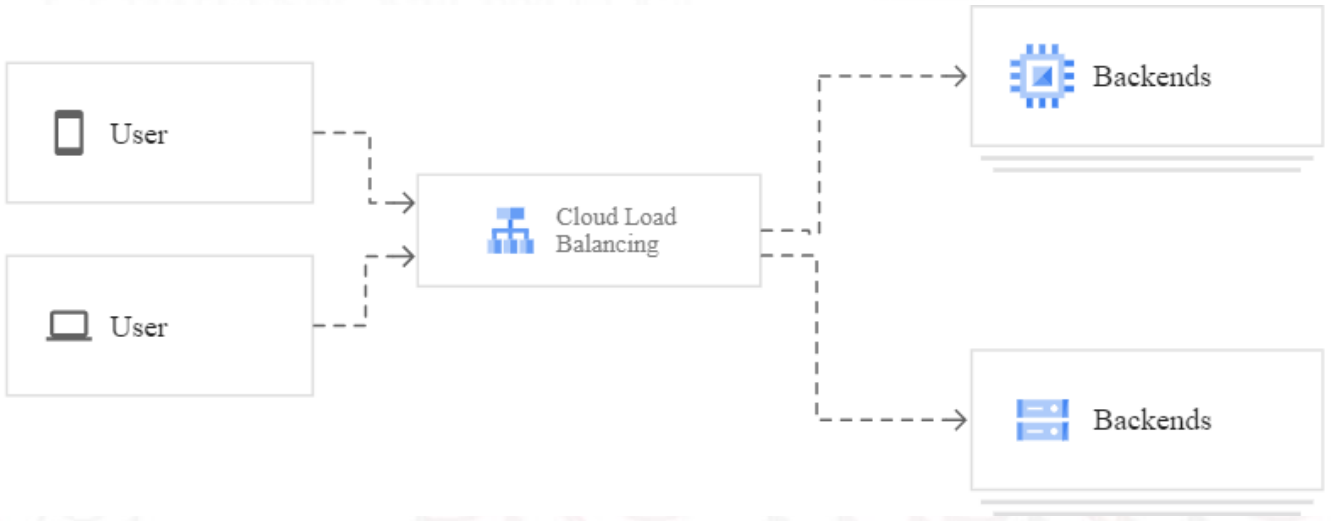
3.Cost savings

4.Disaster recovery

Load balancing in Cloud Computing

"Cloud load balancing is defined as the method of splitting workloads and computing properties in a cloud computing."

- A load balancer distributes user traffic across multiple instances of your applications.
- By spreading the load, load balancing reduces the risk that your applications experience performance issues



Why?

For Traffic-

- Single-server solution in which the server is upgraded to a higher performance server.
- Second is a multiple-server solution in which a scalable service system on a cluster of servers is built.
- Load balancing is beneficial with almost any type of service, like HTTP, SMTP, DNS, FTP, and POP/IMAP. It also rises reliability through redundancy.

Types

1. **Software-based load balancers:**

- Software-based load balancers run on standard hardware (desktop, PCs) and standard operating systems.

2. **Hardware-based load balancer:**

- Hardware-based load balancers are dedicated boxes which include Application Specific Integrated Circuits (ASICs) adapted for a particular use.
- ASICs allows high speed promoting of network traffic and are frequently used for transport-level load balancing

Major Examples of Load Balancers –

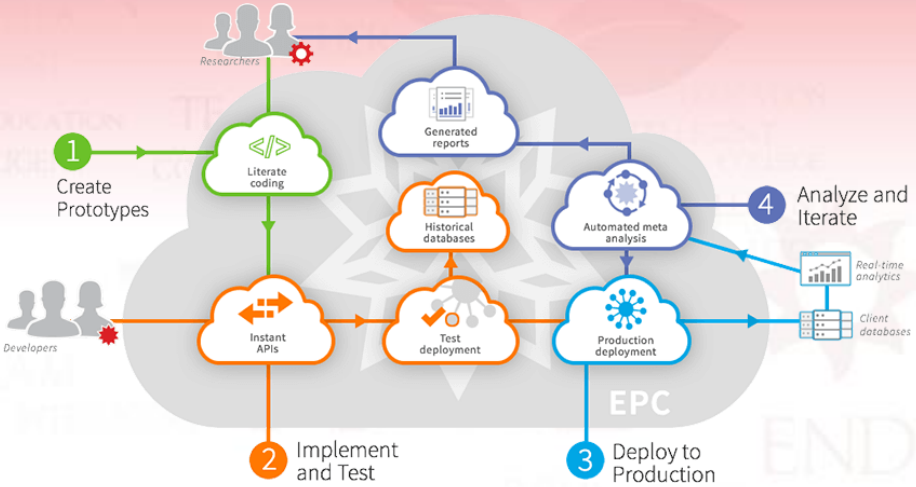
1. **Direct Routing Requesting Dispatching Technique:** IBM's Net Dispatcher.

- A real server and load balancer share the virtual IP address

2. Dispatcher-Based Load Balancing Cluster: A dispatcher does smart load balancing by utilizing server availability, workload, capability and other user-defined criteria to regulate where to send a TCP/IP request. The dispatcher module of a load balancer can split HTTP requests among various nodes in a cluster.

3.Linux Virtual Load Balancer:

- It is an opensource enhanced load balancing solution used to build extremely scalable and extremely available network services such as HTTP, POP3, FTP, SMTP, media and caching and Voice Over Internet Protocol (VoIP).
- It is simple and powerful product made for load balancing and fail-over. The load balancer itself is the primary entry point of server cluster systems and can execute Internet Protocol Virtual Server (IPVS), which implements transport-layer load balancing in the Linux kernel also known as Layer-4 switching.



Cloud Deployment for Enterprises

"Cloud deployment is the process of deploying an application through one or more hosting models—software as a service (SaaS), platform as a service (PaaS) and/or infrastructure as a service (IaaS)—that leverage the cloud. This includes architecting, planning, implementing and operating workloads on cloud."

Benefits of cloud deployment

1. Faster and simplified deployments.
2. Cost savings.
3. Platform for growth.
4. New digital business models.
5. Business resiliency.
6. Agility and scalability.
7. Geographic reach.
8. Operational efficiency.
9. A competitive edge.
10. Empowered users.

Which Deployment is better for Enterprise

JECRC UNIVERSITY
BUILD YOUR WORLD

Cloud Model	Public Cloud	Private Cloud	Community Cloud	Hybrid Cloud
Ease of setup	Very easy to setup	Very hard to setup as your team creates the system	Easy to setup because of community practices	Complex to setup due to interconnected systems
Ease of use	Very easy to use	Complex and requires on in-house team	Relatively easy to use as members help solve problems and protocols	Difficult to use if the system was not setup properly
Data control	Low-provider has complete control	Very high- ownership is with your system	High - if members collaborate	Very high- with right setup
Reliability	Prone to outrages and failures	High with right team	Depends on the community policy	High- with the setup
Scalability	Low, most providers offer limited resources and predefined setups	Very high- there are no other tenants	Fixed capacity tends to limit scalability	High - with right setup
Cost	Inexpensive	Very expensive	Members share cost	Cost-effective
Demand for in-house hardware	No	In-house hardware is preferable	No	In-house hardware is not a must

Requirements for Cloud Computing

https://www.f5.com/services/resources/white-papers/controlling-the-cloud-requirements-for-cloud-computing

Read the White paper on user requirements in Cloud

7 Requirements for Building Your Cloud Infrastructure

1. **Heterogeneous Systems Support**

- Latest hardware, virtualization and software solutions, but they should also support a data center's existing infrastructure.
- Both commodity and proprietary systems are required when building out their clouds.
- Additionally, cloud management providers must integrate with traditional IT systems in order to truly meet the requirements of the data center.

2. Service Management

- Administrators should have a simple tool for defining and metering service offerings.
- A service offering is a quantified set of services and applications that end users can consume through the provider — whether the cloud is private or public.
- Service offerings should include resource guarantees, metering rules, resource management and billing cycles.

3. Dynamic Workload and Resource Management

- In order for a cloud to be truly on-demand and elastic while consistently able to meet consumer service level agreements (SLAs), the cloud must be workload- and resource- aware.
- Cloud computing raises the level of abstraction to make all components of the data center virtualized, not just compute and memory.

4. Reliability, Availability and Security-

- To be fully reliable and available, the cloud needs to be able to continue to operate while data remains intact in the virtual data center regardless if a failure occurs in one or more components.
- Additionally, since most cloud architectures deal with shared resource pools across multiple groups both internal and external, security and multi-tenancy must be integrated into every aspect of an operational architecture and process.

5. Integration with Data Center Management Tools

- Many components of traditional data center management sill require some level of integration with new cloud management solutions .
- Within most data centers, a variety of tools are used for provisioning, customer care, billing, systems management, directory, security and much more.
- These include both current virtualization tools from VMware and Citrix, but also the larger data center management tools from companies like IBM and HP.

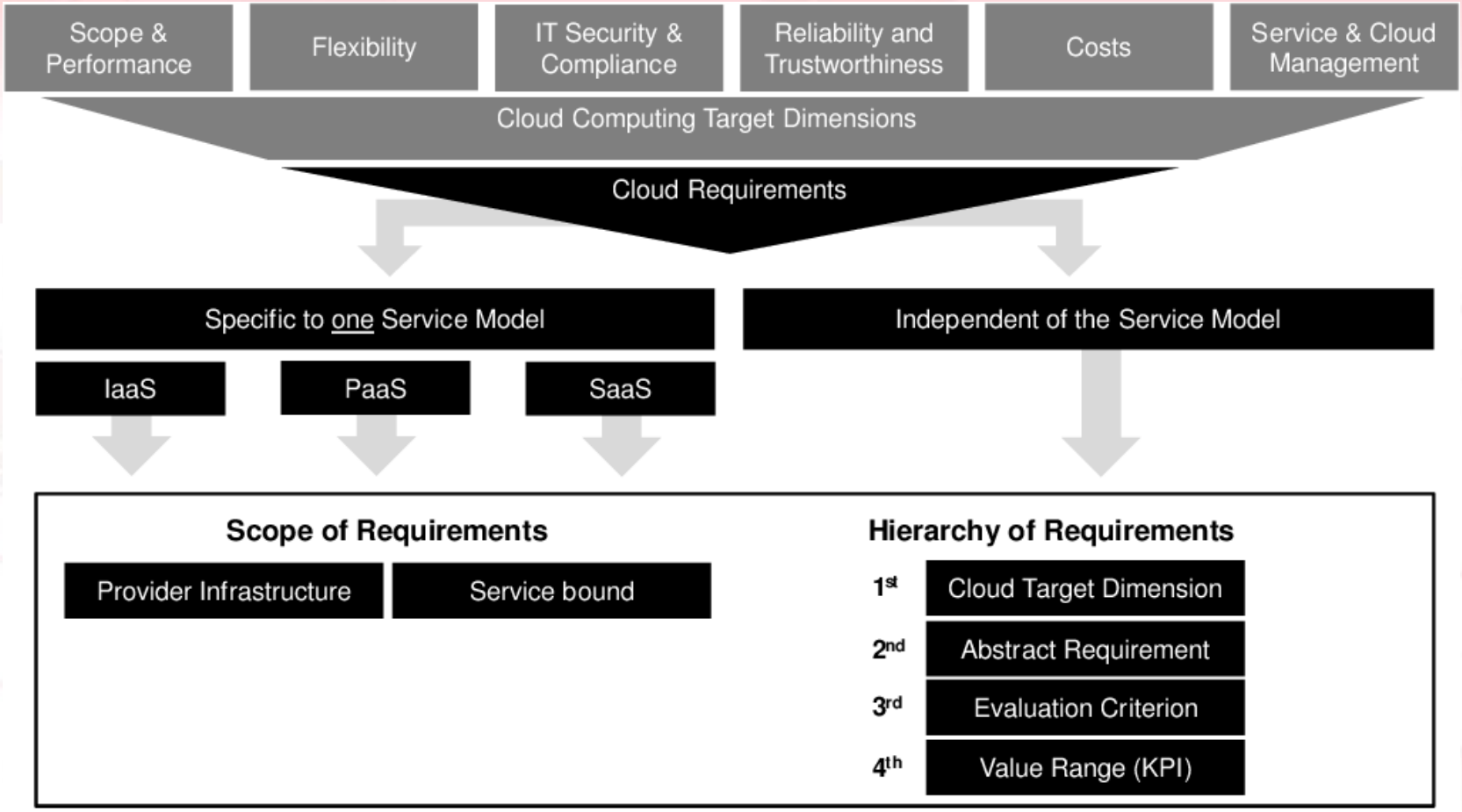
6. Visibility and Reporting:

- Without strong visibility and reporting mechanisms the management of customer service levels, system performance, compliance and billing becomes increasingly difficult.
- Data center operations have the requirement of having real-time visibility and reporting capabilities within the cloud environment to ensure compliance, security, billing and chargebacks as well as other instruments, which require high levels of granular visibility and reporting.

7. Administrator, Developer and End User Interfaces

- Self-service portals and deployment models shield the complexity of the cloud service from the end user.
- Within the self-service portal, the consumer of the service should be able to manage their own virtual data center, create and launch templates, manage their virtual storage, compute and network resources and access image libraries to get their services up and running quickly.

- Similarly, administrator interfaces must provide a single pane view into all of the physical resources, virtual machine instances, templates, service offerings, and multiple cloud users. On top of core interfaces, all of these features need to be interchangeable to developers and third parties through common APIs.


Scope & Performance
Flexibility
IT Security & Compliance
Reliability and Trustworthiness
Costs
Service & Cloud Management
Cloud Computing Target Dimensions
Cloud Requirements
Specific to one Service Model
Independent of the Service Model
IaaS
PaaS
SaaS
Scope of Requirements
Provider Infrastructure
Service bound
Hierarchy of Requirements
1st
Cloud Target Dimension
2nd
Abstract Requirement
3rd
Evaluation Criterion
4th
Value Range (KPI)