Cloud computing

Unit-IV

Workflow Management Systems and Clouds - Architecture of Workflow Management Systems - Utilizing Clouds for Workflow Execution- A Classification of Scientific Applications and Services in the Cloud- SAGA based Scientific Applications that Utilize Clouds. MapReduce Programming Model- Major MapReduce Implementations for the Cloud- MapReduce Impacts and Research Directions. A Model for Federated Cloud Computing - Traditional Approaches to SLO Management- Types of SLA -Life Cycle of SLA - SLA Management in Cloud- Automated Policy based Management. .

1.Define Workflow management system.

A workflow management system is defined as a process consisting of services of steps that simplifies the execution and management of cloud application.

2.Explain the architecture of Workflow management system.

Scientific applications are modeled as work flows consisting of tasks, data elements, control sequences and data dependencies.

Workflow management systems are responsible for managing and executing these workflows.

The Cloud bus workflow management system consists of components that are responsible for Landlines tasks, data and resources.

The architecture consists of three major parts.

- The user Interface
- The Core System
- The Plug-ins

User Interface:

The user interface allows end users for work with

- Workflow Composition
- Workflow Execution Planning
- Submission
- Monitoring

These features are delivered through a web portal or through stand-alone applications that is installed of the user's end.

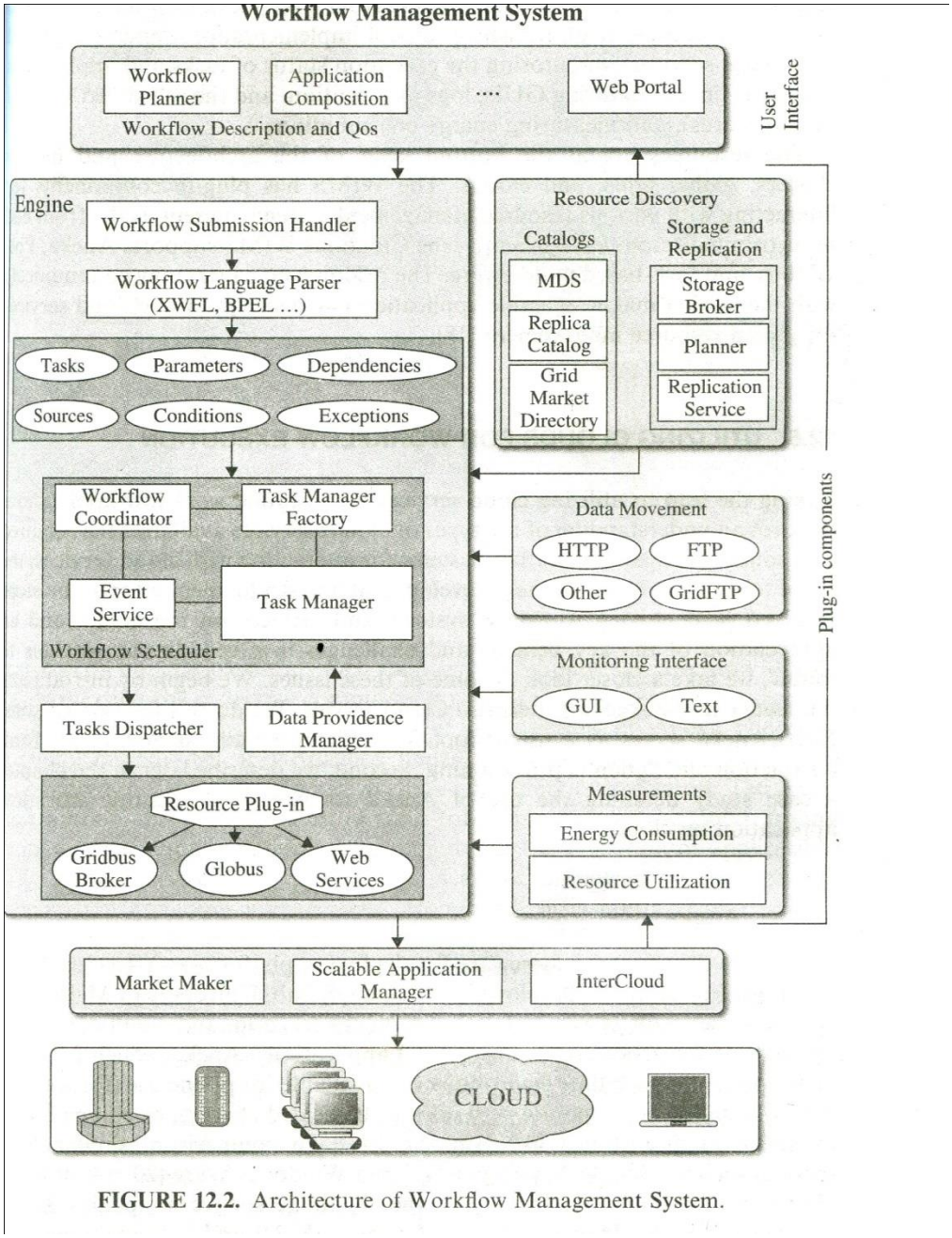


FIGURE 12.2. Architecture of Workflow Management System.

The Core System:

The core components are responsible for managing the execution of workflows. They facilitate the transaction of high-level workflow description into task and data objects.

These objects are used by the execution sub system. The scheduling component applies user selected scheduling policies and plans to the work flow of various stages on their execution.

Plug-ins:

The Plug-ins support workflow execution on different environments and platforms. The plug-ins are used for querying task transferring the execution status of tasks and applications and measuring the energy consumption.

The resources are at the bottom layer of the architecture which includes clusters global grids and clouds. The resources managers may communicate with the

- Market Maker
- Sealable Application Manager
- Intercloud Services for global resource manager

3.What is Aneka?

Aneka is a software platform and framework for developing distributed applications on the cloud. Aneka provides developers with a rich set of API's for using the resources by expressing application logic with a variety of programming abstraction.It is a workflow management tool.

4.Explain in detail about Aneka Implementation on clouds Workflow Execution.

Aneka:

Aneka is a distributed middleware for deploying platform as a service. Aneka, which is both a development and runtime environment, is available for public use for a cost. It can be installed on corporate networks or dedicated clusters or it can be hosted on Infrastructure clouds like Amazon Ec2 to support work flow management.

Aneka was developed on Microsoft.Net framework 2.0 and is compatible with other implementation. Aneka can run on popular platforms such as Microsoft windows, Linux and Macosx.

The runtime environment consists of a Aneka containers running on physical or virtualized models. Each of these containers can be configured to play a specific role such as scheduling or execution.

The Aneka service stack provides services for infrastructure management, application execution management, accounting, licensing and security.

Dynamic resource Provisions:

This service enables horizontal scaling depending on the overall load in the cloud. The platform is elastic in nature and can provision additional resources on-demand from external physically virtualized resource pools, in order to meet the QOS requirements of applications.

Development Environment:

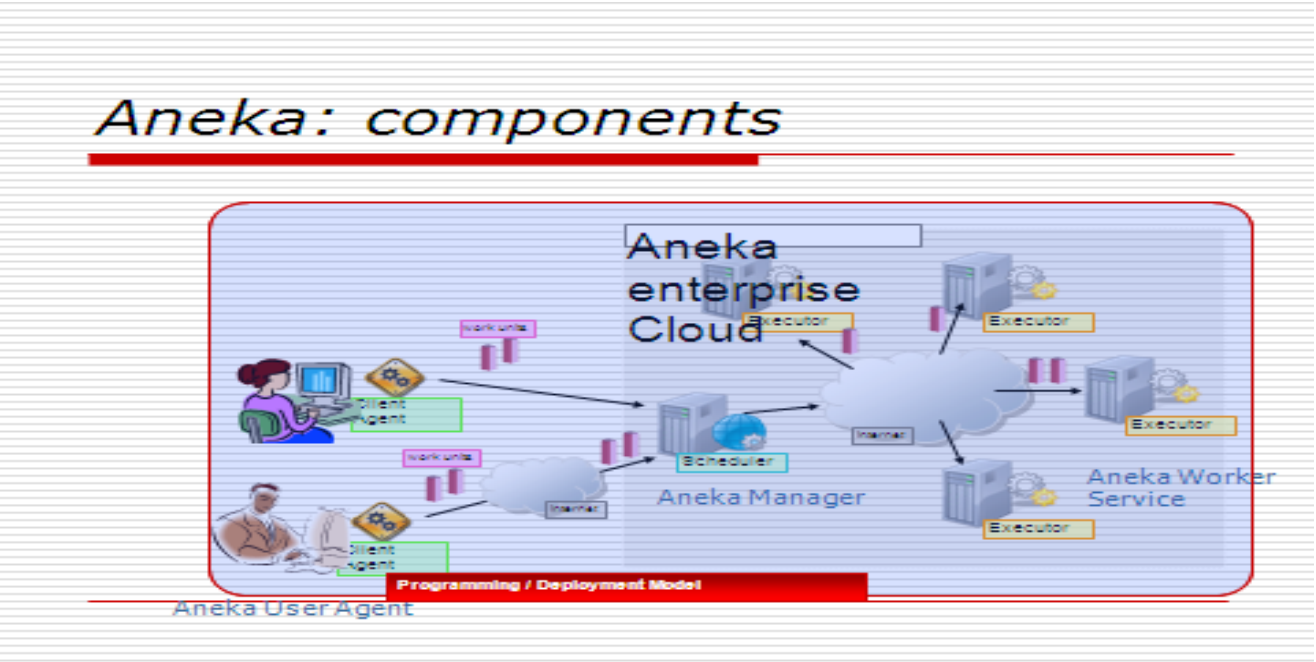
This development environment provides a rich set of API's for developing applications that can utilize free resources of the infrastructure. These APIs expose different programming abstractions, such as the

1.Task Model
2. Thread Model
3.Map Reduce

Storage Service :

The storage service provides a temporary repository for application files such as input files that are required for task execution and output files that are the result of execution.

Any output files produced as a result of the execution are uploaded back to the storage servers. From here they are staged-out to the remote storage location.



.5.What is Scientific Application?

Scientific computing involves the construction of mathematical models and numerical solution techniques to solve scientific, social scientific and engineering problems

6. What are the classification of Scientific Applications and services in the Cloud?

Scientific computing involves the construction of mathematical models and numerical solution techniques to solve scientific, social scientific and engineering problems.

There are three layers consists in the cloud as

1. Software as Service (SaaS)
2. Platform as Service (PaaS)
3. Infrastructure as Service(IaaS)

It is important to learn that how these classification of cloud possibly support scientific application.

Software as Service Layer :

It provides ready-to-Run services that are deployed and configured for the users.

User has no control over the underlying cloud infrastructure

No client side software required

All data manipulated in remote infrastructure.

It can be used Scientific Portal or a visualization tool.

Service Providers:Google Apps, Sales Force

Example:

TeraGrid Science Gateway

Platform as a Service:

PaaS model provides the capability of developing application using programming tools like Java, Python.

Example:

- Microsoft Dryad, Google Map Reduce

Infrastructure As Service (IaaS):

Majority of scientific applications rely on IaaS cloud services.

- Only IaaS provides sufficient programmatic control to express decomposition and Dynamic execution modes that are more important for scientific Applications.

  PaaS model provides the capability of developing application using programming tools like Java, Python.
  Example:
  Microsoft Dryad, Google Map Reduce

7.What is SAGA?

SAGA means Simple API for Grid Applications. It is used to develop scientific applications in the cloud. It provides framework for implementing higher level programming for Scientific Applications.

8.Discuss various SAGA-Based scientific application tools in cloud environment.

SAGA is used to develop scientific application that can utilize the cloud infrastructure from vanilla cloud such as EC2 to open source cloud such as Eucalyptus.

It provides framework for implementing higher level programming for Scientific Applications.

It is the ultimate approach to develop scientific applications in cloud platform.

The SAGA-Based Scientific application tools are

1. **SAGA MapReduce**
2. **SAGA Montage**

SAGA MapReduce:

SAGA MapReduce provides Application Development and runtime environment for scientific Applications.

It gives maximum control over the deployment, Distribution and runtime decomposition.

It is a prominent tool for PaaS Model.

MapReAduce *job* usually splits the input data-set into independent chunks which are processed by the *map tasks* in a completely parallel manner. The framework sorts the outputs of the maps, which are then input to the *reduce tasks*.

The framework takes care of scheduling tasks, monitoring them and re-executes the failed tasks.

SAGA Montage:

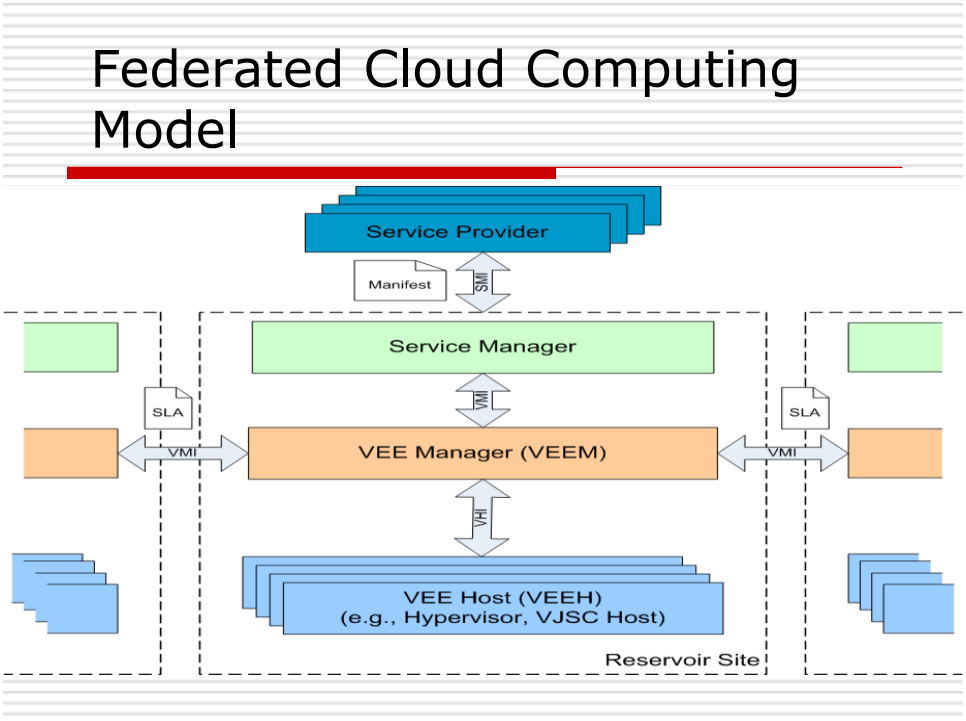
- It is designed to take multiple astronomical images from telescope and other instrument and stitch them together.
- Montage is a set of programming modules or tools , executable program that can run on a single computer, parallel or distributed system.

9.What is Federal Cloud Computing?

A federated cloud computing is the deployment and management of multiple external and internal cloud computing services to match business needs.

10.Explain in detail about Federated Cloud Model

- All cloud computing providers have a finite capacity of resources. To grow beyond this capacity, cloud computing providers should be able to form federation of providers such that they can collaborate and share their resources.
- Each provider can buy or sell on-demand resources from other providers.



Federated Cloud Model Components:

This Federated Cloud Model consists of

the following components

1. Infrastructure Providers (IPs)
2. Service Providers (SPs)
3. Service Application Software
4. Virtual Execution Environment Manager(VEEM)
5. Virtual Execution Environment Host(VEEH)
6. Service Management Interface
7. VEE Management Interface

Infrastructure Providers(IPs):

Infrastructure Providers provide seemingly infinite pool of computational, Within each IP, optimal resource utilization is achieved by partitioning physical resources through virtualization layer into Virtual Execution Environment.

Service Providers(SPs):

- Service Providers lease the resources from Infrastructure Providers and these resources to customers.
- There is a contract and SLA between SPs and IPs

Service Application Software:

- It is a set of software components that collectively to achieve a common goal.
- Each component of such service applications executes in a dedicated VEE.
- **Virtual Environment Manager(VEEM)**:

  It is a fully isolated runtime environments that abstract away the physical characteristics of the resources and enable resource sharing. It is responsible for the optimal placement of VEEs into VEE Hosts to optimize the process.

- It is free to place and move VEEs anywhere even on the remote site as long as the placement satisfies the constraints.
- It is responsible for the federation of remote sites.

Virtual Execution Environment Host(VEEH) :

It consists of

1.Virtualized Computational Resources

2.Virtualization Layer(Hypervisor)

3.All Management enablement Components.

It is responsible for the basic control and monitoring of VEEs and their resources such as

1.Creating a VEE

2. Allocating resources to VEE

3. Monitoring VEE

4.Migrating a VEE

VEEs belonging to the same application may be placed on multiple VEEHs.

VEEHs must support transparent VEE migration to any compatible VEEH within the Federated Cloud, regardless of the site location.

Service Management Interface :

Each layer will be able to interact with each other using SMI with its service manifest.

VEE Management Interface :

- VMI's support of VEEM-to-VEEM communication that simplifies cloud federation interoperability.
- It also implements different and independent IT optimization strategies.

11.What is SLA?

A service-level agreement (SLA) is a contract between an external service provider and its customers or between ISPa and SPs.

A service level agreement, or SLA, is a formal set of service commitments made to a customer by a service provider.

12.What is SLO?

A service level objective is a criteria that is used to evaluate the performance of a business or technology service.

13.What are the traditional approaches to Service Level Objective ?

A service level objective is a criteria that is used to evaluate the performance of a business or technology service.

The existing approaches used to measure the Quality Of Service(QOS) in cloud are

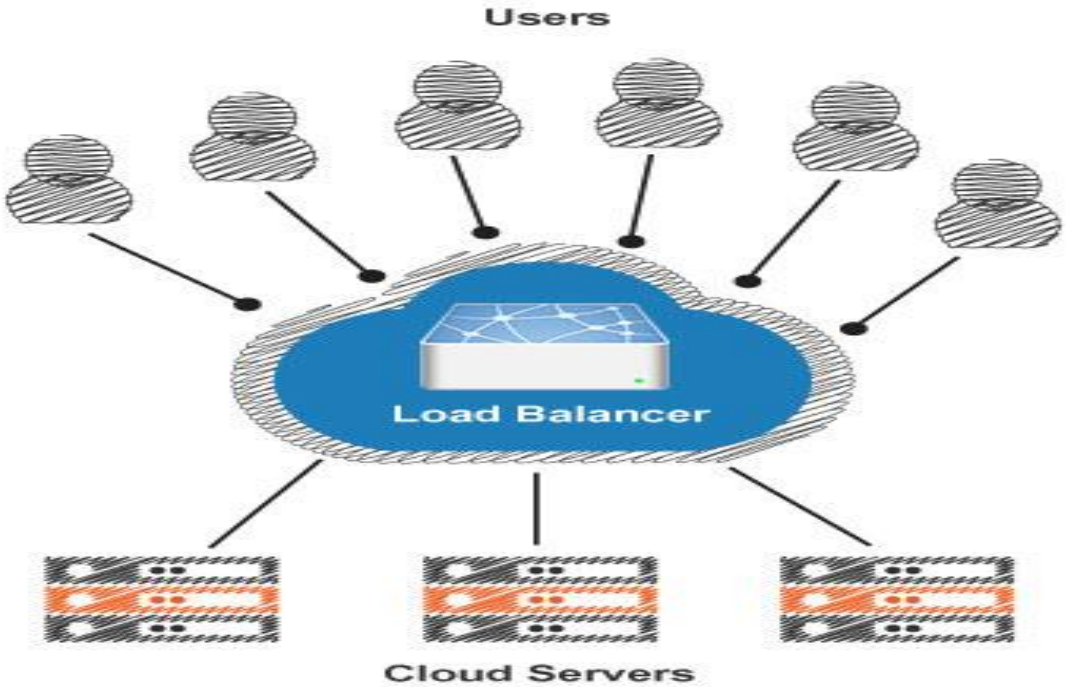
1.Load Balancing Approach

2. Admission Control Approach

Load Balancing Approach:

- **Cloud load balancing** is the process of distributing workloads and **computing** resources in a **cloud computing** environment.
- **Load balancing** allows enterprises to manage application or workload demands by allocating resources among multiple computers, networks or servers.
- Load Balancing algorithm is executed on a physical machine(front-end node) that interfaces with clients.

- This machine receives the incoming request and distribute these request to different physical machines(Back-end nodes).
- These backend nodes are responsible for serving the incoming requests.



Load Balancing Algorithm:

The category of load balancing algorithm

1.Class–Agnostic

2.Class-Aware

3.Admission Control

Class-Agnostic:

- The front-end node not aware of the category of the request such as browsing, payment, selling, buying….

Class-Aware :

This algorithm aware the type of request send from the clients and decide which back-end server should execute.

Admission Control:

Admission Control Algorithm play an important role in deciding set of request that should be admitted into the application server which is very heavy load.

1.Request-based Algorithm

2.Session-based algorithm

Request-Bases Algorithm:

It rejects new requests if the servers running to their capacity.

Session-Based Algorithm:

- Once the session is admitted into the server, all future requests belonging to that session are admitted and new sessions are rejected.

14.What are the types SLA ?

- There are two types of SLA
- 1.Infrastructure SLA
- 2.Application SLA

Infrastructure SLA:

Infrastructure Service provider offers guarantees on availability of the infrastructure such as

1.Server Machine

2.CPU Power

3.Network Connectivity

Application SLA:

- Service providers are flexible in allocating and de-allocating computing resources among the application hosted in the server.
- It is agreement between a customer and service providers indicating performance criteria and cost structure.
- Application SLA may not be a single SLA and it may be set of SLAs based on service performance.
- Customer can switch from one SLA to another SLA during run time.

15.Discuss the Life Cycle of SLA.

- Each SLA goes through a sequence of steps.
- Such sequence of step is called SLA life Cycle and consists of the following five phases.

1.. Contract Definition

2. Publishing and Discovery

3. Negotiation

4. Operationalization

5. De-Commissioning

Contract Definition:

- Generally Service Providers define a set of service offering in standard templates.
- These templates may be in the form of on-line catalog.
- This is called SLA Template.

Publishing and Discovery:

- Service Providers advertise these base service offering through standard publication media.
- Customers can search different competitive offering and shortlist a few that fulfill their requirements.

Negotiation:

- Once the customer has discovered a service provider , before signing the agreement , both parties engages in negotiation to be mutually agreed upon.

Operationalization:

It is known as SLA Enforcement or execution of SLA agreement.

It includes

1. Monitoring
2. Performance Metrics
3. Identifying deviation and correcting
4. Detecting SLA violation and provide the penalty paid option.

De-Commissioning:

- It involves termination of all activities performed under particular SLA when the hosting relationship between service providers and customers end.

16.Explain SLA Management activities.

SLA Management of applications hosted on cloud platform involves five phases

- **1. Feasibility Study**
- **2.On-Boarding Application**
- **3.Pre-Production**
- **4.Production**

5.Termination

Different activities performed under each of these phase.

1. Feasibility Study:

Feasibility study on hosting application on cloud platforms.

Three kinds of feasibility

- 1.Technical Feasibility
- 2.Infrastrucure Feasibility
- 3.Financial Feasibility

Technical Feasibility:

- Ability of application to scale out
- Compatibility of Data Centre
- Availability of specific hardware and software required.
- Preliminary information on application performance.

Infrastructure Feasibility:

Determining the availability of infrastructural resources in sufficient quanity to meet the porjeced demand.

Financial Feasibility:

It involves determining approximate cost to be incurred by MSP.

MSP Means Managed Service Providers

2.On-Boarding Application:

Once the customer and MSP agree to host the application based on feasibility study , the application is moved from customer server to Cloud platform.This moving activity is called On-Boarding.

On-Boarding Activities:

Activity 1:

Packing of the application for deploying on physical or virtual environment.

Making application as deployable components using Open Virtualization Format(OVF).

Activity 2:

The packaged application is directly on the physical server to capture aze the performance characteristics.

Activity 3:

The application is executed on a virtualized platform and perfromance characterizes are noted.

Activity 4:

Based on the measured performance characteristics, different possible SLA are identified.

The resource required and cost involved in each SLA are also computed.

Activity 5:

- Once the customer agrees to the set of SLO and the cost , MSP starts creating different policies required by the data centre for automated management.

3.Pre-Production

- Once the policies are completed , the application is hosted in a simulated production environment.
- Customer verifies and validated the application performance and other details given in the SLA.
- Once both parties agree on the cost, term and conditions of the SLA , MSP allows the application to go on live.

4.Production :

In this phase, the application is made accessible to its end users under the agreed SLA.

5.Termination:

When the customer wishes to withdraw the hosted application and doesn't wish to continue to use the services of the MSP , the termination activity is initiated.

17.Discuss Automated Policy Based Management in detail

There are three types of policy. They are

- Business Policy
- Operational Policy
- Provisioning Policy

Business Policy:

Business Policy help prioritize access to the resources. It includes

1. Application class-Platinum,Gold,Silver.t
2. Whether application breaching the SLA
3. Whether application has already breached the SLA
4. Number of applications breached by the same customer
5. Number of applications about to breach by the same customer.
6. Type of action to be taken

Operational Policy:

It specifies functional relationship between the infrasructural attributes and SLA goals.

It helps identifying the quantum of resources to be allocated to various parts of applications.

Provisioning Policy:

It helps to identifying a sequnce of actions corresponding to user request such as

1.Scale-in

2.Scale-out

3.Start

4.Stop

5.Suspend

6.Resume

Automatic Operalization of Policies:

Automation of these policies are done by various software components such as

1.Prioritization Engine

2. Provisioning Engine

3. Rules Engine

4. Monitoring System

5. Auditing

6. Accounting /Billing System

1.Prioritization Engine:

Identifying user requests based on priority and make it executed.

It is a business Policy

2.Provisioning Engine:

It is based on provision policy which makes set of necessary steps to carry out application by providing resources.

3.Rules Engine:

This component works based on operation policy.

It defined sequence of action to be taken under different condition based on SLA.

4.Monitoring System:

It collects the defined metrics from SLA and these metrics are used for monitoring resource failure and evaluating opertional policy.

5.Auditing:

The predefined SLA should be monitored and recorded.

Non-compliance leads to strict penalties.

6.Accounting and Billing System:

It is used to make bill based on

1. Payment Model
2. Resources Utilized
3. Fixed Cost
4. Recurring Cost

Unit V

Grid and Cloud- HPC in the Cloud: Performance related Issues -Data Security in the Cloud- The Current State of Data Security in the Cloud- Homo Sapiens and Digital Information- Risk- Identity- The Cloud, Digital Identity and Data Security - Content Level Security :Pros and Cons- Legal Issues in Cloud Computing - Data Privacy and Security Issues- Cloud Contracting models- Case Studies : Aneka and CometCloud. .

1.What is Grid Computing?

Grid computing is a processor architecture that combines computer resources from various domains to reach a main objective.

2.What is HPC?

High Performance Computing most generally refers to the practice of aggregating computing power the use of parallel processing for running advanced application programs efficiently, reliably and quickly.

Example : GRID

3.Discuss Grid Versus Cloud

Sno	GRID COMPUTING	CLOUD COMPUTING
1	Distributed resource of computational Power	Centralized resource of Computational power.
2	Grid forms cluster of Physical resources which are faster.	Virtual cluster of resources are economic but slow
3	Parallel processing possible with physical cluster resource.	Cloud doesn't support parallel processing.
4	Grid technology was designed using bottom-up approach.	Cloud technology was designed using top-down approach.
5	Grid is difficult to be used , does not give performance guarantee.	Cloud is easy to use , scalable and always gives user what they want.
6	It is used by narrow community of scientist to solve specific problem,	It is used by all communities.

4.What are the performance related issues linked to the adoption of cloud In the High Performance Computing(HPC)?

There are three important issues occurred related with cloud implementation in HPC.

They are

1. Difference performance evaluation between HPC and Cloud paradigm
2. A Comparison of cloud and HPC approach in terms of advantages and drawbacks.
3. New performance evaluation techniques and tools to support HPC in Cloud System.

Difference performance evaluation between HPC and Cloud paradigm:

The difference between typical HPC and cloud paradigm are given below.

Issues	HPC	CLOUD
Cost	Buy-and –Maintain Paradigm	Pay-per-use Paradigm
Performance Optimization	Tuning of the application to hardware	Joint tuning of application and hardware
System Dimensioning	Performance Under System Administrator Control	Performance under user control.

A Comparison of cloud and HPC approach in terms of advantages and drawbacks

The next issue is performance comparison between classical HPC system and the new Cloud paradigm. It is possible to point out the advantages and disadvantages of the two approaches and will enable us to understand how cloud can be useful for HPC.

Advantages:

The advantages of HPC in the cloud are clear.

It's scalable, on-demand, fast and inexpensive.

Some organizations are concerned about security in the public cloud. And others may worry about the latency effect of moving large amounts of data.

Once the data is in the cloud, it gives HPC customers a unique advantage: it doesn't need to move anymore. Keeping it in a cloud environment makes collaboration easier. Scientific research teams often want to work with other teams in the same interest area, but they may be distributed around the world.

Drawbacks:

HPC customers with one big challenge in a cloud computing environment: getting their data into the cloud in the first place. Scientific research applications often deal with data in the Terabyte range. Uploading it to someone else's server can be like pushing a data lake through a straw.

New performance evaluation techniques and tools to support HPC in Cloud System.

Very few performance measuring tools are provided by CSP or third parties.

These tools are useful only to measure for the virtualized environment.

Ex: **CloudWatch offered by Amazon.**

5.What is Cloud Security?

Cloud Security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

6.Discuss the Current State of Data Security in the Cloud

Cloud security has clearly emerged with both a technological and business case, but from a security perspective, it's still a bit in a state of flux.

A key challenges that many information security professionals are struggling with is how to classify the cloud and define the appropriate type of controls to secure data entering the cloud.

The cloud is inherently untrusted since it is not simply an extension of the organization, but it's an entirely separate environment that is out of the organization's control.

In the cloud computing environment, it becomes particularly serious because the data is located in different places even in all the globe. Data security and privacy protection are the two main factors of user's concerns about the cloud technology.

Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture.

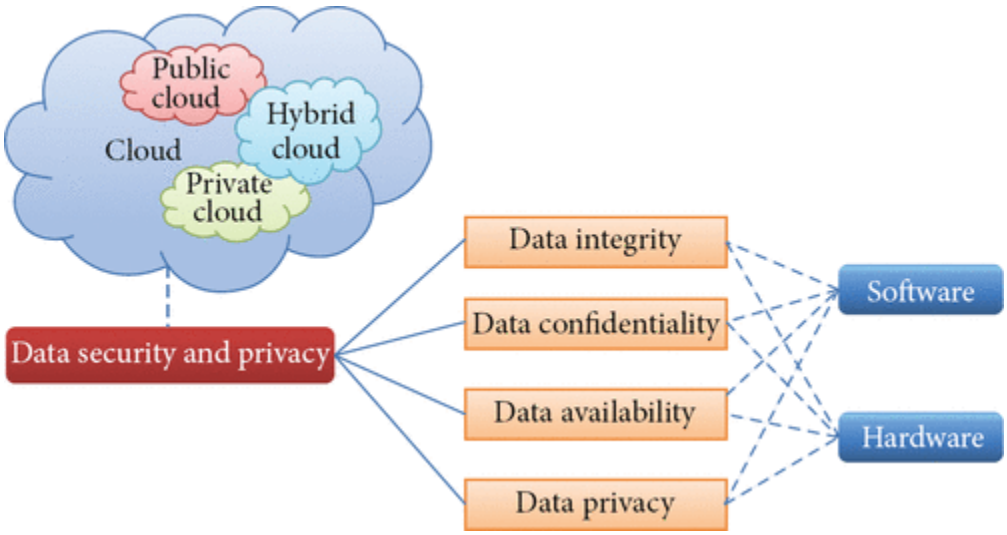
This study is to review different security techniques and challenges from both software and hardware aspects for protecting data in the cloud and aims at enhancing the data security and privacy protection for the trustworthy cloud environment.

7.What is Homo Sapiens?

It means cloud computing is seen as a revolutionary move forward in the use of technology to enhance the modern human communication.

8.Explain in detail about data security risk in cloud computing?

Cloud computing model faces old and new data security risks. Data are uploaded into a cloud and stored in a data centre and these data are accessed by users from these data centre maintained by Cloud Service Providers such as Google, Amazon, Microsoft and so on.The most obvious risk is associated with the storage of that data. This action has several risk associated with it. There are



Risk 1:

A user uploading or creating cloud-based data that are stored and maintained by a third party providers and the data may be hijacked on the way into the data base.

Action to be taken:

It is necessary to protect the data during upload into the data centre to ensure that the data do not get hijacked on the way into the database.

It is necessary to the stored data in the data centers to ensure that they are encrypted all times.

Access those data need to be controlled and the control should be applied to

1. Hosting Company
2. Administrator of the Hosting Company.

Risk 2:

Access Control Risk-

Access control becomes a much more fundamental issue in cloud –based system.

Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment.

Action to be taken:

Information-centric security is an approach to information security paradigm that emphasizes the security of the information itself rather than the security of networks, applications, or even simply data.

Risk 3:

Use of Content after Access:

This risk is potentially higher in cloud network. A user printing of a sensitivity document within the office of a company after accessing data from the cloud.

Action to be taken:

More privacy techniques to be applied to avoid this kind of risk and ensure that the accessed content should not be faced any risk

Risk 4:

The development of Web 2.0 technologies has created a dynamic method of communicating information through blogs, social networking sites, web conferencing, wikis. Data within these domains are more at risk.

Action to be taken:

Cloud computing needs to ensure that protection is applied at the inception of the information, in a content centric manner, ensuring that a security policy becomes as integral part of that data throughout its life cycle.

Encryption is a vital component of the protection policy but further control over the access of that data and the use of that data must be designed.

Conclusion:

We can thus conclude that the risk of an organization or individual using the cloud to store, manage, distribute and share its information has several layers and each layer must be given more importance to reduce risks and these risks should be approached as a whole.

9.What is Digital Identity?

A **digital identity** is a number, code, record, object or collection of attributes that are used by information technologies to identify entities such as people, organizations, users and customers.

Example: This includes usernames and passwords, online search activities, birth date, social security

10.What is Content Level Security/ Content-Centric Security? Discuss its Pros and Cons.

Content Level Security is designed to control what content of file or document is permitted to a user through the cloud. It protects the contents as follows

1. Certain section of the content is visible certain persons
2. Copy protection
3. Sharing of content to only authorized people

4. Only authorized people allowed to access the content.

Advantages :

1.Document Centric:

Complete control over your content down to the document.

2.Remote Wipe:

Eliminate Access to your content at any time from anywhere

3.Content Tracking:

It enables content owners to understand when, how and for how long a user accessed the content.

4.Authorized Access:

Protect the content of document by assigning access to persons who hold a managed information card which contain certain claims.

5.Individual Content Control:

Content access can be based on an individual identity , individual content control and some users can be given stronger rights restrictions than others.

6.Protection from Administrator:

Content level security does not allow the cloud server administrator to access the content from the cloud server.

Simple to use :

Container security is done in a much simpler way of securing data. Content level security can be easily done for database and storage level using existing encryption techniques.

Other benefits:

Data protected at the content level has other benefits such as

1. **Greater control**
2. **More focused on access control**
3. **Increased granular protection over content**
4. **Assurance within the cloud-hosted system.**

Disadvantages:

The implementation of content level security becomes difficult for the clouds which use multi-centre storage and replication of data.

11.What are the legal issues in cloud computing system?

- One of the foremost and fundamental concerns faced by an organization while migrating to cloud services is with respect to the security and privacy of its data.
- However, despite the lack of clarity, most developed countries including EU, UK and the United States are at different stages of creating a legal framework for cloud-based services.
- The UK's Cloud Industry Forum has formulated a code of practice for Cloud service providers. Similarly, New Zealand has a Cloud Computing code of practice.
- In the US there is proposal to enact a Cloud Computing Act. In the EU, a Cloud Computing Information Assurance Framework has been proposed.

Cross border transfer of data:

The global nature of cloud architecture coupled with the diversity of legal mechanisms

Privacy Shield lays down seven privacy principles which are worth mentioning and which should comprise the yardstick to which any cross border transfer of data should be subjected to:

a) Notice: Information to an end user/ consumer that their data is being collected and how it will be used;

b) Choice: Individual's right to opt out of collection and forward transfer of data to third parties;

c) Safety: Safeguards to prevent loss of collected information;

d) Data Integrity and purpose limitation: Data must be relevant and reliable for the purpose it was collected;

e) Access: Individual's right to access information held about him and to correct or delete it, if inaccurate;

f) Enforcement & Liability: Effective means to enforce these rules.

Encryption and data security:

Encryption is one of the key tools employed by an organization to ensure security and privacy of its data in a cloud architecture where the data is frequently in transit and in cases of a multi-tenant environment- where data is stored on a physical hardware that is often shared with third parties.

Liability Issue:

- The liability assumed when entering into a contract in which either party to the contract fails to perform in accordance with the terms, otherwise known as a breach of contract.

Contract Law:

- Contract law is a body of law that governs, enforces, and interprets agreements related to an exchange of goods, services, properties, or money.
- The branch of civil law that deals with interpretation and enforcement of contracts between two or more parties.

Data Portability:

- **Data portability** is the ability to move **data** among different application programs, computing environments or **cloud** services.
- **Data portability** is growing more important as an increasing number of organizations store greater and greater quantities of **data** in the **cloud**.

COPYRIGHT

- Copyright is a legal means of protecting an author's work.
- It is a type of intellectual property that provides exclusive publication, distribution, and usage rights for the author.

This means whatever content the author created cannot be used or published by anyone else without the consent of the author.

Compliance:

Contract Compliance is state of acting in conformance with the predefined and agreed rules or guidelines.

Compliance Issues

- International issues – cross-border data transfer, compliance with foreign jurisdiction laws, export controls

12.What is Contract?

- A contract is a legally enforceable agreement between two or more parties where each assumes a legal obligation that must be completed to provide a product or Service.

13.What are the types of contracts?

A contract is a legally enforceable agreement between two or more parties where each assumes a legal obligation that must be completed to provide a product or Service. Contracts can be classified as follows.

1.Licensing Agreements Versus Service Agreements

2.On-Line Agreements Versus Standard Contracts

3.Importance of Privacy Policies Terms and Conditions

4.Risk Allocation and Limitation of Liability

Licensing Agreements Versus Service Agreements:

- A software license agreement is the legal contract between the licensor and/or author and the purchaser of a piece of software which establishes the purchaser's rights
- A software license agreement details how and when the software can be used, and provides any restrictions that are imposed on the software.
- A software license agreement also defines and protects the rights of the parties involved in a clear and concise manner.
- Most of software license agreements are in digital form and are not presented to the purchaser until the purchase is complete.

Service Agreement

- A service agreement is an agreement between two persons or businesses where one agrees to provide a specified service to the other.
- In cloud computing models, the access to the cloud-based technology is provided as a service contract.

  A service contract provide all the basic terms and conditions that provide adequate

  protection to the cloud user
- There are two contracting models under which a cloud provider will grant access to its services
- .On-Line Agreement
- Standard Contract

On-line Agreement Versus Standard Contract

On-Line Agreement:

- It is a click wrap agreement with which a cloud user will be presented before initially accessing the service . It is a non-negotiable agreement.
- Example:

When user enters into when he/she checks an "I Agree" box.

Standard Contract

- It is a negotiated , signature-based contract will have its place and time with all terms and condition.

Privacy Policy and Terms and Condition

A **privacy policy** is a statement or a legal document (in **privacy** law) that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. It fulfills a legal requirement to protect a customer or client's **privacy**.

- **It's required by law if you collect personal information from users.**
- **It's required by third-party services you may use**
- **Users are interested in their privacy**
- **It's ubiquitous**

Risk Allocation and Limitation of Liability:

A limitation of liability clause stipulates that a party will be obligated to pay to the other in such an event under the terms of an agreement.

This clause limits the amount as well as the types of damages a party can recover from the other.

Risk Allocation

- Allocation of risk in commercial contracts represents a key negotiation point. Each party to a commercial contract seeks to minimize its risk and maximize its reward.
- Allocation of risk is central to all commercial contract negotiations.
- Each party to a commercial contract seeks to minimize its risk and maximize its reward, which creates an inherent tension between contracting parties.
- Parties can manage risk by carefully negotiating and drafting many common contractual provisions.

Example

- Representations and warranties.
- Indemnification.
- Limitation of liability.
- Express contractual remedies.
- Payment terms.

14.CASE STUDY:

ANEKA TOOL:

ANEKA Cloud Platform:

ANEKA is a software platform and a framework for developing distribution application on the cloud. It simplifies the computing resources of a heterogeneous network of workstations and servers or data centers on demand.

Aneka provides developers with a rich set of API's for using the resources by expressing application logic with a variety of programming abstraction. It is a workflow management tool.

Aneka is a distributed middleware for deploying platform as a service. Aneka, which is both a development and runtime environment, is available for public use for a cost.

It can be installed on corporate networks or dedicated clusters or it can be hosted on Infrastructure clouds like Amazon Ec2 to support work flow management.

Aneka was developed on Microsoft.Net framework 2.0 and is compatible with other implementation. Aneka can run on popular platforms such as Microsoft windows, Linux and Macosx.

The runtime environment consists of a Aneka containers running on physical or virtualized models. Each of these containers can be configured to play a specific role such as scheduling or execution.

The Aneka service stack provides services for infrastructure management, application execution management, accounting, licensing and security.

Dynamic resource Provisions:

This service enables horizontal scaling depending on the overall load in the cloud. The platform is elastic in nature and can provision additional resources on-demand from external physically virtualized resource pools, in order to meet the QOS requirements of applications.

Development Environment:

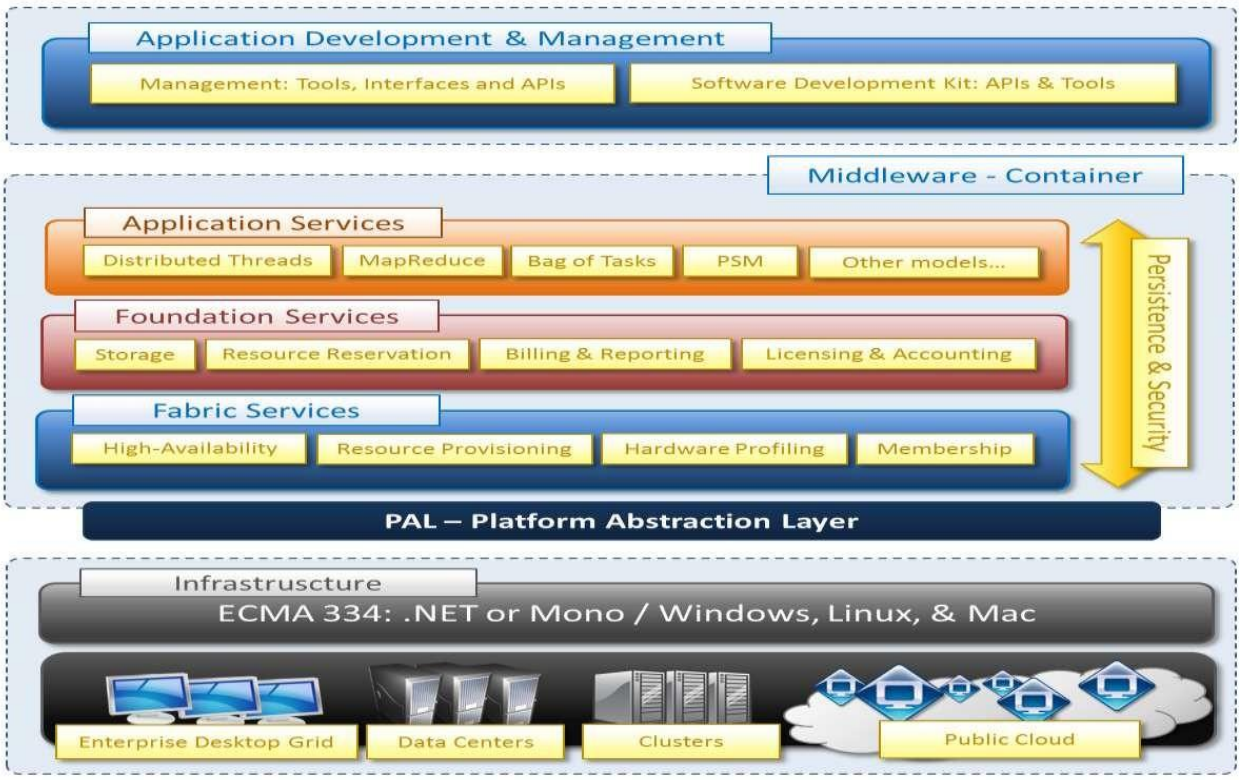
This development environment provides a rich set of API's for developing applications that can utilize free resources of the infrastructure. These APIs expose different programming abstractions, such as the

1.Task Model
2. Thread Model
3.Map Reduce

Storage Service :

The storage service provides a temporary repository for application files such as input files that are required for task execution and output files that are the result of execution.

Any output files produced as a result of the execution are uploaded back to the storage servers. From here they are staged-out to the remote storage location.



Execution Service :

They are responsible for scheduling and executing applications. Each of the programming models supported by Aneka defines specialized implementations of these services for managing the execution of a unit of work defined in the model.

Foundation Service:

These are the core management service of the Aneka container . They are in charge of metering application , allocating resources for execution, managing the collection of available nodes and keeping the services registry updated.

Fabric Services:

They provide access to the resources managed by the cloud . An important service in this layer is Resource Provisioning Service which enables horizontal scaling in the cloud.

Resource Provisioning makes Aneka elastic and allows it to grow or to shrink dynamically to meet the Quality of Service requirements of Applications.

Conclusion:

Aneka cloud can be easily deployed on different hardware , a desk top PC, a workstation, a server , a cluster and even a virtual machines. This flexibility allows quick setup of heterogeneous execution environment on top of which distributed applications can run.

15. What is Cloud Bursting?

Cloud bursting is an application deployment model in which an application runs in a private cloud or data center and bursts into a public cloud when the demand for computing capacity spikes.

16. What is Autonomic Cloud Bridging?

Autonomic Cloud Bridging is to connect Comet Cloud and a virtual cloud which consists of Public Cloud, Data Centre and Grid by the dynamic needs of resources for the application.

17.CASE STUDY 2:

COMET CLOUD

Comet Cloud is an autonomic computing engine for cloud and grid environments.

It supports highly heterogeneous and dynamic cloud and grid infrastructure, integration of public and private clouds and autonomic cloud bursts.

Autonomic Behaviour of Comet Cloud:

Autonomic Cloud Bursting:

The main goal of autonomic cloud bursting is to seamlessly and securely integrate private enterprises clouds and data centers with public utility clouds on-demand. It helps dynamic deployment of applications components onto to a public cloud to support dynamic workloads.

Key Features of Autonomic Cloud Bursting:

1.Load Dynamic:

The computational environment dynamically grow or shrink in response to dynamic application workload.

2. Accuracy :

The computational environment on comet cloud dynamically adapt to satisfy the accuracy requirements.

3.Collaboration of different groups:

Different groups can run the same application with different dataset policies,. As collaboration groups join or leave the work , the computational environment must grow or shrink to satisfy their SLA.

Economics:

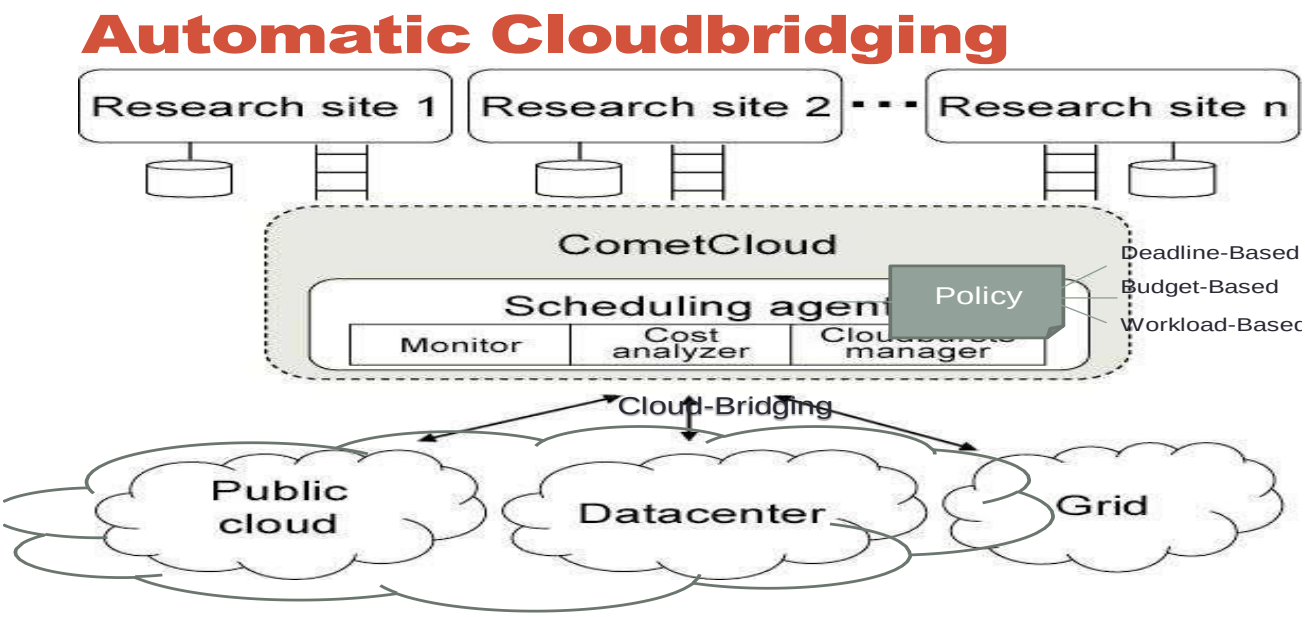
Application tasks can have vary heterogeneous and dynamic priorities and must be assigned resources and scheduled accordingly based on budget and economic model.

Failures :

The computation must be able to manage failures without impacting application quality of service.

Autonomic Cloud Bridging:

Autonomic Cloud Bridging is to connect Comet Cloud and a virtual cloud which consists of Public Cloud, Data Centre and Grid by the dynamic needs of resources for the application.



Conclusion:

Comet Cloud supports autonomic cloud bursting and cloud bridging for the real world cloud application. It also integrates all local computational environment and public cloud services dynamically and provide to manage cloud resources on demand.