PART-A
SHORT QUESTIONS WITH SOLUTIONS

Q1. List any four components that communicates with other component in IaaS implementation.

Ans:

(i) **Pricing Billing Component:** It maintains the execution cost of virtual machine instances and maintains data for which the user is charged.

(ii) **Monitoring Component:** It tracks the execution of vitual machine instances and maintains the data used for analyzing the system performance.

(iii) **Reservation Component:** It stores the data of virtual machine instances.

(iv) **QoS/ SLA Management Component:** It maintains a repository of SLAs agreed by the users and ensures the execution of virtual machine instances with complete QoS.

Q2. Draw and list the layers of cloud computing services.

Ans: The services offered by cloud computing can be divided into three layers (or) classes namely,

(a) Infrastructure-as-a-Service (IaaS)

(b) Platform-as-a-Service (PaaS)

(c) Software-as-a-Service (SaaS).

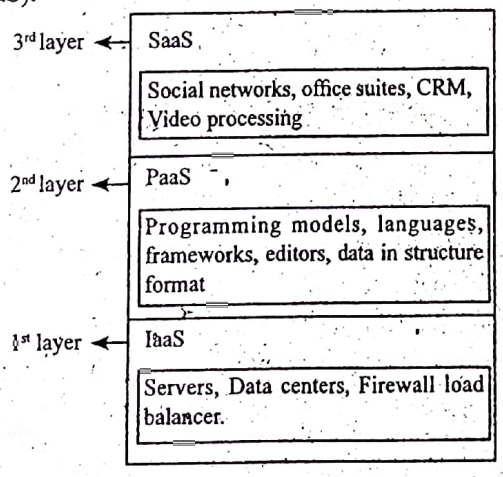


Figure: Layered Architecture of Services

Q3. List the features of public clouds. **Model Paper-II, Q1(c)**

Ans: The features of public clouds are as follows,

(i) Serves a wide range of customers across the globe

(ii) Provides an isolated virtual computing environment

(iii) Provides effective monitoring, guaranteed performance and negotiable Quality of Service.

(iv) Stores the history of usage

(v) Provides complete accountability.

Q4. What are hybrid clouds?

Ans: Hybrid clouds are a heterogeneous distributed system formed from a private cloud that combines resources or services from pubic clouds. They maintain private information within their in-house. They grow and shrink automatically by supplying the external resources and releasing them whenever required.

Deployment and management of hybrid clouds is done by infrastructure management software and PaaS solutions. Infrastructure management software like openNebula opens up the abilities of integrating resources from public clouds. The virtual machine that is obtained manages all the virtual machine instances on a local basis.

Q5. List some of the benefits of SaaS. Model Paper-I, Q1(c)

Ans: The benefits of SaaS are,

1. Reduces software and ownership costs,
2. Improves SLAs
3. Provides simple applications to which data can be integrated
4. Performs rapid implementation
5. Provides stand -alone and configurable applications
6. Provides pricing as per subscription and pay-as-you-go (PAYG) model.

Q6. What are the characteristics that identify Platform-as-a-Service solution? Model Paper-III, Q1(c)

Ans: The characteristics that identify platform-as-a-service solution are as follows,

(i) **Runtime Framework:** It executes the end user code based on the rules set by the user and provider.

(ii) **Abstraction:** It offers methods for deployment and management of applications on the cloud. It offers high level abstraction.

(iii) **Automation:** It automates the deployment of applications to the infrastructure and provides scalability by giving additional resources whenever required.

(iv) **Cloud Services:** It offers services that simplifies the development and delivery of elastic and more likely available cloud applications.

Q7. Write short notes on virtual infrastructure manager.

Ans: A Virtual Infrastructure Manager(VIM) can be defined as a software kit that is responsible for aggregating and aggregating multiple resources on a single platform. This aggregation and assangement is important because the infrastructure-as-a-service providers often find it to difficult to build a cloud infrastructure comprising of both physical and virtual resources. The features of virtual infrastructure manager are as follows,

1. Virtualization support
2. Self service on demand resource
3. Storage virtuatization
4. Virtual networking.

Q8. Compare centralized system with distributed systems. Model Paper-IV, Q1(c)

Ans:

	Centralized System		Distributed System
(i)	Entire processing is done at the server.	(i)	Processing is distributed among the client and the server.
(ii)	Complete database control is left to the central server.	(ii)	Decentralized database control.
(iii)	Full fledged security is provided.	(iii)	High security is needed but difficult to provide.
(iv)	Operating system software installation is not needed for terminal nodes.	(iv)	Operating system software installation is mandatory for both the clients and the servers.
(v)	Centralized backup recovery mechanism.	(v)	Backup and recovery mechanisms on all clients and servers.
(vi)	System software can be easily upgraded.	(vi)	It is very difficult to upgrade the software because of integrity issues.

(vii)	High maintenance cost.	(vii)	Low maintenance cost.
(viii)	High hardware cost and low networking cost.	(viii)	Less hardware cost compared to centralized system (i.e., mainframe) but networking cost is more.
(ix)	Limited number of terminal nodes can be added.	(ix)	Any number of client nodes can be added.
(x)	If the server breaksdown, entire system will collapse.	(x)	The server specific functionalities will be effected in case of server breakdown.
(xi)	No resource sharing.	(xi)	Supports resource sharing between the clients.

Q9. Write short notes on following,

(a) SOAP

(b) WSDL.

Ans:

(a) **SOAP:** SOAP is defined as a simple XML-based protocol which permits applications to exchange XML-based messages over computer networks using HTTP(Hyper Text Transfer Protocol).

(b) **WSDL:** WSDL stands for "Web Services Description Languages". It is an XML-based language that defines the webservices. It is a specification defining how to describe and locate webservices in a common XML language. WSDL2.0 is recent version of specification. It specifies how the interaction takes place between client and a webservice, how to encode parameters and return values in a message and which protocol to be used for the data transmission.

Q10. List the goals of OGSA.

Ans: The goals defined by OGSA are as follows,

(i) It provides facilities to manage resources over heterogeneous, distributed environment.

(ii) It defines open standards, published interfaces to provide interoperability over resources.

(iii) It makes use of extensive industry standard integration technologies.

(iv) It fulfils the quality of service requirement.

(v) It defines loosely coupled and interoperable web service standards.

PART-B
ESSAY QUESTIONS WITH SOLUTIONS
3.1 CLOUD COMPUTING AND SERVICE MODELS

Q11. Discuss about following terms,

(i) Public cloud

(ii) Private cloud

(iii) Hybrid cloud.

Ans:

(i) Public Cloud: Public clouds offer services that can be accessible to anyone from anywhere at point of time. The structural view of public cloud represents a distributed system containing one or more datacenters which are interconnected together. Services offered by the cloud are implemented on the top of datacenters. Users can use these service by signing -in with the cloud provider and entering their personal and billing details. On the other hand, the architectural view of pubic clouds represent a distributed system which can be of any type. It contains one or more data centers upon which the cloud services are implemented and delivered to the users.

Pubic cloud offers solutions that helps in reducing the costs related to IT infrastructure. They handle heavy loads on the local infrastructure. The can eithger grow or shrink depending upon the requirement of business. They offer Iaas, PaaS and SaaS services. Amazon EC2 is an IaaS, Google AppEngine is a PaaS and Salesforce .com is a SaaS.

The architecture of public cloud is designed to support wide range of users that handles heavy loads. The datacenters of public clouds can be distributed geographically so as to minimize the burden of loads. For example, the datacenters of Amazon Web Services are installed in US and in Europe. Their customers have the freedom of selecting the services from either of the three regions us-west-1, us-east-1 or eu-west-1.

Features

- Serves a wide range of customers across the globe
- Provides an isolated virtual computing environment
- Provides effective monitoring, guaranteed performance and negotiable Quality of Service.
- Stores the history of usage
- Provides complete accountability.
- Ability to scale on demand and sustain peak foods.

ii) Private Cloud: Private clouds are virtual distributed systems whose resource provisioning model is restricted upto certain oundaries. These boundaries are set by its company. Private clouds are dependent upon private infrastructure and stores the usiness operations in house (ie., under their own organization). They offer high security since all the private information exists ithin the organization. The billing system bills each and every department of the organization based on their usage. It tests the pplications and systems at lower costs. It provides QoS which performs operations like clustering and failover, monitoring and aintenance, disaster recovery, data replication and uptime services corresponding tc the application. Private clouds allow the sers to adopt specific procedures during the deployment and execution phase of applications. This operation is necessary if the rganization is following the standards of some third-party organization.

eatures: Private clouds provide the following features,

) **Security of Customer Information:** Customer information is secured by maintaining the data in-house.

(b) **Infrastructure that Guarantees Service Level Agreements (SLAs):** Quality of service is guaranteed with the following operations like replication of data clustering and failover monitoring and maintenance of system, recovery from disaster and uptime services that are equivalent to the requirements of application.

(c) **Compliance with Typical Methods and Operations:** Organizations which conform to third-party standards must have to use their own procedures while deploying and executing applications.

(iii) **Hybrid Cloud:** Hybrid clouds are a heterogeneous distributed system formed from a private cloud that combines resources or services from pubic clouds. They maintain private information within their in-house. They grow and shrink automatically by supplying the external resources and releasing them whenever required. The following figure, shows the implementation of hybrid clouds.

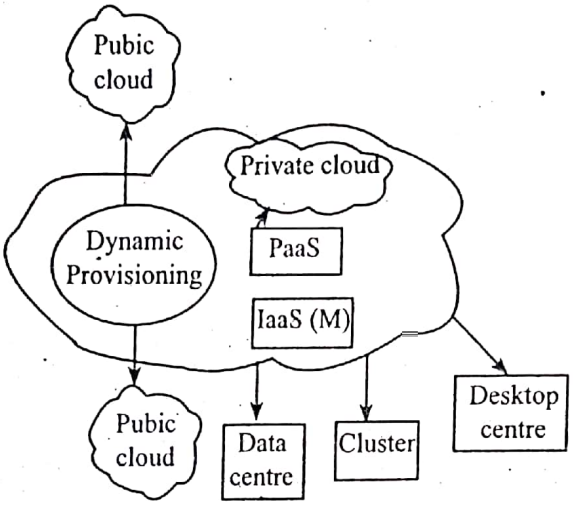


Figure: Implementation of Hybrid Clouds

Dynamic provisioning plays an important role in this implementation. The issues related to scalability are resolved by leveraging the external resources to meet the capacity demands. These resources will be rented out temporarily and released later. This process in known as "cloud-bursting". Hybrid clouds are mostly applicable to IT infrastructure. From IaaS point of view, dynamic provisioning is a method of gaining the virtual machines to increase the performance of resulting distributed system. It then releases those virtual machines.

Deployment and management of hybrid clouds is done by infrastructure management software and PaaS solutions. Infrastructure management software like openNebula opens up the abilities of integrating resources from public clouds. The virtual machine that is obtained manages all the virtual machine instances on a local basis. OpenNebula integrates the advanced schedules(like Harizea) to provide cost-based scheduling. Dynamic provisioning is implemented in PaaS solutions with a guarantee that the execution of applications are under the QoS satisfied and agreed by the users. The Aneka PaaS solutions provide provisioning services capable of leveraging various I-as-a-S provides for scaling the cloud infrastructure.

Q12. Explain about data center networking structure.

Ans: The networking structure of data center consists of group of servers that ranges from thousands to millions. This server cluster is a core part of cloud.

A server cluster comprises of following nodes,

(i) **Cluster Nodes:** These nodes helps in performing computations.

(ii) **Control Nodes:** These nodes are used for monitoring and managing cloud activities.

(iii) **Gateway Nodes:** These nodes are used for providing access point service as well as for enforcing security control on entire cloud.

The data center networking structure is shown below,

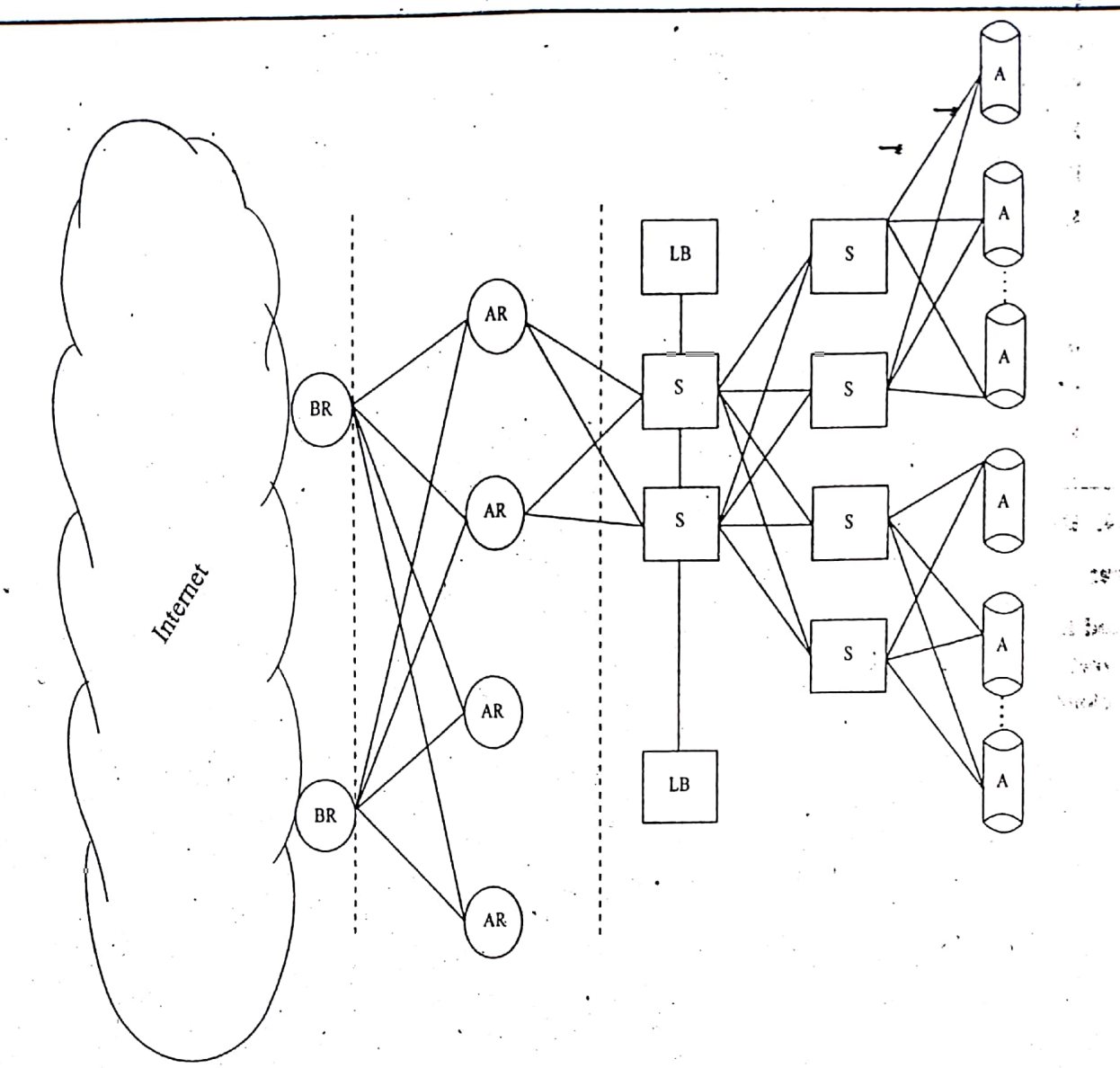


Figure: Networking Structure of Data Center

From above figure,

BR represents Border Router

AR represents Access Router

S represents Switches

LB represents Load Balancer

A represents physical memory.

A data center consists of memory cache, databases and disks on server nodes. The multilayer datacenter networking architecture is designed to provide optimized Internet access to several users across the world. This can be done by making use of IP based commodity networks like 10 Gbps Ethernet network. This architecture consists of the following two layers.

Layer 1: It connects data centers to Internet with the help of Access Router(AR) and Border Router(BR).

Layer 2: It connects server racks with fast switches as hardware core.

Q13. Explain the cloud design objectives.

Ans:

Cloud Design Objectives: The following are the design objectives of cloud computing.

1. **Performing Cloud Computing on Data Center:** Cloud computing can be performed on data centers by shifting the computer processing, software delivery and storage of desktop/local server to datacenters over the Internet.

2. **Using Service Provisioning and Cloud Economics:** Cloud services are provided (to the users) by assigning SLAs to consumers and end users. These services must ensures efficiency in computing, power consumption and storage. Moreover, pricing of these services must be done using pay-as-you-go policy.

3. **Ensuring Performance Scalability:** The cloud computing services, software and infrastructure services must ensure performance scalability even if the number of users present in the cloud gets increased.

4. **Ensuring Data Privacy Protection:** Data privacy protection mechanism should be used in order to make cloud service as trusted service.

5. **Achieving High Quality of Cloud Services:** To achieve high quality of cloud services, the quality of service requirements of cloud computing should be standardize. This helps in making cloud services interoperatable among multiple cloud providers.

6. **Using New Standards and Interfaces:** New standards must be included in the cloud to solve data lock problem on data centers/cloud providers standard APIS and access protocol must be included to provide high flexibility and portability.

Q14. Discuss about cloud ecosystem.

Ans:

Model Paper-I, Q4(a)

Cloud Ecosystem: A cloud ecosystem helps in developing private cloud. This cloud provides remote access to resources across Internet. These resources can be accessed using various web service interfaces(like Amazon EC2). The figure below illustrates the cloud ecosystem for developing private clouds.

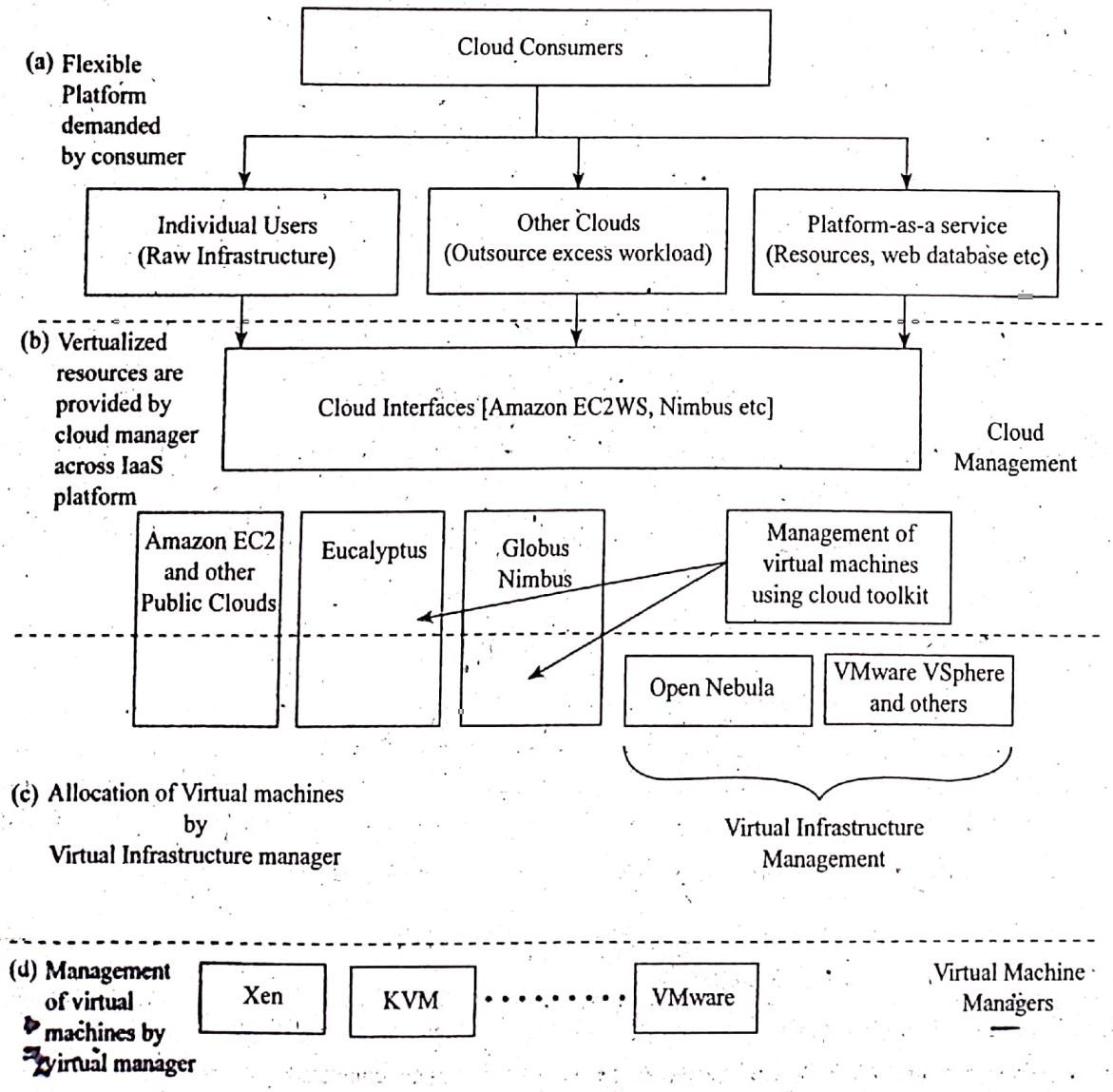


Figure: Cloud Ecosystem

The above ecosystem defines four levels for building private cloud. These levels are as follows,

(i) Cloud consumer level

(ii) Cloud management level

(iii) Virtual Infrastructure (VI) management level

(iv) Virtual Machine (VM) management level.

(i) **Cloud Consumer Level:** In this level, the consumers are provided with a flexible platform.

(ii) **Cloud Management Level:** In this level, virtualized resources are provided by cloud manager across IaaS platform.

(iii) **Virtual Infrastructure (VI) Management Level:** At this level, the virtual machines are assigned to multiple server cluster by the virtual infrastructure manager.

(iv) **Virtual Machine (VM) Management Level:** At this level, virtual machines which are installed on host machines are managed by the virtual machine manager.

Q15. Explain about Infrastructure-as-a-Service(IaaS).

Ans:

Infrastructure-as-a-Service(IaaS): Infrastructure/Hardware-as-a-Service(IaaS) delivers customizable infrastructure as per requirements. It includes single sever to huge infrastructures that constitutes network devices, load balancers, database and web servers. It performs hardware virtualization by configuring and interconnecting virtual machines. This forms a distributed system upon which the applications are installed and deployed, the virtual machines comprise of atomic components whose deployment and pricing depends upon the features of virtual hardware. Virtual hardware comprises of memory, processors and disk storage. The following figure shows the implementation of IaaS.

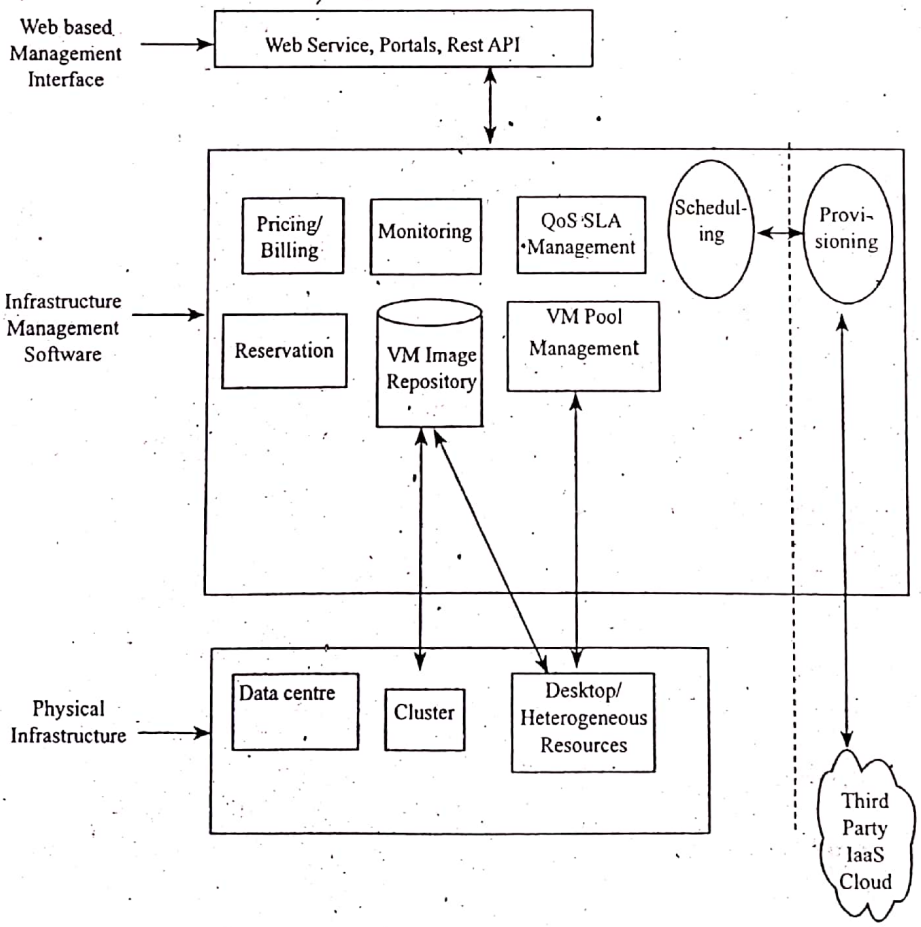


Figure: Implementation of IaaS

This implementation constitutes three major layers- physical infrastructure, infrastructure management software and web based management interface. The web based management interface is the user interface which provides access to the services that are given by the infrastructure management software layer. These services include web services, RESTful API sand mashups. The infrastructure management software layer is responsible for the management of virtual machines. The schedule plays on important role in the execution of virtual machines. It communicates with other components that perform various tasks. Following are those components and their tasks.

Pricing/Billing Component: It maintains the execution cost of virtual machine instances and maintains data for which the user is charged.

Monitoring Component: It tracks the execution of virtual machine instances and maintains the data used for analyzing the system performance.

Reservation Component: It stores the data of virtual machine instances.

QoS/ SLA Management Component: It maintains a repository of SLAs agreed by the users and ensures the execution of virtual machine instances with complete QoS.

VM Image Repository Component: It provides a catalog of virtual machine images which can be used by users for uploading their images. It also allows the users to create virtual instances.

VM Pool Management Component: It tracks the live instances.

Provisioning Component: It communicates with the scheduler to provide a virtual machine instance outside the local physical infrastructure.

The bottom layer i.e., physical infrastructure has heterogeneous environment constituting PCs, workstations and clusters. he desktop grids evolve from this layer. Here, the computing resources are employed to provide huge computing power.

16. Discuss about Platform-as-a-Service(PaaS) and Software-as-a-Service (SaaS).

ns:

latform-as-a-Service(PaaS): Platform-as-a-Service provides a development and deployment platform for running applications. comprises of a middleware upon which the applications are built. Middleware is responsible for managing the applications. ne applications are provided with a runtime environment and do not use any service for managing the infrastructure. The nplementation of PaaS automates the following processes,

Deployment of applications into the infrastructure

Configuration of application components

Provisioning and configuration of load balancers and databases

Managing the modifications done to the system depending upon the standards set by the user.

The core middleware in PaaS manages the resources and scales the applications based on the users demands. It exposes terfaces that are responsible for programming and deploying applications on the cloud. The interfaces can be web-based or ogramming APIs and libraries. PaaS implementation is classified into three types. They are,

Implementation	Vendors and products → Product Type
PaaS-I	
1. Adopts standards of cloud computing for developing and deploying the applications.	Force.com → Middleware and infrastructure
2. Offer an integrated development environment within web browser in which the applications can be designed, developed and deployed.	Longjump → Middleware and infrastructure
PaaS-II	
1. Provides scalable infrastructure for web applications	AppScale → Middleware GigaSpaces XAP → Middleware
2. Provides scaling capabilities by enhancing the runtime by means of additional components	GoogleAPP Engine → Middleware and Engine Yard → Middleware and Infrastructure Heroku → Middleware and Infrastructure Joyent Smart Platform → Middleware and Infrastructure
PaaS-III	
1. Provides cloud programming platform for any type of application.	Mrcriosoft Azure → Middleware and Infrastructure Datasynapse → Middleware Cloud IQ → Middleware Mahjras of Aneka → Middleware Applenda → Middlewaere saaSGrid Guigas paces → Middleware datagord

Software-as-a-Service(SaaS): Software-as-a-Service(SaaS) is a software delivery model that provides the applications to be accessed by means of internet which serves as a web-based service. It reduces the users overhead of managing the complex hardware and software by offloading the tasks to third parties. The role of third parties is to develop applications and provide their access to users via a web browser. This feature cuts down the installation, upfront and license costs for the software. It allows the users to access the application website and sign-in to it by entering their credential and billing details. These details are secured and maintained by the providers and are made available whenever they are required.

SaaS is a "one -to-many" model that allows applications to be shared across multiple users. It provides the following benefits,

1. Reduces software and ownership costs
2. Improves SLAs
3. Provides simple applications to which data can be integrated
4. Performs rapid implementation
5. Provides stand-alone configurable applications
6. Provides pricing as per subscription and pay-as-you-go(PAYG) model.

SaaS application provides services to CRM, ERP and social networking. SalesForce.com is an example of CRM services. It serves applications by providing customer relationship and human resource management, enterprise resource planning and various other features. It also allows SalesForce.com to integrate with third-party applications. These features makes salesForce.com applications more customizable and extensible. Social networking applications include facebook and LinkedIn. SaaS provides features for networking and allow them to integrate with third-party applications and incorporate their features.

3.2 ARCHITECTURAL DESIGN OF COMPUTE AND STORAGE CLOUDS

Q17. Explain the generic cloud architecture.

Ans:

Model Paper-I, Q4(b)

Generic Cloud Architecture: The security-aware cloud (generic cloud) architecture is shown below,

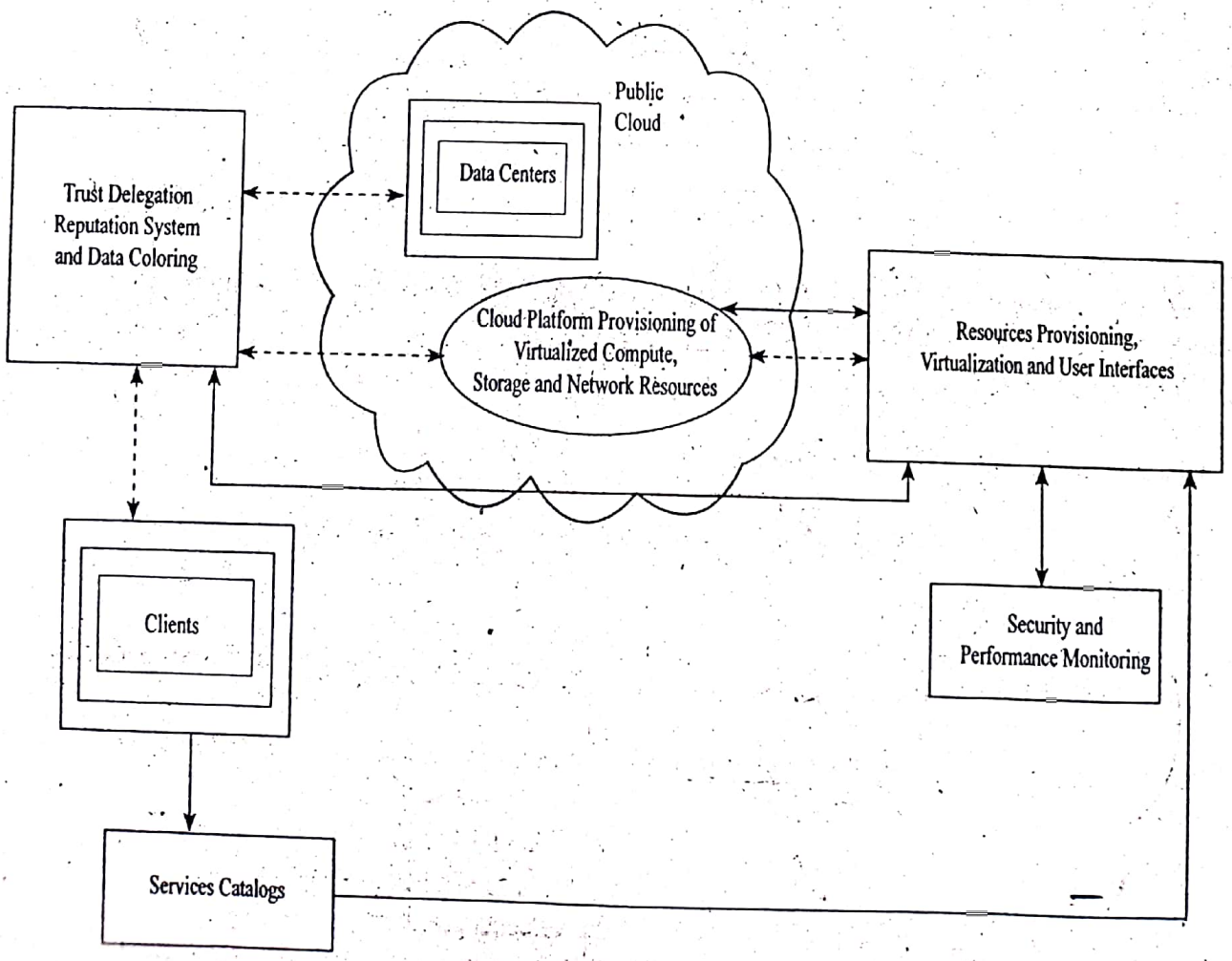


Figure: Cloud architecture

In the above cloud architecture, the Internet cloud forms a massive server cluster. These servers uses various data center resources to perform web services/distributed applications collectively. The formation of cloud platform is done by provisioning/ deprovisioning the server resources, database resources and storage resources.

In this architecture, servers are nothing but physical or virtual machines. Here, user interface is used for processing the requested services and provisioning tools which helps the cloud system to deliver the service request.

Beside this, the cloud platform also consists of distributed storage and its associated services. The resources which are used in cloud computing environment are transformed into data centers managed by third parties. In this architecture, software is nothing but a service.

In cloud architecture, a framework is built for processing the large-scale data that is stored in the storage system. This architecture uses a distributed file system instead of database system. In addition to this, the cloud platform also demand resources like database systems, firewalls, Storage Area Networks(SANs) and security devices. The web service providers uses special kind of Application Programming Interfaces(APIs) that allow developers to exploit Internet cloud. The usage and performance of provisional cloud resources are tracked using monitoring and metering tools.

The software infrastructure used in cloud platform is capable of maintaining/managing all the hardware resources. To overcome issues like performance, pricing ratio, reliability, power consumption and high coloring cost, the cloud computing providers like Google and Microsoft have built huge data centers(with thousand of services) across the world.

Q18. Explain the layered cloud architecture development.

Ans: Model Paper-II, Q4(a)

Layered Cloud Architecture Development: The layered cloud computing architecture development is shown in below figure,

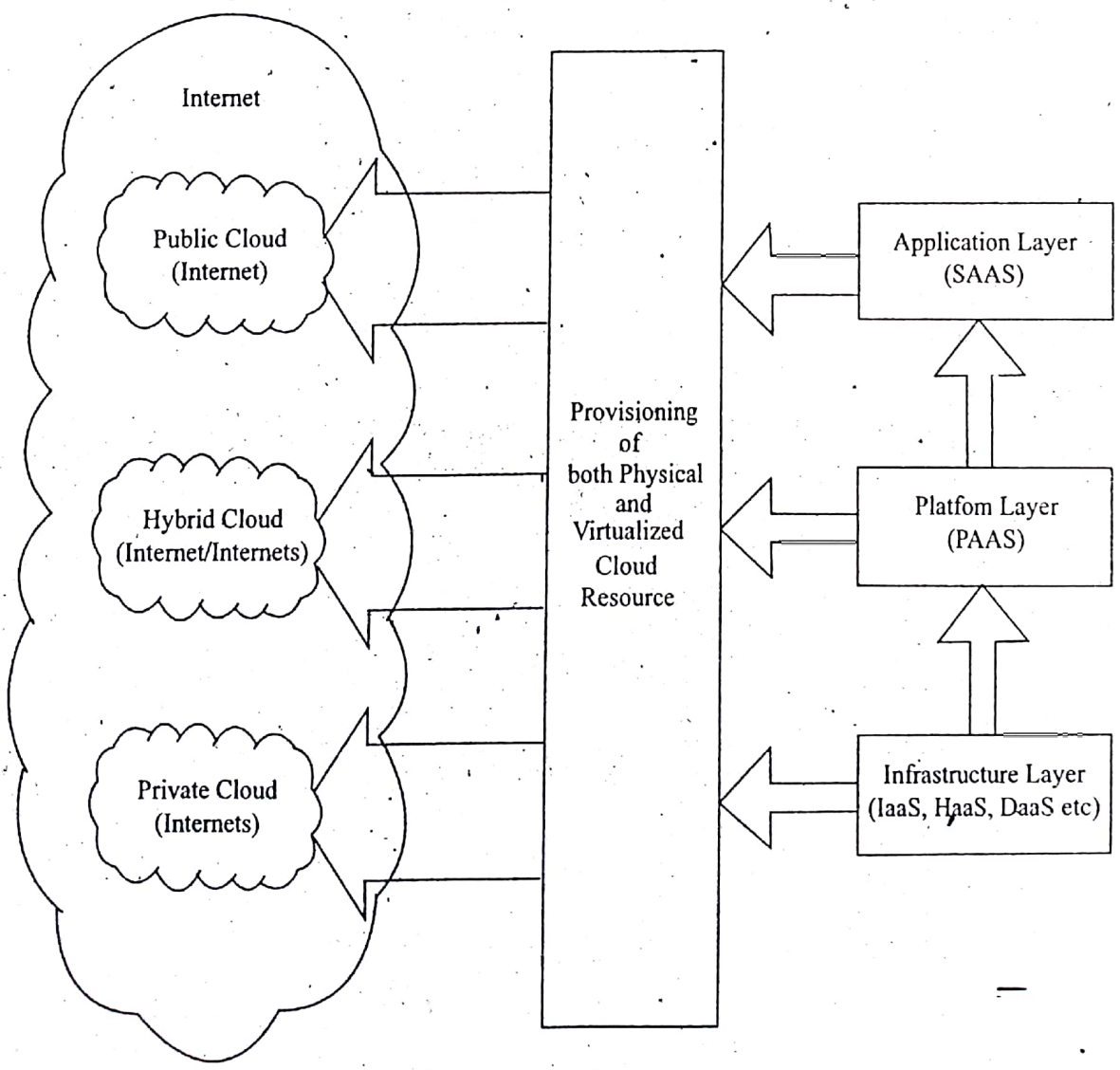


Figure: Layered Cloud Architecture

The layered cloud architecture consists of three development layers. These layers are built using bottom-up approach. These are as follows,

1. Infrastructure layer
2. Platform layer
3. Application layer.

The above three layers are built using bottom-up approach with a dependency relationship between them. Implementation of these layers are done using virtualized and standardized hardware and software resources facilitated in the cloud. Moreover, the services offered by the public, private and hybrid clouds are delivered to the user by providing networking support over Internet and Intranet.

1. **Infrastructure Layer:** Infrastructure layer is the first layer of cloud architecture. This layer is deployed first inorder to provide Infrastructure-as-a-Service(IaaS) services to the customers. It acts as the basis for developing the platform layer. It makes use of virtualized hardware resources for storage, networking and computing purpose. These resources offers flexibility based on user requirement. Moreover, the concept of virtualization helps in optimizing the infrastructure management process and also in automated provisioning of resources.

2. **Platform Layer:** Platform layer is the second layer of cloud architecture. This layer is deployed for offer Platform-as-a-Srevice (PaaS) services. It acts as basis for developing/implementing the application layer. It is a general purpose layer which is mainly used for maintaining software resources frequently. It provides scalable, dependent and secure platform environment that allow users to,

   (i) Create an application

   (ii) Perform test on operational flows

   (iii) Analyze the results of execution and

   (iv) Monitor the performance.

   Since virtualized cloud platform is present between infrastructure layer and application layer, it is considered as a system middleware.

3. **Application Layer:** Application layer is the second layer of cloud architecture. This layer offers Software-as-a-Service(SaaS) services to the applications. It is built using different software modules that are required for SaaS applications. The service applications of this layer consists of daily office management tasks like information retrieval service, document processing services as well as authentication service.

Q19 Discuss in brief about market oriented cloud architecture.

Ans:

Market Oriented Cloud Architecture: The market oriented cloud computing architecture is designed to allocate cloud resources based on user requirement. The primary objectives of this architecture is to,

1. Maintain specific level of Quality of Service(QoS) needed by the cloud providers.
2. Maintain balance between supply and demand of cloud resources.
3. Generate Feedbacks to cloud consumers and cloud providers on economic incentives.
4. Implement Quality of Service(QoS) based on resource allocation mechanism.
5. Minimize the potential cost of providers.

The market cloud computing architecture is shown in the figure below,

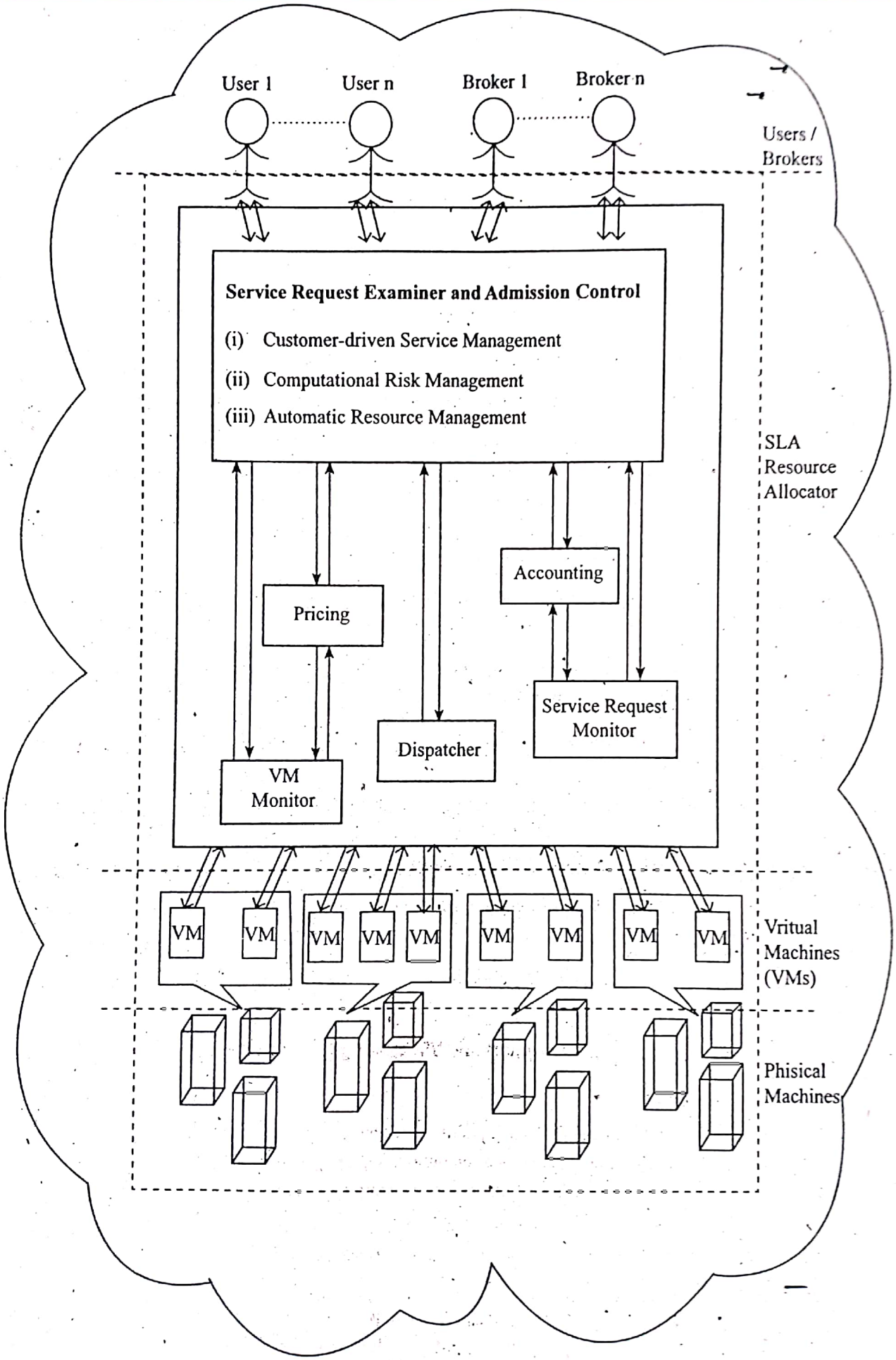


Figure: Market Oriented Cloud Architecture

The above architecture comprises of the following entities,

(i) **Users/Brokers:** Users/Brokers are responsible for initiating service request (across the world) and submit it to the data center and cloud.

(ii) **SLA Resource Allocator:** SLA resource allocator is placed in between the cloud service provider(data center) and external users/brokers. It is responsible for providing interaction between data center and users inorder to facilitate SLA oriented resource management. To support the SLA oriented resource management the SLA resource allocator provides interaction between mechanisms like VM monitor mechanism, pricing mechanism, dispatcher mechanism, accounting mechanisms and service request monitor mechanism.

Service Request Examiner and Admission Control: The service requests which are initiated by users/brokers is initially submitted to the service requests examiner. Then this request is interpreted by service request examiner in order to check its QoS requirement. Based on the result obtained, the acceptance/rejection of request is decided. The role of service request examiner is,

(i) To provide resource overloading. As a result of this most of the requests will be unsuccessful due to less availability of resources.

(ii) To maintain status information on resource availability and workload processing.

(iii) To allocate requests to virtual machines and search resource entitlements for virtual machines.

The various mechanism are discussed below,

(a) **VM Monitor Mechanism:** This mechanism helps in maintaining information about the VMs availability as well as its resource entitlement.

(b) **Pricing Mechanism:** This mechanism helps in deciding the changes to be made upon service requests depending on submission time, pricing rates, resource availability etc.

(c) **Dispatcher Mechanism:** This mechanism helps in executing the service requests which are accepted by service request examiner on the allocated VM.

(d) **Accounting Mechanism:** This mechanism helps in computing the total cost charged to the users. This computation is done by storing the information about actual resources used. This information is later used by server request examiner and admission control for making decision on resource allocation.

(e) **Service Request Monitor Mechanism:** This mechanism helps in maintaining information about those service requests which are successfully executed.

This architecture uses multiple VMs to concurrently execute applications on a single physical machine containing multiple operating system environments.

Q20 Briefly explain about virtualization support and VM cloning for disaster recovery.

Ans:

Virtualization: Virtualization is a mechanism in which multiple independent operating systems are made to run on a single physical computer. It is one of the unique feature of cloud computing. Server virtualization on shared cluster provides enhance web services. Virtual machines are considered as containers of cloud computing. To deploy virtual machines on physical nodes the provisioning tools, initially determines the corresponding physical machine and later executes them on virtual nodes. Since the process of development and deployment of virtual machines done simultaneously, this leads to the elimination of various run time problems.

In cloud computing, the concept of virtualization helps in virtualizing the hardware infrastructure as well as its resources without considering the computing resources, physical resources, scalability and fault tolerance.

Figure below, shows server virtualization in data center and cloud application,

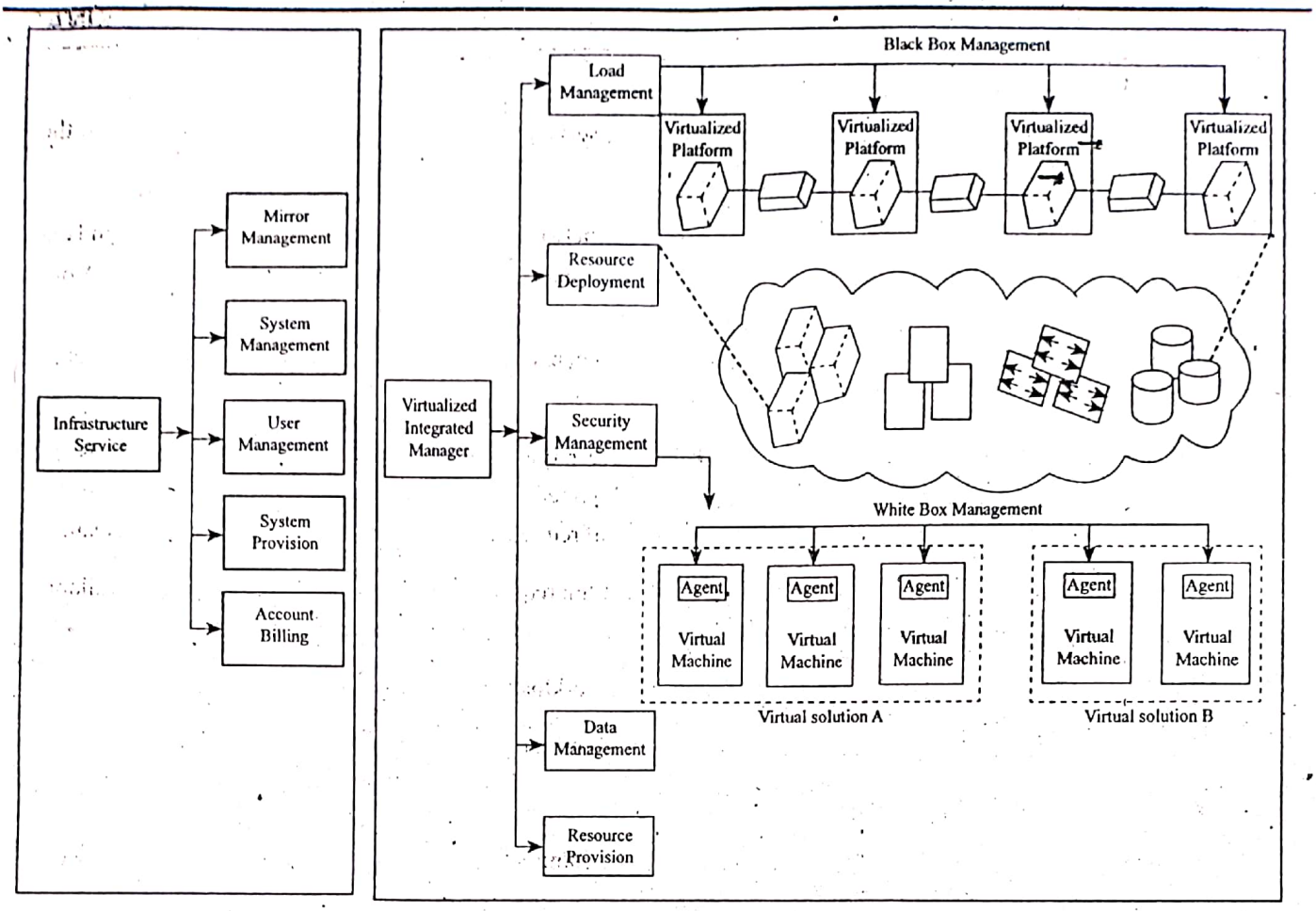


Figure: Virtualized Infrastructure

Hardware Virtualization: Hardware virtualization is done using virtualized software. This software is referred to as system virtualization software. It is responsible for simulating the execution of hardware resources as well as unmodified operating system. It is considered as a platform on which new cloud applications can be built. These applications can be executed on any operating system irrespective of any programming environment.

The virtualize cloud computing platform helps in performing the following tasks,

(i) It provides a run time environment for executing legacy softwares like traditional operating systems and unusual applications.

(ii) It provides flexible runtime services to run application in any environment.

(iii) It is mainly used for hosting third-party programs.

(iv) It provides runtime environment that ensure flexibility and also helps in fulfilling users demand.

(v) It provides an environment that allow the user to have complete privilege on the system.

Virtualize system software facilitates a hardware analog mechanism that helps in executing unmodified operating system directly on hardware which is present prior to software. A user can gain complete access right on their respective virtual machines. However, it is possible to mount multiple virtual machines on similar physical server and allow their execution on distinct operating systems. To carry out this execution on a virtual machine a virtual disk storage and virtual networks must be established. Virtualization is done using specialized servers which are capable of producing virtualized resource pool whereas virtualize infrastructure is carried out using virtualizing integration managers which are capable of handling load management, resource management, data management, provisioning functions as well as security management.

VM Cloning for Disaster Recovery: The traditional approach used for disaster recovery recovers the failed system from a different physical system. Use of such an approach consumes a lot of time, cost and involves complex processes. This is because the process requires the following operations to be performed.

1. Configuring hardware
2. Installing operating system
3. Configuring operating system
4. Installing backups
5. Restarting the system.

In a virtual machine environment, the time consumption can be minimized because recovery of one virtual machine from another does not require installing and configuring of operating system and backup agents. Thus making the recovery process 40% faster than the traditional approach.

In this type of recovery system, clones of active virtual machines are created and stored at remote server. When an active VM fails, its clone gets activated as live migration over the shared Internet. This type of activation consumes a little amount of time. Cloud control center captures a snapshot of the active state of failed VM before subjecting the clone to live migration for a quicker activation. Modifications and updations of data and states are forwarded to the suspended virtual machine to keep its state updated.

Q21. Explain about architectural design challenges.

Ans: Model Paper-II, Q4(b)

Architectural Design Challenges: The architectural design challenges are described as follows,

1. **Service Availability and Data-Lock in Problem:** If cloud services are managed by single cloud providers then this may lead to single point failure due to resource unavailability. To avoid such situation, multiple cloud providers/data centers located at various geographical location must be considered. Thus management of cloud services by multiple cloud providers protect the data from failure and also helps in achieving high resource availability. However, Distributed Denial of Service(DDOS) attack is another availability obstacle. In this type of attack, Internet hacker/illegitimate users threatens to effect the income of Software-as-a-Service(SaaS) providers by interrupting the services and making them unavailable.

Eventhough the software stack of cloud architecture provides improved interoperability on various cloud platforms, its Application Programming Interfaces(APIs) need to be standardize. This is because, standardize APIs allow SaaS developer to deploy data and services on several cloud providers site. This helps protect the data from single point failure and also mitigates the data-lock in problems.

2. **Data Privacy and Security Concerns:** Public cloud networks can expose the system to various security attacks like hypervisor malware, hijacking, man in the middle attack, guest hopping etc. Inaddition to this, there are two types of attacks that makes the system vulnerable to attacks. These are,

(i) Active attack

(ii) Passive attack.

(i) **Active Attack:** In this type of attack, the hacker/ illegitimate users try to steal the password or data which is sensitive to the system.

(ii) **Passive Attack:** In this type of attack, the hacker try to modify the kernel data structure with the intention of damaging the cloud services.

To overcome from the above obstacles, various technologies like storage, virtual LANs and network middleboxes i.e., firewalls, packet filters are included in the cloud.

3. **Unpredictable Performance and Bottleneck:** Cloud architecture allows virtual machines to share multiple CPUs and main memory but it does not support I/O sharing. This may lead to I/O interference problem between virtual machines. To overcome this problem I/O architecture must be improved so as to virtualized interrupts and I/O channels.

The rise in Internet applications are pulled beyond the cloud limits then transmission and placement of data in cloud computing becomes complex. To overcome this problem, all the weak servers must be eliminated from cloud application.

4. **Distributed Storage and Widespread Software Bugs:** In cloud application, the database will grow and shrink based on requirement. Hence for this reason distributed SANs must be incorporated as a new storage in cloud architecture. This storage helps in creating scalable cloud application which also meets the increasing demands of cloud application.

Debugging must be performed on large scale distributed data center so as to detect bugs. But this phenomenon is not supported in cloud computing. Thus to detect the software bugs, virtual machine must be used in cloud computing. The concept of virtualization applied on virtual machine helps in capturing the most critical information of the system without compromising the security. Besides this, debugging is applied over simulators to identy the software bugs.

5. **Cloud Scalability, Interoperability and Standardization:** The storage and network bandwidth of pay-as-you-go (PAYG) model is calculated depending on the total number of bytes needed for virtualization levels. Hence, due to this reason automatic scaling must be performed on load variation. So as to reduce cost without violating SLAs.

The packaging and distribution of VMs can be done using Open Virtualization Format (OVF) which specifies open, secure, portable, efficient and extensible format. Apart from this, it also specifies a format to distribute software to be incorporated in VMs. Typically, the VM format is independent of any particular host platform or virtualization platform and guest operating system. The idea behind this is to resolve virtual platform-agnostic packaging along with certification and integrity of packaged software. The virtual appliances are sustained by package so as to cover multiple VMs.

6. **Software Licensing and Reputation Sharing:** Cloud computing providers depends upon open source software since licensing models for commercial software does not support utility computing. Hence, the commercial software companies must change their licensing structure to perform better cloud computing services. Cloud providers must consider licensing schemes like pay-for-use and bulk-use-licensing scheme to expand their business.

Reputation sharing can have adverse effects on the reputation of entire cloud. That is if single customer carry unauthorized functions/activities then this may affect the entire cloud. To overcome this must enforce various reputation guarding services on cloud. Besides this, legal liabilities must be resolved at SLA level.

3.3 PUBLIC CLOUD PLATFORMS

Q22. Explain the five major cloud platforms and their service offerings.

Ans: Model Paper-III, Q4(a)

Public Clouds and Service Offerings: Computing and IT administrators, software vendors and end users are ordering for cloud services whereas, at top level individual users and organizational users are ordering for various services.

Providers	Services
Application providers at SaaS Level	Individual users
IaaS and PaaS providers	Business organizations
IaaS providers compute, storage and communication resources	Applications and organizational users
Platform providers	Infrastructure services and organizational users

Cloud services depends on new advances in machine virtualization, service-oriented architecture, grid infrastructure management and power efficiency. These services are purchased by consumers in the form of IaaS, PaaS and SaaS.

So, that the cloud dealers are selling their utility services to more number of users and the cloud industry is supporting the demand growth by business users to sold their computing and storage jobs to professional providers. So, that the service charge is less than the actual price for users to change the outdated servers regularly.

	Model	IBM	Amazon	Google	Microsoft	Salesforce
1.	PaaS	It is used in blue cloud, web sphere cloud, burst appliance, research compute cloud.	–	It is used to search by App Engine[Google App Engine].	It is used in Windows Azure.	It is used to search as Force.com
2.	IaaS	Ensembles	It provides Amazon web services.	–	Windows Azure	–
3.	SaaS	It provides Lotus Live	–	It provides Gmail and Documents.	It provides .NET Services, Dynamic Consumer Relationship Management.	It provides services such as online consumer relationship management, gift-tag.
4.	Virtualization	–	Operating system and Xen.	It has application container.	It has operating system level/ Hypel-v	–
5.	Service offerings	It offers services like service-oriented architecture, B2, Tivoli service automation manager, rational application developer, web 2.0	It offers services like elastic compute cloud, simple storage service, simple queue service, simple database.	It offers services like GFS, chubby, Bigtable, Map Reduce.	It offers services like live, SQL Hotmail.	It offers services like Apex, visual force, record security.
6.	Security Features	It has some features like web sphere2 and power virtual machine tuned for protection.	It has some features like PK1, VPN, Elastic Block store to recover from failure.	It has some features like chubby locks for security enforcement.	It has replicated data, rule-based access control.	It has some features like admin/ record security, users metadata API.

7.	User Interfaces	–	It has interface like elastic compute cloud, command-line tools.	It has web-based admin, console.	It has windows azure portal.	–
8.	Web API	Yes	Yes	Yes	Yes	Yes
9.	Programming support	It supports AMI programming language.	–	It supports python programming language.	It supports .NET framework language.	–

Q23. Explain about Google App Engine(GAE).

Ans:

Google App Engine(GAE): It is a cloud computing platform service and Platform-as-a-Service (PaaS). It is used for deploying web applications on Google Search Engine. It is a web application platform introduced by Google. This platform supports scalable web applications on huge data centers associated with Google search engine.

Google is one of the famous search engine introduces cloud development on huge data centers. These data centers enable a user to run various cloud applications. The google data center includes various cloud services in G-mail, Google Earth, Google Docs etc.

GAE Architecture: Figure below illustrates the Google cloud architecture platform,

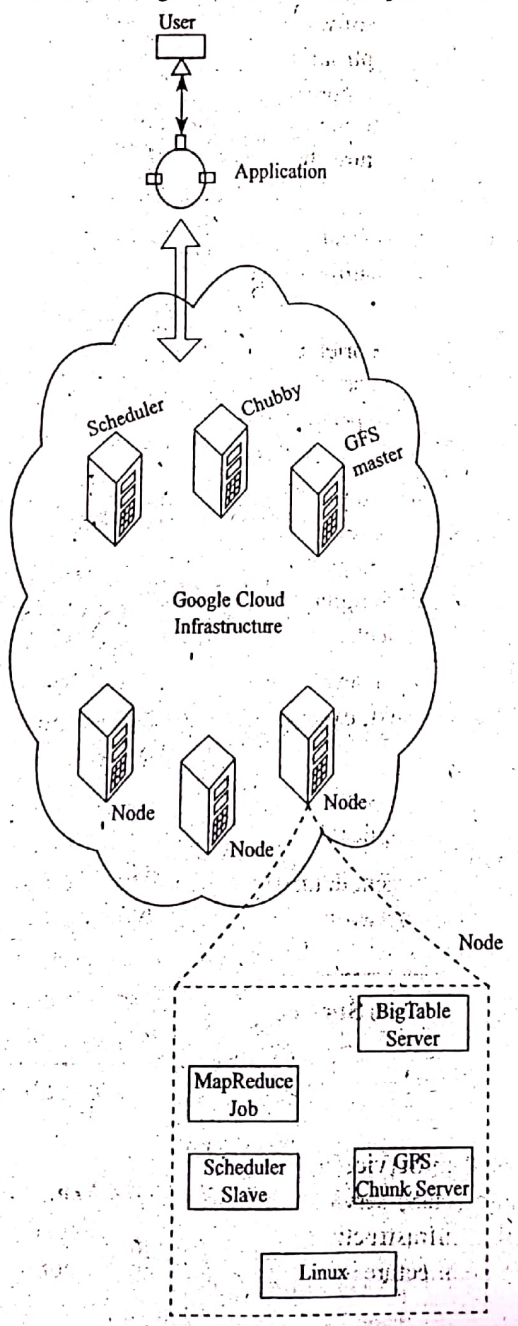


Figure: Google Could Platform

The Google cloud architecture defines basic blocks that are used for delivering cloud services to the cloud application providers. The basic blocks of Google cloud architecture that run on cluster configuration are as follows,

1. Google File System(GFS)
2. MapReduce jobs
3. Chubby
4. BigTable server.

1. **Google File System(GFS):** It allow users to store huge amount of data.
2. **MapReduce Jobs:** It is a famework that helps in developing application program.
3. **Chubby:** It enforces locking service on distributed applications.
4. **BigTable Server:** It provides storage service to access structural/unstructural data.

Google App Engine (GAE) uses Google infrastructure for running user program. It also make use of various software components. The front end of these components uses application framework like ASP, JSP and J2EE. GAE also supports development languages like Java and python. This front end is considered as a dynamic web serving infrastructure that supports common technologies.

GAE provides platform for developing user application. This platform includes five components. The functionalities of these components are discussed below,

(i) **Data Store:** This component provides object oriented services, distributed services and data storage services to the user depending on BigTable technique. It perform secure data management operations.

(ii) **Application Runtime Environment:** This component provides a scalable web programing and execution platform for running user application. Java and python are the two programming development languages supported by application run time environment.

(iii) **Software Development Kit:** This component develops local applications and also allow users to text, execute and runs the application code.

(iv) **Administration Console:** This component is used for managing the development cycle of user applications.

(v) **Web Service Infrastructure:** This component defines interfaces for flexibly using managing network and storage resources of GAE.

Q24. Give a brief description of Amazon Web Service (AWS).

Ans:

Amazon Web Service (AWS): Amazon Web Service(AWS) cloud offers wide range of infrastructure (IaaS) services. It provides high reliable and high scalable infrastructure for deploying web scale solutions. The AWS architecture is shown in the figure below,

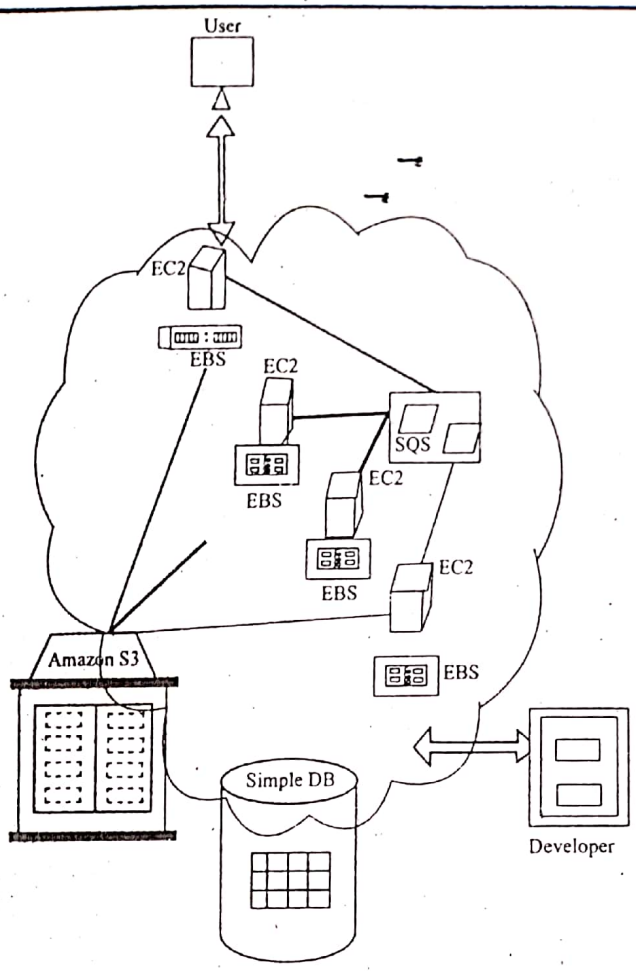


Figure: AWS (Amazon Web Service) Cloud Architecture

The AWS cloud architecture defines the following building blocks,

1. EC2
2. S3
3. EBS
4. SQS.

1. **EC2:** EC2 stands for Elastic Cloud Computing. It offers a virtualized platform for running cloud applications on virtual machine.
2. **S3:** S3 stands for Simple Storage Service. It facilitates user with object-oriented storage services.
3. **EBS:** EBS stands for Elastic Block Service. It makes use of block storage interface to substantiate traditional applications.
4. **SQS:** SQS(or) Simple Queuing Service ensure reliability while performing message exchange from one process (i.e., sender) to other process (i.e., receiver).

In AWS, data objects are accessed using SOAP standard.

Q25. Explain about Microsoft Azure.

Ans:

Microsoft Azure: Windows Azure is a service platform and cloud computing operating system hosted in data center of Microsoft corporation. The microsoft's cloud platform architecture is as follows,

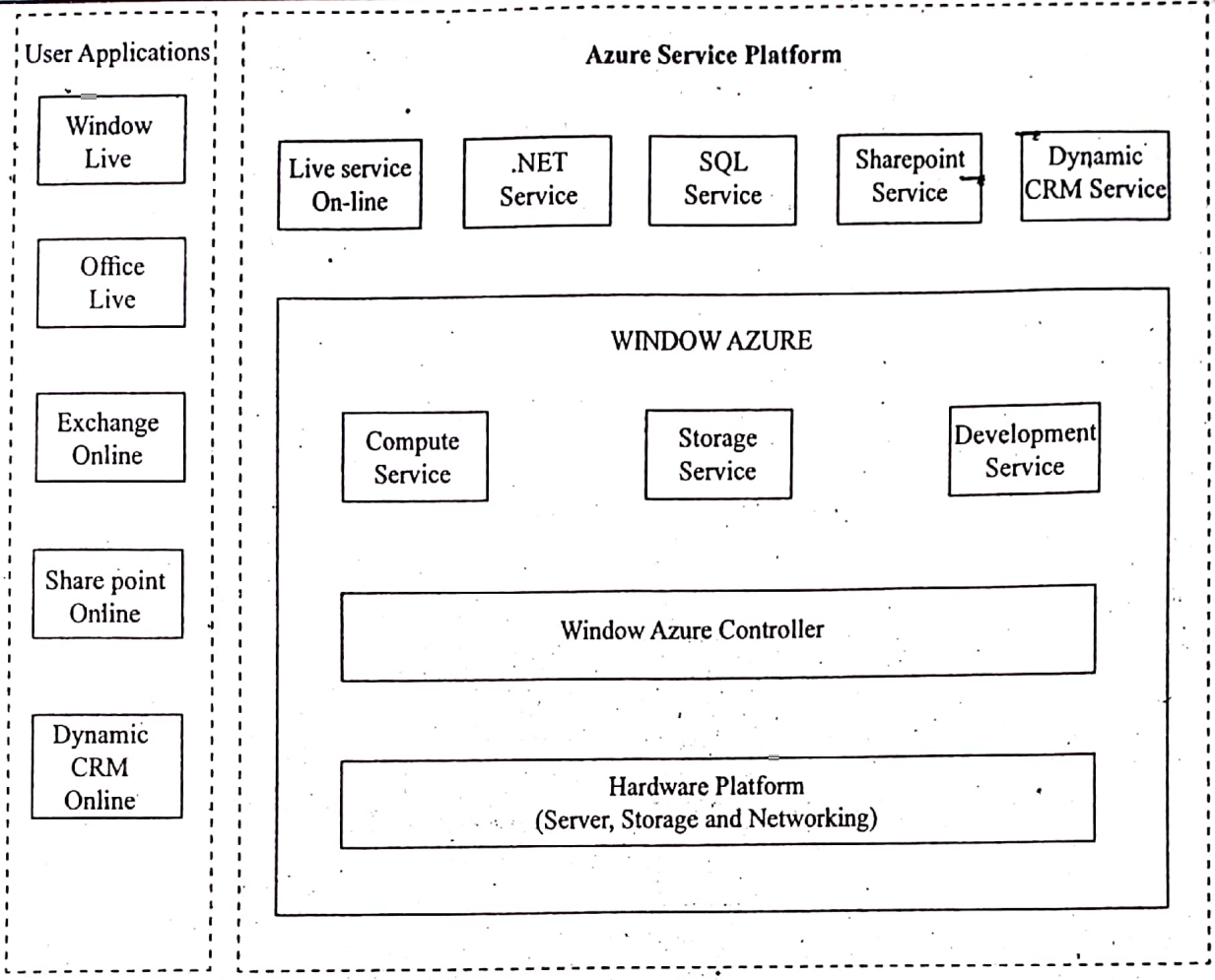


Figure: Microsoft's Cloud Platform

The above cloud platform includes three main components,

1. User applications
2. Window Azure
3. Azure Service platform.

This platform offers various functionalities to develop, host and provide services. It also offers developers on-need basics computing and storage facility to host, expand and manage web-based applications.

1. **User Applications:** Traditional software application like window live, office live, exchange online, sharepoint and dynamic CRM online interacts with cloud services of azure.
2. **Window Azure:** Window azure provides a cloud platform developed on window operating system using microsoft virtualization technology.
3. **Azure Service Platform:** It controls the servers, storage and network resources of data centers. The various cloud level services which are included at the top of infrastructure are as follows,
   - (i) **Live Service On-line:** It allow the users to traverse across the different microsoft live applications and use the data present on different machines simultaneously.
   - (ii) **.NET Service:** It is a package that allow users to develop application on local hosts and execute them on cloud machine.
   - (iii) **SQL Service:** It is a function that allow users to traverse relational database of SQL Server in the cloud.
   - (iv) **Sharepoint Service:** It creates a platform for developing scalable and manageable business application.
   - (v) **Dynamic CRM Service:** It offers a business platform that helps the software developers to control CRM applications in fields like financing, marketing etc.

3.4 INTER CLOUD RESOURCE MANAGEMENT

Q26. Explain about extended cloud computing services.

Ans: Model Paper-III, Q4(b)

Extended Cloud Computing Services: The following are the various cloud computing service models along with their extensions.

1. Cloud application services(SaaS)
2. Cloud software environment services(PaaS)
3. Cloud software infrastructure services(IaaS, DaaS, CaaS)
4. Collocation cloud services(LaaS)
5. Network cloud services(NaaS)
6. Hardware/virtualization cloud services(HaaS)

The six layers of cloud service model is shown in figure below.

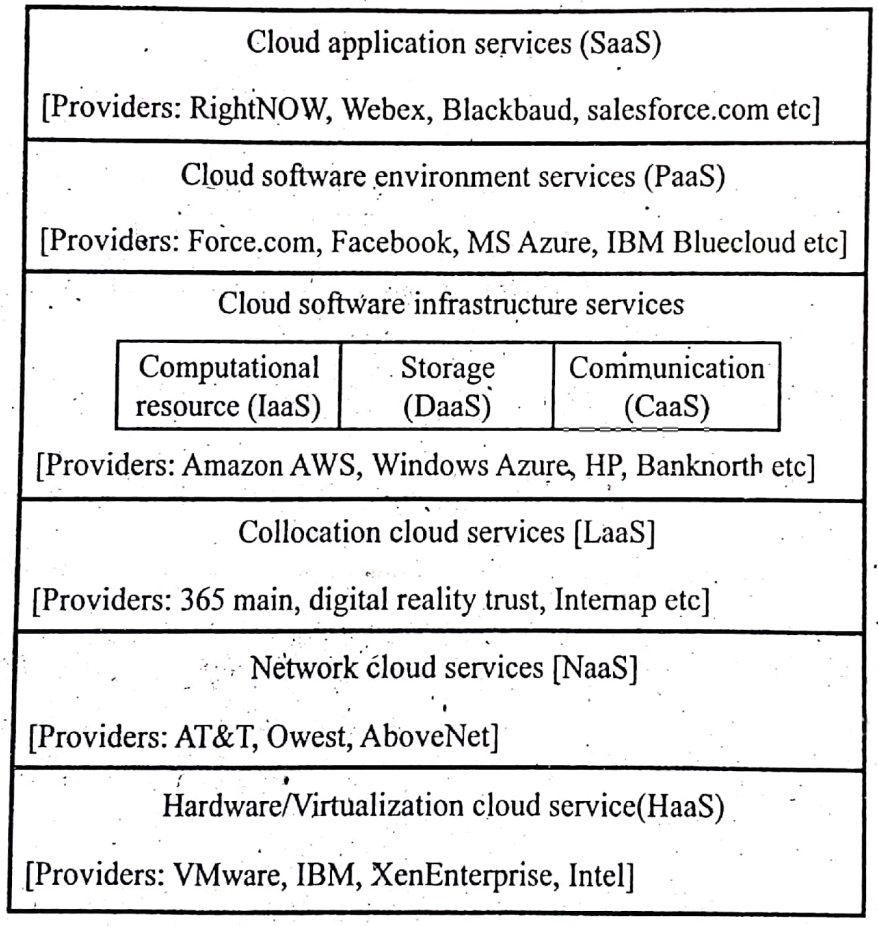


Figure: Six Layers of Cloud Services

The six layers of cloud service's defines applications based on,

- Hardware
- Network
- Collocation
- Infrastructure
- Platform
- Software.

1. **Cloud Application Services(SaaS):** This layer offers Software-as-a-Service(SaaS) services. It is top-most layer of cloud service. This service enables the delivery of built in applications to the end users. These applications are accessed by the end user through a web browser.
2. **Cloud Software Environment Services(PaaS):** This layer offers Platform-as-as-Service(PasS) services. It is present prior to infrastructure layer. This layer allow the users to develop and deploy an application without having any knowledge about the underlying details of the platform they are working on.
3. **Cloud Software Infrastructure Services(IaaS, DaaS, CaaS):** This layer provides Infrastructure-as-a-Service(IaaS) service. It is present below PaaS service layer.

   This service provides the user with all the infrastructure for developing and deploying the application. This layer provides two extended services like,

   (i) Data-as-a-Service(DaaS)

   (ii) Communication-as-a-Service(CaaS).

   (i) Data-as-a-Service(DaaS): DaaS services provides computation in IaaS.

   (ii) Communication-as-a-Service(CaaS): CaaS services allow to deployment of communication devices on pay-as-you-go basis.
4. **Collocation Cloud Services(LaaS):** This layer offers Location-as-a-Service(LaaS) services. This layer provides security to network and hardware resources along with housing and power.
5. **Network Cloud Services(NaaS):** This layer offers Network-as-a-Service(NaaS) services. This layer helps in interconnecting the hardware components using virtual LANs.
6. **Hardware/Virtualization Cloud Service(Haas):** This layer is the bottom most layer of cloud services. It offers Hardware-as-a-Service(HaaS) services.

However, among these six services, the top three services i.e., SaaS, PasS and IaaS are mostly preferred. The table below distinguishes, the three cloud models based on different cloud players.

Cloud Models	Cloud Players		
	IT Administrator/Cloud Providers	Software Developers	End Users/Business Users
IaaS	SLAs are monitored	Deployment and data storage	Deployment and data storage
PaaS	(i) SLAs are monitored (ii) Service platform is enabled.	Allow users to work on different platforms with the help of configurators and APIs.	Development of web software along with testing.
SaaS	(i) SLAs are monitored (ii) Software is deployed.	Development and deployment of software.	Business software is used.

Q27. Explain about resource provisioning and platform deployment.

Ans:

Provisioning: The process of selecting, deploying and managing software resources (like database system, load balance etc.) and hardware resource (like CPU, storage and network) of an application in order to achieve high performance referred to as "Resource Provisioning". It is a technique that is applied on large scale distributed system. In cloud computing environment, the cloud providers assign Service Level Agreements(SLAs) to end users so as to offer cloud service to them, depending on the SLAs resources like CPU, bandwidth and memory to the users based on their requirement.

Provisioning of resources must be done efficiently inorder to eliminate the under provisioning and over provisioning users.

Under Provisioning of Resources: If the resources are provisioned less then that of the user requirement then this may result in penalties.

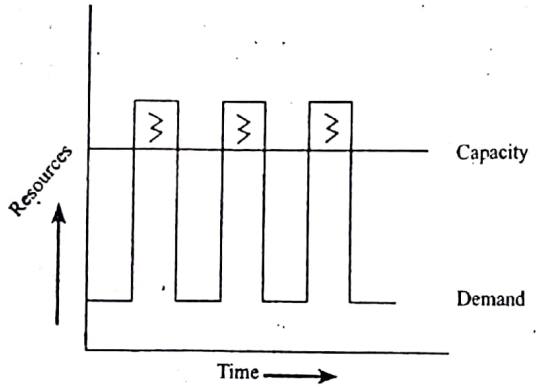


Figure (a): Under Provisioning

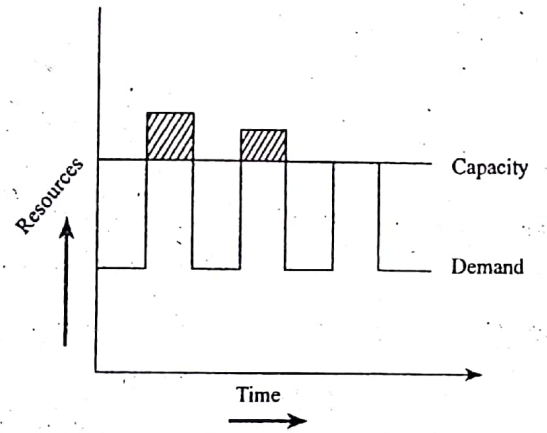


Figure (b): Under Provisioning and then Over Provisioning

Over Provisioning of Resources: If the resources are provisioned more than that of the user requirement then this may give rise to under utilization i.e., heavy wastage of resources which inturn leads to decrease in revenue rate.

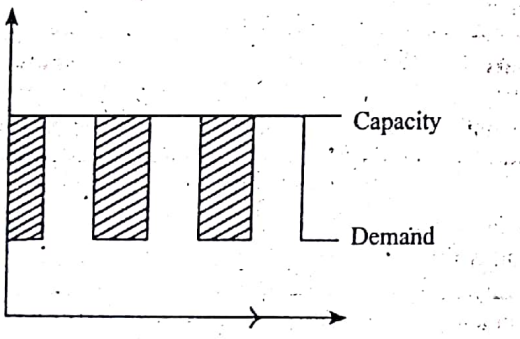


Figure (c): Over Provisioning of Resources

Provisioning of resources cannot be done efficiently to following reasons,

- Unpredictable consumer demands
- Failure in hardware and software resources
- Heteregeneous services
- Power management
- Conflicts in SLAs assigned between consumer and service providers.

Provisioning of resources on virtual machines is done depending on the cloud architecture and also on management of cloud infrastructure. Resource provisioning technique provides quick data and service in cloud infrastructure. Even though resource provisioning is a tedious task, various resource provisioning methods are employed so as to provision resources depending on users requirement.

Resource Provisioning Techniques: Resource provisioning techniques helps in provisioning resources on large scale distributed system like cloud computing environment. These techniques helps in meeting various Quality of Service (QoS) parameters such as availability, reliability, response time, security, throughput etc., by avoiding Service Level Agreement (SLA) violations.

The following are the three resource provisioning techniques.

(a) Demand-driven resource provisioning technique

(b) Event-driven resource provisioning technique

(c) Popularity-driven resource provisioning technique.

(a) **Demand-driven Resource Provisioning Technique:** This technique helps in adding/removing computing resources depending on the utilization level of those that are allocated to them. That is if one processor is used for more than the threshold time the demand driven method automatically allocates the resources based on the demand.

(b) **Event-driven Resource Provisioning Technique:** This technique helps in adding/removing computing resources depending on the time event. This type of provisioning may result in minimum loss of QoS requirements, resource wastage etc.

(c) **Popularity-driven Resource Provisioning Technique:** This technique provides computing resources depending on popularity on Internet. This type of provisioning may result in resource wastage etc.

Dynamic Resource Deployment: Dynamic resource deployment is done to achieve performance scalability.

In cloud computing, virtual machines are considered as a basic block that helps in creating execution environment over sevetal resource sites. However, to achieve performance scalability a java-implemented software system called Inter-grid managed infrastructures was developed. This system allow users to create cloud execution environment prior to participating grid resources.

The inter-grid infrastructure use two Inter-Grid Gateways(IGG) so as to allocate resource between local cluster and deploy application. A predefined peering arrangement is established between the gateways that creates an e.e by enabling resource allocation from multiple grids.

Figure below illustrates cloud resource deployment,

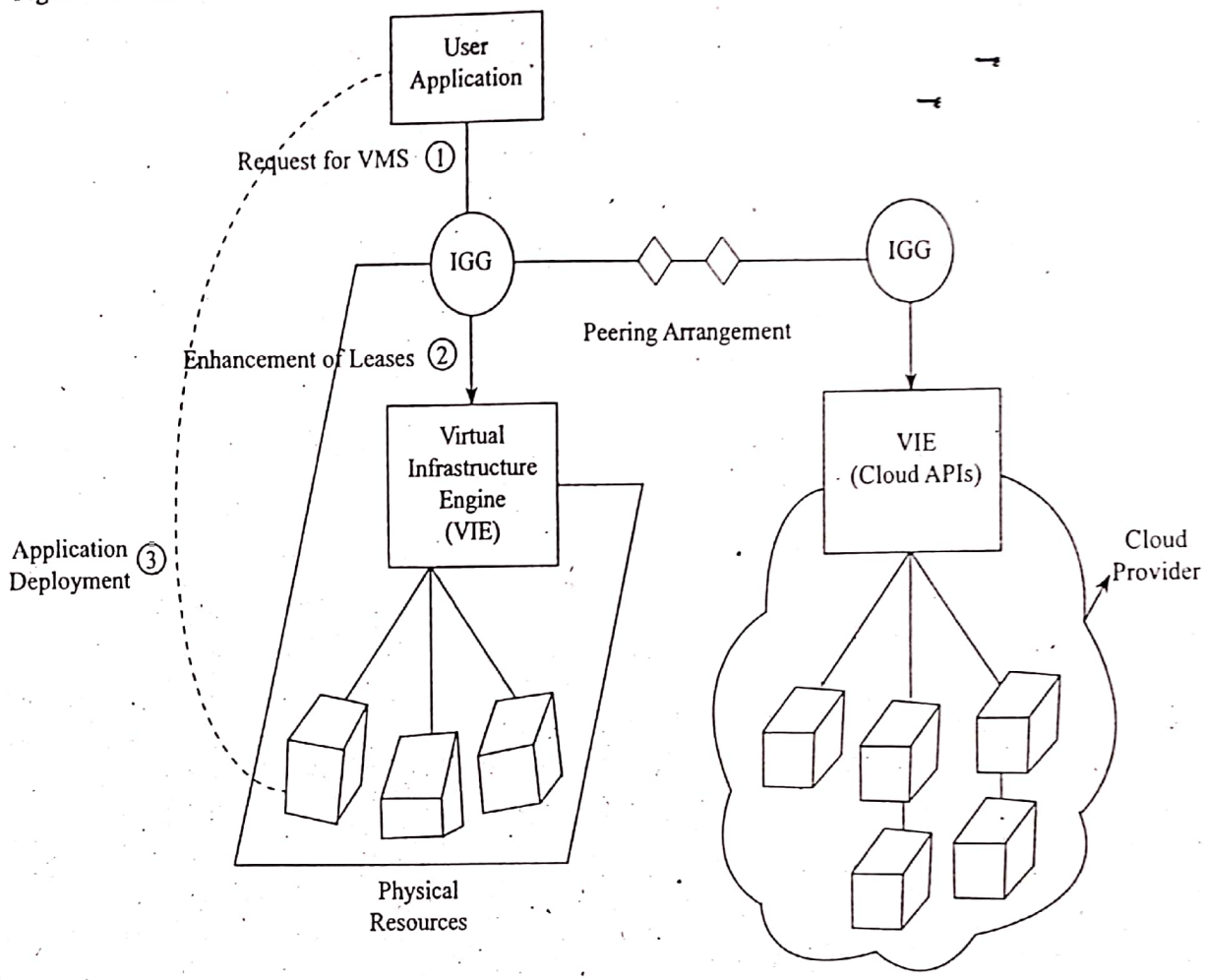


Figure: Inter-grid Gateway that allow Resource Deployment

In the above figure, IGG forms application deployment in three steps. Those are,

(a) Request for virtual machine is made

(b) Enhancement for leases

(c) Deploying virtual machines as per the request.

The peering arrangement of the grid is managed by Inter grid gateway. Multiple inter grid gateways allow coordination between inter-grid resources.

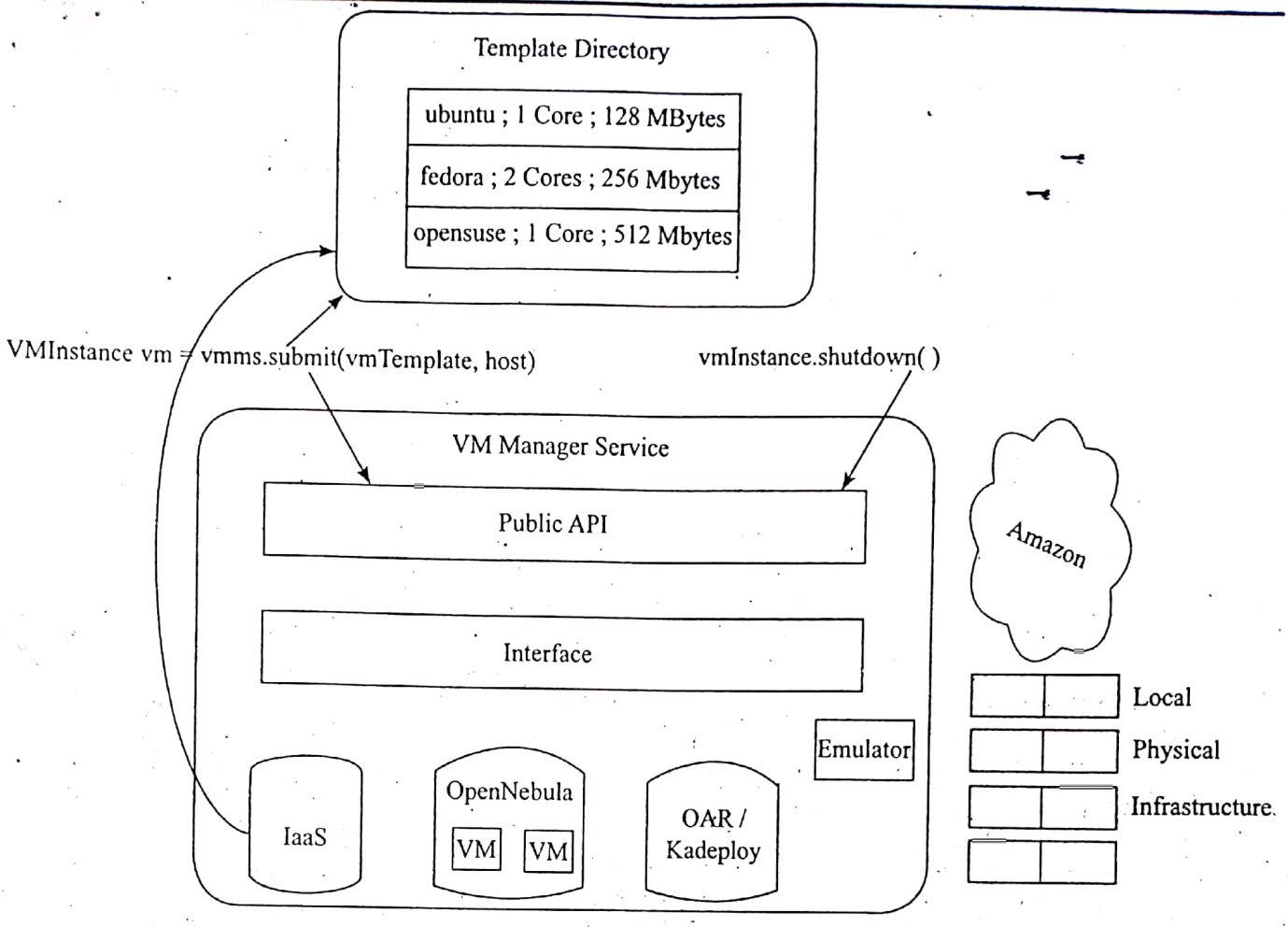
It is also responsible for allocating resources to various cloud provider. The request redirection policies helps in determining which peering grid must be selected for processing the service request.

Inter grid gateway creates a Distributed Virtual Environment(DVE) for executing applications on virtual cluster. Moreover, the DVE manages the components of IGG is responsible for managing, allocating resources to users. Beside this, they are two other components, that is scheduler component and communication component. A scheduler component is used for implementing the provisioning policies on the gateway. Whereas the communication component allow asynchronous message passing mechanisms for sending and receiving messages.

Q28. Explain about virtual machine creation and management.

Ans:

Virtual Machine Creation and Management: The figure below illustrates how virtual machine manager creates and manages the cloud applications. Cloud applications can be created on multiple virtual machines. To do this, virtual manager interacts with each other to facilitate cloud creation and management on multiple virtual machines.



Virtual Machine Manager: The virtual machine manager provides interaction between gateway and resources. It is responsible for managing the virtual machines which are deployed on group of physical resources.

Virtual Machine Templates: Virtual machine templates provides description about virtual machines. It includes information like,

(i) The amount of memory required by virtual machines.

(ii) The total number of cores/processors that are assigns virtual machine.

(iii) The operating system installed on virtual machine requires booting by kernal.

(iv) The disk image which defines file system of virtual machine.

(v) The pricing mechanism of virtual machine.

Distributed VM Management: A distributed virtual machine manager is responsible for making virtual machine request from gateway and application also for quering their states information. After the request is made, the virtual manager obtains the list of virtual machine request made from the gateway. This list contain information about the public IP addresses(or) private IP address of requested machines along with Secure Shell Tunnels (SSH). Here, the user must provide information regarding the VM templates they require and also the instances they, need, deadline, wall time and also the address of another gateway.

If the local gateway is unable to process the requested service then this request is sent to the virtual machine so as to process the request. The virtual machine manager is responsible for managing the virtual machine configuration, setting the SSH tunnels, executing the VM tasks etc.

3.5 CLOUD SECURITY AND TRUST MANAGEMENT

Q29. Discuss in detail about cloud security in defense strategies.

Ans:

Model Paper-IV, Q4(a)

Cloud Security in Defense Strategies: A secure cloud ecosystem eliminates the problems like hacking, viruses, spam, privacy violations, copyright violations, rumors, cheating, pornography etc. Cloud security can be provided to cloud service models (i.e. IaaS, PaaS and SaaS) by enforcing the following,

To securing the data centers biometric readers, CCTV, motion detection and man traps must be deployed.

2. To secure the network Fault-tolerant connected firewalls externally, third party vulnerability assessments and Intrusion Detection Systems (IDS) must be used.

3. To ensure platform security secure socket layer, data decryption techniques, password policies and system trust certification must be deployed.

Figure below illustrates the mapping between the various cloud models and deployed security measures.

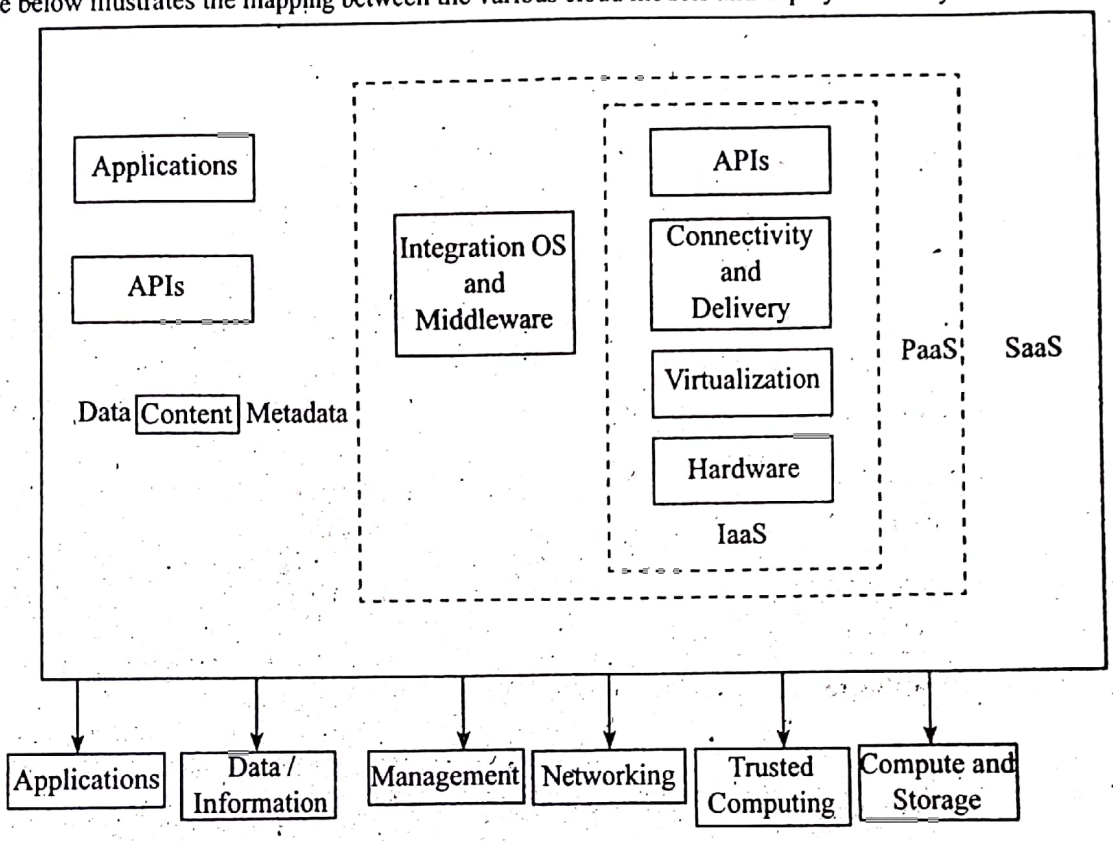


Figure: Mapping between Various Cloud Service Models

A secure cloud architecture consist of,

(a) Servers which are physical machines / virtual machines.

(b) User interface for processing the request service.

(c) Provisioning tools for delivering the requested service.

The security-aware cloud architecture avoids various malware-based attacks like virus, network worms and Distributed Denial of Service (DDOS) service attack. Such types of attacks can exploit the vulnerability of the system by compromising the functionality of systems (or) by allowing unauthorize users such as intruders to access the critical information of system. Thus, to protect cluster server and data centers, security defenses(or) security measures are need. So as to protect,

- Server from malicious software attacks like malware, worms and viruses.
- Hypervisors (or) Virutual machines from software based attacks, server disruptions, vulnerability and denial of service attacks.
- Data and information from natural disasters, loss and corruption.

Cloud Defense Methods: Cloud computing platform includes various types of attacks like hypervisor malware, guest hopping, hijacking, man-in-the-middle attack, active attacks which manipulate kernel data structure to damage cloud data, passive attacks.

The concept of virtualization in cloud computing provides enhance cloud security. This is because, virtual machines additional software layer that protects the data from failure. A virtualize cloud service partitions the single physical machine to several virtual machines. This partitioning is done so as to protect data from Denial Of Service (DOS) attack by providing better security isolation.

The various cyber security protection schemes which are employed to protect public cloud and data centers from various types of attacks are as follows,

(i) **Choosing Secure Data Centers and Computer Buildings:** This mechanism enhances the cloud security by choosing security aware data centers and safer computer building at hazard free location. These data center are deployed with buffer zone, bomb detection, earthquake proof, camera surveillance etc.

(ii) **Making Use of Redundant Utilities at Various Sites:** This mechanism allow to use of multiple power supply, additional network connections multiple databases at several sites. There by ensuring data consistency, data water making and user authentication at multiple sites.

(iii) **Trust Delegation and Negotiation:** This mechanism offers cross certificates so as to delegate trust at various data centers domain. Trust negotiation resolves the conflicts arising among the Certificate Authorities(CAs).

(iv) **Internet Worm Containment and Distributed Denial of Service Defense:** This mechanism ensure enhance security of data centers and cloud platform by making internet worm containment and distributed defense against Distributed Denial Of Service(DDOS) attack.

(v) **Using Reputation System for Data Centers:** This mechanism make use of reputation system that uses peer to peer technology. A user can build hierarchy of reputation system between data centers and distributed file systems.

(vi) **Fine Grained File Access Control Mechanism:** This mechanism allow additional security beyond firewalls and IDSes.

(vii) **Copyright Protection and Privacy Protection:** This mechanism ensures privacy by making use of methods like peer collusion prevention method filtering of poisoned content, alteration detection etc.

(viii) **Privacy Protection:** This mechanism employs various privacy protection techniques like double authentication, biometric identification, disaster recovery, privacy enforcement using data watermarking etc.

Q30. Explain the data and software protection techniques.

Ans:

Data and Software Protection Techniques: The various data and software protection techniques are as follows,

(i) **Data Integrity and Privacy Protection:** Cloud application for large data sets are basically build on software environment using various software tools. This application software are also used in MapReduce, EC2, Hadoop, BigTable, WebSphere2, GAE etc. In cloud, a software environment is needed to provide data integrity and privacy protection. This software environment posses the following features,

1. It provides a special Application Programming Interface (API) for performing user authentication and also to send emails using commercial accounts.
2. It provides fine grained access control to protect data from intrudes/hackers and to ensure data integrity.
3. It allow shared data sets to protect the data from deletion, copy right violations and malicious alterations.
4. It uses firewalls on end users site so as to share data sets from Java, JavaScript and applets.
5. It secures the cloud service providers/Internet service providers from security attacks.
6. It establishes VPN channels across resource sites so as to perform secure data transmission of critical data objects.

(ii) **Data Coloring and Cloud Watermarking:** In cloud computing environment, data sets and file sharing may effect the privacy, security and copyright information. Hence, to avoid such situation, trusted software that offers rich set of tools needed to create cloud application over protected data sets. In cloud, the two software schemes that are used to protect the software files from getting distributed in cloud environment are as follows,

(a) **Cloud Water Marking:** It manages digital copyright.

(b) **Data Coloring Scheme:** It assigns unique colors to each data object.

However, to provide enhance security, data coloring and cloud water marking mechanisms are applied together at various security levels on the data centers. The figure below explains the concept of data coloring with cloud water marking.

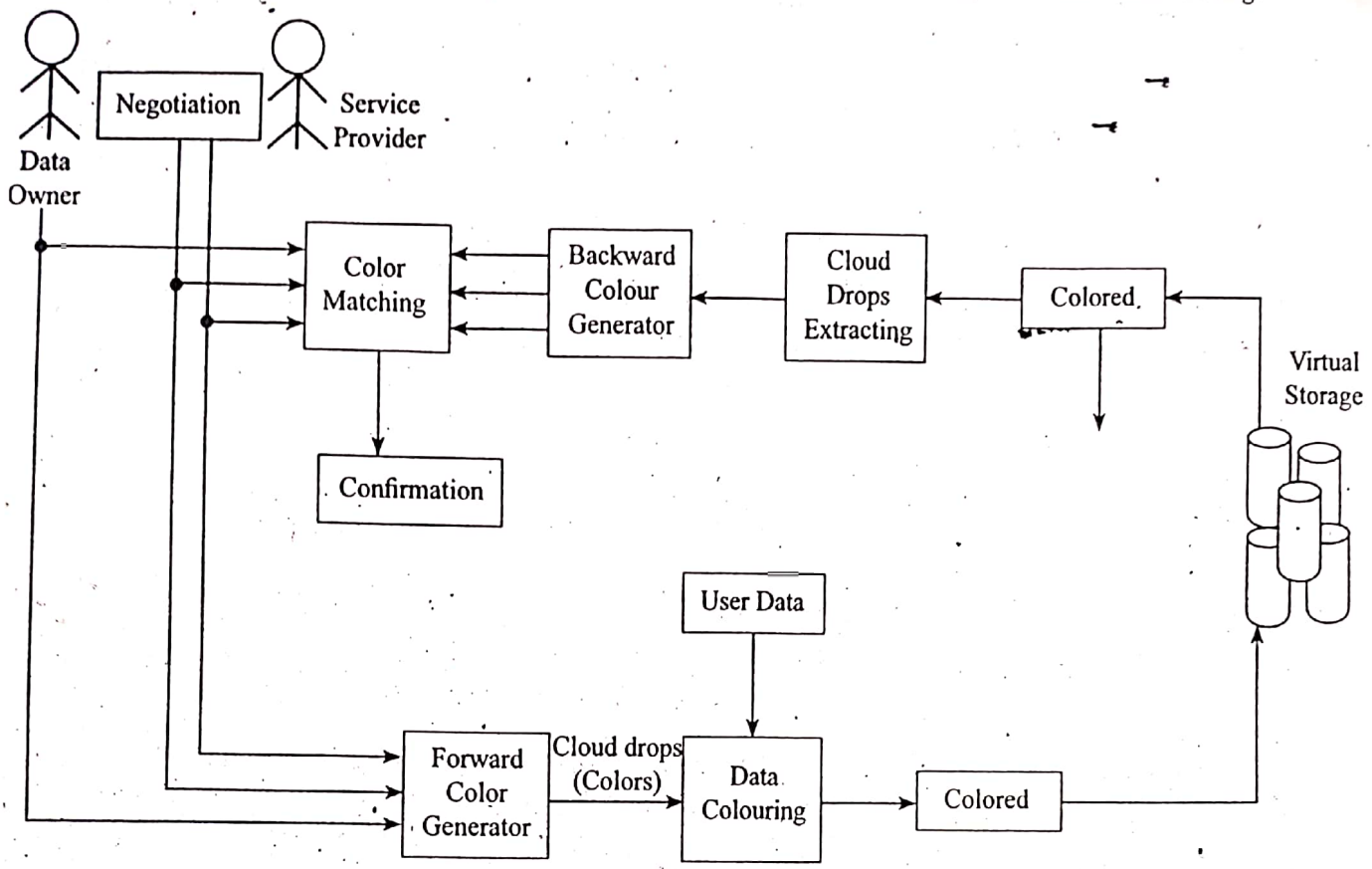


Figure: Data Coloring with Cloud Water Marking

In the above mechanism, the user identifications are colored using various colors. These colored objects are matched ·ith the associated data colors. This matching is done in order to implement the trust management events. Later, the process for enerating, embedding and extracting of cloud watermarks are applied to colored object by the cloud storage providers. Besides ıis, data protection techniques are also applied to these objects.

:) **Data Lock-in Problem and Proactive Solutions:** In cloud computing, data and computation programs are moved to :rver clusters which are managed by cloud service providers. The retrieval and execution of such data and program from server uster on other platform cannot be done easily hence this result is data lock-in problem. This problem restrict the use of cloud ɔmputing. Data lock-in give rise to two problems.

(i) Lack-of-interoperability

(ii) Lack-of-compatability.

Data lock-in problem can be avoided by using standardized Application Programming Interfaces (APIs). This can be done · developing standardize virtual platforms on OVF. An OVF creates an efficient, extensible, secure and open format for virtual achine. This allow secure software distribution and also to facililate mobility or data from one application to another on virtual achine.

---

31. Discuss about reputation-guided protection of data centers.

ns:

:putation-guided Protection of Data Centers: Reputation-guided protection system protects the data centers/cloud user mmunities. An overview of reputation system design for social networks or cloud platform is as follows,

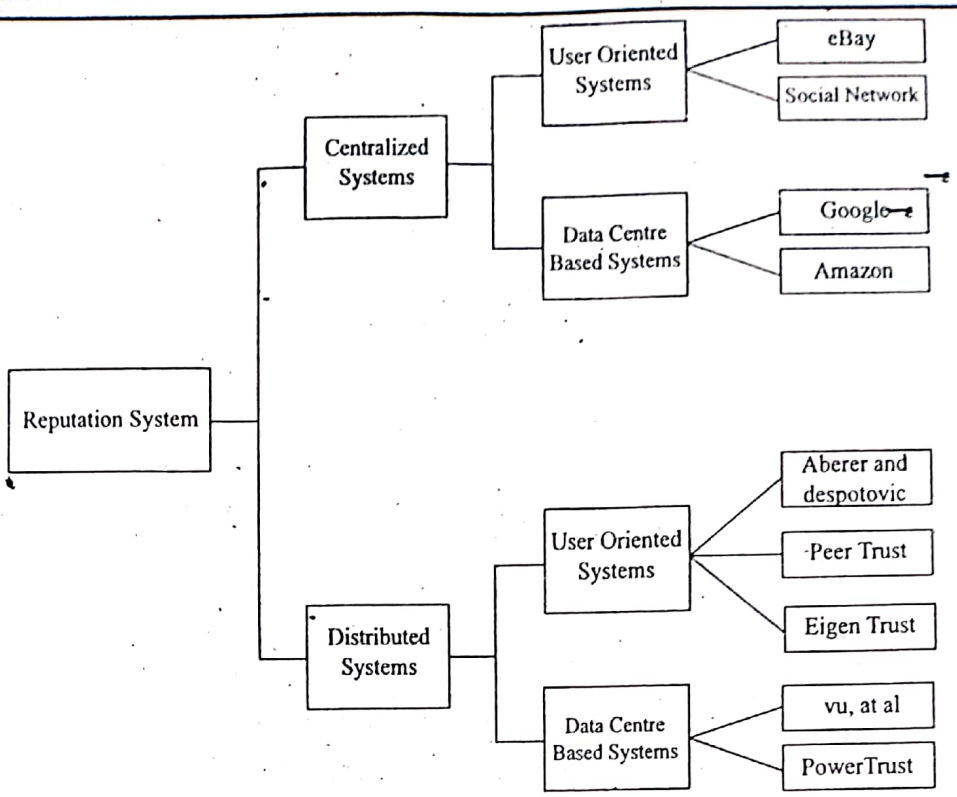


Figure: Reputation Systems

Reputation is nothing but a public opinion evaluated from a group of people, person, product, service an agent, a resource owner etc. Traditional reputation system was mainly designed to support P2P systems, e-commerce systems or multi agent systems etc.

The above figure illustrates the two types of reputation systems designed for P2P systems or social networks.

These systems are divided into two basic categories depending upon their implementation. These categories are as follows,

1. Centralized system
2. Decentralized system.

1. **Centralized System:** In this system, reputation systems are managed by single central authorized. A centralized reputation system can be implemented easily but require powerful and reliable server resources.

2. **Decentralized System:** In this system, reputation systems are managed by multiple central authorities who works together. Distributed reputation systems are capable of handle failure states with more scalability and reliability.

These reputation systems are further subdivided as,

(a) User-oriented reputation systems

(b) Data-center based reputation systems.

a) **User Oriented Reputation System:** In this system, reputations are modelled for individual users/agent.

Example: eBay, social network for centralized reputation system and Aberer, PeerTrust and EigenTrust for distributed reputation system.

b) **Data-center Based Reputation System:** In this system, reputations are modelled for resources based on the services/ product offered by cloud.

Example: Google, Amazon for centralized system and vu, et al, PowerTrust for distributed system.

The redesigned reputation system for cloud offers the following benefits,

i) It provides data consistency on multiple databases.

ii) It makes use of copy right protection mechanisms to secure the data present in the cloud.

iii) It maintains data integrity and data consistency by separating user data from SaaS programs.

iv) It allow users to access the requested data.

v) It ensures data consistency by assigning unique names to data objects.

Q32. Discuss in detail about trust overlay network.

Ans:

Trust: Trust is important factor of cloud computing. It is typically build between user and cloud service provider. A user can trust a service provider if it ensures information security and privacy. Any violation in this regard makes it difficult for users to trust the service provider.

Trust Overlay Network: Trust refers to personal opinion. Trust overlay network has been designed to support trust cloud services. It models trust relationship across the data center modules. This network uses Distributed Hash Tables(DHT) inorder to achieve fast global reputation aggregation. The development of trust overlay network must be done using two layers. These layers helps in achieving fast reputation aggregation, dissemination, fast updations etc. The construction of overlay networks is shown in figure below,

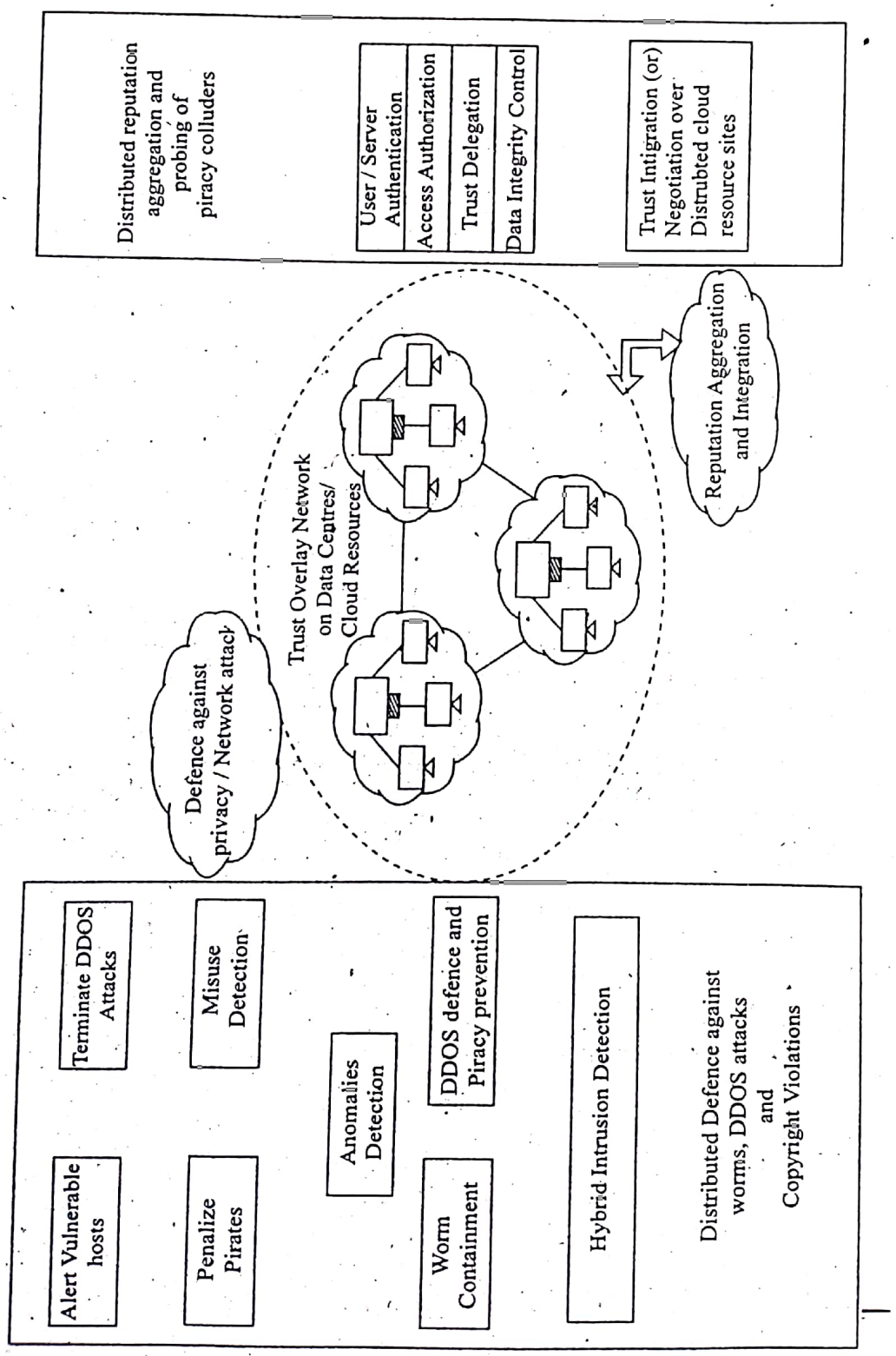


Figure: Trust Overlay Network

The two special layers of trust overlay network are as follows,

1. Distributed defense against worms, DDOS attack and copyright violations
2. Trust integration/negotiation over distributed cloud resource site.

1. **Distributed Defense Against Worms, DDOS Attack and Copyright Violations:** This overlay provides support to worm containment, intrusion detection system against virus, DDOS attacks and worms. It also facilitate content poisoning technique as well as protection scheme to avoid copyright violations on multiple data centers.

2. **Trust Integration/Negotiation Over Distributed Cloud Resource Site:** This overlay manages the user or server authentications, access authorization, data integrity, trust delegation across multiple resource sites. It facilitate trust negotiation and reputation aggregation on multiple resource sites.

Beside this, the trust overlay network also allow trust interactions among cloud users and data-center providers. To enforce privacy, user identifications are colored using data object colors. Moreover, content provisioning technique is used to protect the copyright of digital content.

In addition to this, a security-aware cloud architecture is preferred inorder to protect the infrastructure of virtualized cloud. Trust is basically provided to cloud platform by assigning Service Level Agreements (SLAs), enforcing security policies or by deploying counter measures to defend from network attacks.

3.6 SERVICE ORIENTED ARCHITECTURE, MESSAGE ORIENTED MIDDLEWARE

Q33. Discuss in brief about service oriented architecture.

Ans:

Service Oriented Architecture (SOA): SOA is defined as the process of exchanging data through different applications. It is a method that helps in integrating business processes by dividing large applications into smaller modules (services).

An SOA uses new distributed application as an interface to design a software system. It provides an architectural method to develop sophisticated systems through set of loosely coupled interconnected blocks as a service. The World Wide Web Consortium (W3C) defines SOA as a distributed system architecture. This architecture posses the following characteristics,

1. **Logical View:** An SOA defines abstract, logical view of a program, business processes, database etc., as to perform business level operations. It also specify how message exchange takes place between provider agents and requester agents.
2. **Message Orientation:** Internal structure of provider agent and requester agents comprises of features like process structure, database structure and implementation language. Such features are extracted away from SOA in simple term while using SOA discipline the user should not consider about the way the agent implementing service is built. One of the advantage of this is legacy system. Thus, by avoiding the knowledge of internal structure of agent, a user can include any software component/application in accordance with the formal service definition.
3. **Description Orientation:** Machine-executable metadata gives description of a service supporting public nature of the SOA. This description includes only those details that are known to the public and one essential for using a service. The semantics of a service must be either documented directly or indirectly by its description.
   (a) **Granularity:** Service makes use of less number operations along with large and complex messages.
   (b) **Network Orientation:** Services are adjusted across the network.
   (c) **Platform-Neutral:** The requested messages are transmitted on a platform neutral environment using standardized format and are received by the receiver through an interface. Here XML format helps the meeting in desired constraint.

Q34. Explain about REST System.

Ans: Model Paper-IV, Q4(b)

REST System: REST stands for Representational State Transfer(REST). It is a software architecture used by various distributed hypermedia systems that is on world wide web. This software architecture is used by popular enterprises and software networks like Google, Yahoo, Amazon, Face book, Twitter etc.

The REST architecture is shown in figure below,

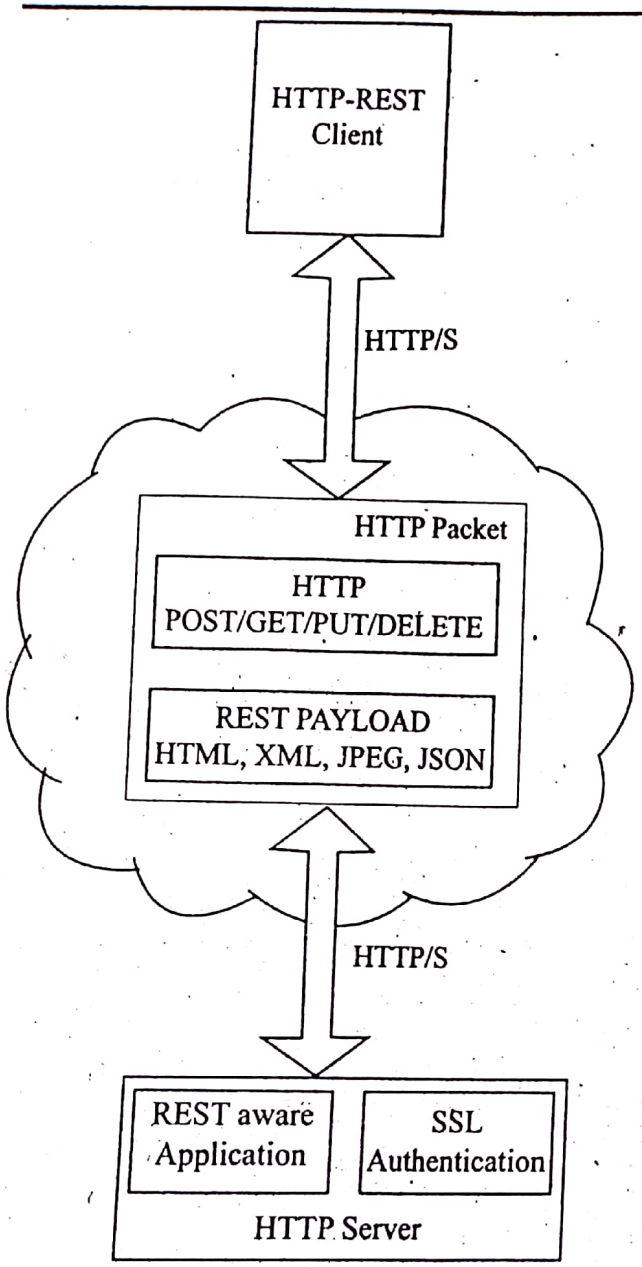


Figure: REST Architecture

This architecture is designed based on the following four principles,

1. **Resource Identification Via URIs:** The REST web service define set of resources for identifying targets which want to interact with their client. 'Resources' are the key abstractions of REST Web service. A resource is nothing but a unique name or named information. Example document and images are termed as resources. Each resource is associated with a Uniform Resource Identifier(URI). A URI provides global addressing space for resources which interacts with components and facilitating service discovery.

2. **Uniform Constrained Interface:** HTTP standards as well as client/server cacheable protocols provides interaction with REST ful web services. Moreover to manipulate resources, four operations are used. These are,

(a) **PUT:** It allows creation of new resource.

(b) **GET:** It is used for retrieving the current state of resources.

(c) **POST:** It allows transfer of resources to new state.

(d) **DELETE:** It destroys the created resources.

3. **Self-Descriptive Message:** REST message provides information regarding message processing. Hence, by using these messages, the intermediaries can directly deal with message content without passing it.

Beside this, REST also decouple resources from their representation. Due to this reason, the message content can be accessed using various formats like plain text format HTML, MIME, JSON, PDF, JPEG and so on. Moreover the resource metadata is used for various purposes like cache control, detecting transmission errors, message authentication etc.

4. **Stateless Interaction:** REST provides stateless interactions. This helps in,

- ❖ Improving visibility
- ❖ Ensure reliability by recovering from failure rate
- ❖ Increasing scalability.

However such interactions decreases the network performance of the system by including repetative data.

Q35. Explain in detail about webservice.

Ans:

Web Service: Service is outcome of an applications. Webservice is a self-contained, self-describing modular application. It is designed for accessing software application on web. According to W3C working group, web service is considered as a software system developed to facilitates interoperable interactions between two machines. It defines a interface which is in machine executable formats. This interface allow systems to interact with web service in a manner similar to SOAP messages.

The various web-services are as follows,

(i) **SOAP(Simple Object Access Protocol):** SOAP is defined as a simple XML-based protocol which permits applications to exchange XML-based messages over computer networks using HTTP(Hyper Text Transfer Protocol).

(or)

SOAP is a mechanism in which object accessing is carried out in a simple way thereby allowing applications to call remote methods.

Merits of SOAP

- Servers of SOAP presents simple functions.
- SOAP is not only platform independent but also language independent.
- SOAP supports different transport protocols like HTTP, SMTP etc.
- It provides easy communication through proxies and firewalls.
- SOAP is simple with its far-ranging nature.
- Consuming is easy with SOAP.
- SOAP is considered as a lightweight protocol.

Demerits of SOAP

- SOAP is slower than CORBA, since it uses XML format.
- The use of HTTP fixes the roles of the interacting parties. Only single party (client) is allowed to use the services of other party (client).
- Due to the use of HTTP as a transport protocol, another disadvantage is to identify the appropriate method for a particular operation.
- As HTTP is used by SOAP, a firewall only allows web browsing but not all HTTP-using packets.

(ii) Universal Description Discovery and Integration(UDDI): UDDI is an XML based registry that forms one of the important and basic building block for web services. It was initially started by Microsoft, IBM and Ariba that allowed businesses from world wide to register information on the internet, so that it can be accessed by customers and/or partners.

Advantages of UDDI

- It allows a business to expand its potential business partnership by finding other businesses.
- It streamlines online transactions by permitting companies to discover one another on the web and make their systems interoperable for e-commerce.
- It boosts every business irrespective of their size, to accelerate their business presence in the overall global market.

UDDI Registry: It is an implementation of UDDI specification that is accessed by a set of software services called UDDI registry services.

There are two types of UDDI registers, which are as follows,

(a) Public

(b) Private.

(a) Public: Public registry is an open source UDDI registry that can be utilized by everyone to register or access the business and service information on the web. It is a virtual system built on multiple nodes called "UDDI Business Registry" (UBR) where every node provides same information, quality of service through synchronized replication of data.

(b) Private: Private registry is an exclusive or reserved registry that can be accessed only by the organization or group who owns it or by people who has the permission from the owner. It also utilizes the same replicated nodes system as public registry. But, it requires additional resources to ensure security and integrity of data from unauthorized users.

(iii) WSDL: WSDL stands for "Web Services Description Languages". It is an XML-based language that defines the webservices. It is a specification defining how to describe and locate webservices in a common XML language. WSDL2.0 is recent version of specification. It specifies how the interaction takes place between client and a webservice, how to encode parameters and return values in a message and which protocol to be used for the data transmission. WSDL document contains the following details such as,

- Webservices which are invoked by website.
- Webservice methods.
- Parameters which are required to pass to webservice methods.
- Results that are returned on request.
- Data format which is used by user to access webservice.

In WSDL, services are defined as collection of network end points or ports. For the purpose of reuse of definitions, abstract definitions of messages and ports are separated from their concrete use. Messages are defined as abstract descriptions of data and port types are defined as abstract collection of operations. The specifications of protocol and data format for a specific port type creates a reusable binding in which protocol and message format are bounded by operations and messages.

To provide webservices over the internet, WSDL can be used along with SOAP and XML schema. A client program which is connected to the webservice can determine the functions available on the server by reading WSDL.

Thus, WSDL describes the entire mechanism involved in the transfer of data from client to the webservice.

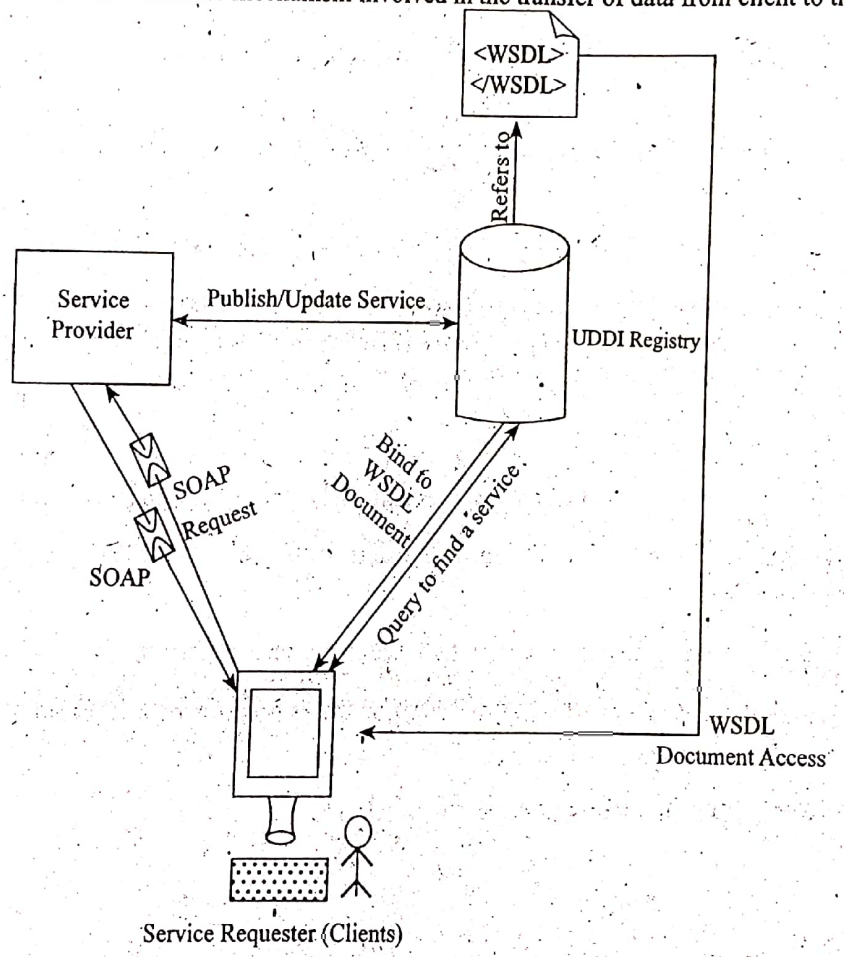


Figure: User, UDDI Registry, Provider Interaction in Web Service

Q36. Briefly explain the Enterprise Multitier Architecture.

Ans:

Enterprise Multitier Architecture: The traditional enterprise multitier architecture uses two-tier client/server model. This architecture has been designed inorder to encapsulate and integrate distinct functionatities of enterprise applications. This architecture uses presentation layer, application layer and data management layer to perform logical processing. However this model deals with the following drawbacks,

i) Deployment and enhancement of new applications was a tedious task.

ii) Change management was difficult.

To overcome the above issues, a three-tier system architecture has been designed. The three-tier architecture is an extension two-tier client/server architecture. The three-tier enterprise architecture is shown below,

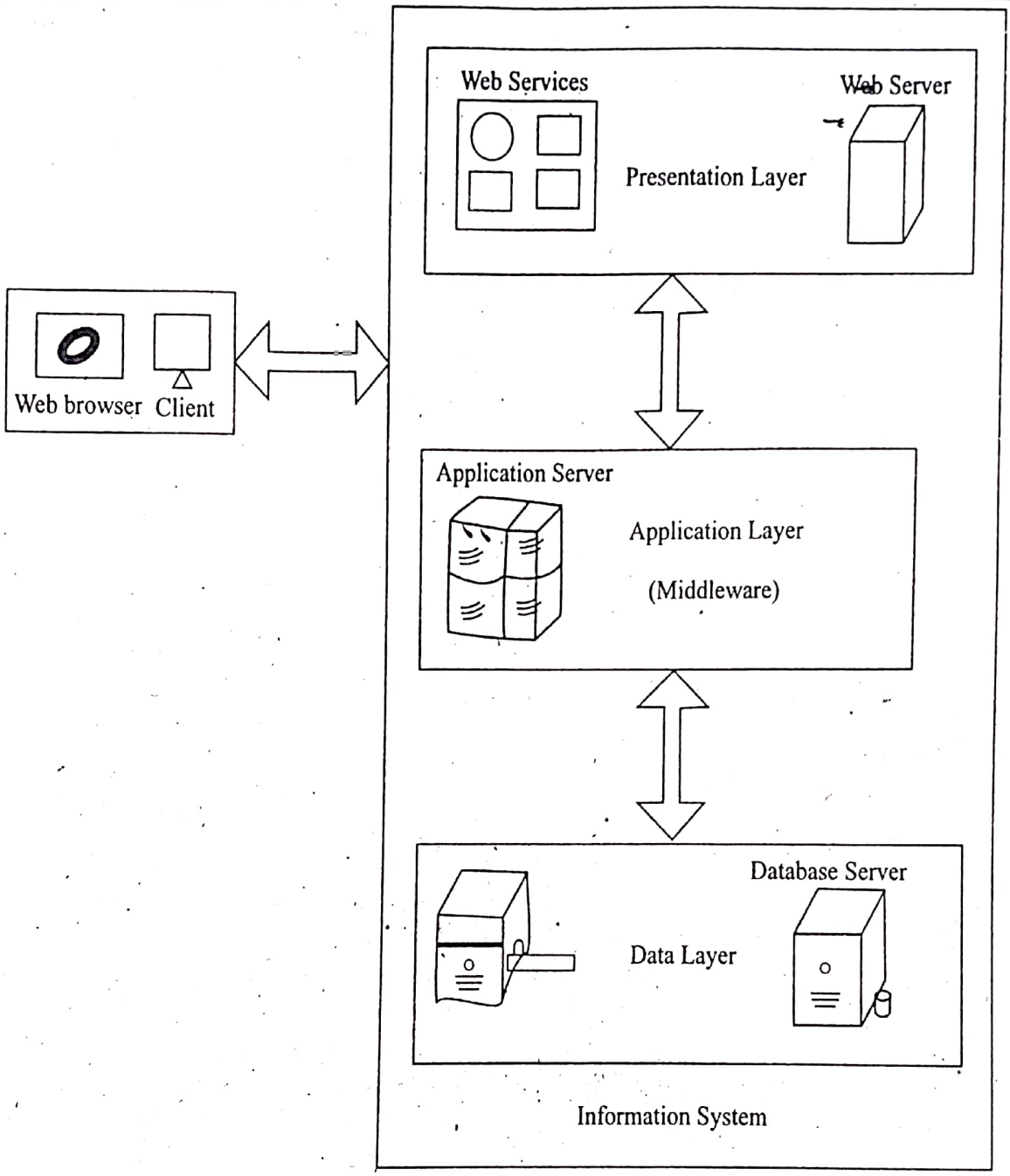


Figure: Three Tier Architecture

The above architecture separates the application logic from the resource management layer. The three tier architecture consists of the following three layers,

1. **Presentation Layer:** Presentation layer is the top most tier of the three tier enterprise architecture. This layer provides information to the external entities and also allow their interaction with the system. This interaction can be done by submitting the requested operation and by generating responses to and from the system and external entities.

2. **Business/Application Layer/Middleware Layer:** Business layer /application layer/middleware layer is the middle tier of the three tier enterprise architecture. This layer is responsible for implementing the requested client operations. This layer also manages the user authentications, resource access, query processing made by clients and database servers.

3. **Resource Management/Data Layer:** Resource management/data layer is the bottom most layer of three-tier enterprise architecture. This layer is responsible for implementing the various data sources present on information system.

Due to excessive use of internet, the three tier architecture is extended as N-tier architecture. This N-tier architecture provides the following enhancements,

(i) Integrates SOAP-based and REST web services into the application.

(ii) Subdivides the data to data storage tier and data access tier.

(iii) Includes an additional layer called wrapper tier to provide data access to both data bases and web services.

(iv) Includes an additional webservice layers at the top of the information system. This layer provides interaction with standard internet protocols.

Q37. Write short notes on WSI Protocol Stack.

Ans:

WSI Protocol Stack: WSI protocol stack supports various features like,

(i) Transport protocols

(ii) Message/extensions and invocations

(iii) Description

(iv) Quality of Service(QoS)

(v) Process and Composition.

(i) **Transport Protocols:** WSI protocol stack uses various transportation protocols like HTTP, SMTP, FTP, IIOP etc.

(ii) **Message/Extensions and Invocations:** The WSI protocol stack defines a Simple Object Access Protocol(SOAP). It is a web service that specifies the non-functional requirements and quality of service in the messages. It is a reliable protocol that defines transaction services like WS-Addressing, WS-Transaction and WS-Coordination while transmitting messages.

In SOAP data/messages can be encoded using a special mark-up language ie., XML. The messages are stored in between two tags i.e., start and end tags. Since XML is used for performing transmission, overhead can occur due to increase in transmission rate. Data processing in XML comprises of calculations, description of memory and complete size of data, number of data fields, limited-profile devices like PDAs and smart phones.

iii) **Description:** The WSI protocol defines various message description services like Web Service Description Language(WSDL), Universal Description Discovery Integration(UDDI), WS-policy and WS-Resource properties.

iv) **Quality of Service(QoS):** The SOAP based web service used on protocol stack which provides reliable communication using various policies like WS-security, WS-reliable messaging and WS-Resource lifetime inorder to fulfill required Quality of-Service requirement.

v) **Process and Composition:** WSI protocol stack allows composition of softwares using reusable and loosely coupled software components. However to provide interaction between the web service a standard executable language called Business Process Execution Language(BPEL4) is used. It is an XML-based language present at top of web service specification. It defines and manages the web processes. It helps the organization to automate the business processes.

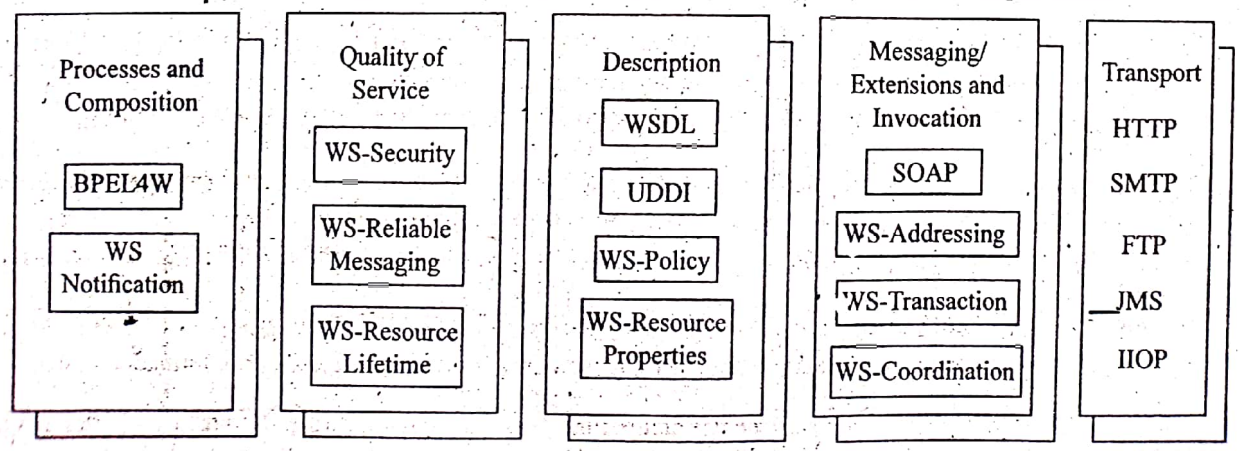


Figure: WSI Protocol Stack and its Features

Q38. Briefly explain about Grid Services of OGSA.

Ans:

Grid Services of OGSA: Open Grid Service Architecture(OGSA) is a service oriented architecture. It defines set of common standards for grid based applications. These standards specify how different components of heterogeneous gird system communicate with each other. The primary aim of OGSA is to provide a well-defined architecture for QoS features of grid system like resource management, problem determination etc. In OGSA registers, computational tasks and data resources are nothing but service. These services are considered as the basic blocks of OGSA-based grid.

The goals defined by OGSA are as follows,

(i) It provides facilities to manage resources over heterogeneous, distributed environment.

(ii) It defines open standards, published interfaces to provide interoperability over resources.

(iii) It makes use of extensive industry standard integration technologies.

(iv) It fulfils the quality of service requirement.

(v) It defines loosely coupled and interoperable web service standards.

The high level architectural view of grid services are defined by OGSA. These services are implemented on multiple interfaces. These interfaces specify various operations that are invoked while performing message exchange depending on Open Grid Service Infrastructure (OGSI). The OGSI architecture is shown in the below,

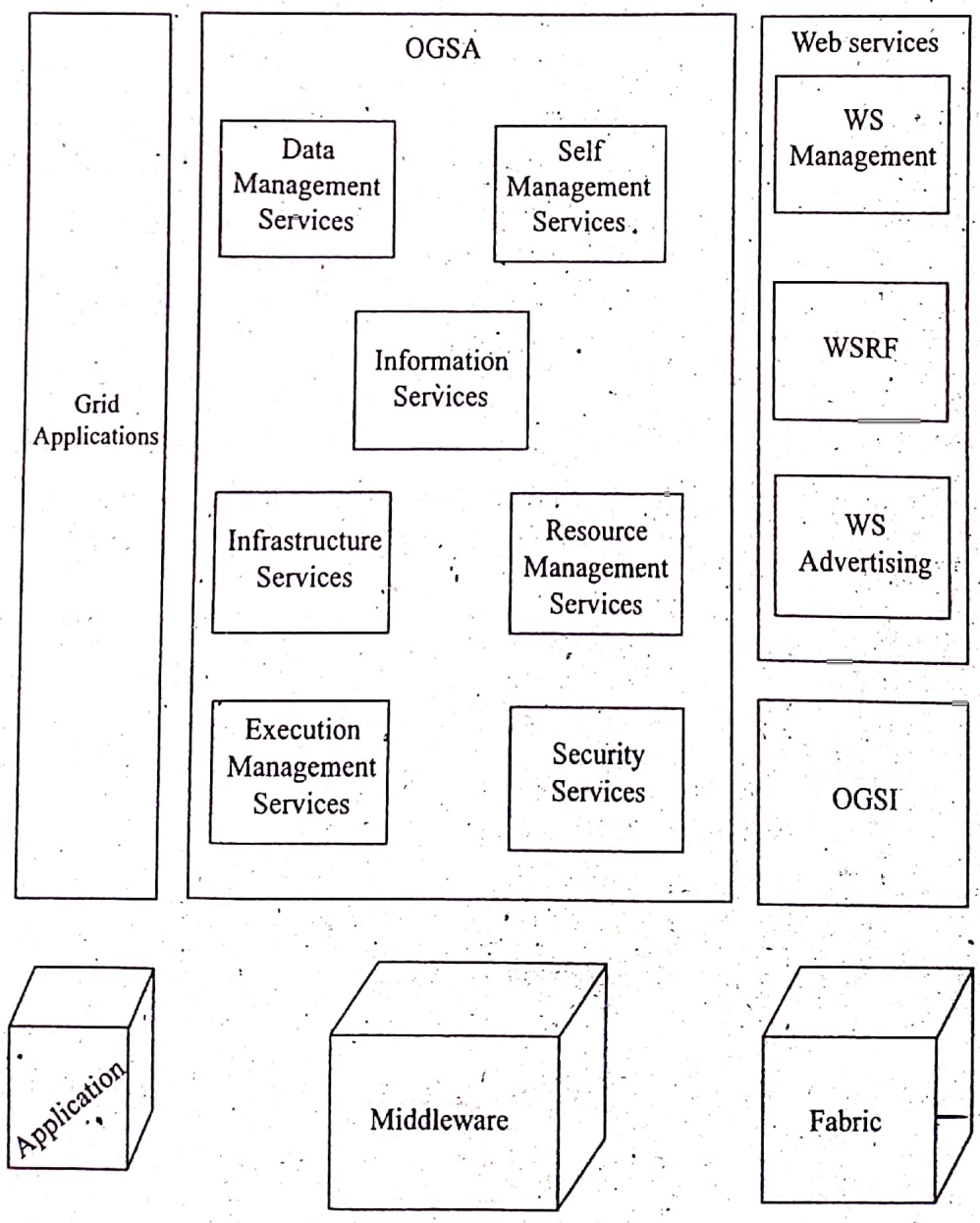


Figure: OGSA Architecture

The services provided by OGSA are as follows,

(i) **Infrastructure Services:** It defines common functionalities like naming a service. These functionalities are utilized by other higher level services.

(ii) **Execution Management Services:** It deals with various task management issues like placements, provisioning and life cycle management of services.

(iii) **Data Management Services:** It facilitates data management capabilities like transmission of data (as per the users request), transformation of data into new formats, run queries and perform updations, maintenance of replicated copies of data. These services deals with issues like data consistency, integrity and persistency.

(iv) **Resource Management Services:** It manages the grid resources in the following manner,

(a) Manages the resources individuals.

(b) Manages the resources as grid components.

(c) Manages the OGSA infrastructure.

It also provides capabilities to monitor resources, deploy and configure the applications so as to meet the required QoS. The OGSA resource management service contains the information model and data model of grid resources and services.

(v) **Security Services:** It enforces security-related policies on organizations to ensure secure resource sharing. It mainly deals with essential functionalities like data authentication, data authorization and data integrity.

(vi) **Information Services:** It provides efficient access to the information present on grid and its resources. The term information is considered as either dynamic (data/events) or static. A dynamic data/events are used for monitoring the status whereas the static data is used in discovery.

(vii) **Self Management Service:** It provides service-level attainment to set of services with automation. This service decreases the code and also reduces the system management complexity.

Web Services: The web services defined in this architecture provides support to dynamic systems that are loosely coupled. There by thus does not satisfy all the needed grid requirements of distributed systems.

WSDL: In OSGA architecture, Web Service Description Languages(WSDL) are applied on extensions by OGSI. This is done to implement grid service instance on multiple systems.

Beside this, a network-wide pointer is also used. This pointer points to grid service instance to make them accessible to remote client applications.

Web Service Resource Framework(WSRF): It is a generic frame work which allow joint cooperation between grid and web service communities. Beside this, various other specifications like WS-Addressing and WS-Notification are also included. This framework allow access to persistent resources. This helps in implementing and managing multiple services.

The stateful information corresponding to a web service is maintained in a special entity called resource. A service can have multiple resources. Each resource is assigned with a unique key and are stored either in memory or in secondary storage file / database. The process of passing web service and resources is referred to as WS-Resource. The WS-Resources are addressed using End Point Reference (EPR) construct defined by WS-Addressing specification.

Resources contain data terms these data terms are called resource properties. It includes information about service data value, current service states, meta data, value information required for managing states etc.

Q39. Explain in detail about the message oriented middleware.

Ans:

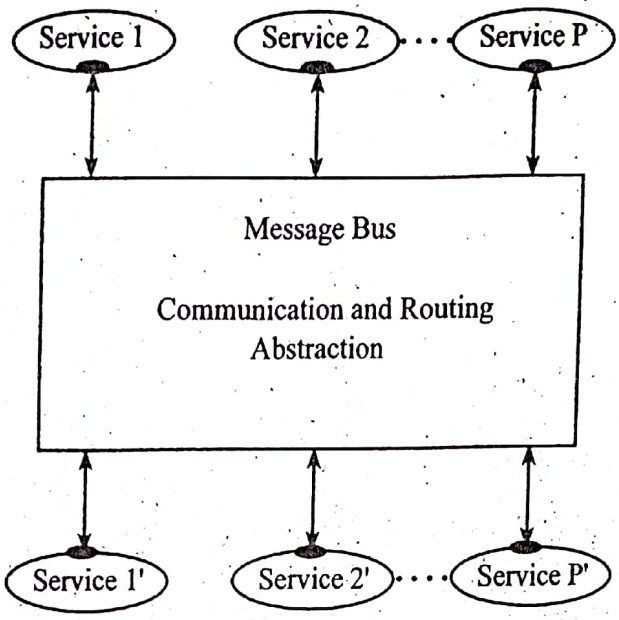
Message Oriented Middleware: Message oriented middleware provides support to distributed computing. It mainly deals with,

(i) Enterprise bus

(ii) Publish-subscribe model

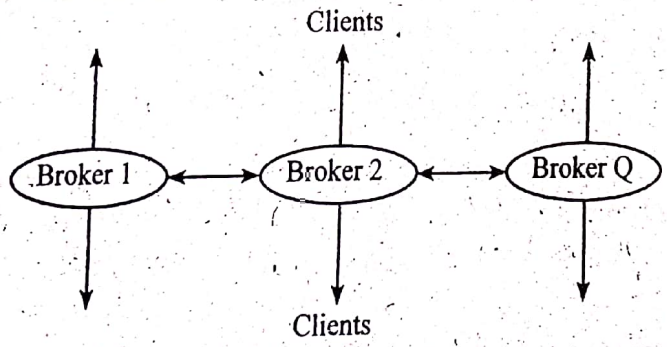
(iii) Queuing and messaging systems.

(i) **Enterprise Bus:** The "Enterprise Service Bus" (ESB) integrates various components that allow communication between the service requesting messages in different styles like SOAP, REST or Java EMI. The messages are send onto bus by injecting a message which contain sufficient information regarding the services that must be delivered to destination. This is done to ensure accurate delivery. Consider the below figure,



In above figure, service is shown as filled ovals. These are called as client interfaces. The message bus is represented as connecting services as [↔] various software (or) hardware can also be used for sending and receiving messages.

A message bus can also be implemented as a set of "brokers", in distributed compution. A broker is responsible for scaling multiple clients having a huge message traffic. This brokers are also known as special server (or) services that can carry out transformations and can send and receive the messages.



A single broker can also be implemented as managers of queues. This is nothing but, MQ (or) "Message Queue". The use of MQ in parallel computing that, it associates master with workers in "farm" model. Here, a "master" defines a work item and place it in queue to allow multiple workers to access it.

(ii) **Publish-Subscribe Model:** "Publish-subscribe" is a model provides a connection between source and destination for passing a message in the bus. The role of publisher is to assign distinct names to the messages depending on the vocabulary. The subscriber receives the message which contains the information related to the messages. This model uses the content-based delivery system in which the information is in query format as SQL. The message filtering is done so as to provide content-based message selection. In this many-to-many relationship is established between publishers and subscribers. This message provides the execution of event-based programming models and notifications.

(iii) **Queuing and Messaging Systems:** The various service / standards used in queuing and messaging systems are as follows,

(a) **Java Message Service:** Java Message Service (JMS) is considered as one of the useful service in queuing and messaging system. This messaging system describes a collection of interfaces that allow communication semantics in pub or sub and queuing systems.

(b) **Advanced Message Queuing Protocol(AMQP):** It allows wire-format communication.

(c) **Mule MQ:** It is a messaging framework defined in ESB system. This messaging framework is developed using Java programming language. It is developed to simplify the integration of various existing systems like JMS, Web Services, SOAP, JDBC and traditional HTTP. It supports protocols like POP, IMAP, FTP, RMI, SOAP, SSL and SMTP.

(d) **ACTIVE MQ:** It is a open source message broker of Apache.

(e) **WebSphere MQ:** It offers an enterprise bus. It is mainly used by IBM.

For exchanging messages Time-decoupled delivery is an important constraint. Fault tolerance is an important feature that helps the messaging systems to back up their messages and provides definitive guarantees.