SYLLABUS
[Academic Session: 2016–17]

CLOUD COMPUTING [ETIT–407]

Instructions to Paper Setters:

1. *Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 25 marks.*
2. *Apart from Question No. 1, rest of the paper shall consist of four units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Eachquestion should be 12.5 marks*

Objectives: To enable students to understand the basic concepts of Cloud Computing and to apply these concepts for designing, evaluating, simulations and comparing various applications in Cloud Computing.

UNIT I

Introduction to Cloud Computing

Overview of Parallel Computing, Grid Computing, Distributed Computing and its Variants (eg. MANETs, Peer to Peer, Cloud), Introduction to Autonomic Computing, Evolution of Cloud Computing and it's vision, Issues and Challenges in Cloud Computing, Applications of Cloud Computing. **[T1, T2][No. of Hours: 10]**

UNIT II

Cloud Computing Architecture

Cloud Computing Architectures: features of Clouds: components, types, technologies, Service Models (Services: IaaS, PaaS, SaaS), Deployment Models (Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud) various cloud management platforms and tools. **[T1, T2][No. of Hours: 12]**

UNIT III

Virtualization of Clouds

Virtualization: Introduction, Evolution, Virtualized Environment characteristics, Server Virtualization, VM Provisioning and Manageability, VM Migration Services, VM Provisioning in the Cloud Context, and Future Research Directions. Cloud Security Mechanisms (Encryption, PKI, SSO, IAM), Service Management in Cloud Computing(SLA, Billing & Accounting etc). **[T1, T2][No. of Hours: 12]**

UNIT IV

Advanced Cloud Applications

Specialized Cloud Architecture: Direct I/O Access, Load Balanced Virtual Switches, Multipath Resource Access, Federated Clouds, Basics of Cloud Mobility, Enterprise cloud computing: Data, Processes, Components, Architectures, applications, Enterprise Software(ERP, SCM, CRM) Case Studies on Open Source and Commercial available tools and platforms (Microsoft Azure, Google AppEngine, Amazon Web services, Hadoop, Eucalyptus, Cloud SIM etc). **[T1, T2][No. of Hours: 11]**

MODEL PAPER–I
END TERM EXAMINATION
SEVENTH SEMESTER [B.TECH]
CLOUD COMPUTING [ETIT–407]

Time : 3 hrs. **M.M. : 75**

Note: *Attempt all questions as per internal choice indicated*

Q.1. (a) Define parallel computing. **(3)**

Ans. With parallel computing, each processing step is completed at the same time. Simulation and video processing are two examples. This is usually done with the same hardware platform or across a custom network or interconnect.

Parallel computing is a type of computation in which many calculations are carried out simultaneously, operating on the principle that large problems can often be divided into smaller ones, which are then solved at the same time. There are several different forms of parallel computing: bit-level, instruction-level, data, and task parallelism. Parallelism has been employed for many years, mainly in high-performance computing, but interest in it has grown lately due to the physical constraints preventing frequency scaling.

Q.1. (b) Explain direct I/O access architecture. **(3)**

Ans. When the CPU is using programmed input/output, it is typically fully occupied for the entire duration of the read or write operation, and is thus unavailable to perform other work. With DMA, the CPU first initiates the transfer, then it does other operations while the transfer is in progress, and it finally receives an interrupt from the DMA controller when the operation is done. This feature is useful at any time that the CPU cannot keep up with the rate of data transfer, or when the CPU needs to perform useful work while waiting for a relatively slow I/O data transfer. Many hardware systems use DMA, including disk drive controllers, graphics cards, network cardsand sound cards. DMA is also used for intra-chip data transfer in multi-core processors. Computers that have DMA channels can transfer data to and from devices with much less CPU overhead than computers without DMA channels. Similarly, a processing element inside a multi-core processor can transfer data to and from its local memory without occupying its processor time, allowing computation and data transfer to proceed in parallel.

DMA can also be used for "memory to memory" copying or moving of data within memory. DMA can offload expensive memory operations, such as large copies or scatter-gather operations, from the CPU to a dedicated DMA engine. An implementation example is the I/O Acceleration Technology.

Q.1. (c) Explain IaaS services. **(4)**

Ans. Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. IaaS is one of three main categories

of cloud computing services, alongside Software as a Service (SaaS) and Platform as a Service (PaaS).

In an IaaS model, a third-party provider hosts hardware, software, servers, storage and other infrastructure components on behalf of its users. IaaS providers also host users' applications and handle tasks including system maintenance, backup and resiliency planning.

IaaS platforms offer highly scalable resources that can be adjusted on-demand. This makes IaaS well-suited for workloads that are temporary, experimental or change unexpectedly.

Other characteristics of IaaS environments include the automation of administrative tasks, dynamic scaling, desktop virtualization and policy-based services.

IaaS customers pay on a per-use basis, typically by the hour, week or month. Some providers also charge customers based on the amount of virtual machine space they use. This pay-as-you-go model eliminates the capital expense of deploying in-house hardware and software. However, users should monitor their IaaS environments closely to avoid being charged for unauthorized services.

Q.1. (*d*) Define Hadoop. **(6)**

Ans. Hadoop is a complete eco-system of open source projects that provide us the framework to deal with big data. Let's start by brainstorming the possible challenges of dealing with big data (on traditional systems) and then look at the capability of Hadoop solution.

Following are the challenges I can think of in dealing with big data:

1. High capital investment in procuring a server with high processing capacity.

2. Enormous time taken

3. In case of long query, imagine an error happens on the last step. You will waste so much time making these iterations.

4. Difficulty in program query building

How Hadoop solves all of these issues :

1. High capital investment in procuring a server with high processing capacity: Hadoop clusters work on normal commodity hardware and keep multiple copies to ensure reliability of data. A maximum of 4500 machines can be connected together using Hadoop.

2. Enormous time taken : The process is broken down into pieces and executed in parallel, hence saving time. A maximum of 25 Petabyte (1 PB = 1000 TB) data can be processed using Hadoop.

3. In case of long query, imagine an error happens on the last step. You will waste so much time making these iterations : Hadoop builds back up data-sets at every level. It also executes query on duplicate datasets to avoid process loss in case of individual failure. These steps makes Hadoop processing more precise and accurate.

4. Difficulty in program query building : Queries in Hadoop are as simple as coding in any language. You just need to change the way of thinking around building a query to enable parallel processing.

Hadoop works in a similar format. On the bottom we have machines arranged in parallel. These machines are analogous to individual contributor in our analogy. Every machine has a data node and a task tracker. Data node is also known as HDFS (Hadoop Distributed File System) and Task tracker is also known as map-reducers.

Data node contains the entire set of data and Task tracker does all the operations. You can imagine task tracker as your arms and leg, which enables you to do a task and data node as your brain, which contains all the information which you want to process. These machines are working in silos and it is very essential to coordinate them. The Task trackers (Project manager in our analogy) in different machines are coordinated by a Job Tracker. Job Tracker makes sure that each operation is completed and if there is a process failure at any node, it needs to assign a duplicate task to some task tracker. Job tracker also distributes the entire task to all the machines.

A name node on the other hand coordinates all the data nodes. It governs the distribution of data going to each machine. It also checks for any kind of purging which have happened on any machine. If such purging happens, it finds the duplicate data which was sent to other data node and duplicates it again. You can think of this name node as the people manager in our analogy which is concerned more about the retention of the entire dataset.

Q.1. (*e*) Define Peer to Peer technology. **(2)**

Ans. Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or work loads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.

Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided. Emerging collaborative P2P systems are going beyond the era of peers doing similar things while sharing resources, and are looking for diverse peers that can bring in unique resources and capabilities to a virtual community thereby empowering it to engage in greater tasks beyond those that can be accomplished by individual peers, yet that are beneficial to all the peers.

Q.1. (*f*) Define cloud in computing. **(5)**

Ans. Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine.

In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services — such as servers, storage and applications —are delivered to an organization's computers and devices through the Internet.

How Cloud Computing Works: The goal of cloud computing is to apply traditional super computing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive online computer games.

To do this, cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared ITinfrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Cloud Computing Standards: The standards for connecting the computer systems and the software needed to make cloud computing work are not fully defined at present time, leaving many companies to define their own cloud computing technologies. Cloud computing systems offered by companies, like IBM's "Blue Cloud" technologies for example, are based on open standards and open source software which link together computers that are used to to deliver Web 2.0 capabilities like mash-ups or mobile commerce.

Cloud Computing in the Data Center and for Small Business: Cloud computing has started to obtain mass appeal in corporate data centers as it enables the data center to operate like the Internet through the process of enabling computing resources to be accessed and shared as virtual resources in a secure and scalable manner.

For a small and medium size business (SMB), the benefits of cloud computing is currently driving adoption. In the SMB sector there is often a lack of time and financial resources to purchase, deploy and maintain an infrastructure (e.g. the software, server and storage).

In cloud computing, small businesses can access these resources and expand or shrink services as business needs change. The common pay-as-you-go subscription model is designed to let SMBs easily add or remove services and you typically will only pay for what you do use.

Q.1. (g) What do you understand by cloud security. **(2)**

Ans. Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use.

Q.2. Explain type of cloud(s) and explain them. **(12.5)**

Ans. Cloud computing is typically classified in the following three ways:

1. Public cloud: In Public cloud the computing infrastructure is hosted by the cloud vendor at the vendorâ premises. The customer has no visibility and control over where the computing infrastructure is hosted. The computing infrastructure is shared between any organizations.

2. Private cloud: The computing infrastructure is dedicated to a particular organization and not shared with other organizations. Some experts consider that private clouds are not real examples of cloud computing. Private clouds are more expensive and more secure when compared to public clouds.

Private clouds are of two types: On-premise private clouds and externally hosted private clouds. Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. Externally hosted private clouds are cheaper than On-premise private clouds.

3. Hybrid cloud: Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud. A related term is Cloud Bursting. In Cloud bursting organization use their own computing infrastructure for normal usage, but access the cloud using services like Salesforce cloud computing for high/peak load requirements. This ensures that a sudden increase in computing requirement is handled gracefully.

4. Community cloud: Involves sharing of computing infrastructure in between organizations of the same community. For example all Government organizations within the state of California may share computing infrastructure on the cloud to manage data related to citizens residing in California.

Classification based upon service provided

Based upon the services offered, clouds are classified in the following ways:

1.Infrastructure as a service (IaaS) involves offering hardware related services using the principles of cloud computing. These could include some kind of storage services (database or disk storage) or virtual servers. Leading vendors that provide Infrastructure as a service are Amazon EC2, Amazon S3,Rackspace Cloud Servers and Flexiscale.

2. Platform as a Service (PaaS) involves offering a development platform on the cloud. Platforms provided by different vendors are typically not compatible. Typical players in PaaS are Googles Application Engine, Microsofts Azure, Salesforce.com force.com .

3. Software as a service (SaaS) includes a complete software offering on the cloud. Users can access a software application hosted by the cloud vendor on pay-per-use basis. This is a well-established sector. The pioneer in this field has been Salesforce.coms offering in the online Customer Relationship Management (CRM) space. Other examples are online email providers like Googles gmail and Microsofts hotmail, Google docs and

Microsofts online version of office called BPOS (Business Productivity Online Standard Suite).

The above classification is well accepted in the industry. David Linthicum describes a more granular classification on the basis of service provided. These are listed below:

1. Storage-as-a-service
2. Database-as-a-service
3. Information-as-a-service
4. Process-as-a-service
5. Application-as-a-service
6. Platform-as-a-service
7. Integration-as-a-service
8. Security-as-a-service
9. Management/Governance-as-a-service
10. Testing-as-a-service
11. Infrastructure-as-a-service

Q.3. Explain Case study on Hadoop's advanced cloud application. **(12.5)**

Ans: Azure HDInsight deploys and provisions managed Apache Hadoop clusters in the cloud, providing a software framework designed to process, analyze, and report on big data with high reliability and availability. HDInsight uses the Horton works Data Platform (HDP) Hadoop distribution. Hadoop often refers to the entire Hadoop ecosystem of components, which includes Apache HBase, Apache Spark, and Apache Storm, as well as other technologies under the Hadoop umbrella.

Big data refers to data being collected in ever-escalating volumes, at increasingly higher velocities, and in an expanding variety of unstructured formats and variable semantic contexts.

Big data describes any large body of digital information, from the text in a Twitter feed, to the sensor information from industrial equipment, to information about customer browsing and purchases on an online catalog. Big data can be historical (meaning stored data) or real-time (meaning streamed directly from the source).

For big data to provide actionable intelligence or insight, not only must you collect relevant data and ask the right questions, but also the data must be accessible, cleaned, analyzed, and then presented in a useful way. That's where big data analysis on Hadoop in HDInsight can help.

Hadoop ecosystem on HDInsight: HDInsight is a cloud implementation on Microsoft Azure of the rapidly expanding Apache Hadoop technology stack that is the go-to solution for big data analysis. It includes implementations of Apache Spark, HBase, Storm, Pig, Hive, Sqoop, Oozie, Ambari, and so on. HDInsight also integrates with business intelligence (BI) tools such as Power BI, Excel, SQL Server Analysis Services, and SQL Server Reporting Services.

Clusters on Linux

Azure HDInsight deploys and provisions Hadoop clusters in the cloud on Linux.

Category	Hadoop on Linux
Cluster OS	Ubuntu 12.04 Long Term Support (LTS)
Cluster Type	Hadoop, Spark, HBase, Storm
Deployment	Azure portal, Azure CLI, Azure PowerShell
Cluster UI	Ambari
Remote Access	Secure Shell (SSH), REST API, ODBC, JDBC

Hadoop, HBase, Spark, Storm, and customized clusters

HDInsight provides cluster configurations for Apache Hadoop, Spark, HBase, or Storm. Or, you can customize clusters with script actions.

- **Hadoop (the "Query" workload):** Provides reliable data storage with HDFS, and a simple Map Reduce programming model to process and analyze data in parallel.
- **Apache Spark:** A parallel processing framework that supports in-memory processing to boost the performance of big-data analysis applications, Spark works for SQL, streaming data, and machine learning. See Overview: What is Apache Spark in HDInsight?
- **HBase (the "NoSQL" workload):** A NoSQL database built on Hadoop that provides random access and strong consistency for large amounts of unstructured and semi-structured data - potentially billions of rows times millions of columns. See Overview of HBase on HDInsight.
- **Apache Storm (the "Stream" workload):** A distributed, real-time computation system for processing large streams of data fast. Storm is offered as a managed cluster in HDInsight. See Analyze real-time sensor data using Storm and Hadoop.

Q.4. (a) Explain Migration service in virtualization. **(10)**

Ans. Cloud-to-cloud migration (C2C) is the movement of physical or virtual machines–along with their associated configurations; operating systems, applications and storage-from one cloud computing provider to another. Cloud-to-cloud migration allows an organization to switch cloud computing providers without first transferring data to in-house servers. Having the ability to move easily between cloud providers is an important consideration when choosing a cloud provider. The cost of a cloud migration should not outweigh the advantages of moving to a new cloud provider.

From scalability to cost-efficiency, cloud computing delivers a range of benefits to an enterprise. And when it comes to provisioning new capacity, there are three distinct cloud computing advantages organization don't want to miss: the ability to scale on-demand, paying only for the compute resources used and end-to-end service automation.

'Unfortmately', cloud computing strategies aren't always easy to carry out-especially when migrating existing cloud workloads between cloud providers or public and private

clouds. That migration process typically requires many manual steps, and the process itself can be difficult to scale. If these migrations aren't handled effeciently, organizations pay for cloud resources they don't use.

Before being able to move workloads between different cloud platforms, organizations must first move their on-premises applications to the cloud. And that's not always an easy feat.

Cloud migration practices:

1. Make infrastructure immutable to avoid doing change management on an ongoing basis: This involves creating immutable components such as base images, network configurations and software dependencies, rather than changing configuration and upgrading servers each time a change is required.

2. Design an application blueprint by defining all components and embedded configuration fields, so it can be duplicated in the cloud.

3. Embed security and ensure high availability: There are three common approaches to migrating applications to the cloud.

The first two approaches are "lift and shift" and refactoring.

The third and more sophisticated option is extension on redesign.

Lift and shift means moving an application directly to a cloud host. In many cases, the approach works fine but it won't take advantage of the cloud platform's full capabilities. Refactoring which involves making modest application code changes to ensure a smoother migration. The best approaches, though are extension-or heavily modifying code to fit the new cloud environment - or a complete redesign to optimize the application for cloud.

Q.4. (*b*) What is server virtualization in cloud computing? **(2.5)**

Ans. Server virtualization is the masking of server resources, including the number and identity of individual physical servers, processors, and operating systems, from server users. The server administrator uses a software application to divide one physical server into multiple isolated virtual environments. The virtual environments are sometimes called virtual private servers, but they are also known as guests, instances, containers or emulations.

Q.5. Explain service management in cloud computing. **(12.5)**

Ans. Cloud service management is concerned with aligning both worlds, that is, the world of cloud computing and service management and introducing good cloud management practices among customer, consumer and supplier organisations.

Cloud computing and cloud-based services are not new technology. Cloud principles were followed even for Main frames circa 1950s and 1960s.

There are many frameworks and methods for the management of IT and for service management. In most cases, cloud computing is described as a business model for use

of other underlying technologies and not as a technology. Those underlying technologies, such as virtualization, provide the basis for employing cloud computing concepts. Cloud in itself if not a technology.

Cloud Computing – Purpose & Scope

The purpose and scope of cloud service management:

Purpose

- Establish appropriate methods for the management and operation of cloud based services.
- Embed cloud service management practices into existing IT development and support structures.

Scope

- Oversight of the design, development and transition of cloud based services.
- Management and operation of cloud based services.

Cloud Computing – Features

- Cloud is a style of computing where scalable and elastic IT related capabilities are delivered as a service to consumers using internet technologies.
- Cloud is not defined as a set of technologies, but rather a model for delivering, managing and consuming information technology resources and services.

Cloud Computing – Definition

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing recourses, that is, networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model is composed of five essential characteristics, three service models and four deployment models

The 5 essential Operational Characteristics are:

- **On Demand Self Service** – Automated consumer centric search, selection and provisioning.
- **Measured Service** – Metered resource usage with monitoring, reporting and charging mechanisms.
- **Broad Network Access** – Cloud service accessible connectivity to a range of devices and networks.
- **Resource Pooling** – Shared resources for one or many tenants supporting different demand and supply capacity.
- Rapid Elasticity – automated provisioning and scaling for one or many tenants.

The 3 Service Models are:

- **Software as a Service (SaaS)** – Applications which provide business value for users.

• **Platform as a Service (PaaS)** – Applications which provide specialised software components and programming tools.

• **Infrastructure as a Service (IaaS)** – Applications which provide computing infrastructure resources as a service.

The 4 Cloud Deployment Models are:

• **Private Cloud** – This cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers, for example, business units.

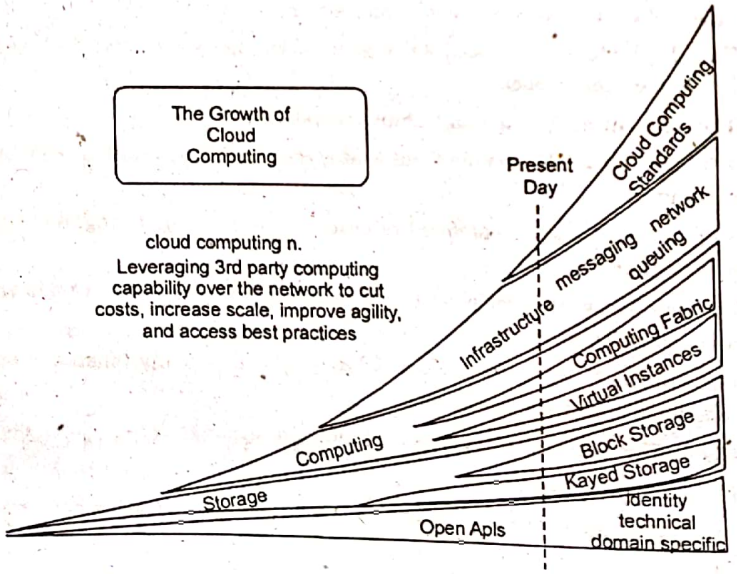
• **Community Cloud** – This cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns.

• **Public Cloud** – This cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organisation or a combination of these.

• **Hybrid Cloud** – This cloud infrastructure is a composition of two or more distinct cloud infrastructures, such as private and public community that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability.

Q.6. (a) Explain various future aspects of cloud computing. (7)

Ans. Cloud computing is a convenient, on-demand model for network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Conceptually it refers to a model of scalable, real-time, internet-based information technology services and resources, satisfying the computing needs of users, without the users incurring the costs of maintaining the underlying infrastructure.



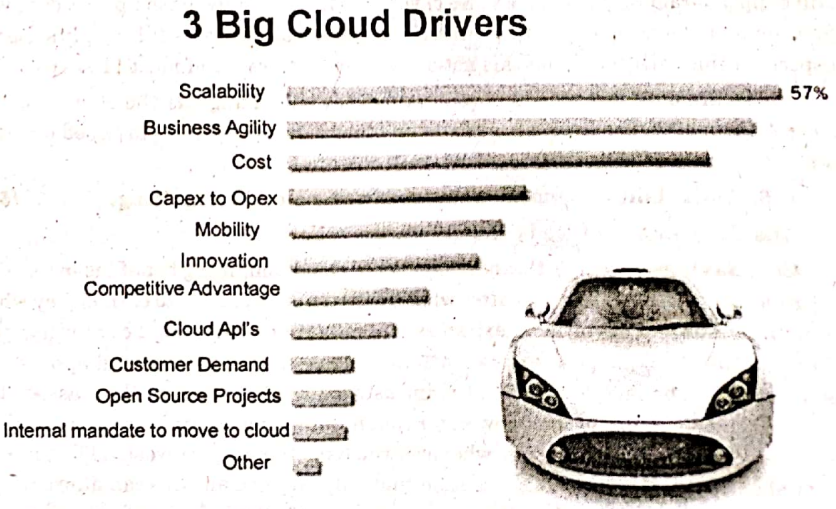
A great appeal of the cloud is the potential to create new solutions in the future that were not technically or economically feasible without the use of cloud services. Keeping in view the above; Imagine you are living in year 2025, and going to lunch with a former colleague in your new flying car. The two of you wonder, "Whatever happened to cloud computing?"

As a buzzword, like buzzwords of the past, cloud computing will eventually be baked into all our technology and barely discussed as a concept. Cloud computing in 10 years will have gone off in various directions, all systemic to how we handle enterprise computing in the future. Here are just two paths:

In 10 years, pervasive cloud services will be the standard for assembling business solutions. We will leverage core services that either exist within our enterprise or from public cloud providers to assemble and reassemble business solutions. These services will be utility-based, perhaps primitive storage and compute or security and governance or more sophisticated business uses, such as market forecasting services.

While services certainly reside in the clouds today, in 10 years, they should be built around the same set of standards and thus be more compatible, no matter which public provider you leverage. Moreover, they should be dynamically discoverable and self-healing, and they may exist as private services you own and maintain. Alternatively, they could be public services you leverage from any public cloud provider.

In 10 years, cloud-based data will include context to better understand that data. Data today exists largely in siloed systems, which makes it difficult to access and difficult to gather for business intelligence. As more data moves to the cloud, enterprises will understand how to holistically leverage this information; using the ability to instantly query petabytes of private business findings using data services (see previous predi- ion). We're already on this path today with the big data movement.



There are obviously some inhibitors in the adoption of cloud computing. The plain fact is most organizations can barely deal with designing, implementing, operating and maintaining their infrastructure, let alone things like their security. This is why SaaS and cloud environments will win out in the end. Lets face it, once you admit to yourself that you don't have the resources that the provider does, you will realize that giving up control allows people who do this as core to their mission perform the task. Is hosting infrastructure and applications and security really core to your business model?

1. Performance – Do you really think you are going to build a more robust or higher performing platform than your service providers?

2. ROI – I don't know if SaaS and cloud is cheaper overall. It certainly is cap ex versus operational expense. But my experience shows me that while outsourcing via SaaS or otherwise is not necessarily cheaper, it provides a greater value.

3. Market churn – Frankly you are as likely to go out of business as your service provider is. But that being said, whether that vendor is a cloud or SaaS provider or a traditional vendor, them going out of business is always a risk. One you can minimize with due dilligence, but not really model specific.

4. Privacy – OK it is different from security, but stop right there. I would argue with the state of most enterprise data centers and organizations, your privacy is better protected at a service provider who has made that a priority. I think they do it for multiple customers and do it better.

5. Security – This is the bogeyman of the cloud. Again similar to privacy, what makes you think you do security any better than the service provider does? Or their SaaS security partner for that matter? Fact is you still have all of the security problems you do when your data is under your own control, maybe even less when in the cloud.

As per predictions, In 10 years, public data services will include information such as key economic indicators, average sales trends within verticals, or other points that will supply a framework to make sense of your data. You simply mash up that data with your own business information to realize the potential for powerful insights. Again, aspects of this exist today, but this notion is beyond the reach of most IT shops.

These are only two aspects of computing that will change as the cloud becomes more embedded in our lives. I'm sure many other derivative concepts based on cloud computing will linger as well.

Q.6. (*b*) Explain various advantages of using cloud computing. **(5.5)**

Ans. Advantages of Cloud Computing are as follows:

Cost Savings: Perhaps, the most significant cloud computing benefit is in terms of IT cost savings. Businesses, no matter what their type or size, exist to earn money while keeping capital and operational expenses to a minimum. With cloud computing, you can save substantial capital costs with zero in-house server storage and application requirements. The lack of on-premises infrastructure also removes their associated operational costs in the form of power, air conditioning and administration costs. You pay for what is used and disengage whenever you like - there is no invested IT capital to worry about. It's a common misconception that only large businesses can afford to use the cloud, when in fact, cloud services are extremely affordable for smaller businesses.

Reliability: With a managed service platform, cloud computing is much more reliable and consistent than in-house IT infrastructure. Most providers offer a Service Level Agreement which guarantees 24/7/365 and 99.99% availability. Your organization can benefit from a massive pool of redundant IT resources, as well as quick failover mechanism - if a server fails, hosted applications and services can easily be transited to any of the available servers.

Manageability: Cloud computing provides enhanced and simplified IT management and maintenance capabilities through central administration of resources, vendor managed infrastructure and SLA backed agreements. IT infrastructure updates and maintenance are eliminated, as all resources are maintained by the service provider. You enjoy a simple web-based user interface for accessing software, applications and services – without the need for installation - and an SLA ensures the timely and guaranteed delivery, management and maintenance of your IT services.

Strategic Edge: Ever-increasing computing resources give you a competitive edge over competitors, as the time you require for IT procurement is virtually nil. Your company can deploy mission critical applications that deliver significant business benefits, without any upfront costs and minimal provisioning time. Cloud computing allows you to forget about technology and focus on your key business activities and objectives. It can also help you to reduce the time needed to market newer applications and services.

MODEL PAPER–II
END TERM EXAMINATION
SEVENTH SEMESTER (B.TECH)
CLOUD COMPUTING [ETIT–407]

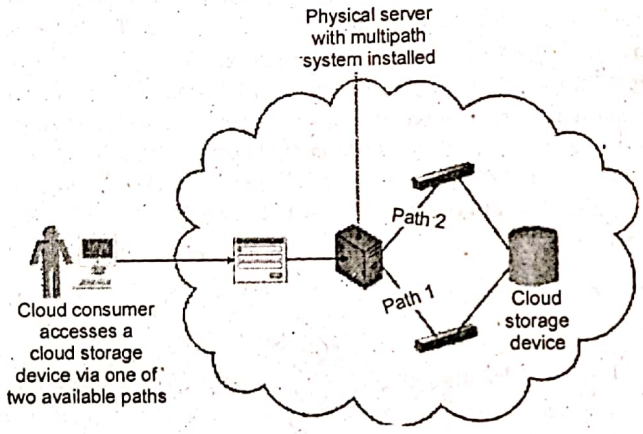
M.M. : 75

Time : 3 hrs.

Note: *Attempt all questions as per internal choice indicated*

Q.1. (a) Define multipath resource access. **(3)**

Ans. Accessability of data from a cloud following various paths for same destination:



Q.1. (b) What is Enterprise cloud computing? **(3)**

Ans. Enterprise cloud computing is the special case of utilizing cloud computing for competitive advantage through breakout opportunities both for cost savings and, more importantly, for business innovation in terms of unprecedented speed and agility with vastly improved collaboration among business partners and customers. What does "cloud computing" mean for the enterprise? More important than the question of "what is it?" is why it matters. Here are three key points.

(1) On the cost side of the equation, many, but not all, IT and data center costs can be reduced and tied directly to usage, up or down as needs go up or down (rapid elasticity).

(2) But there's more, much more, on the revenue side. Risk and startup expenses for innovation initiatives can be cut dramatically, letting companies take more small bets and test out more new ideas. With no upfront capital expense, new projects can be scaled up instantly if they take off, or shut down quickly if they fail. Massive scalability and up-or-down elasticity give companies a whole new sandbox for testing new business ideas and growing them if they take off.

(3) Companies don't work alone, and, on average, over 20 companies make up today's value chains. Cloud computing allows a company to collaborate in new ways with its trading partners, and collaboration is the key to gaining competitive advantage

across the value chain. By establishing shared workspaces in "Community Clouds" employees from multiple companies can work together as a "virtual enterprise network" and function as though they were a single company. They all participate in the same value delivery system, sharing computing, communication and information resources. This is especially important as no one company "owns" the overall value chain.

Q.1. (c) Explain cloud computing application areas. **(4)**

Ans. 1. Infrastructure as a service (IaaS) and platform as a service (PaaS)

When it comes to IaaS, using an existing infrastructure on a pay-per-use scheme seems to be an obvious choice for companies saving on the cost of investing to acquire, manage and maintain an IT infrastructure. There are also instances where organizations turn to PaaS for the same reasons while also seeking to increase the speed of development on a ready-to-use platform to deploy applications.

2. Private cloud and hybrid cloud: Among the many incentives for using cloud, there are two situations where organizations are looking into ways to assess some of the applications they intend to deploy into their environment through the use of a cloud (specifically a public cloud). While in the case of test and development it may be limited in time, adopting a hybrid cloud approach allows for testing application workloads, therefore providing the comfort of an environment without the initial investment that might have been rendered useless should the workload testing fail.

Another use of hybrid cloud is also the ability to expand during periods of limited peak usage, which is often preferable to hosting a large infrastructure that might seldom be of use. An organization would seek to have the additional capacity and availability of an environment when needed on a pay-as you-go basis.

3. Test and development: Probably the best scenario for the use of a cloud is a test and development environment. This entails securing a budget, setting up your environment through physical assets, significant manpower and time. Then comes the installation and configuration of your platform. All this can often extend the time it takes for a project to be completed and stretch your milestones.

With cloud computing, there are now readily available environments tailored for your needs at your fingertips. This often combines, but is not limited to, automated provisioning of physical and virtualized resources.

4. Big data analytics: One of the aspects offered by leveraging cloud computing is the ability to tap into vast quantities of both structured and unstructured data to harness the benefit of extracting business value.

Retailers and suppliers are now extracting information derived from consumers' buying patterns to target their advertising and marketing campaigns to a particular segment of the population. Social networking platforms are now providing the basis for analytics on behavioral patterns that organizations are using to derive meaningful information.

5. File storage: Cloud can offer you the possibility of storing your files and accessing, storing and retrieving them from any web-enabled interface. The web services interfaces are usually simple. At any time and place you have high availability, speed, scalability and security for your environment. In this scenario, organizations are only paying for the amount of storage they are actually consuming, and do so without the worries of overseeing the daily maintenance of the storage infrastructure.

There is also the possibility to store the data either on or off premises depending on the regulatory compliance requirements. Data is stored in virtualized pools of storage hosted by a third party based on the customer specification requirements.

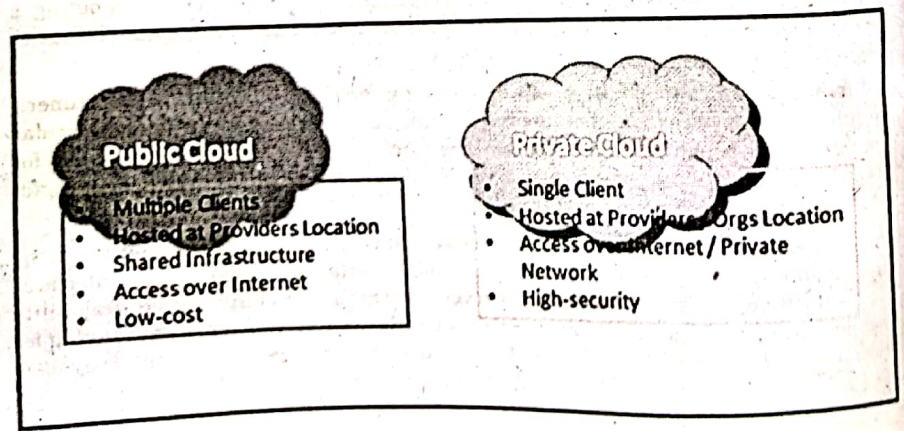
6. Disaster recovery: This is yet another benefit derived from using cloud based on the cost effectiveness of a disaster recovery (DR) solution that provides for a faster recovery from a mesh of different physical locations at a much lower cost that the traditional DR site with fixed assets, rigid procedures and a much higher cost.

7. Backup: Backing up data has always been a complex and time-consuming operation. This included maintaining a set of tapes or drives, manually collecting them and dispatching them to a backup facility with all the inherent problems that might happen in between the originating and the backup site. This way of ensuring a backup is performed is not immune to problems such as running out of backup media , and there is also time to load the backup devices for a restore operation, which takes time and is prone to malfunctions and human errors.

Q.1. (*d*) Difference between private and public cloud. **(6)**

Ans. Private Cloud: A private cloud hosting solution, also known as an internal or enterprise cloud, resides on company's intranet or hosted data center where all of your data is protected behind a firewall. This can be a great option for companies who already have expensive data centers because they can use their current infrastructure. However, the main drawback people see with a private cloud is that all management, maintenance and updating of data centers is the responsibility of the company. Over time, it's expected that your servers will need to be replaced, which can get very expensive. On the other hand, private clouds offer an increased level of security and they share very few, if any, resources with other organizations.

Public Cloud: The main differentiator between public and private clouds is that you aren't responsible for any of the management of a public cloud hosting solution. Your data is stored in the provider's data center and the provider is responsible for the management and maintenance of the data center. This type of cloud environment is appealing to many companies because it reduces lead times in testing and deploying new products. However, the drawback is that many companies feel security could be lacking with a public cloud. Even though you don't control the security of a public cloud, all of your data remains separate from others and security breaches of public clouds are rare.



Q.1 (*e*) What id Hybrid cloud? **(2)**

Ans. Hybrid cloud is a cloud computing environment which uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms. By allowing workloads to move between private and public clouds as computing needs and costs change, hybrid cloud gives businesses greater flexibility and more data deployment options.

Q.1. (*f*) Explain SSO security management. **(5)**

Ans. Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications. The service authenticates the end user for all the applications the user has been given rights to and eliminates further prompts when the user switches applications during the same session. On the back end, SSO is helpful for logging user activities as well as monitoring user accounts.

In a basic web SSO service, an agent module on the application server retrieves the specific authentication credentials for an individual user from a dedicated SSO policy server, while authenticating the user against a user repository such as a light weight directory access protocol (LDAP) directory.

Some SSO services use protocols such as Kerberos and the security assertion markup language (SAML). SAML is an XML standard that facilitates the exchange of user authentication and authorization data across secure domains. SAML-based SSO services involve communications between the user, an identity provider that maintains a user directory, and a service provider. When a user attempts to access an application from the service provider, the service provider will send a request to the identity provider for authentication. The service provider will then verify the authentication and log the user in. The user will not have to log in again for the rest of his session. In a Kerberos-based setup, once the user credentials are provided, a ticket-granting ticket (TGT) is issued. The TGT fetches service tickets for other applications the user wishes to access, without asking the user to re-enter credentials.

Although single sign-on is a convenience to users, it present risks to enterprise security. An attacker who gains control over a user's SSO credentials will be granted access to every application the user has rights to, increasing the amount of potential damage. In order to avoid malicious access, it's essential that every aspect of SSO implementation be coupled with identity governance. Organizations can also use two factor authentication (2FA) or multifactor authentication (MFA) with SSO to improve security.

Q.1. (*g*) Explain Cloud sim. **(2)**

Ans. Cloud Sim Automation is a Java command line tool based on Cloud Sim and Cloud Reports classes that is able to read specifications of Cloud Sim simulation scenarios from a YAML file, a very human readable data format. Simulation scenarios can be written inside a YAML file and Cloud Automation Tool reads these simulation scenarios, creates and runs them on Cloud Sim.

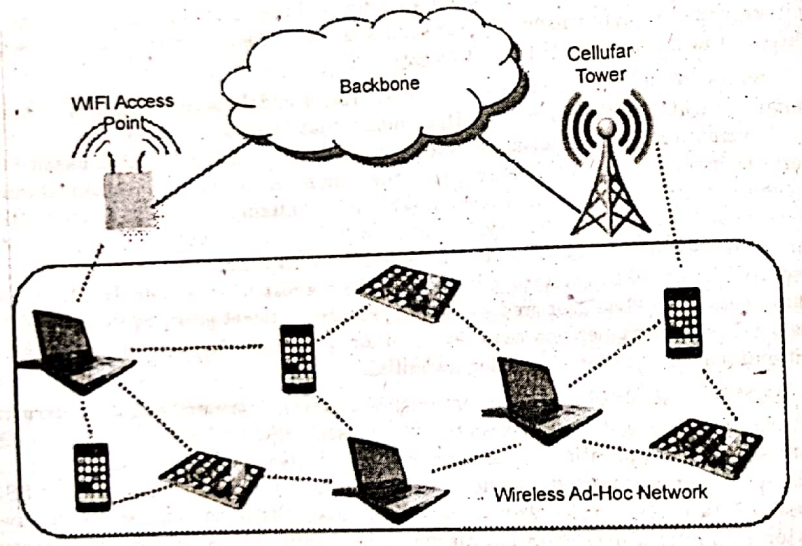
The tool releases researchers of the need to write Java code just to run simulation scenarios. By this way, the attention can be focused on the problem to be solved, such as creation of new algorithms to load balancing, new virtual machine scheduling policies, VM placement, resource provisioning, workload prediction, server consolidation, energy efficiency, cost reduction and so on.

Q.2. Define MANET with example.

Ans. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic[1]. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).



With the rapid development of wireless communication technology and the extensive usage of mobile communication equipment, wireless ad hoc networks are getting more and more attention. Nowadays, wireless ad hoc networks are not only used in military, but also been applied to civilian application, including home area networks, mobile communication networks, and so on. Wireless ad hoc networks are envisioned to be one of the most important parts of future Internet. However, in civilian wireless ad hoc networks, nodes often belong to different parties who have their own interests and always want to maximize their own benefits. Such selfish behaviour can hurt the robustness and availability of wireless ad hoc networks. In our work, we adopt solution concepts from microeconomics and game theory to study important incentive problems in wireless ad hoc networks, including spectrum allocation and routing. Our objective is to achieve a series of cooperation-incentive mechanisms with high availability, low cost,

and high adaptability, through the following four closely related studies: game-theoretic problem modeling, impossibility analyzing, strong incentive mechanism designing, and systematic evaluation methodology developing.

Q.3. Explain Microsoft Azure platform (12.5)

Ans. Refer ans 2 and 3 modal paper 1 cloud computing.

Microsoft Azure is a cloud computing platform and infrastructure created by Microsoft for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers.

It provides both PaaS and IaaS services and supports many different programming languages, tools and frameworks, including both Microsoft-specific and third-party software and systems.

Q.4. (a) Explain IAM with example. (10)

Ans. An identity management access (IAM) system is a framework for business processes that facilitates the management of electronic identities. The framework includes the technology needed to support identity management.

An identity access management (IAM) system is a framework for business processes that facilitates the management of electronic identities. The framework includes the technology needed to support identity management.

IAM technology can be used to initiate, capture, record and manage user identities and their related access permissions in an automated fashion. This ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorized and audited.

Poorly controlled IAM processes may lead to regulatory non-compliance because if the organization is audited, management will not be able to prove that company data is not at risk for being misused.

Why you need IAM

It can be difficult to get funding for IAM projects because they don't directly increase either profitability or functionality. However, a lack of effective identity and access management poses significant risks not only to compliance but also an organization's overall security. These mismanagement issues increase the risk of greater damages from both external and inside threats.

Keeping the required flow of business data going while simultaneously managing its access has always required administrative attention. The business IT environment is ever evolving and the difficulties have only become greater with recent disruptive trends like bring-your-own-device (BYOD), cloud computing, mobile apps and an increasingly mobile workforce. There are more devices and services to be managed than ever before, with diverse requirements for associated access privileges.

With so much more to keep track of as employees migrate through different roles in an organization, it becomes more difficult to manage identity and access. A common problem is that privileges are granted as needed when employee duties change but the access level escalation is not revoked when it is no longer required.

This situation and request like having access like another employee rather than specific access needs leads to an accumulation of privileges known as privilege creep. Privilege creep creates security risk in two different ways. An employee with privileges beyond what is warranted may access applications and data in an unauthorized and potentially unsafe manner. Furthermore, if an intruder gains access to the account of a user with excessive privileges, he may automatically be able to do more harm. Data loss or theft can result from either scenario.

Typically, this accumulation of privilege is of little real use to the employee or the organization. At best, it might be a convenience in situations when the employee is asked to do unexpected tasks. On the other hand, it might make things much easier for an attacker who manages to compromise an over-privileged employee identity. Poor identity access management also often leads to individuals retaining privileges after they are no longer employees.

Q.4. (*b*) What are federated clouds? **(2.5)**

Ans. The United States government cloud computing plan, officially called the Federal Cloud Computing Initiative, is a plan to transition the US federal government's information technology infrastructure to web-based IT services. Launched in September of 2009 by the Obama administration, the initiative seeks to identify common services and solutions amongst the government's agencies and adopt a cloud computing business model to support them.

Q.5. Explain Case study on Amazon's advanced cloud application **(12.5)**

Ans. Traditionally, businesses have had to build and maintain infrastructure to run on-premises applications. With the Software-as-a-Service (SaaS) model, businesses can consume applications that are hosted online, enabling them to lower their costs by paying only for what they use, enjoy seamless and painless upgrades in functionality, and integrate easily with their existing data and systems.

Application providers who are building SaaS-based applications quickly learn that owning and operating the infrastructure on which these solutions are hosted can be expensive and complex, especially when customer demand is uncertain.

Whether you are an enterprise looking for a cloud environment in which to deploy your existing on-premises solutions, or an application vendor evaluating a cloud platform on which to deploy a new application or SaaS offering, you should consider the following questions:

- Can I use the programming language and application platform of my choice?
- Can I use the operating system and environment on which my existing applications are already deployed?
- What commitments or contracts will my cloud provider require? Will I have to make an up-front investment?
- How quickly can I respond to spikes and lulls in demand from my customers or application computing loads?
- Does my cloud provider have experience in maintaining a global, redundant, and resilient infrastructure?

- What security considerations has my cloud provider addressed?

Application Hosting Using AWS: Amazon Web Services (AWS) delivers reliable, scalable, and cost-effective computing resources on which to host your applications. You can use the following AWS components alone or combined to host your application(s):

Amazon Elastic Compute Cloud (Amazon EC2). Amazon EC2 provides resizable compute capacity in the cloud. You define your virtual Amazon EC2 environment with the operating system, services, databases, and application platform stack required for your hosted application. Amazon EC2 provides a full management console and APIs to manage your compute resources.

Amazon Simple Storage Service (Amazon S3). Amazon S3 provides a simple web services interface to store and retrieve any amount of data, at any time, from anywhere on the web. It is durable, highly available, and secure. Amazon S3 also stores multiple redundant copies of your data.

Amazon Relational Database Service (Amazon RDS). Amazon RDS makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable database capacity while managing time-consuming database administration tasks.

Amazon CloudFront. Amazon CloudFront provides a high performance, globally distributed content delivery system. Your application can use Amazon CloudFront to easily distribute or stream content to your users with low latency, high data transfer speeds, no commitments, and seamless integration with Amazon S3.

Amazon Simple Queue Service (Amazon SQS). Amazon SQS provides a high performance, secure queuing system for your application that enables you to reliably distribute work between your application's processes.

Amazon DevPay. Amazon DevPay is a simple-to-use online billing and account management service that makes it easy for you to sell applications that are built in, or run on top of, Amazon Web Services

Q.6. (*a*) Explain various cloud management tools. **(7)**

Ans. Several providers have products designed for cloud computing management(VMware, OpenQRM, CloudKick, and Managed Methods), along with the big players like BMC, HP, IBM Tivoli and CA. Each uses a variety of methods to warn of impending problems or send up the red flag when a sudden problem occurs. Each also tracks performance trends.

While they all have features that differentiate them from each other, they're also focused on one key concept: providing information about cloud computing systems. If your needs run into provisioning, the choices become more distinct than choosing "agent vs. agentless" or "SNMP vs. WBEM."

The main cloud infrastructure management products offer similar core features:

- Most support different cloud types (often referred to as hybrid clouds).
- Most support the on-the-fly creation and provisioning of new objects and the destruction of unnecessary objects, like servers, storage, and/or apps.

• Most provide the usual suite of reports on status (uptime, response time, quota use, etc.) and have a dashboard that can be drilled into.

When it comes to meeting those three criteria, there are a few vendors that offer pervasive approaches in handling provisioning and managing metrics in hybrid environments: RightScale, Kaavo, Zeus, Scalr and Morph. There are also options offered by cloud vendors themselves that meet the second and third criteria, such as CloudWatch from Amazon Web Services.

The large companies known for their traditional data center monitoring applications have been slow to hit the cloud market, and what products they do have are rehashes of existing applications that do little in the way of providing more than reporting and alerting tools. CA is on an acquisition spree to fix this and just acquired 3Tera, a cloud provisioning player.

An example of the confusion in the industry is IBM's Tivoli product page for cloud computing. You'll notice that clicking the Getting Started tab results in a 404 error. Nice work, IBM.

Meanwhile, HP's OpenView (now called Operations Manager) can manage cloud-based servers, but only insofar as it can manage any other server. BMC is working on a cloud management tool, but doesn't have anything beyond its normal products out at the moment.

Q.6. (*b*) Explain Deployment models in cloud computing **(5.5)**

Ans. Cloud hosting deployment models represent the exact category of cloud environment and are mainly distinguished by the proprietorship, size and access. It tells about the purpose and the nature of the cloud. Most of the organisations are willing to implement cloud as it reduces the capital expenditure and controls operating cost. In order to know which deployment model matches your website requirements it is necessary to know the four deployment models.

Public Cloud: is a type of cloud hosting in which the cloud services are delivered over a network which is open for public usage. This model is a true representation of cloud hosting; in this the service provider renders services and infrastructure to various clients. The customers do not have any distinguishability and control over the location of the infrastructure. From the technical viewpoint, there may be slight or no difference between private and public clouds' structural design except in the level of security offered for various services given to the public cloud subscribers by the cloud hosting providers.

Public cloud is better suited for business requirements which require managing the load; host application that is SaaS-based and manage applications that many users consume. Due to the decreased capital overheads and operational cost this model is economical. The dealer may provide the service free or in the form of the license policy like pay per user. The cost is shared by all the users, so public cloud profits the customers more by achieving economies of scale. Public cloud facilities may be availed free an e.g. of a public cloud is Google.

Private Cloud: is also known as internal cloud; the platform for cloud computing is implemented on a cloud-based secure environment that is safeguarded by a firewall

which is under the governance of the IT department that belongs to the particular corporate. Private cloud as it permits only the authorized users, gives the organisation greater and direct control over their data. What exactly constitutes a private cloud? It is difficult to define because when it's classified according to the services there are significant variations. Whether the physical computers are hosted internally or externally they provide the resources from a distinct pool to the private cloud services. Businesses that have dynamic or unforeseen needs, assignments which are mission critical, security alarms, management demands and uptime requirements are better suited to adopt private cloud. Obstacles with regards to security can be evaded in a private cloud, but in case of natural disaster and internal data theft the private cloud may be prone to vulnerabilities.

Hybrid Cloud: is a type of cloud computing, which is integrated. It can be an arrangement of two or more cloud servers, i.e. private, public or community cloud that is bound together but remain individual entities. Benefits of the multiple deployment models are available in a hybrid cloud hosting. A hybrid cloud can cross isolation and overcome boundaries by the provider; hence, it cannot be simply categorized into public, private or community cloud. It permits the user to increase the capacity or the capability by aggregation, assimilation or customization with another cloud package / service. In a hybrid cloud, the resources are managed and provided either in-house or by external providers. It is an adaptation among two platforms in which the workload exchanges between the private cloud and the public cloud as per the need and demand.

Resources that are non-critical like development and test workloads can be housed in the public cloud that belongs to a third-party provider. While the workloads that are critical or sensitive must be housed internally. Consider an e-commerce website, which is hosted on a private cloud that gives security and scalability, since security is not a prime concern for their brochure site it is hosted on a public cloud which is more economical as compared to a private cloud. Businesses that have more focus on security and demand for their unique presence can implement hybrid cloud as an effective business strategy. When facing demand spikes the additional resources that are required by a particular application can be accessed from the public cloud. This is termed as cloud bursting and is available with the hybrid cloud.

Organisations can use the hybrid cloud model for processing big data. On a private cloud, it can retain sales, business and various data and can initiate analytical queries over the public cloud as the public cloud is effective to meet the demand spikes. Hybrid cloud hosting is enabled with features like scalability, flexibility and security. If one is ready to overlook a few challenges like application program interface incompatibility, network connectivity issues and capital expenditures, then the hybrid cloud would be an appropriate option.

Community Cloud: is a type of cloud hosting in which the setup is mutually shared between many organisations that belong to a particular community, i.e. banks and trading firms. It is a multi-tenant setup that is shared among several organisations that belong to a specific group which has similar computing apprehensions. The community members generally share similar privacy, performance and security concerns. The main intention of these communities is to achieve their business related objectives. A community cloud may be internally managed or it can be managed by a third party

provider. It can be hosted externally or internally. The cost is shared by the specific organisations within the community, hence, community cloud has cost saving capacity. A community cloud is appropriate for organisations and businesses that work on joint ventures, tenders or research that needs a centralised cloud computing ability for managing, building and implementing similar projects.

Organisations have understood that cloud hosting has a lot of potential. To be the best among the rest, selection of the right type of cloud hosting is needed. Thus, you need to know your business and analyze the demands. Once the appropriate type of cloud hosting is selected, you can achieve your business related goals more easily, you can channelize all your efforts to take those strategic steps that will help your business to succeed.

MODEL PAPER–III
END TERM EXAMINATION
SEVENTH SEMESTER (B.TECH)
CLOUD COMPUTING [ETIT–407]

Time : 3 hrs. **M.M. : 75**

Note: *Attempt all questions as per internal choice indicated*

Q.1. (a) What are the various versions of cloud computing? Write few differences between them. **(3)**

Ans. A consumer would call for just a link to the internet and can commence accessing them. The technique of electronic mail conduit and server is all in the cloud that implies on the web and that is fully managed by the Google, Yahoo etcetera. The consumer will get to entry the computer software alone and taking pleasure in the advantages.

Cloud computing is divided into three segments, this kind of as: connectivity, application and storage. Just about every segment has its very own uses and they will give several goods in person and business close to the earth. This will give computer software applications, computations, storage resources, info access without necessitating cloud buyers to know the details, like place of the computing infrastructure.

End to end users can access the cloud dependent documents and applied by the internet internet browser or a mobile application or a desktop, while the company data and computer software are stored on the server at a distant place. The suppliers of cloud apps try to give the greater performance and services as if the software package plans are put in locally on the end-user's computer system.

At the commencing stage of cloud computing is a broader principle of shared expert services and converged infrastructure. This form of surroundings would permit the enterprises to get their program up and to operate more quickly, with less maintenance and simpler manageability, and also lets IT to rapidly adjust the assets like networking, servers and storage, to satisfy unpredictable and fluctuating enterprise demands.

With this cloud computing, the potential of IT can be adjusted easily and speedily to accommodate alterations in need. This will also enable the IT suppliers to make the expenses of IT as transparent. Running in the cloud surroundings requirements IT workers and leaders to develop several capabilities.

Deployment Versions of Cloud Computing:

Public Cloud: This is founded to fulfill the prerequisite of several companies that have identical needs and they want to share the infrastructure. In addition to this economically it is desirable as the assets like workstations, storage are shared and used in the neighbourhood.

Group Cloud: This will share the infrastructure amongst unique enterprises from a distinct group with mutual concerns, regardless of whether they are managed by 3rd

occasion or internally and hosted externally or internally. The expenditures would spread above less people than the public cloud to comprehend the likely of its cost saving. (3)

Q.1. (*b*) What is community cloud?

Ans. A community cloud is a multi-tenant infrastructure that is shared among several organizations from a specific group with common computing concerns. Such concerns might be related to regulatory compliance, such as audit requirements, or may be related to performance requirements, such as hosting applications that require a quick response time.

The goal of a community cloud is to haveparticipating organizations realize the benefits of a public cloud such as multi-tenancy and a pay-as-you-go billing structure but with the added level of privacy, security and policy compliance usually associated with a private cloud. The community cloud can be either on-premises or off-premises, and can be governed by the participating organizations or by a third-party managed service provider (MSP).

Q.1. (*c*) Explain PaaS. (4)

Ans. Platform as a service (PaaS) is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app. PaaS can be delivered in two ways: as a public cloud service from a provider, where the consumer controls software deployment with minimal configuration options, and the provider provides the networks, servers, storage, OS, 'middleware' (i.e.; java runtime, .net runtime, integration, etc.), database and other services to host the consumer's application; or as a private service (software or appliance) inside the firewall, or as software deployed on a public infrastructure as a service.

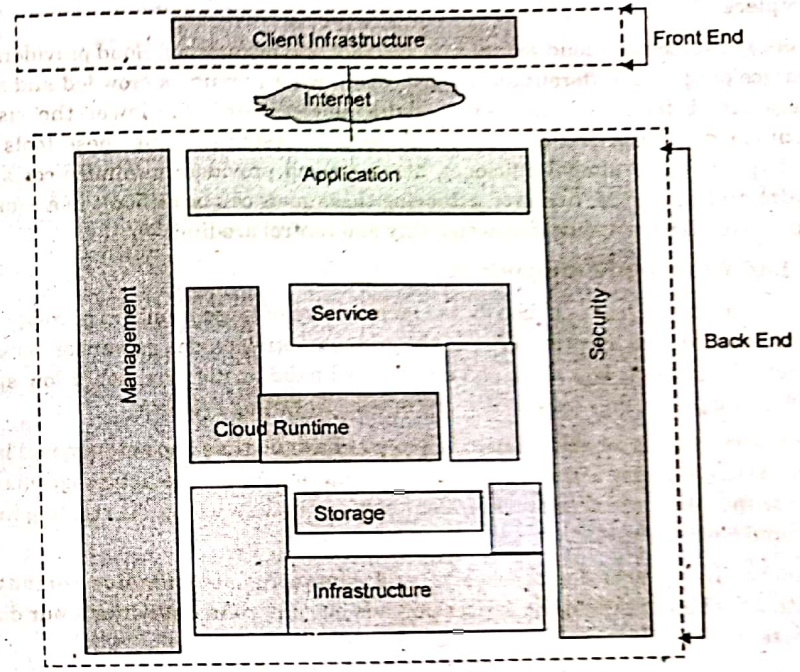
PaaS provides an environment for developers and companies to create, host and deploy applications, saving developers from the complexities of the infrastructure side (setting up, configuring and managing elements such as servers and databases). PaaS can improve the speed of developing an app, and allow the consumer to focus on the application itself. With PaaS, the consumer manages applications and data, while the provider (in public PaaS) or IT department (in private PaaS) manages runtime, middleware, operating system, virtualization, servers, storage and networking. Developmenttools provided by the vendor are customized according to the needs of the user. The user can choose to maintain the software, or have the vendor maintain it.

PaaS offerings may also include facilities for application design, application development, testing and deployment, as well as services such as team collaboration, web service integration, and marshalling, database integration, security, scalability, storage, persistence, state management, application versioning, application instrumentation, and developer community facilitation. Besides the service engineering aspects, PaaS offerings include mechanisms for service management, such as monitoring workflow management, discovery and reservation.

Q.1. (*d*) What are the components of cloud computing architecture? (6)

Ans. Cloud computing architecture refers to the components and subcomponents required for cloud computing. These components typically consist of a front end platform

(fat client, thin client, mobile device), back end platforms (servers, storage), a cloud based delivery, and a network (Internet, Intranet, Intercloud). Combined, these components make up cloud computing architecture.



Front End: The front end refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, Example - Web Browser.

Back End: The back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

Q.1. (*e*) What is service management in cloud computing? (2)

Ans. Cloud service delivery, cloud service management and cloud monitoring tools enable providers to keep up with the continually shifting capacity demands of a highly elastic environment.

Cloud monitoring and cloud service management tools allow cloud providers to ensure optimal performance, continuity and efficiency in virtualized, on-demand environments. These tools — software that manages and monitors networks, systems and applications — enable cloud providers not just to guarantee performance, but also to better orchestrate and automate provisioning of resources.

Cloud monitoring tools, specifically, enable cloud providers to track the performance, continuity and security of all of the components that support service delivery: the

hardware, software and services in the data center and throughout the network infrastructure.

Through successful cloud service management and monitoring, cloud providers can use service quality to differentiate themselves in what remains a crowded and noisy marketplace.

Through successful cloud service management and monitoring, cloud providers can use service quality to differentiate themselves in what remains a crowded and noisy marketplace. Effective cloud service management also helps lower the risk of frequent cloud outages that can jeopardize security systems. Using these tools also supports greater operational efficiency, helping cloud providers minimize costs and maximize profit margins. However, achieving these goals can be difficult in a complex virtual delivery environment where visibility and control are limited.

Q.1. (f) What is grid computing? **(5)**

Ans. Grid computing is a distributed architecture of large numbers of computers connected to solve a complex problem. In the grid computing model, servers or personal computers run independent tasks and are loosely linked by the Internet or low-speed networks. Computers may connect directly or via scheduling systems.

Most applications for grid computing projects have no time dependency, and large projects typically deploy across many countries and continents. Search programs and others use the idle power of computers, also known as cycle-scavenging, running in the background for many weeks.

Another likely area for the use of grid computing is pervasive computing applications, wherein intelligent devices pervade our environment without our direct awareness.

Pervasive computing (also called ubiquitous computing) is the growing trend towards embedding microprocessors in everyday objects so they can communicate information. The words pervasive and ubiquitous mean "existing everywhere." Pervasive computing devices are completely connected and constantly available.

Q.1. (g) Define autonomic computing. **(2)**

Ans. Autonomic computing refers to the self-managing characteristics of distributed computing resources, adapting to unpredictable changes while hiding intrinsic complexity to operators and users.

Q.2. What are the various issues and challenges in cloud computing? (12.5)

Ans. Cloud Computing has already started to revolutionise the way we store and access data. We currently see smartphone applications use cloud computing technology to allow users to store and access data they previously couldn't on a smart device.

Although cloud computing is on its way to becoming a huge success and whilst it is clear there is a lot of business value, there are reservations amongst some CIOs about using some cloud technologies. Let's explore some of the challenges and concerns.

1. Security & Privacy: Security is a great concern for CIOs when moving their data to the cloud. Although security in the cloud is generally reliable and proficient,

CIOs need to know that the cloud provider they chose to work with has a fully secure cloud environment.

CIOs are becoming more reluctant to hand over important data to a third party provider. With the growth in data breaches and the potential financial penalties and loss of reputation for companies who fall victim, moving your private data to an external provider is more daunting than ever.

A well-established cloud computing vendor will ensure they have the latest sophisticated security systems in place to defend against threats.

The cloud provider should be able to answer all the above questions in detail, so that you know exactly where your data is stored and how they will protect your data against internal and external threats. Moreover, how can you retrieve that data if it becomes necessary.

2. Service Quality: Service quality is often one of the most significant factors that businesses cite as a reason for not moving their business applications to the cloud. Often businesses feel as though the SLAs provided by the cloud providers today are not adequate to assure the requirements for running a production application on the cloud, especially those related to availability, performance and scalability.

According to a recent survey 43% of IT decision makers are planning to invest more into cloud computing this year. CIOs need assurance that the company's data will be secure and available, and the service reliable at all times. Ensuring maximum upkeep of the service is paramount for the profitability and sustainability of the business.

Without proficient service quality and comprehensive answers to the above questions, businesses will be reluctant to host their critical infrastructure within the cloud.

3. Downtime & Accessibility: Service quality doesn't have to be compromised when your data is in the cloud. Accessing your data when you need it is a basic requirement from many organisations. The challenge with the cloud is that the data is accessed via an internet connection rather than a local connection. So when the network or internet connection is down, it also means that cloud services are also down; thus data cannot be accessed.

Performance of the cloud infrastructure can be affected by the load, environment and number of users. Ensuring that your cloud infrastructure is resilient to outages is vital. Whilst it is almost impossible to mitigate all server outages, a reputable provider will have robust resilience measures in place to protect your data.

4. Access to data: Cloud-based servers do not always have the most effective or appropriate customer service support systems. CIOs often express their concerns around data ownership and losing control of their data when moving to the cloud, but this shouldn't be an issue. Selecting where and how your data is stored is an important element within the decision making process. Integration is a problem for many organisations. Ensuring that all of the applications are able to seamlessly integrate with one another is also a common challenge.

5. Transition to the cloud: Many cloud adoption challenges are unknown due to the fact that cloud technology is still in its relative infancy. CIOs are challenged deciding on the best way to transition to the cloud and finding a cloud solution that meets the aims of the businesses, whilst improving efficiencies.

Although transitioning to the cloud is a complex and involved process, there isn't one route to success. CIOs must ensure that the proposed solution compliments their business model. There are various ways businesses can transition to the cloud. Whether it's via private, public or hybrid technologies, identifying the right service model for your business is a vital step.

Migrating data poses a number of risks for organisations if not handled correctly. Developing a data migration strategy that integrates seamlessly with the current IT infrastructure is key to overall success.

CIOs are challenged with finding the right service model for their business. Finding a provider that will allow you to create a customised computing environment is vital.

The first step in transitioning to the cloud is being able to identify the challenges and working with your chosen cloud provider to navigate around these barriers in order to facilitate a successful cloud environment for the business. Whether Public, Private or Hybrid, making sure you ask the right questions and understand the risks for your business is imperative.

Q.3. Explain provisioning and manageability in virtualization. **(12.5)**

Ans. Cloud computing has evolved from a single sever being provisioned for a single customer, to a hosting provider and then to a business continuity and disaster recovery provider. Along the way, technology overcame physical limitations with devices like load balancers. WAN optimization compression, caching and content delivery networks (CDNs). We learned to integrate devices-built. APIs, consolidated racks of servers in racks of blades and learned to provide automated provisioning. Cloud architecutre is simply the logical conclusion of the decade's long evolution. We now have unprecedented levels of virtualization of hardware, software, network and storage and are on the verge of putting it all together.

Infrastructure as a service (laaS) is a cloud computing model based on the premise that the entire infrastructure is deployed in an on-demand model. This almost always takes the form of a virtualized infrastructure and infrastructure services that enables the customer to deploy virtual machines as components that are managed through a console. The physical resources-servers, storage and network are maintained by the cloud provider while the infrastucture deployed on top of those components is managed by the user. Note that the user of laaS is almost always a team comprised of IT experts in the required infrastructure components.

laaS leverges the dynamic control plane to enable on-demand scalability through the rapid and automatic provisioning of compute resources. In the case of virtualized architecture-the most common form of laaS architecture this involves the automatic deployment and launch of new instances of a virtual machine. The amount of instances launched will match the amount needed to meet capacity, with the expectation that instances will be decommissioned as demand decreases.

In the layer of the architecture each component is responsible for providing actionable data to the other components and performing specific task to successfully execute an auto-provisioning or decommissioning scenario.

laaS is often considered utility computing because it treats compute resources much like utilities (such as electricity) are treated. When the demand for capacity increases, more computing resource are provided by the provider. As demand for capacity decreases, the amount of computing resources available decreases appropriately. This enables the "on-demand" as well as the "pay-per-use" properties cloud architecture.

Compute resources are one of the most basic components of the cloud-bare-metal resources such as CPU, memory, and disk-that utimately power applications built within the cloud. This might be a hosting service provider with hundreds or thousand of installed server systems waithing to be used by subscribers or it could be a single blade-chassis with extremely dense resources designed for virtual segmentation.

This layer typically conjures the image of a traditional server. Of course, today's systems are much more complicated and versatile. They can have massive numbers of processing cores and memory that can be carved into virtual systems auto-provisioning network interface cards that can dynamically be configured from 10MB to multi-gigabit; and both direct attached and network-attached storage system to support the needs of the application software that will eventually reside on top of it.

Manage Resources: Manage resources are the components required to turn bare metal into usable server platform with the appropriate CPU memory, and disk resources necessary to support the applications that will be built upon them. Manage resources are also responsible for continuing to monitor the resource needs and ensuring that the application receives all the compute resources it needs-and moving the application or finding additional resources.

This components is most often synonymous with virtual machine management or software provisioning system which can take the bare metal and apply operating systems, patches, and application logic and apply higher-level network connectivity (IP addressing and more).

It is necessary to share information between the layer of compute resources and manage resources so as not to waste compute resourcees that could be better used by another application.

Q.4. (a) Explain case study of Google app engine. **(10)**

Ans. Google App Engine (often referred to as GAE or simply App Engine) is a platform as a service (PaaS) cloud computing platform for developing and hosting web applications in Google-managed data centers. Applications are sandboxed and run across multiple servers. App Engine offers automatic scaling for web applications as the number of requests increases for an application, App Engine automatically allocates more resources for the web application to handle the additional demand.

Currently, the supported programming languages are Python, Java (and, by extension, other JVM languages such as Groovy, JRuby, Scala, Clojure), Go, and PHP. Node.js is also available in the Managed VM environment. Google has said

that it plans to support more languages in the future, and that the Google App Engine has been written to be language independent.

Python web frameworks that run on Google App Engine include Django, CherryPy, Pyramid, Flask, web2py and webapp2, as well as a custom Google-written webapp framework and several others designed specifically for the platform that emerged since the release. Any Python framework that supports the WSGI using the CGI adapter can be used to create an application; the framework can be uploaded with the developed application. Third-party libraries written in pure Python may also be uploaded.

Google App Engine supports many Java standards and frameworks. Core to this is the servlet 2.5 technology using the open-source Jetty Web Server, along with accompanying technologies such as JSP. JavaServer Faces operates with some workarounds.

Though the datastore used may be unfamiliar to programmers, it is easily accessed and supported with JPA, JDO, and by the simple low-level API. There are several alternative libraries and frameworks you can use to model and map the data to the datastore such as Objectify, Slim3 and Jello framework. Jello framework is a full-stack Java framework optimized for Google App Engine that includes comprehensive Data Authorization model and a powerful RESTful engine.

Reliability and Support: All billed High-Replication Datastore App Engine applications have a 99.95% uptime SLA.

App Engine is designed in such a way that it can sustain multiple datacenter outages without any downtime. This resilience to downtime is shown by the statistic that the High Replication Datastore saw 0% downtime over a period of a year.

Paid support from Google engineers is offered as part of Premier Accounts. Free support is offered in the App Engine Groups, Stack Overflow, Server Fault, and GitHub, however assistance by a Google staff member is not guaranteed.

Restrictions

- Developers have read-only access to the filesystem on App Engine. Applications can use only virtual filesystems, like gae-filestore.
- App Engine can only execute code called from an HTTP request (scheduled background tasks allow for self calling HTTP requests).
- Users may upload arbitrary Python modules, but only if they are pure-Python; C and Pyrex modules are not supported.
- Java applications may only use a subset (The JRE Class White List) of the classes from the JRE standard edition.
- Datastore cannot use inequality filters on more than one entity property per query.
- A process started on the server to answer a request can't last more than 60 seconds (with the 1.4.0 release, this restriction does not apply to background jobs anymore).
- Does not support sticky sessions (a.k.a. session affinity), only replicated sessions are supported including limitation of the amount of data being serialized and time for session serialization.

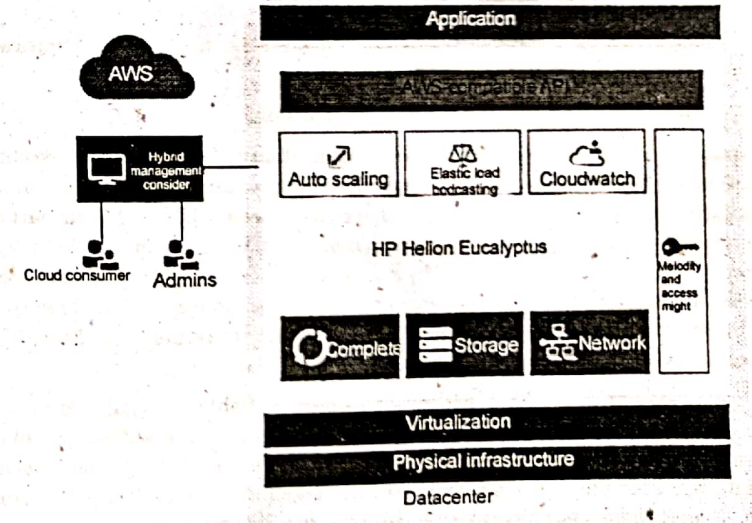
Q.4. (b) What is cloud sim? **(2.5)**

Ans. Cloud sim is a framework for modeling and simulation of cloud computing infrastructures and services. Originally built primarily at the Cloud Computing and Distributed Systems (CLOUDS) Laboratory, The University of Melbourne, Australia, Cloud Sim has become one of the most popular open source cloud simulators in the research and academia. Cloud Sim is completely written in Java.

Q.5. Explain Case study on Eucalyptus advanced cloud application. **(12.5)**

Ans. Eucalyptus is free and open-source computer software for building Amazon Web Services (AWS)-compatible private and hybrid cloud computing environments marketed by the company Eucalyptus Systems. Eucalyptus is the acronym for Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems. Eucalyptus enables pooling compute, storage, and network resources that can be dynamically scaled up or down as application workloads change. Eucalyptus Systems announced a formal agreement with AWS in March 2012 to maintain compatibility.

Eucalyptus commands can manage either Amazon or Eucalyptus instances. Users can also move instances between a Eucalyptus private cloud and the Amazon Elastic Compute Cloud to create a hybrid cloud. Hardware virtualization isolates applications from computer hardware details.



Eucalyptus architecture overview

Terminology:

•**Images** - An image is a fixed collection of software modules, system software, application software, and configuration information that is started from a known baseline (immutable/fixed). When bundled and uploaded to the Eucalyptus cloud, this becomes aEucalyptus machine image (EMI).

• **Instances** - When an image is put to use, it is called an instance. The configuration is executed at runtime, and the Cloud Controller decides where the image will run, and storage and networking is attached to meet resource needs.

• **IP addressing** - Eucalyptus instances can have public and private IP addresses. An IP address is assigned to an instance when the instance is created from an image. For instances that require a persistent IP address, such as a web-server, Eucalyptus supplies elastic IP addresses. These are pre-allocated by the Eucalyptus cloud and can be reassigned to a running instance.

• **Security** - TCP/IP security groups share a common set of firewall rules. This is a mechanism to firewall off an instance using IP address and port block/allow functionality. At TCP/IP layer 2 instances are isolated. If this were not present, a user could manipulate the networking of instances and gain access to neighbouring instances violating the basic cloud tenet of instance isolation and separation.

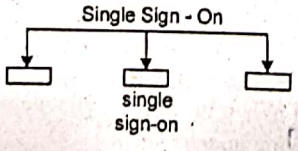
• **Networking** - There are three networking modes. In Managed Mode Eucalyptus manages a local network of instances, including security groups and IP addresses. In System Mode, Eucalyptus assigns a MAC address and attaches the instance's network interface to the physical network through the Node Controller's bridge. System Mode does not offer elastic IP addresses, security groups, or VM isolation. In Static Mode, Eucalyptus assigns IP addresses to instances. Static Mode does not offer elastic IPs, security groups, or VM isolation.

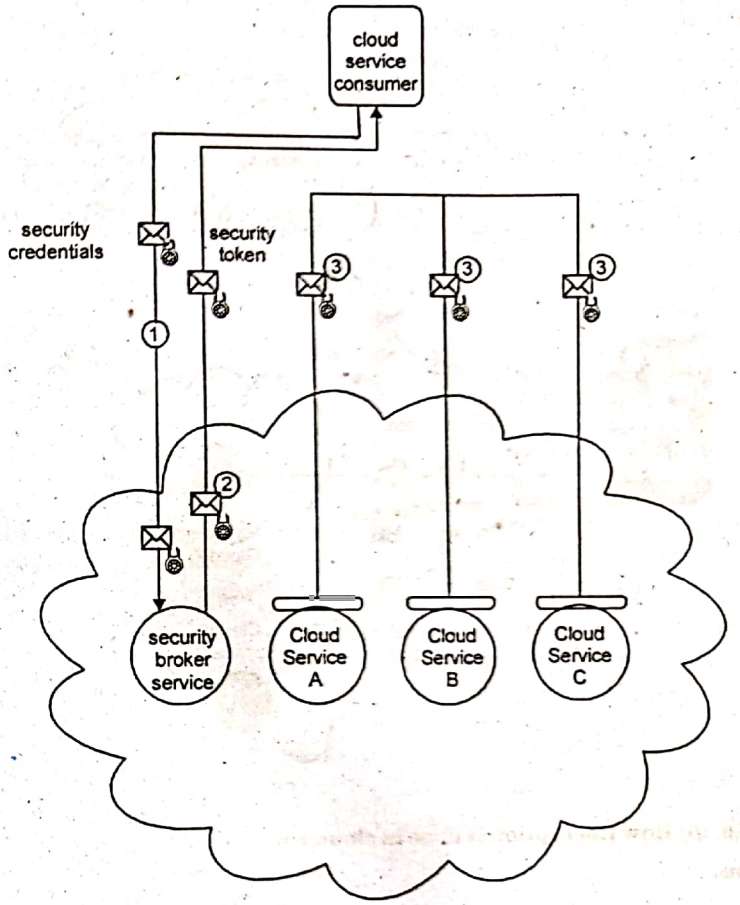
• **Access Control** - A user of Eucalyptus is assigned an identity, and identities can be grouped together for access control.

Q.6. (a) Define SSO cloud security mechanism. **(7)**

Ans. Single Sign-On Propagating the authentication and authorization information for a cloud service consumer across multiple cloud services can be a challenge, especially if multiple cloud services or cloud-based IT resources need to be invoked as part of the same overall runtime activity. The single sign-on (SSO) mechanism enables one cloud service consumer to be authenticated by a security broker, which establishes a security context that is persisted while the cloud service consumer accesses other cloud services or cloud-based IT resources. Otherwise, the service consumer would need to re-authenticate itself with every subsequent request.

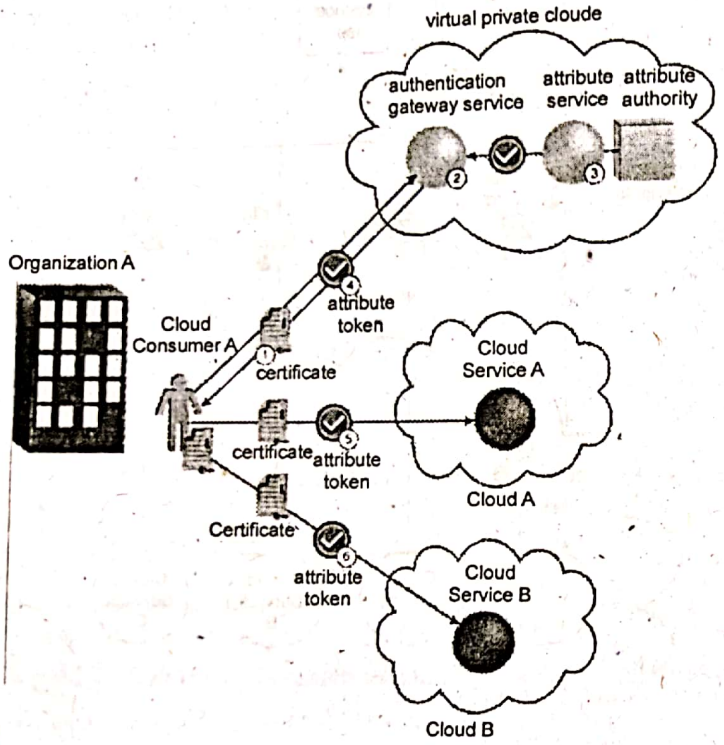
An advantage to the SSO mechanism is how it enables mutually independent services and IT resources to generate and circulate runtime authentication and authorization credentials. The credentials initially provided by the cloud consumer remain valid for the duration of the user's session, while its security context information is shared with the other IT resources. The SSO mechanism's security broker is especially useful when a cloud consumer needs to access cloud services residing on different clouds.





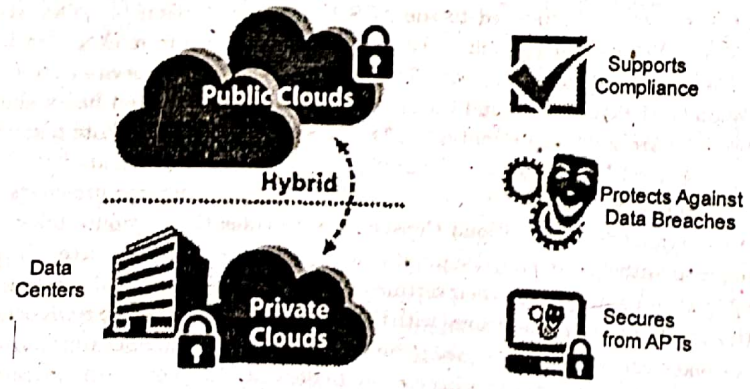
Cloud Consumer A is directed to the AGS for authentication (1). The AGS authenticates Cloud Consumer A and requests an attribute token from Organization A's attribute service (2). Incorporating an STS function, the attribute service issues an attribute token to the AGS for Cloud Consumer A. The attribute token has a short lifespan, typically around 2 to 3 minutes (3). The AGS provides the attribute token to Cloud Consumer A, which supports access control as an SSO model with attributes of the cloud consumer. The attributes will be used by the cloud service providers to determine access privileges (4). Cloud Consumer A provides the attribute token to Service A to prove authentication and support an access decision for its resources. Cloud Consumer A is also required to use their certificate and a holder-of-key (HOK) assertion as part of the attribute exchange protocol with the cloud service. Without an HOK check, the attribute token can be stolen and used by an attacker (5). Using an SSO architecture, the cloud consumer provides the attribute token to Service B to prove authentication and support an access decision for its resources. Again, Cloud Consumer A is required to do an HOK check as part of the attribute exchange protocol (6).

Example



Q.6. (b) How Encryption is done in cloud computing? **(5.5)**

Ans.



For both enterprises using cloud environments and cloud service providers, encryption is a critical requirement for securing data files. Vormetric Cloud Encryption

easily and simply provides the protection, encryption key management, fine-grained access controls and advanced security intelligence data to protect sensitive data-at-rest within public, private or hybrid cloud environments. With Vormetric encryption for your cloud implementations, you can:

• **Support Compliance** – Meet compliance requirements for data file encryption, separation of duties and access controls for protected data, including PCI-DSS and Data Across Borders.

• **Protect against data breach incidents** - Help to protect from data breach incidents with secure encryption, encryption key management and policy-based access controls to protected data files in cloud environments – Including the risks posed by exposure of customer data to cloud providers and of data exposure due to the shared, comingled data storage used to support cloud environments.

•**Secure from advanced persistent threats** – Vormetric Cloud Encryption provides the raw security intelligence about data access to information protected by encryption that enables a Security Information and Event Management (SIEM) solution to recognize an advanced persistent threat, or malicious insider.

The Vormetric Cloud Encryption is a single, scalable solution that can easily encrypt any file, database or application, anywhere it resides on supported operating systems and file systems — without sacrificing application performance and while avoiding key management complexity.

• **Transparent** – Vormetric Cloud Encryption includes seamless encryption key management within the solution and is completely transparent to applications and users – allowing existing processes and usage to continue with no changes. Protecting any data file within cloud environments simply, easily and efficiently.

• **Fine grained access controls** – By design, the Vormetric Cloud Encryption solution supports detailed, policy-based separation of duties to offer a higher degree of security. Prevent cloud administrators, root, network system administrative or unauthorized programmatic access to restricted data while allowing appropriate user and application usage. Lock out the cloud provider's visibility into your data, while also removing the risk that shared data file storage may result in exposure of your private information.

• **Security Intelligence** – Vormetric log data is designed for easy integration with SIEM solutions, providing them with the detailed information on usage, access and access attempts that enables SIEM solutions to identify compromised accounts, applications and even administrators.

Enable Enterprises to Transition Confidently to the Cloud

Vormetric encryption for cloud environments allows organizations to take control of their data protection for public, private and hybrid cloud implementations as well as traditional on-premises data center resources. A single, centrally managed infrastructure across all environments allows for management of cloud data security as well as data security for physical and virtual data center resources.

Cloud Service Providers Create high value services with enhanced data security

For any cloud service – Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), Managed Private Cloud offerings, SaaS hosting or others - the Vormetric Cloud Encryption is a perfect fit; multi-tenant ready, scalable, secure implementation, and including the APIs and interfaces required to work with existing infrastructure.

Unlock new opportunities for your cloud offering by directly addressing the concerns of enterprise customers that use of a cloud service will expose them to the financial costs of losing legally protected data, theft of intellectual property and regulatory non-compliance. Vormetric cloud encryption enables enhanced services with that include higher levels of data protection, meet key components of regulatory standards, and distinguish your cloud encryption solution from competitors.

e

FIRST TERM EXAMINATION [SEPT. 2016]
SEVENTH SEMESTER [B.TECH]
CLOUD COMPUTING [ETIT–407]

Time: 1½ hrs. **M.M. : 30**

Note: *Attempt three questions including Q. no. 1, which is compulsory.*

Q. 1. Write short note on following :

(a) : Peer to Peer variant of distributed computing.

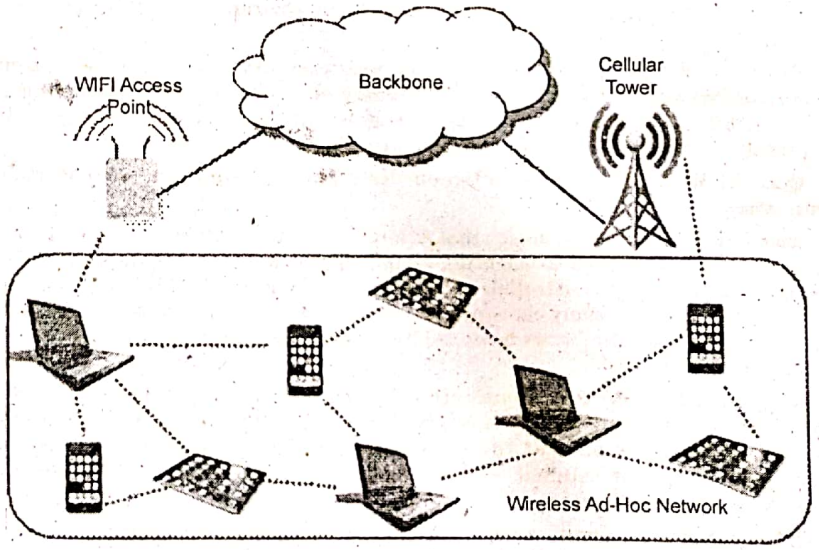
Ans: Refer Q. no. 1(e) page no. 3 Model paper I End Term Exam.

(b) : MANETs .

Ans: A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic[1]. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).



With the rapid development of wireless communication technology and the extensive usage of mobile communication equipment, wireless ad hoc networks are getting more and more attention. Nowadays, wireless ad hoc networks are not only used in military, but also been applied to civilian application, including home area networks, mobile communication networks, and so on. Wireless ad hoc networks are envisioned to be

one of the most important parts of future Internet. However, in civilian wireless ad hoc networks, nodes often belong to different parties who have their own interests and always want to maximize their own benefits. Such selfish behaviour can hurt the robustness and availability of wireless ad hoc networks. In our work, we adopt solution concepts from microeconomics and game theory to study important incentive problems in wireless ad hoc networks, including spectrum allocation and routing. Our objective is to achieve a series of cooperation-incentive mechanisms with high availability, low cost, and high adaptability, through the following four closely related studies: game-theoretic problem modeling, impossibility analyzing, strong incentive mechanism designing, and systematic evaluation methodology developing.

(c) Autonomic computing.

Ans. Autonomic computing refers to the self-managing characteristics of distributed computing resources, adapting to unpredictable changes while hiding intrinsic complexity to operators and users.

(d) Grid Computing.

Ans. Grid computing is a distributed architecture of large numbers of computers connected to solve a complex problem. In the grid computing model, servers or personal computers run independent tasks and are loosely linked by the Internet or low-speed networks. Computers may connect directly or via scheduling systems.

Most applications for grid computing projects have no time dependency, and large projects typically deploy across many countries and continents. Search programs and others use the idle power of computers, also known as cycle-scavenging, running in the background for many weeks.

Another likely area for the use of grid computing is pervasive computing applications, wherein intelligent devices pervade our environment without our direct awareness.

Pervasive computing (also called ubiquitous computing) is the growing trend towards embedding microprocessors in everyday objects so they can communicate information. The words pervasive and ubiquitous mean "existing everywhere." Pervasive computing devices are completely connected and constantly available.

Q.2. (a) Write difference between distributed computing and Parallel computing.

Ans. Parallel computing means that different activities happen at the same time. The term was mostly used in scientific computing (consumer computers until very recently simply were not parallel) where it typically means: spread out a single application over many many cores/processors/processes to get it done bigger/faster. Current big parallel computers have 100 thousand to a million parallel processors/cores/threads/whatever.

Distributed computing comes from the business world where you have distributed systems such as airline reservation systems, where many people access and modify the same data at the same time. The machinery involved here is typically much looser coupled, and the activities in a distributed system are typically far less synchronized.

Q.2. (b) Discuss various areas of applications of cloud computing. (1½)

Ans. 1. Infrastructure as a service (IaaS) and platform as a service (PaaS)

When it comes to IaaS, using an existing infrastructure on a pay-per-use scheme seems to be an obvious choice for companies saving on the cost of investing to acquire, manage and maintain an IT infrastructure. There are also instances where organizations turn to PaaS for the same reasons while also seeking to increase the speed of development on a ready-to-use platform to deploy applications.

2. Private cloud and hybrid cloud: Among the many incentives for using cloud, there are two situations where organizations are looking into ways to assess some of the applications they intend to deploy into their environment through the use of a cloud (specifically a public cloud). While in the case of test and development it may be limited in time, adopting a hybrid cloud approach allows for testing application workloads, therefore providing the comfort of an environment without the initial investment that might have been rendered useless should the workload testing fail.

Another use of hybrid cloud is also the ability to expand during periods of limited peak usage, which is often preferable to hosting a large infrastructure that might seldom be of use. An organization would seek to have the additional capacity and availability of an environment when needed on a pay-as you-go basis.

3. Test and development: Probably the best scenario for the use of a cloud is a test and development environment. This entails securing a budget, setting up your environment through physical assets, significant manpower and time. Then comes the installation and configuration of your platform. All this can often extend the time it takes for a project to be completed and stretch your milestones.

With cloud computing, there are now readily available environments tailored for your needs at your fingertips. This often combines, but is not limited to, automated provisioning of physical and virtualized resources.

4. Big data analytics: One of the aspects offered by leveraging cloud computing is the ability to tap into vast quantities of both structured and unstructured data to harness the benefit of extracting business value.

Retailers and suppliers are now extracting information derived from consumers' buying patterns to target their advertising and marketing campaigns to a particular segment of the population. Social networking platforms are now providing the basis for analytics on behavioral patterns that organizations are using to derive meaningful information.

5. File storage: Cloud can offer you the possibility of storing your files and accessing, storing and retrieving them from any web-enabled interface. The web services interfaces are usually simple. At any time and place you have high availability, speed, scalability and security for your environment. In this scenario, organizations are only paying for the amount of storage they are actually consuming, and do so without the worries of overseeing the daily maintenance of the storage infrastructure.

There is also the possibility to store the data either on or off premises depending on the regulatory compliance requirements. Data is stored in virtualized pools of storage hosted by a third party based on the customer specification requirements.

6. Disaster recovery: This is yet another benefit derived from using cloud based on the cost effectiveness of a disaster recovery (DR) solution that provides for a faster recovery from a mesh of different physical locations at a much lower cost that the traditional DR site with fixed assets, rigid procedures and a much higher cost.

7. Backup: Backing up data has always been a complex and time-consuming operation. This included maintaining a set of tapes or drives, manually collecting them and dispatching them to a backup facility with all the inherent problems that might happen in between the originating and the backup site. This way of ensuring a backup is performed is not immune to problems such as running out of backup media , and there is also time to load the backup devices for a restore operation, which takes time and is prone to malfunctions and human errors.

Q.3. (a) What are features of cloud in cloud computing ?

Ans : Refer Q. no. 1(f) page no. 3 Model paper I End Term Exam.

Q.3. (b) Describe service model of cloud in cloud architecture .

Ans : Refer Q. no. 2 page no. 5 Model paper I End Term Exam.

Q.4. Discuss various deployment model of cloud in cloud architecture.

Ans : Cloud hosting deployment models represent the exact category of cloud environment and are mainly distinguished by the proprietorship, size and access. It tells about the purpose and the nature of the cloud. Most of the organisations are willing to implement cloud as it reduces the capital expenditure and controls operating cost. In order to know which deployment model matches your website requirements it is necessary to know the four deployment models.

Public Cloud: is a type of cloud hosting in which the cloud services are delivered over a network which is open for public usage. This model is a true representation of cloud hosting; in this the service provider renders services and infrastructure to various clients. The customers do not have any distinguishability and control over the location of the infrastructure. From the technical viewpoint, there may be slight or no difference between private and public clouds' structural design except in the level of security offered for various services given to the public cloud subscribers by the cloud hosting providers.

Public cloud is better suited for business requirements which require managing the load; host application that is SaaS-based and manage applications that many users consume. Due to the decreased capital overheads and operational cost this model is economical. The dealer may provide the service free or in the form of the license policy like pay per user. The cost is shared by all the users, so public cloud profits the customers more by achieving economies of scale. Public cloud facilities may be availed free an e.g. of a public cloud is Google.

Private Cloud: is also known as internal cloud; the platform for cloud computing is implemented on a cloud-based secure environment that is safeguarded by a firewall which is under the governance of the IT department that belongs to the particular corporate. Private cloud as it permits only the authorized users, gives the organisation greater and direct control over their data. What exactly constitutes a private cloud? It is difficult to define because when it's classified according to the services there are significant variations. Whether the physical computers are hosted internally or externally they provide the resources from a distinct pool to the private cloud services. Businesses that have dynamic or unforeseen needs, assignments which are mission critical, security alarms, management demands and uptime requirements are better suited to adopt private cloud. Obstacles with regards to security can be evaded in a private cloud, but in case of natural disaster and internal data theft the private cloud may be prone to vulnerabilities.

Hybrid Cloud: is a type of cloud computing, which is integrated. It can be an arrangement of two or more cloud servers, i.e. private, public or community cloud that is bound together but remain individual entities. Benefits of the multiple deployment models are available in a hybrid cloud hosting. A hybrid cloud can cross isolation and overcome boundaries by the provider; hence, it cannot be simply categorized into public, private or community cloud. It permits the user to increase the capacity or the capability by aggregation, assimilation or customization with another cloud package / service. In a hybrid cloud, the resources are managed and provided either in-house or by external providers. It is an adaptation among two platforms in which the workload exchanges between the private cloud and the public cloud as per the need and demand.

Resources that are non-critical like development and test workloads can be housed in the public cloud that belongs to a third-party provider. While the workloads that are critical or sensitive must be housed internally. Consider an e-commerce website, which is hosted on a private cloud that gives security and scalability, since security is not a prime concern for their brochure site it is hosted on a public cloud which is more economical as compared to a private cloud. Businesses that have more focus on security and demand for their unique presence can implement hybrid cloud as an effective business strategy. When facing demand spikes the additional resources that are required by a particular application can be accessed from the public cloud. This is termed as cloud bursting and is available with the hybrid cloud.

Organisations can use the hybrid cloud model for processing big data. On a private cloud, it can retain sales, business and various data and can initiate analytical queries over the public cloud as the public cloud is effective to meet the demand spikes. Hybrid cloud hosting is enabled with features like scalability, flexibility and security. If one is ready to overlook a few challenges like application program interface incompatibility, network connectivity issues and capital expenditures, then the hybrid cloud would be an appropriate option.

Community Cloud: is a type of cloud hosting in which the setup is mutually shared between many organisations that belong to a particular community, i.e. banks and trading firms. It is a multi-tenant setup that is shared among several organisations that belong to a specific group which has similar computing apprehensions. The community members generally share similar privacy, performance and security concerns. The main intention of these communities is to achieve their business related objectives. A community cloud may be internally managed or it can be managed by a third party provider. It can be hosted externally or internally. The cost is shared by the specific organisations within the community, hence, community cloud has cost saving capacity. A community cloud is appropriate for organisations and businesses that work on joint ventures, tenders or research that needs a centralised cloud computing ability for managing, building and implementing similar projects.

Organisations have understood that cloud hosting has a lot of potential. To be the best among the rest, selection of the right type of cloud hosting is needed. Thus, you need to know your business and analyze the demands. Once the appropriate type of cloud hosting is selected, you can achieve your business related goals more easily, you can channelize all your efforts to take those strategic steps that will help your business to succeed.

END TERM EXAMINATION [DEC. 2016]
SEVENTH SEMESTER [B.TECH]
CLOUD COMPUTING [ETIT–407]

M.M. : 75

Time : 3 hrs.

NOTE: *Attempt any five questions including Q. no. 1, which is compulsory.*

(5×5=25)

Q. Answer the following.

Q.1. (a) What are the milestones that led to cloud computing ? Explain.

Ans: Three major milestones have led to Cloud computing: mainframe computing, cluster computing, and Grid computing.

(a) Mainframes: These were the first examples of large computational facilities leveraging multiple processing units. Mainframes were powerful, highly reliable computers specialized for large data movement and massive IO operations. They were mostly used by large organizations for bulk data processing such as online transactions, enterprise resource planning, and other operations involving the processing of significant amount of data. Even though mainframes cannot be considered distributed systems, they were offering large computational power by using multiple processors, which were presented as a single entity to users. One of the most attractive features of mainframes was the ability to be highly reliable computers that were "always on" and capable of tolerating failures transparently. No system shut down was required to replace failed components, and the system could work without interruptions. Batch processing was the main application of mainframes. Now their popularity and deployments have reduced, but evolved versions of such systems are still in use for transaction processing (i.e., online banking, airline ticket booking, supermarket and telcos, and government services).

(b) Clusters : Cluster computing started as a low-cost alternative to the use of mainframes and supercomputers. The technology advancement that created faster and more powerful mainframes and supercomputers has eventually generated an increased availability of cheap commodity machines as a side effect. These machines could then be connected by a high-bandwidth network and controlled by specific software tools that manage them as a single system. By starting from the 1980s, clusters became the standard technology for parallel and high-performance computing. Being built by commodity machines, they were cheaper than mainframes, and made available high-performance computing to a large number of groups, including universities and small research labs. Cluster technology considerably contributed to the evolution of tools and framework for distributed computing, some of them include:

Condor , Parallel Virtual Machine (PVM), and Message Passing Interface (MPI). One of the MPI is a specification for an API that allows many computers to communicate with one another. It defines a language independent protocol that supports point-to-point and collective communication. MPI has been designed for high-performance, scalability, and portability. At present, it is one of the dominant paradigms for developing parallel applications.

Attractive features of clusters was that the computational power of commodity machines could be leveraged to solve problems previously manageable only on expensive supercomputers. Moreover, clusters could be easily extended if more computational power was required.

(c) Grids: Grid computing appeared in the early 90s as an evolution of cluster computing. In analogy with the power grid, Grid computing proposed a new approach to access large computational power, huge storage facilities, and a variety of services. Users can "consume" resources in the same way as they use other utilities such as

power, gas, and water. Grids initially developed as aggregation of geographically dispersed clusters by means of Internet connection. These clusters belonged to different organizations and arrangements were made among them to share the computational power. Different from a "large cluster", a computing grid was a dynamic aggregation of heterogeneous computing nodes, and its scale was nationwide or even worldwide. Several reasons made possible the diffusion of computing grids: (*i*) clusters were now resources quite common; (*ii*) they were often under-utilized; (*iii*) new problems were requiring computational power going beyond the capability of single clusters; (*iv*) the improvements in networking and the diffusion of Internet made possible long distance high bandwidth connectivity. All these elements led to the development of grids, which now serve a multitude of users across the world.

Cloud computing is often considered as the successor of Grid computing. In reality, it embodies aspects of all of these three major technologies. Computing Clouds are deployed on large data centers hosted by a single organization that provides services to others. Clouds are characterized by the fact of having virtually infinite capacity, being tolerant to failures, and always on as in the case of mainframes.

In many cases, the computing nodes that form the infrastructure of computing Clouds are commodity machines as in the case of clusters. The services made available by a Cloud vendor are consumed on a pay-per-use basis and Clouds implement fully the utility vision introduced by Grid computing.

Q.1. (b) What is virtualization ? What are its benefits ?

Ans: virtualization is a single system file that acts like a real computer, and can be thought of as a logical representation of a server or computer. How do you know if virtualization is the right way to proceed for your business?

Let's look into how virtualization works and what it might add to your enterprise. Multiple virtual computers live on one piece of hardware. You can have a virtual server or virtual desktop. Virtualization is accomplished through software. The concept of virtualization is fairly encompassing and can include devices, servers, operating systems, applications and networks.

Benefits of Virtualization in Cloud Computing:

Dynamic Architecture: Virtualization results in a more dynamic and flexible architecture. Virtual servers are easy to create and maintain. Storage for the virtual machine grows as needed. A virtual machine can run its own operating system. For example, even though the great majority of your programs are Windows based, one aspect of your business might require Linux. Or you may need to run software on an obsolete platform. Virtualization allows many operating systems to co-exist on the same hardware.

Easy Beta Testing Environment: You can also do beta testing in a virtual development environment and avoid corruption of other software. A crash on one virtual computer is confined to that system and other virtual computers on the same hardware are unaffected. If there's one workstation hardware failure, the user can go to a functioning workstation and pick up exactly where she left off.

Quick Back Up and Recovery: Not only does virtualization support the present tense, it's a simple matter to go back in time as well. With the snapshotting function of virtualization, you capture an image of a server at a given moment and can revert to that place anytime. To also prevent downtimes most virtual server environments such as iSySair Cloud Hosting, are equipped with the ability to automatically backup data at a second data center to ensure maximum data security even if there is a disaster, or technical glitch with one data center.

Cost Reduction: Perhaps the most compelling reason to virtualize is a reduced Total Cost of Ownership (TCO). There is a reduced data center footprint because multiple servers share space on one machine. That consolidation translates into a lower energy bill, and the subsequent reduced energy usage is good for the environment. Virtualized machines reduce downtime, as data can be migrated with minimal interruption, which

is known as live migration. Because data is on the server and not spread out over many desktops, virtualization offers increased security, with easier and centralized administration.

Q.1. (c) Mention the characterstics of PaaS solution.

Ans: The Essential Characteristics of PaaS :

Runtime Framework: This is the "software stack" aspect of PaaS, and perhaps the aspect that comes first to mind for most people. The PaaS runtime framework executes end-user code according to policies set by the application owner and cloud provider. PaaS runtime frameworks come in many flavors, some based on traditional application runtimes, others based on 4GL and visual programming concepts, and some with pluggable support for multiple application runtimes.

Abstraction: Platform-oriented cloud platforms are distinguished by the higher level of abstraction they provide. With IaaS, the focus is on delivering to users "raw" access to physical or virtual infrastructure. In contrast, with PaaS, the focus is on the applications that the cloud must support. Whereas an IaaS cloud gives the user a bunch of virtual machines that must be configured and to which application components must be deployed, a PaaS cloud provides the user a way to deploy her applications into a seemingly limitless pool of computing resources, eliminating the complexity of deployment and infrastructure configuration.

Automation: A PaaS environment is a bit like a swan on a pond — graceful and elegant above the water, and paddling its little legs off below the water. The aforementioned abstraction provides the elegant user experience "above the water," while high levels of automation provide the "paddling" beneath the surface. PaaS environments automate the process of deploying applications to infrastructure, configuring application components, provisioning and configuring supporting technology like load balancers and databases, and managing system change based on policies set by the user.

While IaaS is known for its ability to shift capital costs to operational costs through outsourcing, only PaaS is able to slash costs across the development, deployment and management aspects of the application lifecycle.

Cloud Services: PaaS offerings provide developers and architects with services and APIs that help simplify the job of delivering elastically scalable, highly available cloud applications. These cloud services provide a wide variety of capabilities, and in many instances are key differentiators among competing PaaS offerings.

Examples of cloud services include services and APIs for distributed caching, queuing and messaging, workload management, file and data storage, user identity, analytics, and more. By providing built-in cloud services, platform offerings eliminate the need to integrate many disparate components and decrease time-to-market for applications on the platform.

Q.1.(d) Distinguish the features of Customer relationship management (CRM) and enterprise resourse planning (ERP) applications.

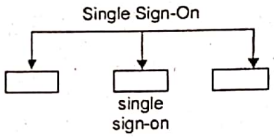
Ans: CRM at its simplest is systems and processes for managing a company's interactions with current and potential customers. When we talk about CRM we usually are talking about CRM Software. CRM software is used to organise, automate and synchronise sales, marketing and customer service. CRM has developed to include all areas of the customer experience, keeping the customer happy and in turn keeping them loyal and more valuable to your business. It is the process of identifying potential leads/prospects, nurturing them and guiding them through the sales process to close the business. Once they are a customer it is ensuring that you maintain that relationship and encourage repeat business – either more frequent orders or higher value.

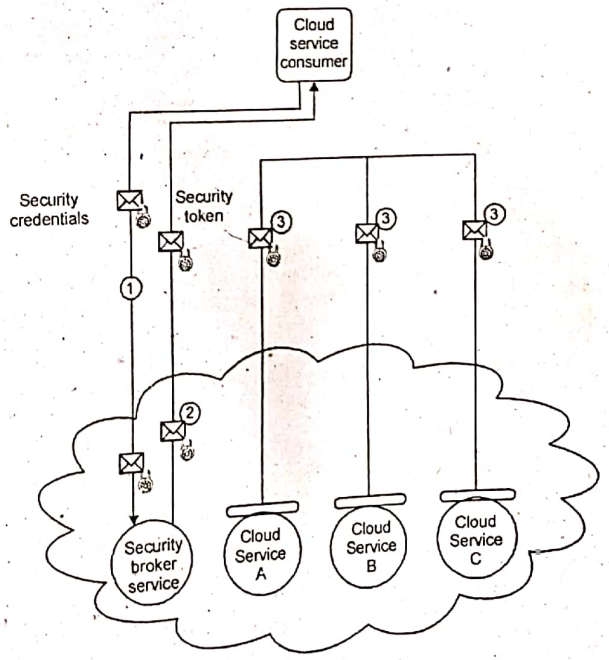
Where CRM manages the customer, ERP is used to manage the business. ERP is a system for improving the efficiency of business processes. Like CRM, ERP allows for the rapid sharing of standardised information throughout all departments. Employees all enter information into the ERP system, creating a real-time, enterprise-wide snapshot. Problems in any area will automatically create alerts in other affected areas. This allows departments to begin planning for issues before they become a problem in that department. In short, by allowing the business to focus on the data, instead of the operations, ERP provides a method for streamlining business processes across the board. Microsoft Dynamics ERP can directly integrate with Dynamics CRM.

ERP and CRM systems use different approaches to increase profitability. ERP focuses on reducing overheads and cutting costs. By making business processes more efficient, ERP reduces the amount of capital spent on those processes. CRM works to increase profits by producing greater sales volume.

Q.1.(e) Mention the advantages of Single Sign-On (SSO).

Ans: Single Sign-On Propagating the authentication and authorization information for a cloud service consumer across multiple cloud services can be a challenge, especially if multiple cloud services or cloud-based IT resources need to be invoked as part of the same overall runtime activity. The single sign-on (SSO) mechanism enables one cloud service consumer to be authenticated by a security broker, which establishes a security context that is persisted while the cloud service consumer accesses other cloud services or cloud-based IT resources. Otherwise, the service consumer would need to re-authenticate itself with every subsequent request.

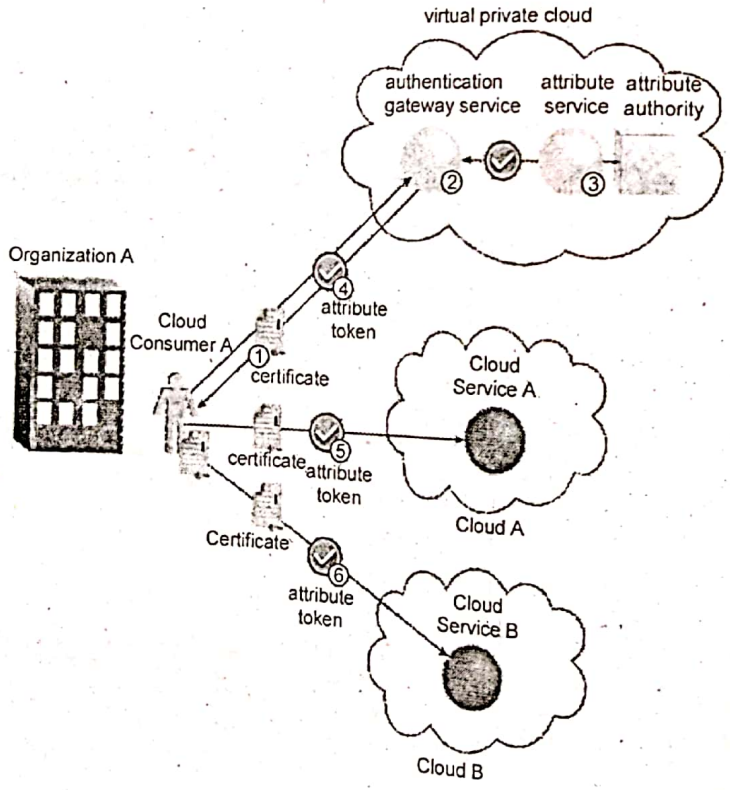




An advantage to the SSO mechanism is how it enables mutually independent services and IT resources to generate and circulate runtime authentication and authorization credentials. The credentials initially provided by the cloud consumer remain valid for the duration of the user's session, while its security context information is shared with the other IT resources. The SSO mechanism's security broker is especially useful when a cloud consumer needs to access cloud services residing on different clouds.

Cloud Consumer A is directed to the AGS for authentication (1). The AGS authenticates Cloud Consumer A and requests an attribute token from Organization A's attribute service (2). Incorporating an STS function, the attribute service issues an attribute token to the AGS for Cloud Consumer A. The attribute token has a short lifespan, typically around 2 to 3 minutes (3). The AGS provides the attribute token to Cloud Consumer A, which supports access control as an SSO model with attributes of the cloud consumer. The attributes will be used by the cloud service providers to determine access privileges (4). Cloud Consumer A provides the attribute token to Service A to prove authentication and support an access decision for its resources. Cloud Consumer A is also required to use their certificate and a holder-of-key (HOK) assertion as part of the attribute exchange protocol with the cloud service. Without an HOK check, the attribute token can be stolen and used by an attacker (5). Using an SSO architecture, the cloud consumer provides the attribute token to Service B to prove authentication and support an access decision for its resources. Again, Cloud Consumer A is required to do an HOK check as part of the attribute exchange protocol (6).

Example:



Q.2. (a) Compare the following: **(6)**

(i) Parallel computing

Ans: Refer Q. no. 1(a) page no. 1 Model paper I End term exam .

(ii) Grid computing

Ans: Grid computing is a distributed architecture of large numbers of computers connected to solve a complex problem. In the grid computing model, servers or personal computers run independent tasks and are loosely linked by the Internet or low-speed networks. Computers may connect directly or via scheduling systems.

Most applications for grid computing projects have no time dependency, and large projects typically deploy across many countries and continents. Search programs and others use the idle power of computers, also known as cycle-scavenging, running in the background for many weeks.

Another likely area for the use of grid computing is pervasive computing applications, wherein intelligent devices pervade our environment without our direct awareness.

Pervasive computing (also called ubiquitous computing) is the growing trend towards embedding microprocessors in everyday objects so they can communicate information. The words pervasive and ubiquitous mean "existing everywhere." Pervasive computing devices are completely connected and constantly available.

(iii) Distributed computing

Ans: Distributed computing is a field of computer science that studies distributed systems. A distributed system is a model in which components located on networked computers communicate and coordinate their actions by passing messages. The components interact with each other in order to achieve a common goal. Three significant characteristics of distributed systems are: concurrency of components, lack of a global clock, and independent failure of components. Examples of distributed systems vary from SOA-based systems to massively multiplayer online games to peer-to-peer applications.

A computer program that runs in a distributed system is called a distributed program, and distributed programming is the process of writing such programs. There are many alternatives for the message passing mechanism, including pure HTTP, RPC-like connectors and message queues.

A goal and challenge pursued by some computer scientists and practitioners in distributed systems is location transparency; however, this goal has fallen out of favour in industry, as distributed systems are different from conventional non-distributed systems, and the differences, such as network partitions, partial system failures, and partial upgrades, cannot simply be "papered over" by attempts at "transparency" .

Q.2. (b) Describe the deployment and accessing cloud environment models in detail. **(6.5)**

Ans: Cloud hosting deployment models represent the exact category of cloud environment and are mainly distinguished by the proprietorship, size and access. It tells about the purpose and the nature of the cloud. Most of the organisations are willing to implement cloud as it reduces the capital expenditure and controls operating cost. In order to know which deployment model matches your website requirements it is necessary to know the four deployment models.

Public Cloud: is a type of cloud hosting in which the cloud services are delivered over a network which is open for public usage. This model is a true representation of cloud hosting; in this the service provider renders services and infrastructure to various clients. The customers do not have any distinguishability and control over the location of the infrastructure. From the technical viewpoint, there may be slight or no difference between private and public clouds' structural design except in the level of security

offered for various services given to the public cloud subscribers by the cloud hosting providers.

Public cloud is better suited for business requirements which require managing the load; host application that is SaaS-based and manage applications that many users consume. Due to the decreased capital overheads and operational cost this model is economical. The dealer may provide the service free or in the form of the license policy like pay per user. The cost is shared by all the users, so public cloud profits the customers more by achieving economies of scale. Public cloud facilities may be availed free an e.g. of a public cloud is Google.

Private Cloud: is also known as internal cloud; the platform for cloud computing is implemented on a cloud-based secure environment that is safeguarded by a firewall which is under the governance of the IT department that belongs to the particular corporate. Private cloud as it permits only the authorized users, gives the organisation greater and direct control over their data. What exactly constitutes a private cloud? It is difficult to define because when it's classified according to the services there are significant variations. Whether the physical computers are hosted internally or externally they provide the resources from a distinct pool to the private cloud services. Businesses that have dynamic or unforeseen needs, assignments which are mission critical, security alarms, management demands and uptime requirements are better suited to adopt private cloud. Obstacles with regards to security can be evaded in a private cloud, but in case of natural disaster and internal data theft the private cloud may be prone to vulnerabilities.

Hybrid Cloud: is a type of cloud computing, which is integrated. It can be an arrangement of two or more cloud servers, i.e. private, public or community cloud that is bound together but remain individual entities. Benefits of the multiple deployment models are available in a hybrid cloud hosting. A hybrid cloud can cross isolation and overcome boundaries by the provider; hence, it cannot be simply categorized into public, private or community cloud. It permits the user to increase the capacity or the capability by aggregation, assimilation or customization with another cloud package / service. In a hybrid cloud, the resources are managed and provided either in-house or by external providers. It is an adaptation among two platforms in which the workload exchanges between the private cloud and the public cloud as per the need and demand.

Resources that are non-critical like development and test workloads can be housed in the public cloud that belongs to a third-party provider. While the workloads that are critical or sensitive must be housed internally. Consider an e-commerce website, which is hosted on a private cloud that gives security and scalability, since security is not a prime concern for their brochure site it is hosted on a public cloud which is more economical as compared to a private cloud. Businesses that have more focus on security and demand for their unique presence can implement hybrid cloud as an effective business strategy. When facing demand spikes the additional resources that are required by a particular application can be accessed from the public cloud. This is termed as cloud bursting and is available with the hybrid cloud.

Organisations can use the hybrid cloud model for processing big data. On a private cloud, it can retain sales, business and various data and can initiate analytical queries over the public cloud as the public cloud is effective to meet the demand spikes. Hybrid cloud hosting is enabled with features like scalability, flexibility and security. If one is ready to overlook a few challenges like application program interface incompatibility, network connectivity issues and capital expenditures, then the hybrid cloud would be an appropriate option.

Community Cloud: is a type of cloud hosting in which the setup is mutually shared between many organisations that belong to a particular community, i.e. banks and trading firms. It is a multi-tenant setup that is shared among several organisations

that belong to a specific group which has similar computing apprehensions. The community members generally share similar privacy, performance and security concerns. The main intention of these communities is to achieve their business related objectives. A community cloud may be internally managed or it can be managed by a third party provider. It can be hosted externally or internally. The cost is shared by the specific organisations within the community, hence, community cloud has cost saving capacity. A community cloud is appropriate for organisations and businesses that work on joint ventures, tenders or research that needs a centralised cloud computing ability for managing, building and implementing similar projects.

Organisations have understood that cloud hosting has a lot of potential. To be the best among the rest, selection of the right type of cloud hosting is needed. Thus, you need to know your business and analyze the demands. Once the appropriate type of cloud hosting is selected, you can achieve your business related goals more easily, you can channelize all your efforts to take those strategic steps that will help your business to succeed.

Q.3. (a) Discuss the scalability and security issues in cloud computing. (4)

Ans: Scalability

The ability to scale on demand is one of the biggest advantages of cloud computing. Often, when considering the range of benefits of cloud, it is difficult to conceptualize the power of scaling on-demand, but organizations of all kinds enjoy tremendous benefits when they correctly implement auto scaling. Many of the issues and challenges experienced before the advent of cloud are no longer issues: Engineers now working on cloud implementations remember working at companies that feared the Slashdot effect – a massive influx of traffic that would cause servers to fail.

With AWS auto scaling, we can greatly reduce the risks associated with traffic overflow causing server failure. Furthermore, and somewhat contrary to our intuition, auto scaling can reduce costs as well. Instead of running instances based on projected (assumed) usage and leaving excess resources in place as a buffer, we only run resources matched to actual usage, on a moment-to-moment basis.

These price and scalability advantages are not without their own complexities. While we can scale on demand, applications need to be able to scale with the environment. This might seem straightforward when running a website benefitting from an elastic load balancer distributing traffic across multiple instance that scales with increased demand. Yet, there are other considerations that need to be made when accounting for scaling session information, uploads, and data.

Security issues

(a) Data Storage Security

(b) Data Transmission Security

(c) Application Security

(d) Security on Cloud Integrity

(e) Security related to Third-Party

When running an application on cloud system, requires configuring a suitable backup routine so that it is safe in the event of a data-loss incident. It does not matter if this is a corrupt entry in a database file, deletion of user data or even a more disastrous data loss. Usually, the data requires to backup to portable media on a regular basis. IaaS or explicit service implementation modules (PaaS) are responsibility of a cloud computing system. Cloud system is responsible for determining and eventually instantiating a free- to-use instance of requested service implementation type on request of any user. Then, the address for accessing that new instance is to be communicated back to the requesting user. Generally, this task requires some metadata on the service implementation modules, at least for identification purposes. For the specific PaaS,

case of web services provided via the cloud, this metadata may also cover all web service description documents related to the specific service implementation. For instance, the web service description document itself should not only be present within the service implementation instance, but also be provided by the cloud system in order to deliver it to its users on demand. Most of these metadata descriptions are usually required by any user prior to service invocation in order to determine the appropriateness of a service for a specific purpose. Thus, these metadata should be stored outside of the cloud system, resulting in a necessity to maintain the correct association of metadata and service implementation instance

Q.3. (*b*) Explain autonomic computing. **(4)**

Ans: Autonomic computing refers to the self-managing characteristics of distributed computing resources, adapting to unpredictable changes while hiding intrinsic complexity to operators and users.

Q.3. (c) Explain the issues and challenges in cloud computing. **(4.5)**

Ans : Cloud Computing has already started to revolutionise the way we store and access data. We currently see smartphone applications use cloud computing technology to allow users to store and access data they previously couldn't on a smart device.

Although cloud computing is on its way to becoming a huge success and whilst it is clear there is a lot of business value, there are reservations amongst some *CIOs* about using some cloud technologies. Let's explore some of the challenges and concerns.

1. Security & Privacy: Security is a great concern for *CIOs* when moving their data to the cloud. Although security in the cloud is generally reliable and proficient,

CIOs need to know that the cloud provider they choose to work with has a fully secure cloud environment.

CIOs are becoming more reluctant to hand over important data to a third party provider. With the growth in data breaches and the potential financial penalties and loss of reputation for companies who fall victim, moving your private data to an external provider is more daunting than ever.

A well-established cloud computing vendor will ensure they have the latest sophisticated security systems in place to defend against threats.

The cloud provider should be able to answer all the above questions in detail, so that you know exactly where your data is stored and how they will protect your data against internal and external threats. Moreover, how can you retrieve that data if it becomes necessary.

2. Service Quality: Service quality is often one of the most significant factors that businesses cite as a reason for not moving their business applications to the cloud. Often businesses feel as though the SLAs provided by the cloud providers today are not adequate to assure the requirements for running a production application on the cloud, especially those related to availability, performance and scalability.

According to a recent survey 43% of IT decision makers are planning to invest more into cloud computing this year. CIOs need assurance that the company's data will be secure and available, and the service reliable at all times. Ensuring maximum upkeep of the service is paramount for the profitability and sustainability of the business.

Without proficient service quality and comprehensive answers to the above questions, businesses will be reluctant to host their critical infrastructure within the cloud.

3. Downtime & Accessibility: Service quality doesn't have to be compromised when your data is in the cloud. Accessing your data when you need it is a basic requirement from many organisations. The challenge with the cloud is that the data is accessed via an internet connection rather than a local connection. So when the network or internet connection is down, it also means that cloud services are also down; thus data cannot be accessed.

Performance of the cloud infrastructure can be affected by the load, environment and number of users. Ensuring that your cloud infrastructure is resilient to outages is vital. Whilst it is almost impossible to mitigate all server outages, a reputable provider will have robust resilience measures in place to protect your data.

4. Access to data: Cloud-based servers do not always have the most effective or appropriate customer service support systems. *CIOs* often express their concerns around data ownership and losing control of their data when moving to the cloud, but this shouldn't be an issue. Selecting where and how your data is stored is an important element within the decision making process. Integration is a problem for many organisations. Ensuring that all of the applications are able to seamlessly integrate with one another is also a common challenge.

5. Transition to the cloud: Many cloud adoption challenges are unknown due to the fact that cloud technology is still in its relative infancy. *CIOs* are challenged deciding on the best way to transition to the cloud and finding a cloud solution that meets the aims of the businesses, whilst improving efficiencies.

Although transitioning to the cloud is a complex and involved process, there isn't one route to success. *CIOs* must ensure that the proposed solution compliments their business model. There are various ways businesses can transition to the cloud. Whether it's via private, public or hybrid technologies, identifying the right service model for your business is a vital step.

Migrating data poses a number of risks for organisations if not handled correctly. Developing a data migration strategy that integrates seamlessly with the current IT infrastructure is key to overall success.

CIOs are challenged with finding the right service model for their business. Finding a provider that will allow you to create a customised computing environment is vital.

The first step in transitioning to the cloud is being able to identify the challenges and working with your chosen cloud provider to navigate around these barriers in order to facilitate a successful cloud environment for the business. Whether Public, Private or Hybrid, making sure you ask the right questions and understand the risks for your business is imperative.

Q.4. (*a*) Explain the following : **(3×2.5 = 7.5)**

(*i*) Infrastructure- as- a -service (IaaS)

(*ii*) Platform -as-a-service (PaaS)

(*iii*) Software-as-a-service (SaaS)

Ans: Refer Q. no. 2 page no. 5 Model paper I End term exam .

Q.4. (*b*) Compare the following : **(5)**

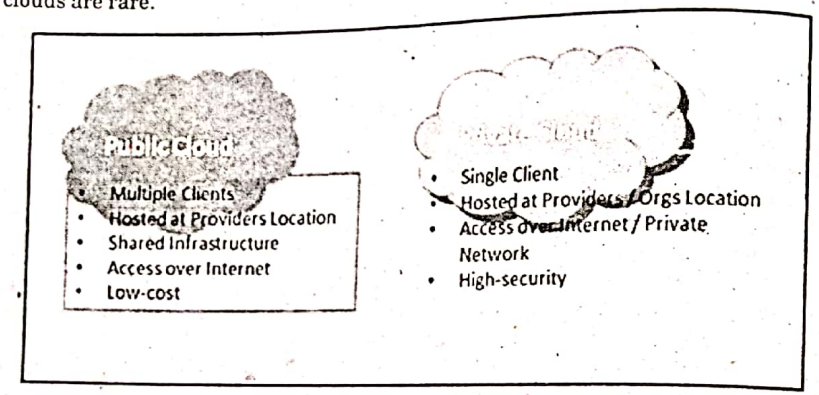
(*i*) Private cloud

(*ii*) Public cloud

Ans : Private Cloud: A private cloud hosting solution, also known as an internal or enterprise cloud, resides on company's intranet or hosted data center where all of your data is protected behind a firewall. This can be a great option for companies who already have expensive data centers because they can use their current infrastructure. However, the main drawback people see with a private cloud is that all management, maintenance and updating of data centers is the responsibility of the company. Over time, it's expected that your servers will need to be replaced, which can get very expensive. On the other hand, private clouds offer an increased level of security and they share very few, if any, resources with other organizations.

Public Cloud: The main differentiator between public and private clouds is that you aren't responsible for any of the management of a public cloud hosting solution. Your data is stored in the provider's data center and the provider is responsible for the management and maintenance of the data center. This type of cloud environment

is appealing to many companies because it reduces lead times in testing and deploying new products. However, the drawback is that many companies feel security could be lacking with a public cloud. Even though you don't control the security of a public cloud, all of your data remains separate from others and security breaches of public clouds are rare.



Q.5. (a) Explain the virtual machine migration services in cloud computing. **(4.5)**

Ans : Refer Q. no. 4(a) page no. 7 Model paper I End term exam .

Q.5.(b) Explain the pros and cons of virtualization in cloud computing. **(5)**

Ans: Pros of Virtualization:

1. It can lower overall capital expenditures: With virtualization, you will no longer need to purchase a server for each of the applications you are going to implement in your organization. You will be able to host multiple virtual servers on a single physical machine, which means that you will have lower overall capital expenditures.

2. It can reduce IT costs: This is one of the biggest advantages associated with using this technology in your IT infrastructure, where you do not have to invest in equipment that are incredibly expensive and in-house IT professionals to be able to easily access various software and servers. Also, virtualization is contrived to be affordable, as you do not have to purchase hardware outright, which means more savings. You simply pay a third party, who own and maintain all servers, for their virtualization services without having to spend additional costs.

3. This technology allows you to automate your important routine IT task. Something that is as simple as patches for your operating system will becomes simpler and quicker.

4. It makes a business energy-efficient: VirtualizationRefer Q. no. 4(a) page no. 7 Model paper I End term exam . is seen as revolutionary advancement due to a number of reasons, and one of those having the most impact is energy savings. By implementing such a technology in your business, you will be able to lessen your carbon footprint immensely, which would eventually make a big difference overall. If your organization is environmentally conscious, then virtualization is the way to go.

5. It promotes greater redundancy: Virtualization technologies can help you improve your uptime by allowing greater security and safety while reducing points of contact.

6. It greatly helps with development: This technology is observed to be very helpful in development environments. For example, if you are running several websites, you can make the coding process of these sites easier by using a virtualized server.

7. It allows for faster deployment: In a virtualized environment, provisioning would become quick and simple. You should know that deploying virtual machines is simpler than deploying the older physical versions.

Cons of Virtualization:

1. It requires high upfront expenditures: Though it was stated that virtualization is cost-effective, when you implement such a strategy from the ground up, it would mean that are you are going to have to invest more money in hardware in the near future. Nevertheless, you will definitely save in the long run, but take note that implementation can get costly.

2. It comes with limitations: One major disadvantage of using virtualization is that it involves various limitations. Take note that not all servers and applications are virtualization-friendly, which means that some aspects of the IT infrastructure of your business might not be compatible with virtualized solutions. You should consider the fact that there are still vendors that do not fully support virtualized environments.

3. It puts data at risk: Since data is crucial to your business, it is of utmost importance that you only choose virtualization solutions that offer adequate data protection. Remember that not having your own server can put your data at risk, making it vulnerable.

4. It comes with the danger of server sprawl: While virtualization is very easy to deploy, there is always the risk that new servers would be added even if they are not necessary. For instance, instead of having 10 virtual servers that you really need, you might have 20 or more.

5. It comes with issues of availability and scalability: Most of the time, the terms availability and scalability are intertwined when it comes to networking, as both are relevant to server virtualization after all. Availability would become a problem if virtualized servers go offline and every website they host would also fail. Scalability is even trickier, considering that virtualization offers a means for several small businesses to share the costs associated with hosting. As you can see, while a business may start out small, there is always the possibility that it could grow big and easily dominate a virtualized server, robbing resources from other websites.

6. It has security flaws: The process of virtualization is designed to separate virtualized resources, but there are still cases where servers were accidentally visible to other people who were not supposed to see them.

7. It comes with the risk of bleed-overs: Bleed-overs are possible issues to be aware of when subscribing to a virtualized server, occurring when the contents of a certain server affect other servers. For instance, a chat room that occasionally hosts live discussions with IT industry professionals would experience its chat members receiving a pop-up window stating that they already exceeded the total bandwidth allocation and being booted out of the chat room. What's worse, this can still happen even if your internet service provider (ISP) was not limiting bandwidth consumption. The thing is, there might be another site that is hosted on the same server implementing a shareware bandwidth limitation program, which can limit bandwidth for the server as a whole.

Many businesses and organizations of today are already taking advantage of virtualization because most of their operations are highly dependent on IT processes. This is regarded as a wise investment that makes management of data more efficient and convenient. However, for your organization, you must make sure that you are aware of both the advantages and advantages of using virtualization to ensure that you will be able to implement and manage it properly.

Q.5. (c) Mention the management issues in virtualization of cloud. **(3)**

Ans : Management issues are

1. reliability
2. availability of services and data
3. security
4. complexity
5. costs
6. regulations and legal issues
7. performance
8. migration
9. reversion
10. the lack of standards
11. limited customization
12. issues of privacy

Q.6. (a) Explain the following cloud security mechanism : (6)

Ans. (i) PKI: To provide security services like confidentiality, authentication, integrity, non-repudiation, etc., PKI is used. PKI is a framework which consists of security policies, communication protocols, procedures, etc. to enable secure and trusted communication between different entities within as well as outside the organization. PKI is built as a hybrid mode of the symmetric and asymmetric encryption. Let's discuss this in brief:

Symmetric Encryption: A single key is used to encrypt and decrypt the message sent between two parties. Symmetric encryption is fast, and this type of encryption is effective only when the key is kept absolutely secret and secure between two parties. But to transmit this secret key over an un-trusted network i.e., Internet, comes asymmetric encryption.

Asymmetric Encryption: A pair of keys is used to encrypt and decrypt the message. The pair of keys is termed as public and private keys. Private keys are kept secret by the owner, and the public key is visible to everyone. Here is how it works: Suppose 'A' and 'B' want to communicate using asymmetric encryption. So 'A' encrypts the message with 'B' public key so that only 'B' can decrypt the message with its private key. After decrypting the message, 'B' will encrypt the message with 'A' public key so that only 'A' can decrypt it using its own private key. Sounds like a perfect solution, doesn't it? Well as far as secrecy is concerned it is, but when it comes to real world scenarios, asymmetric encryption is pretty slow as the keys involved in this process are of 1024, 2048 bits ,etc. and after the initial handshake, for subsequent requests this overhead still needs to be incurred. So what to do?

In comes the PKI approach, which is a hybrid approach of symmetric and asymmetric encryption. In this, the handshake process happens with asymmetric encryption to exchange the secret key used for symmetric encryption. Once the secret key is exchanged, the rest of the communication happens over asymmetric encryption. In this way, security and performance are both achieved. PKI is a hierarchal model which is comprised of the below components:

Certificate Authority (CA): This entity issues certificates for requests received. This can be in-house or trusted third parties CA like 'Verisign', 'COMODO', 'Thwate' etc.

Registration Authority (RA): This entity performs the background checking process on the requests received from end point entities like their business operations in order to avoid issuing any certificate to a bogus entity.

Certificate Revocation List (CRL): This is the list issued that contains a list of the certificates which are no longer valid to be trusted.

End-point Entities: These entities make requests for the certificates in order to prove their identity and gain trust over the Internet.

Certificates Repository: This is the repository which contains a list of issued certificates which the end point entities can retrieve in order to verify the corresponding server. For end users, this repository is usually located in the browser, such as Firefox, IE, Chrome, etc.

As it can be noted, the maintenance of these keys is of utmost importance and losing control over these keys will leave the encryption on data useless. Key management

is an important process and the most challenging process, as any deviation in this could lead to data loss. The key management life cycle involves the following steps:

Creation: The first step in the key management life cycle is to create a key pair and apply access control around it. While creating the key, certain important factors need to be considered like key length, lifetime, encryption algorithm, etc. The new key thus created is usually a symmetric key and it is encrypted with a public key of the public-private key pair.

Backup: Before distributing keys, first of all the backup of keys should be made to some external media. As normally the key created is a symmetric key a.k.a shared key which should be encrypted with a public key from the key pair, then it becomes important to protect the other part of key pair i.e. the private key. Also the policies around the backup media and vaults should be up to the same effect as is designed for any critical business operation to recover from any type of disruption.

Deployment: After the key is created and backed up, then it is ready to be deployed in the encryption environment. It is advisable to not directly put these keys into action on the production environment. The key operations should be analyzed, and if successful the key should be used for encrypted production data.

Monitoring: Monitoring of the crypto systems is very important to check for unauthorized administrative access and key operations such as: creation, backing, restoring, archival and destruction.

Rotation: Keys should be rotated on a regular basis with the keys that are either meant to be expired or need to be changed following a business change. It is important to realize that keys should not be put into system.

Expiration: As per the best practices dictated in compliances like PCI-DSS, it is important that even valid keys need to be changed after a span of time, not only after the keys are expired. Before the expiration phase, key rotation phase should take place by replacing the associated data with new keys.

Archival: Before the destruction of keys, archival of expired and decommissioned keys is important if there is still related data in the environment that needs to be recovered like data for recovery operations. This phase is very important from the business decision perspective, and there are some appliances which never go for the destruction phase that causes a risk to be attached. Archived copy of the keys should be properly secured.

Destruction: After the business use of key is over or its validity expires, secret and private keys should be destroyed in an efficient manner. All the traces of keys should be completely removed from the whole environment, even from the removal media, and vaults where the keys are stored for backup processes. (6)

(ii) SSO

Ans : Refer Q.1. (e) of End Term Examination 2016.

(iii) IAM

Ans : Refer Q. no. 4(a) page no. 19 Model paper II End term exam .

Q.6. (b) Explain the features of service management in cloud computing. (6.5)

Ans: Cloud service delivery, cloud service management and cloud monitoring toots enable providers to keep up with the continually shifting capacity demands of a highly elastic environment.

Cloud monitoring and cloud service management tools allow cloud providers to ensure optimal performance, continuity and efficiency in virtualized, on-demand environments. These tools — software that manages and monitors networks, systems and applications — enable cloud providers not just to guarantee performance, but also to better orchestrate and automate provisioning of resources.

Cloud monitoring tools, specifically, enable cloud providers to track the performance, continuity and security of all of the components that support service delivery: the hardware, software and services in the data center and throughout the network infrastructure.

Through successful cloud service management and monitoring, cloud providers can use service quality to differentiate themselves in what remains a crowded and noisy marketplace.

Through successful cloud service management and monitoring, cloud providers can use service quality to differentiate themselves in what remains a crowded and noisy marketplace. Effective cloud service management also helps lower the risk~of frequent cloud outages that can jeopardize security systems. Using these tools also supports greater operational efficiency, helping -cloud providers minimize costs and maximize profit margins. However, achieving these goals can be difficult in a complex virtual delivery environment where visibility and control are limited.

Q.7. (a) Mention the functional and non-functional requirements of federation cloud. **(4)**

Ans : A federated cloud (also called cloud federation) is the deployment and management of multiple external and internal cloud computing services to match business needs. A federation is the union of several smaller parts that perform a common action.

Federation in a network domain is a model for establishing a large scale and diverse infrastructure for applications. It appears as an interconnection of multiple independent network domains for creating a rich environment with increased benefits to users of individual domains.

Domains in federations are geographically dispersed and owned by different organizations. However, they are considered as a part of a single entity because they operate in a common management framework under a common management authority. Federations are dynamic. They evolve over time based on user requirements. Management and operation of federated environments over administrative domains and multiple networks require specific mechanisms. Federation is useful for prototyping, outsourcing, realization and testing. A central federation control unit communicates a virtual private network (VPN) setup request to gateways to provide requested links, which assures connectivity to all domain resources. Thus, the technology enables setting up secure overlay networks over unsecured network links. Building a federation requires certain entities and control mechanisms. The architecture relies on a centralized approach where functionalities are delivered by centrally administered tools and entities.

Federation in networking systems means users can send messages from one system to another. Federated instant messaging (IM) networks permit communication across different IM clients and platforms. They maintain an open directory allowing the networks to message their users. A few federated networks also work on an interoperability basis, where software from two or more vendors shares data between different platforms.

A central business entity provides the federation control unit and service composition tools where services and components are orchestrated on demand. Interconnected domains are configured and managed in a top-down approach, while domains publish services and capabilities in a bottom-up approach.

Q.7. (b) Explain the features enterprise cloud computing. **(2.5)**

Ans : Refer Q. no. 1(b) page no. 14 Model paper II End term exam .

Q.7. (c) Q: Write short notes for the following Enterprise software: **(6)**

(i) ERP

Ans : Enterprise resource planning (ERP) is a process by which a company (often a manufacturer) manages and integrates the important parts of its business. An ERP

management information system integrates areas such as planning, purchasing, inventory, sales, marketing, finance and human resources.

ERP is most frequently used in the context of software. As the methodology has become more popular, large software applications have been developed to help companies implement ERP.

The ERP software functions like some a central nervous system for a business. It collects information about the activity and state of different divisions of the body corporate and makes this information available to other parts where it can be used productively. Information on the ERP is added in real time by users. Any authorized user with a valid password and access to the network can access the system any time.

ERP resembles the human central nervous system. Its capacity transcends the collective ability of the individual parts to form what is known as consciousness. It helps a corporation become more self-aware by linking information about production, finance, distribution and human resources. ERP connects different technologies used by each individual part of a business, eliminating duplicate and incompatible technology that is costly to the corporation. This involves integrating accounts payable, stock-control systems, order-monitoring systems and customer databases into one system.

The first ERP system to be developed was SAP, a software firm that was established in 1972 by three software engineers based in Mannheim, Germany. SAP's goal was to link different parts of a business by sharing information gathered from those parts to help the company operate more efficiently.

(ii) SCM

Ans : Supply chain management (SCM) is the oversight of materials, information, and finances as they move in a process from supplier to manufacturer to wholesaler to retailer to consumer. Supply chain management involves coordinating and integrating these flows both within and among companies. It is said that the ultimate goal of any effective supply chain management system is to reduce inventory (with the assumption that products are available when needed). As a solution for successful supply chain management, sophisticated software systems with Web interfaces are competing with Web-based application service providers (ASP) who promise to provide part or all of the SCM service for companies who rent their service.

Supply chain management flows can be divided into three main flows:

The product flow

The information flow

The finances flow

The product flow includes the movement of goods from a supplier to a customer, as well as any customer returns or service needs. The information flow involves transmitting orders and updating the status of delivery. The financial flow consists of credit terms, payment schedules, and consignment and title ownership arrangements.

There are two main types of SCM software: planning applications and execution applications. Planning applications use advanced algorithms to determine the best way to fill an order. Execution applications track the physical status of goods, the management of materials, and financial information involving all parties.

Some SCM applications are based on open data models that support the sharing of data both inside and outside the enterprise (this is called the extended enterprise, and includes key suppliers, manufacturers, and end customers of a specific company). This shared data may reside in diverse database systems, or data warehouses, at several different sites and companies.

(iii) CRM

Ans : CRM (customer relationship management) is all aspects of interactions that a company has with its customers, whether it is sales or service-related. While the phrase customer relationship management is most commonly used to describe a

business-customer relationship (B2C), CRM is also used to manage business to business (B2B) relationships. Information tracked in a CRM system includes contacts, clients, contract wins and sales leads and more.

CRM tools make the customer-facing functions of business easier. They help you:

1. Centralize customer information
2. Automate marketing interactions
3. Provide business intelligenc
4. Facilitate communications
5. Track sales opportunities
6. Analyze data
7. Enable responsive customer service

Q.8. (a) Explain the features of any two cloud platforms given as follow : **(5)**

(i) Amazon web services

Ans : Refer Q. no. 5 page no. 20 Model paper II End term exam .

(ii) Microsoft Azure

Ans : Refer Q. no. 3 page no. 19 Model paper II End term exam .

(iii) Google App Engine

Ans : Google App Engine (often referred to as GAE or simply App Engine) is a platform as a service (PaaS) cloud computing platform for developing and hosting web applications in Google-managed data centers. Applications are sandboxed and run across multiple servers. App Engine offers automatic scaling for web applications as the number of requests increases for an application, App Engine automatically allocates more resources for the web application to handle the additional demand.

Currently, the supported programming languages are Python, Java (and, by extension, other JVM languages such as Groovy, JRuby, Scala, Clojure), Go, and PHP. Node.js is also available in the Managed VM environment. Google has said that it plans to support more languages in the future, and that the Google App Engine has been written to be language independent.

Python web frameworks that run on Google App Engine include Django, CherryPy, Pyramid, Flask, web2py and webapp2, as well as a custom Google-written webapp framework and several others designed specifically for the platform that emerged since the release. Any Python framework that supports the WSGI using the CGI adapter can be used to create an application; the framework can be uploaded with the developed application. Third-party libraries written in pure Python may also be uploaded.

Google App Engine supports many Java standards and frameworks. Core to this is the servlet 2.5 technology using the open-source Jetty Web Server, along with accompanying technologies such as JSP. JavaServer Faces operates with some workarounds.

Though the datastore used may be unfamiliar to programmers, it is easily accessed and supported with JPA, JDO, and by the simple low-level API. There are several alternative libraries and frameworks you can use to model and map the data to the datastore such as Objectify, Slim 3 and Jello framework. Jello framework is a full-stack Java framework optimized for Google App Engine,that includes comprehensive Data Authorization model and a powerful RESTful engine.

Reliability and Support: All billed High-Replication Datastore App Engine applications have a 99.95% uptime SLA.

App Engine is designed in such a way that it can sustain multiple datacenter outages without any downtime. This resilience to downtime is shown by the statistic that the High Replication Datastore saw 0% downtime over a period of a year.

Paid support from Google engineers is offered as part of Premier Accounts. Free support is offered in the App Engine Groups, Stack Overflow, Server Fault, and GitHub, however assistance by a Google staff member is not guaranteed.

Restrictions

- Developers have read-only access to the filesystem on App Engine. Applications can use only virtual filesystems, like gae-filestore.
- App Engine can only execute code called from an HTTP request (scheduled background tasks allow for self calling HTTP requests).
- Users may upload arbitrary Python modules, but only if they are pure-Python; C and Pyrex modules are not supported.
- Java applications may only use a subset (The JRE Class White List) of 'the classes from the JRE standard edition.
- Datastore cannot use inequality filters on more than one entity property per query.
- A process started on the server to answer a request can't last more than 60 seconds (with the 1.4.0 release, this restriction does not apply to background jobs anymore).
- Does not support sticky sessions (a.k.a. session affinity), only replicated sessions are supported including limitation of the amount of data being serialized and time for session serialization.

Q.8. (b) Write short note on the following specialized cloud architectures : **(2.5×3=7.5)**

(i) Direct I/O access architecture

Ans : Refer Q. no. 1(b) page no. 1 Model paper I End term exam .

(ii) Load balanced Virtual Switches Architectures

Ans : A load-balanced switch is a switch architecture which guarantees 100% throughput with no central arbitration at all, at the cost of sending each packet across the crossbar twice. Load-balanced switches are a subject of research for large routers scaled past the point of practical central arbitration.

A load-balanced switch has N input line cards, each of rate R, each connected to N buffers by a link of rate R/N. Those buffers are in turn each connected to N output line cards, each of rate R, by links of rate R/N. The buffers in the center are partitioned into N virtual output queues.

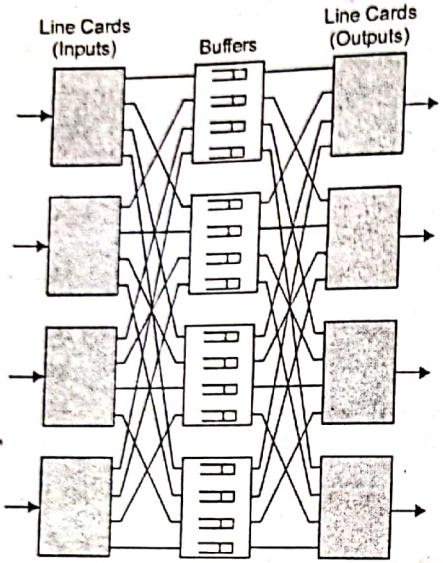
Each input line card spreads its packets evenly to the N buffers, something it can clearly do without contention. Each buffer writes these packets into a single buffer-local memory at a combined rate of R. Simultaneously, each buffer sends packets at the head of each virtual output queue to each output line card, again at rate R/N to each card. The output line card can clearly forward these packets out the line with no contention.

Each buffer in a load-balanced switch acts as a shared-memory switch, and a load-balanced switch is essentially a way to scale up a shared-memory switch, at the cost of additional latency associated with forwarding packets at rate R/N twice.

The Stanford group investigating load-balanced switches is concentrating on implementations where the number of buffers is equal to the number of line cards. One buffer is placed on each line cards, and the two interconnection meshes are actually the same mesh, supplying rate 2R/N between every pair of line cards. But the basic load-balanced switch architecture does not require that the buffers be placed on the line cards, or that there be the same number of buffers and line cards.

One interesting property of a load-balanced switch is that, although the mesh connecting line cards to buffers is required to connect every line card to every buffer,

there is no requirement that the mesh act as a non-blocking crossbar, nor that the connections be responsive to any traffic pattern. Such a connection is far simpler than a centrally arbitrated crossbar.



(iii) Multipath Resource Access Architecture

Ans: Cloud service delivery, cloud service management and cloud monitoring toots enable providers to keep up with the continually shifting capacity demands of a highly elastic environment.

Cloud monitoring and cloud service management tools allow cloud providers to ensure optimal performance, continuity and efficiency in virtualized, on-demand environments. These tools — software that manages and monitors networks, systems and applications — enable cloud providers not just to guarantee performance, but also to better orchestrate and automate provisioning of resources.

Cloud monitoring tools, specifically, enable cloud providers to track the performance, continuity and security of all of the components that support service delivery: the hardware, software and services in the data center and throughout the network infrastructure.

Through successful cloud service management and monitori[illegible]nd providers can use service quality to differentiate themselves in what remains [illegible]wded and noisy marketplace.

Through successful cloud service management and monitoring, cloud providers can use service quality to differentiate themselves in what remains a crowded and S(bisy marketplace. Effective cloud service management also helps lower the risk 6f frequent cloud outages that can jeopardize security systems. Using these tools also supports greater operational efficiency, helping cloud providers minimize costs aifd maximize profit margins. However, achieving these goals can be difficult in a complex virtual delivery environment where visibility and control are limited.

FIRST TERM EXAMINATION [SEPT. 2017]
SEVENTH SEMESTER [B.TECH]
CLOUD COMPUTING [ETIT–407]

Time : 1.5 hrs. **M.M. : 30**

Note: Attempt any three questions including Q.No. 1 which is compulsory.

Q.1. Write short note on the following:-

Q.1. (a) Define federated cloud.

Ans. The United States government cloud computing plan, officially called the Federal Gtoud Computing Initiative, is a plan to transition the US federal government's information technology infrastructure to web-based IT services. Launched in September of 2009 by the Obama administration, the initiative seeks to identify common services and solutions amongst the government's agencies and adopt a cloud computing business model to support them.

Q.1. (b) Mention the characterstics of PaaS solution.

Ans. The Essential Characteristics of PaaS:

Runtime Framework: This is the "software stack" aspect of PaaS, and perhaps the aspect that comes first to mind for most people. The PaaS runtime framework executes end-user code according to policies set by the application owner and cloud provider. PaaS runtime frameworks come in many flavors, some based on traditional application runtimes, others based on 4GL and visual programming concepts, and some with pluggable support for multiple application runtimes.

Abstraction: Platform-oriented cloud platforms are distinguished by the higher level of abstraction they provide. With IaaS, the focus is on delivering to users "raw" access to physical or virtual infrastructure. In contrast, with PaaS, the focus is on the applications that the cloud must support. Whereas an IaaS cloud gives the user a bunch of virtual machines that must be configured and to which application components must be deployed, a PaaS cloud provides the user a way to deploy her applications into a seemingly limitless pool of computing resources, eliminating the complexity of deployment and infrastructure configuration.

Automation: A PaaS environment is a bit like a swan on a pond — graceful and elegant above the water, and paddling its little legs off below the water. The aforementioned abstraction provides the elegant user experience "above the water," while high levels of automation provide the "paddling" beneath the surface. PaaS environments automate the process of deploying applications to infrastructure, configuring application components, provisioning and configuring supporting technology like load balancers and databases, and managing system change based on policies set by the user.

While IaaS is known for its ability to shift capital costs to operational costs through outsourcing, only PaaS is able to slash costs across the development, deployment and management aspects of the application lifecycle.

Cloud Services: PaaS offerings provide developers and architects with services and APIs that help simplify the job of delivering elastically scalable, highly available cloud applications. These cloud services provide a wide variety of capabilities, and in many instances are key differentiators among competing PaaS offerings.

Examples of cloud services include services and APIs for distributed caching, queuing and messaging, workload management, file and data storage, user identity, analytics, and more. By providing built-in cloud services, platform offerings eliminate the need to integrate many disparate components and decrease time-to-market for applications on the platform.

Q.1. (c) How does cloud computing help to reduce the time to market applications and to cut down capital expenses ?

Ans. The world of IT infrastructure development and management keeps growing. As a central and integral part of IT infrastructure development, cloud computing has altered the way businesses view data storage and management.

The adoption of cloud computing is not limited to just large corporations. A survey conducted in 2011 by the Aberdeen Group found that up to 38% of small business, 48% of mid-sized companies and 26% of large companies all adopted cloud computing for one reason or another.

As for the reasons why these companies chose to adopt cloud computing. 55% of them said that they use the cloud as a way to reduce IT costs with an additional 38% utilizing the cloud because of the increased complexity of IT. This means that they needed a solution that was effective, saved time and lowered their IT costs.

Keep in mind that this is a fairly old study and as cloud computing continues to grow these numbers may change. The only constant is that business will continue to want to lower costs. The following cloud computing features can help significantly reduce IT costs.

Cloud Computing Is Flexible

With the cloud, your company's data is accessible anywhere and from any device. As long as your employees can access the internet, they can work from home, on the road, or even on their smartphones. Various departments in your organization can collaborate on a single project without actually having to be physically together!

For example, a company's employees can utilize the cloud to work from various locations around the world. All the data they use and transmit is tracked and stored within the cloud for later assessment or review.

The cloud's flexibility improves efficiency and responsiveness. The more efficient a company's staff is, the more productive they can be. In the long run, you reduce the amount of time it takes to complete a project. Consequently, the overall cost of the project comes down.

Easy to Setup and Manage

Setting up a cloud is easier and cheaper than if you were to use an on-premise data solution. You won't need to purchase any expensive software or hardware to get your system up and running. The cloud computing provider you choose to use will have already done that for you.

The amount you pay to your cloud provider is a very small fraction of what you would spend if you built your own IT infrastructure. This is also on top of the fact that you would have to spend more on maintenance and repairs, something most cloud providers will do for free or at a small fee.

So, cloud computing reduces the initial cost of setting up a reliable data storage and management system. Also, you won't need any IT specialists to develop and manage the data center, further reducing costs.

You Won't Need to Pay for Increased Storage

Most cloud solutions will offer you extensive storage capabilities with unlimited storage space. This is a great advantage to many businesses that previously had to purchase external storage disk space every time their data needs surpassed their current storage space. **With cloud computing, if your storage space needs increase, you can increase your cloud with it.**

Compared to having to buy new storage devices, you save a lot of money in the cloud. The ability of the cloud to scale to correspond with your data needs is one advantage that is friendly to both your data needs and your pocket!

Cloud computing providers keep their systems upgraded to ensure that they meet your IT infrastructure needs. Data security is constantly upgraded and improved, and as a result more businesses are agreeable to using cloud services. This is especially because of the impact cloud computing has on the reduction of capital expenditure.

Q.1. (d) What kind of needs is addressed by Hetrogeneous cloud ?

Ans. Heterogeneity in cloud computing can be considered in at least two ways. The first is in the context of multi-clouds, in which platforms that offer and manage infrastructure and services of multiple cloud providers are considered to be a heterogeneous cloud. Heterogeneity arises from using hypervisors and software suites from multiple vendors. The second is related to low-level heterogeneity at the infrastructure level, in which different types of processors are combined to offer VMs with heterogeneous compute resources. In this paper, the latter is referred to as heterogeneous clouds. While supercomputers have become more heterogeneous by employing accelerators, such as NVIDIA GPUs or Intel Xeon Phis, cloud data centers mostly employ homogeneous architectures. More recently heterogeneous cloud data center architectures have been proposed15 . In the vendor arena, Amazon along with other providers offer GPU-based VMs, but accelerators are not yet fully integrated into the computing ecosystem. This is because it is not yet possible for a programmer to fully develop and execute code oblivious to the underlying hardware. There are a number of efforts in this direction, but the key challenge is achieving a high-level abstraction that can be employed across multiple architectures, such as GPUs, FPGAs and Phis. Further applications that already execute on the cloud cannot be scheduled onto heterogeneous resources. Efforts in this direction are made by the CloudLightning16 project. The concept of a heterogeneous cloud may extend beyond the data center. For example, ad hoc clouds or microclouds could be heterogeneous cloud platforms.

Current cloud infrastructures are mostly homogeneous composed of a large number of machines of the same type – centrally managed and made available to the end user using the three standard service models:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

As clouds increase in size and as machines of different types are added to the infrastructure in order to maximize performance and power efficiency, heterogeneous clouds are being created. The heterogeneous cloud is still at a nascent stage, however, larger cloud infrastructure providers are offering commercial services e.g., Amazon Web Services offers a variety of GPU services. As demand for better processor, price and power performance increases, it is anticipated that larger infrastructure providers will need to cater for several of these processor types and specifically for the emerging HPC public cloud market.

However, integrating and managing these different architectures independently and with an existing general purpose cloud architecture is not without challenges; not least of which is access to a pool of qualified engineers with deep IT knowledge. The adoption of heterogeneous resources will dramatically increase the complexity of an already complex cloud ecosystem. We present self-organisation and self-management as powerful techniques for addressing this complexity.

The adoption of heterogeneous computing resources by cloud consumers will also allow for improved resource efficiency and hence reduced energy use. Market demand for greater resource management at the PaaS and IaaS layers combined with both demand and adoption of heterogenous resources is rapidly increasing complexity of the cloud ecosystem which over time will render traditional cloud management techniques ineffectual.

Q.2. (a) Write difference between distributed computing and Parallel computing.

Ans. Parallel computing means that different activities happen at the same time. The term was mostly used in scientific computing (consumer computers until very recently simply were not parallel) where it typically means: spread out a single application over many many cores/processors/processes to get it done bigger/faster. Current big parallel computers have 100 thousand to a million parallel processors/cores/threads/whatever.

Distributed computing comes from the business world where you have distributed systems such as airline reservation systems, where many people access and modify the same data at the same time. The machinery involved here is typically much looser coupled, and the activities in a distributed system are typically far less synchronized.

Q.2. (b) What are the different variants of distributed computing ?

Ans. A distributed system is a network of autonomous computers that communicate with each other in order to achieve a goal. The computers in a distributed system are independent and do not physically share memory or processors. They communicate with each other using *messages*, pieces of information transferred from one computer to another over a network. Messages can communicate many things: computers can tell other computers to execute a procedures with particular arguments, they can send and receive packets of data, or send signals that tell other computers to behave a certain way.

Computers in a distributed system can have different roles. A computer's role depends on the goal of the system and the computer's own hardware and software properties. There are two predominant ways of organizing computers in a distributed system. The first is the client-server architecture, and the second is the peer-to-peer architecture.

Types of distributed system-

1. Distributed computing system: Distributed computing is a computing concept that, in its most general sense, refers to multiple computer systems working on a single problem. In distributed computing, a single problem is divided into many parts, and each part is solved by different computers. As long as the computers are networked, they can communicate with each other to solve the problem. If done properly, the computers perform like a single entity.

The ultimate goal of distributed computing is to maximize performance by connecting users and IT resources in a cost-effective, transparent and reliable manner. It also ensures fault tolerance and enables resource accessibility in the event that one of the components fails.

2. Distributed information system: A set of **information systems** physically **distributed** over multiple sites, which are connected with some kind of communication network. A **system** where, applications (cooperative among one another) stay on different elaborative nodes and the **information** property, unique, is hosted on different elaborative nodes.

3. Distributed pervasive system.

These system includes

1. Mobile and embedded system
2. Home systems
3. Sensor networks

Q.3. List and discuss different types of virtualization.

Ans- Virtualization is the process of creating a virtual environment on an existing server to run your desired program, without interfering with any of the other services provided by the server or host platform to other users. The Virtual environment can be

single instance or a combination of many such as operating systems, Network or application servers, computing environments, storage devices and other such environments.

While the benefits of virtualization are self-evident, many people are still in the dark when it comes to the many different types of virtualization. Here, we'll show you some of the most common virtualization methods and why they're valuable for your business.

Application Virtualization: This is a process where applications get virtualized and are delivered from a server to the end user's device, such as laptops, smartphones, and tablets. So instead of logging into their computers at work, users will be able to gain access to the application from virtually anywhere, provided an Internet connection is available. This type of virtualization is particularly popular for businesses that require the use of their applications on the go.,

Desktop Virtualization: Similar to Application Virtualization mentioned above, desktop virtualization separates the desktop environment from the physical device and configured as a "virtual desktop infrastructure" (VDI). The major advantages of desktop virtualization is that users are able to access all their personal files and applications from any location and on any PC, meaning they can work from anywhere without the need to bring their work computer. It also lowers the cost of licensing for installing software on desktops and maintenance and patch management is very simple, since all of the virtual desktops are hosted at the same location.

Hardware Virtualization: This is perhaps the most common type of virtualization today. Hardware virtualization is made possible by a virtual machine manager (VM) called the "hypervisor". The hypervisor creates virtual versions of computers and operating systems and consolidates them into one large physical server, so that all the hardware resources can be utilized more efficiently. It also enables users to run different operating systems on the same machine at the same time.

Network Virtualization: Network virtualization is a method that combines all physical networking equipment into a single resource. It is the process of dividing bandwidth into multiple, independent channels, each of which can be assigned to servers and devices in real time. Businesses that would benefit from network virtualization are ones that have a large number of users and need to keep their systems up and running at all times. With the distributed channels, your network speed will increase dramatically, allowing you to deliver services and applications faster than ever before.

Storage Virtualization: This type of virtualization is very easy and cost-effective to implement, since it involves compiling your physical hard drives into a single cluster. Storage virtualization is handy when it comes to planning for disaster recovery, since the data stored on your virtual storage can be replicated and transferred to another location. By consolidating your storage into a centralized system, you can eliminate the hassles and costs of managing multiple storage devices.

Integrating virtualization into your business can be a complex and confusing process. Ideally you will enlist the help of experts to get the job done right. If you're looking for top-quality and reliable virtualization solutions, why not get in touch with our professionals today. We'll make your virtualization experience a quick and painless one.

Q.4. Mention the management issues in virtualization of cloud

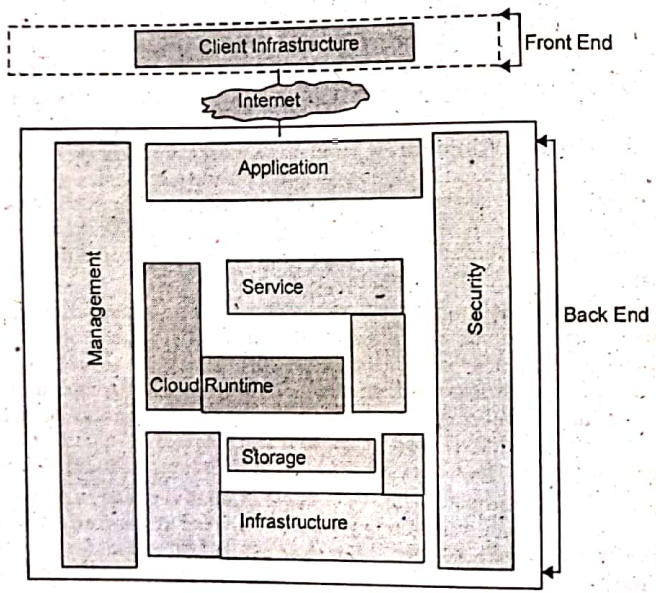
Ans. Management issues are -

1. reliability
2. availability of services and data
3. security
4. complexity
5. costs

6. regulations and legal issues
7. performance
8. migration
9. reversion
10. the lack of standards
11. limited customization
12. issues of privacy

Q. 5. Draw the basic block diagram of computer architecture and also explain it.

Ans. Cloud computing architecture refers to the components and subcomponents required for cloud computing. These components typically consist of a front end platform (fat client, thin client, mobile device), back end platforms (servers, storage), a cloud based delivery, and a network (Internet, Intranet, Intercloud). Combined, these components make up cloud computing architecture.



Front End: The front end refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, Example - Web Browser.

Back End: The back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc

END TERM EXAMINATION [DEC. 2017]
SEVENTH SEMESTER [B.TECH]
CLOUD COMPUTING [ETIT–407]

Time : 3 hrs. **M.M. : 75**

Note: Attempt any five question including Q.No. 1 which is compulsory.

Q.1. Write short note on the following:-

Q.1. (a) What is meant by on premise computing? How it is different from cloud computing? **(4)**

Ans. There are many differences between on-premises computing and cloud computing. Some of the most obvious characteristics include the most biggest difference – how they are accessed. On-premises solutions are just that, on-premises, installed on a user's or users' computers. Cloud solutions, on the other hand, are accessed via the internet, and typically hosted by a third-party vendor. The second big difference is the "pay as you go" or on-demand usage service model (cloud) versus the traditional upfront capital expenditure (on-premises). For accounting purposes, counting this on-demand usage as a "utility" versus a large capital expenditure can be very beneficial. Sometimes this is one of the more enticing aspects of using cloud services—the low cost/low entry point.

Q.1. (b). Which are the technologies that cloud computing relies on? **(4)**

Ans. Refer Q.No. 1, end term examination, page no.-2-2016.

Q.1. (c). Identify the reasons why parallel processing constitutes an interesting option for computing. **(3)**

Ans. Parallel processing is a method of simultaneously breaking up and running program tasks on multiple microprocessors, thereby reducing processing time. Parallel processing may be accomplished via a computer with two or more processors or via a computer network.

Parallel processing is also called parallel computing.

Main Reasons:

- **SAVE TIME AND/OR MONEY:**
- In theory, throwing more resources at a task will shorten its time to completion, with potential cost savings.
- Parallel computers can be built from cheap, commodity components.

- **SOLVE LARGER / MORE COMPLEX PROBLEMS:**
- Many problems are so large and/or complex that it is impractical or impossible to solve them on a single computer, especially given limited computer memory.

• Example: "Grand Challenge Problems" (en.wikipedia.org/wiki/Grand_Challenge) requiring PetaFLOPS and PetaBytes of computing resources.

• Example: Web search engines/databases processing millions of transactions every second

• PROVIDE CONCURRENCY:

• A single compute resource can only do one thing at a time. Multiple compute resources can do many things simultaneously.

• Example: Collaborative Networks provide a global venue where people from around the world can meet and conduct work "virtually".

• TAKE ADVANTAGE OF NON-LOCAL RESOURCES:

• Using compute resources on a wide area network, or even the Internet when local compute resources are scarce or insufficient.

• Example: SETI@home (setiathome.berkeley.edu) has over 1.6 million users in nearly every country in the world. (June, 2017).

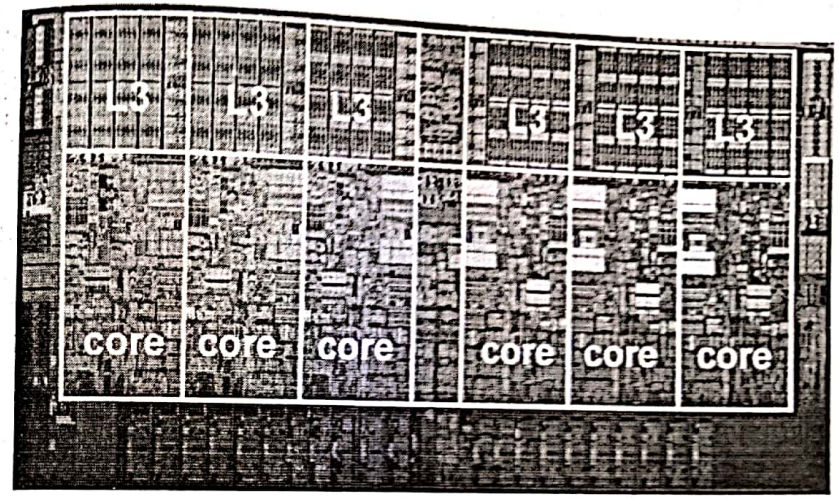
• Example: Folding@home (folding.stanford.edu) over 1.8 million contributors globally (June, 2017)

• MAKE BETTER USE OF UNDERLYING PARALLEL HARDWARE:

• Modern computers, even laptops, are parallel in architecture with multiple processors/cores.

• Parallel software is specifically intended for parallel hardware with multiple cores, threads, etc.

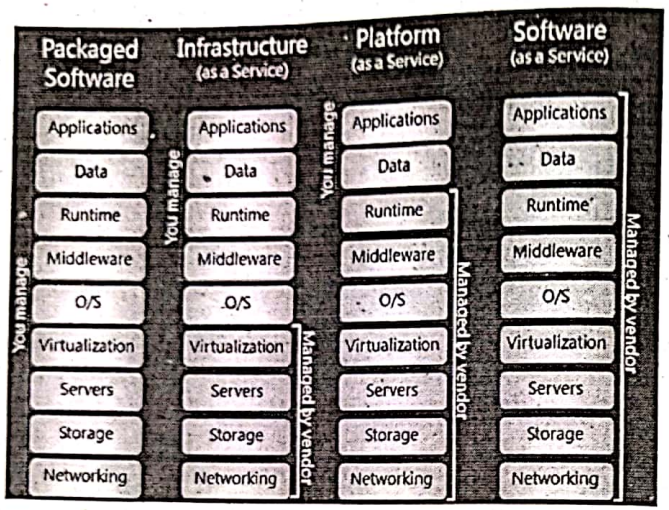
• In most cases, serial programs run on modern computers "waste" potential computing power.



Intel Xeon processor with 6 cores and 6 L3 cache units

Q.1. (*d*) Describe the different categories of options available in PaaS market. Draw the layers of PaaS architecture. (3)

Ans. PAAS: PLATFORM AS A SERVICE cloud platform services, or Platform as a Service (PaaS), are used for applications, and other development, while providing cloud components to software. What developers gain with PaaS is a framework they can build upon to develop or customize applications. PaaS makes the development, testing, and deployment of applications quick, simple, and cost-effective. With this technology, enterprise operations, or a third-party provider, can manage OSes, virtualization, servers, storage, networking, and the PaaS software itself. Developers, however, manage the applications.Enterprise PaaS provides line-of-business software developers a self-service portal for managing computing infrastructure from centralized IT operations and the platforms that are installed on top of the hardware. The enterprise PaaS can be delivered through a hybrid model that uses both public IaaS and on-premise infrastructure or as a pure private PaaS that only uses the latter.Similar to the way in which you might create macros in Excel, PaaS allows you to create applications using software components that are built into the PaaS (middleware). Applications using PaaS inherit cloud characteristic such as scalability, high-availability, multi-tenancy, SaaS enablement, and more. Enterprises benefit from PaaS because it reduces the amount of coding necessary, automates business policy, and helps migrate apps to hybrid model. For the needs of enterprises and other organizations.PaaS solutions are more likely to be explored in the next coming years, once the technologies and the concepts of infrastructure provisioning are fully established. For this reason there are a limited number of implementations for this approach in both the academy and the industry. We can categorize the PaaS approach into two major streams: those who integrate an IT infrastructure on top of which applications will be executed as a part of the value offering and those, which do not. Solutions that include an IT infrastructure are most likely to be found in the industry, while the other ones are more common in the academy.



Q.1. (e) How does cloud computing help to reduce the time to market applications and to cut down capital expenses ?

Ans. The world of IT infrastructure development and management keeps growing. As a central and integral part of IT infrastructure development, cloud computing has altered the way businesses view data storage and management.

The adoption of cloud computing is not limited to just large corporations. A survey conducted in 2011 by the Aberdeen Group found that up to 38% of small business, 48% of mid-sized companies and 26% of large companies all adopted cloud computing for one reason or another.

As for the reasons why these companies chose to adopt cloud computing. 55% of them said that they use the cloud as a way to reduce IT costs with an additional 38% utilizing the cloud because of the increased complexity of IT. This means that they needed a solution that was effective, saved time and lowered their IT costs.

Keep in mind that this is a fairly old study and as cloud computing continues to grow these numbers may change. The only constant is that business will continue to want to lower costs. The following cloud computing features can help significantly reduce IT costs.**Cloud Computing Is FlexibleWith the cloud, your company's data is accessible anywhere and from any device. As long as your employees can access the internet, they can work from home, on the road, or even on their smartphones.** Various departments in your organization can collaborate on a single project without actually having to be physically together!For example, a company's employees can utilize the cloud to work from various locations around the world. All the data they use and transmit is tracked and stored within the cloud for later assessment or review.**The cloud's flexibility improves efficiency and responsiveness.** The more efficient a company's staff is, the more productive they can be. In the long run, you reduce the amount of time it takes to complete a project. Consequently, the overall cost of the project comes down.

Easy to Setup and Manage

Setting up a cloud is easier and cheaper than if you were to use an on-premise data solution. You won't need to purchase any expensive software or hardware to get

your system up and running. The cloud computing provider you choose to use will have already done that for you.The amount you pay to your cloud provider is a very small fraction of what you would spend if you built your own IT infrastructure. This is also on top of the fact that you would have to spend more on maintenance and repairs, something most cloud providers will do for free or at a small fee.

So, cloud computing reduces the initial cost of setting up a reliable data storage and management system. Also, you won't need any IT specialists to develop and manage the data center, further reducing costs.

You Won't Need to Pay for Increased StorageMost cloud solutions will offer you extensive storage capabilities with unlimited storage space. This is a great advantage to many businesses that previously had to purchase external storage disk space every time their data needs surpassed their current storage space. **With cloud computing, if your storage space needs increase, you can increase your cloud with it.**

Compared to having to buy new storage devices, you save a lot of money in the cloud. The ability of the cloud to scale to correspond with your data needs is one advantage that is friendly to both your data needs and your pocket.

Cloud computing providers keep their systems upgraded to ensure that they meet your IT infrastructure needs. Data security is constantly upgraded and improved, and as a result more businesses are agreeable to using cloud services. This is especially because of the impact cloud computing has on the reduction of capital expenditure.

Q.1. (f) What is the most common scenario for a private cloud? (3)

Ans: The Cloud usage scenarios are intended to illustrate the most typical cloud scenarios and are not meant to be an exhaustive list of realizations within a cloud environment.

A. End User to Cloud: In this scenario, an end user is accessing data or applications in the cloud. Common applications of this type include email hosting and social networking sites. A user accesses the application and their data through any browser on any device. The user doesn't want to keep up with anything more than a password; their data is stored and managed in the cloud.

Concerned issues

- **Identity:** The cloud service must authenticate the end user.
- **An open client:** Access to the cloud service should not require a particular platform or technology. • SLAs: Although service level agreements for end users will usually be simpler, cloud vendors must be clear about what guarantees of service they provide.

B. Enterprise to Cloud to End User: In this scenario, an enterprise is using the cloud to deliver data and services to the end user. When the end user interacts with the enterprise, the enterprise accesses the cloud to retrieve data and / or manipulate it, sending the results to the end user. The end user can be someone within the enterprise or an external customer. Concerned issues

- An open client: Access to the cloud service should not require a particular platform or technology.
- Federated identity: In addition to basic identity needed by an end user, an enterprise user is likely to have an identity with the enterprise. The idea is that the enterprise user manages a single ID, with an infrastructure federating other identities that might be required by cloud services.
- Metering and monitoring: All cloud services must be metered and monitored for cost control, charge backs and provisioning.

• Management and Governance: Public cloud providers make it very easy to open an account and begin using cloud services; that ease of use creates the risk that individuals in an enterprise will use cloud services on their own initiative. Management of VMs and of cloud services such as storage, databases and message queues is needed to track what services are used. Governance is crucial to ensure that policies and government regulations are followed wherever cloud computing is used.

• A Common Format for VMs: A VM created for one cloud vendor's platform should be portable to another vendor's platform. Any solution to this requirement must account for differences in the ways cloud vendors attach storage to virtual machines.

• Common APIs for Cloud Storage and Middleware: Common APIs are required for access to cloud storage services, cloud databases, and other cloud middleware services such as message queues. Writing custom code that works only for a particular vendor's cloud service locks theenterprise into that vendor's system and eliminates some of the financial benefits and flexibility that cloud computing provides.

• SLAs and Benchmarks: In addition to the basic SLAs required by end users, enterprises who sign contracts based on SLAs will need a standard way of benchmarking performance. There must be an unambiguous way of defining what a cloud provider will deliver, and there must be an unambiguous way of measuring what was actually delivered.

• Lifecycle Management: Enterprises must be able to manage the lifecycle of applications and documents. This requirement includes versioning of applications and the retention and destruction of data. There are substantial legal liabilities if certain data is no longer available. In some cases an enterprise will want to make sure data is destroyed at some point.

C. Enterprise to Cloud: This scenario involves an enterprise using cloud services for its internal processes. This might be the most common scenario in the early stages of cloud computing because it gives the enterprise the most control. In this scenario, the enterprise uses cloud services to supplement the resources it needs, like:

• For backups or storage of seldom-used data

• Virtual machines in the cloud to bring additional processors online to handle peak loads

• Applications in the cloud (SaaS) for certain enterprise functions

• Cloud databases as part of an application's processing. This could be extremely useful for sharing that database with partners, government agencies, etc. Concerned issues The basic requirements of the Enterprise to Cloud scenario are much the same as those for the Enterprise to Cloud to End User. Additional requirements for this are:

• Deployment: It should be simple to build a VM image and deploy it to the cloud as necessary. When that VM image is built, it should be possible to move that image from one cloud provider to another, compensating for the different mechanisms vendors have for attaching storage to VMs.

• Industry-specific standards and protocols: Many cloud computing solutions between enterprises will use existing standards. The applicable standards will vary from one application to the other and from one industry to the other.

D. Enterprise to Cloud to Enterprise: This scenario involves two enterprises using the same cloud. The focus here is hosting resources in the cloud so that applications from the enterprises can interoperate. A supply chain is the most obvious example for this scenario. Concerned issues The basic requirements of the Enterprise to Cloud to Enterprise scenario are much the same as those for the Enterprise to Cloud scenario. Other requirements for this scenario are:

• **Transactions and concurrency:** For applications and data shared by different enterprises, transactions and concurrency are vital. If two enterprises are using the same cloud-hosted application, VM, middleware or storage, it's important that any changes made by either enterprise are done reliably.

• **Interoperability:** Because more than one enterprise is involved, interoperability between the enterprises is essential.

E. Private Cloud: The Private Cloud scenario is different from the others in that the cloud is contained within the enterprise. This is useful for larger enterprises. For example, if the payroll department has a surge in workload on the 15th and 30th of each month, they need enough computing power to handle the maximum workload, even though their everyday workload for the rest of the month is much lower. With a private cloud, computing power is spread across the enterprise. The payroll department gets extra cycles when they need it and other departments get extra cycles when they need it. This can deliver significant savings across the enterprise. Concerned issues The basic requirements of the Private Cloud scenario are an open client, metering and monitoring, management and governance, deployment, interoperability, a common VM format, and SLAs. Keeping the cloud inside the enterprise removes many of the requirements for identity management, standards and common APIs. 5.6 Hybrid Cloud: This scenario involves multiple clouds working together, including both public and private clouds. A hybrid cloud can be delivered by a federated cloud provider thatcombines its own resources with those of other providers. The provider of the hybrid cloud must manage cloud resources based on the consumer's terms.

F. Concerned issues All of the requirements of the previous scenarios apply here.

• **SLAs:** A machine readable, standard format for expressing an SLA. This allows the hybrid cloud provider to select resources according to the consumer's terms without human intervention.

Q.1. (g) What kind of needs is addressed by Heterogeneous cloud ? (3)

Ans. Heterogeneity in cloud computing can be considered in at least two ways. The first is in the context of multi-clouds, in which platforms that offer and manage infrastructure and services of multiple cloud providers are considered to be a heterogeneous cloud. Heterogeneity arises from using hypervisors and software suites from multiple vendors. The second is related to low-level heterogeneity at the infrastructure level, in which different types of processors are combined to offer VMs with heterogeneous compute resources. In this paper, the latter is referred to as heterogeneous clouds. While supercomputers have become more heterogeneous by employing accelerators, such as NVIDIA GPUs or Intel Xeon Phis, cloud data centers mostly employ homogeneous architectures. More recently heterogeneous cloud data center architectures have been proposed15 . In the vendor arena, Amazon along with other providers offer GPU-based VMs, but accelerators are not yet fully integrated into the computing ecosystem. This is because it is not yet possible for a programmer to fully develop and execute code oblivious to the underlying hardware. There are a number of efforts in this direction, but the key challenge is achieving a high-level abstraction that can be employed across multiple architectures, such as GPUs, FPGAs and Phis. Further applications that already execute on the cloud cannot be scheduled onto heterogeneous resources. Efforts in this direction are made by the CloudLightning16 project. The concept of a heterogeneous cloud may extend beyond the data center. For example, ad hoc clouds or microclouds could be heterogeneous cloud platforms.Current cloud infrastructures are mostly homogeneous composed of a large number of machines of the same type – centrally managed and made available to the end user using the three standard service models:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

As clouds increase in size and as machines of different types are added to the infrastructure in order to maximize performance and power efficiency, heterogeneous clouds are being created. The heterogeneous cloud is still at a nascent stage, however, larger cloud infrastructure providers are offering commercial services e.g., Amazon Web Services offers a variety of GPU services. As demand for better processor, price and power performance increases, it is anticipated that larger infrastructure providers will need to cater for several of these processor types and specifically for the emerging HPC public cloud market.

However, integrating and managing these different architectures independently and with an existing general purpose cloud architecture is not without challenges; not least of which is access to a pool of qualified engineers with deep IT knowledge. The adoption of heterogeneous resources will dramatically increase the complexity of an already complex cloud ecosystem. We present self-organisation and self-management as powerful techniques for addressing this complexity.

The adoption of heterogeneous computing resources by cloud consumers will also allow for improved resource efficiency and hence reduced energy use. Market demand for greater resource management at the PaaS and IaaS layers combined with both demand and adoption of heterogenous resources is rapidly increasing complexity of the cloud ecosystem which over time will render traditional cloud management techniques ineffectual.

Q.1. (*h*) Define federated clouds? (2)

Ans Refer Q.No. 1. (a) First term 2017.

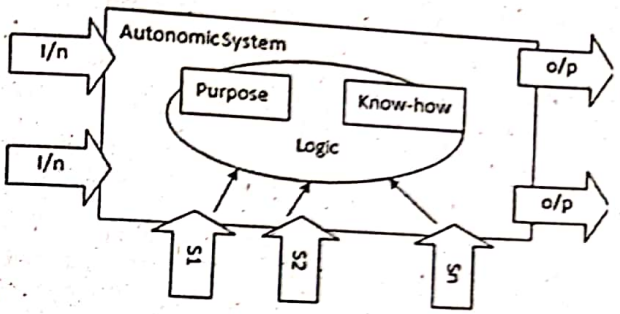
Q.2. (*a*) What is meant by autonomic computing?Why it is considered as pervasive computing ? Explain with examples. (5)

Ans. Autonomic computing is a self-managing computing model named after, and patterned on, the human body's autonomic nervous system. An autonomic computing system would control the functioning of computer applications and systems without input from the user, in the same way that the autonomic nervous system regulates body systems without conscious input from the individual. The goal of autonomic computing is to create systems that run themselves, capable of high-level functioning while keeping the system's complexity invisible to the user.

Autonomic computing is one of the building blocks of pervasive computing, an anticipated future computing model in which tiny - even invisible - computers will be all around us, communicating through increasingly interconnected networks. Many industry leaders, including IBM, HP, Sun, and Microsoftare researching various components of autonomic computing. IBM's project is one of the most prominent and developed initiatives. In an effort to promote open standards for autonomic computing, IBM recently distributed a document that it calls "a blueprint for building self-managing systems," along with associated tools to help put the concepts into practice. Net Integration Technologies advertises its Nitix product as "the world's first autonomic server operating system."

According to IBM, there are eight crucial elements in an autonomic computing system: it must maintain comprehensive and specific knowledge about all its components; it must have the ability to self-configure to suit varying and possibly unpredictable conditions; it must constantly monitor itself for optimal functioning; it must be self-healing and able to find alternate ways to function when it encounters

problems; it must be able to detect threats and protect itself from them; it must be able to adapt to environmental conditions; it must be based on open standards rather than proprietary technologies; and it must anticipate demand while remaining transparent to the user.



Autonomic computing is one of the building blocks of pervasive computing, which is the future of computing model in which many tiny computers will be all around us communicating through increasingly interconnected networks. So if a system for example is self-tuning, does that mean that it never needs to be tuned by a human, or does it mean that a human has to tune it less frequently?Some of the key elements of autonomic computing according to IBM are –

- It must have specific knowledge of all of its components.
- Must have the ability to self configure to suit various unpredictable conditions.
- It must monitor itself for optimum performance and functionality.
- It must be self healing, and able to find alternative ways if encountered with a problem.
- Must detect possible threats and protect it from them.
- It must be able to adapt to environmental conditions.

A basic concept that will be applied in autonomic computing are closed control loops. A well known concept from process control theory. Essentially a closed control loop is a self managing system which monitors some resources (Hardware or Software) and autonomously tries to keep its parameters within a certain range.

The fundamental block of autonomic system is the sensing capability (Sensor S1). This enables the system to observe its external operation. Autonomic system should possess the knowledge of the process i.e. the intention accordingly the knowledge of how to do it i.e. the know-how without any external intervention. The actual operation is defined by the logic which is responsible for making the right decision to fulfil its purpose, influenced by the observation of the operational context (based on the sensors I/P).

Q.2. (b) Differentiate between Grid computing and Distributed computing. (4)

Ans. Refer Q.No. 2(a), End Term Examination,page no.11-2016.

Q.2. (c) What are the different variants of distributed computing ? (3.5)

Ans. A distributed system is a network of autonomous computers that communicate with each other in order to achieve a goal. The computers in a distributed system are independent and do not physically share memory or processors. They communicate with each other using *messages*, pieces of information transferred from one computer to another over a network. Messages can communicate many things: computers can tell other

computers to execute a procedures with particular arguments, they can send and receive packets of data, or send signals that tell other computers to behave a certain way.Computers in a distributed system can have different roles. A computer's role depends on the goal of the system and the computer's own hardware and software properties. There are two predominant ways of organizing computers in a distributed system. The first is the client-server architecture, and the second is the peer-to-peer architecture. Types of distributed system-

1. Distributed computing system. Distributed computing is a computing concept that, in its most general sense, refers to multiple computer systems working on a single problem. In distributed computing, a single problem is divided into many parts, and each part is solved by different computers. As long as the computers are networked, they can communicate with each other to solve the problem. If done properly, the computers perform like a single entity.

The ultimate goal of distributed computing is to maximize performance by connecting users and IT resources in a cost-effective, transparent and reliable manner. It also ensures fault tolerance and enables resource accessibility in the event that one of the components fails.

2. Distributed information system. A set of **information systems** physically **distributed** over multiple sites, which are connected with some kind of communication network. A **system** where, applications (cooperative among one another) stay on different elaborative nod00es and the **information** property, unique, is hosted on different elaborative nodes. 3.Distributed pervasive system.

These system includes

1. Mobile and embedded system
2. Home systems
3. Sensor networks

Q.3. (a) Describe the various issues and challenges in cloud computing. **(5)**

Ans. Cloud Computing Issues & Challenges: Cloud computing is a common term you hear about on and off. And professionals use it without even knowing about the actual concept. So to put it in simple words, cloud computing is storing, accessing, and managing huge data and software applications over the internet. In this technology the entire data is secured by firewall networks. You can use the software without using your computer's hard drive as the software and data is installed in world wide data centres.

1. Data Security concern: When we talk about the security concern of the cloud technology, then a lot of questions remain unanswered. Multiple serious threats like virus attack and hacking of the client's site are the biggest cloud computing data security issues. Entrepreneurs have to think on these issues before adopting cloud computing technology for their business. Since you are transferring your company's important details to a third party so it is important to ensure yourself about the manageability and security system of the cloud.

2. Selecting the perfect cloud set-up: Choosing the appropriate cloud mechanism as per the needs of your business is very necessary. There are three types of clouds configuration such as public, private, and hybrid. The main secret behind successful implementation of the cloud is picking up the right cloud. If you are not selecting the right cloud then maybe you have to face some serious hazards. Some companies having vast data so they prefer private clouds while small organisations usually use public clouds. A few companies like to go for a balanced approach with hybrid clouds. Choose a cloud computing consulting service which is aware and clearly disclose the terms and conditions regarding cloud implementation and data security.

3. Real time monitoring requirements: In some agencies, it is required to monitor their system in real time. It is compulsory term for their business that they continuously monitor and maintain their inventory system. Banks and some government agencies need to update their system in real time but cloud service providers are unable to match this requirement. This is really a big challenge for cloud services providers.

4. Resolving the stress: Every organisation wants to have a proper control and access over the data. It is not easy to handover your precious data to a third party. The main tension between enterprise and executives is they desire to control over the new modes of operations while using technology. These tensions are not unsolvable, but they do suggest that providers and clients alike must deliberately address a suite of cloud challenges in the planning, contracting and managing the services.

5. Reliability on new technology: It is a fact of human nature that we trust on the things present in front of our eyes. Normally entrepreneurs feel hesitation in letting out the organisational information to any unknown service provider. They think that information stored in their office premises is more secure and easily accessible. By using cloud computing they have fear of losing control over the data. They think that data is taken from them and handover to an unknown third party. Security threads are increase as they do not know and where is the information stored and processed. These frights of the unknown service providers must very amicably be dealt with and eliminated form their minds.

6. Dependency on service providers: For uninterrupted services and proper working it is necessary that you acquire a vendor services with proper infrastructural and technical expertise. An authorized vendor who can meet the security standards set by your company's internal policies and government agencies. While selecting the service provider you must carefully read the service level agreement and understand their policies and terms and provision of compensation in case of any outage or lock in clauses.

7. Cultural obstacles: High authority of the company and organisational culture has also become a big obstacle in the proper implementation of the cloud computing. Top authority never wants to store the important data of the company somewhere else where they are not able to control and access the data. They have misconceptions in their minds that cloud computing puts the organisation at the risk by seeping out important details. Their mindset is such that the organization on risk averse footing, which makes it more reluctant to migrate to a cloud solution.

8. Cost barrier: For efficient working of cloud computing you have to bear the high charges of the bandwidth. Business can cut down the cost on hardware but they have to spend a huge amount on the bandwidth. For smaller application cost is not a big issue but for large and complex applications it is a major concern. For transferring complex and intensive data over the network it is very necessary that you have sufficient bandwidth. This is a major obstacle in front of small organisations, which restrict them for implementing cloud technology in their business.

9. Lack of knowledge and expertise: Every organisation does not have sufficient knowledge about the implementation of the cloud solutions. They have not expertise staff and tools for the proper use of cloud technology. Delivering the information and selection the right cloud is quite difficult without right direction. Teaching your staff about the process and tools of the cloud computing is a very big challenge in itself. Requiring an organisation to shift their business to cloud based technology without having any proper knowledge is like asking for disaster. They would never use this technology for their business functions.

10. Consumption basis services charges: Cloud computing services are on-demand services so it is difficult to define specific cost for a particular quantity of services.

These types of fluctuations and price differences make the implementation of cloud computing very difficult and complicated. It is not easy for a normal business owner to study consistent demand and fluctuations with the seasons and various events. So it is hard to budget for a service that could consume several months of budget in a few days of heavy use.

11. Alleviate the threats risk: It is very complicated to certify that the cloud service provider meet the standards for security and threat risk. Every organisation may not have enough mechanism to mitigate these types of threats. Organisations should observe and examine the threats very seriously. There are mainly two types of threat such as internal threats, within the organisations and external threats from the professional hackers who seek out the important information of your business. These threats and security risks put a check on implementing cloud solutions.

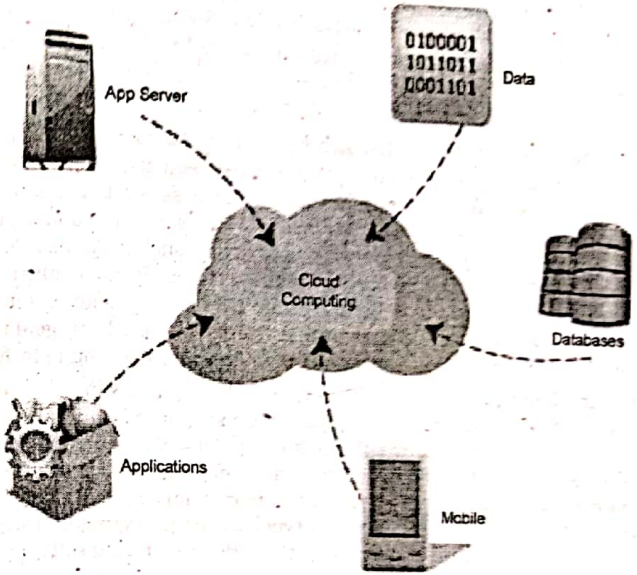
12. Unauthorised service providers: Cloud computing is a new concept for most of the business organisations. A normal businessman is not able to verify the genuineness of the service provider agency. It's very difficult for them to check the whether the vendors meet the security standards or not. They have not an ICT consultant to evaluate the vendors against the worldwide criteria. It is necessary to verify that the vendor must be operating this business for a sufficient time without having any negative record in past. Vendor continuing business without any data loss complaint and have a number of satisfied clients. Market reputation of the vendor should be unblemished.

13. Hacking of brand: Cloud computing carries some major risk factors like hacking. Some professional hackers are able to hack the application by breaking the efficient firewalls and steal the sensitive information of the organisations. A cloud provider hosts numerous clients; each can be affected by actions taken against any one of them. When any threat came into the main server it affects all the other clients also. As in distributed denial of service attacks server requests that inundate a provider from widely distributed computers.

14. Recovery of lost data: Cloud services faces issue of data loss. A proper backup policy for the recovery of data must be placed to deal with the loss. Vendors must set proper infrastructures to efficiently handle with server breakdown and outages. All the cloud computing service providers must set up their servers at economically stable locations where they should have proper arrangements for the backup of all the data in at least two different locations. Ideally they should manage a hot backup and a cold backup site.

15. Data portability: Every person wants to leverage of migrating in and out of the cloud. Ensuring data portability is very necessary. Usually, clients complain about being locked in the cloud technology from where they cannot switch without restraints. There should be no lock in period for switching the cloud. Cloud technology must have capability to integrate efficiently with the on premises. The clients must have a proper contract of data portability with the provider and must have an updated copy of the data to be able to switch service providers, should there be any urgent requirement.

16. Cloud management: Managing a cloud is not an easy task. It consist a lot of technical challenges. A lot of dramatic predictions are famous about the impact of cloud computing. People think that traditional IT department will be outdated and research supports the conclusions that cloud impacts are likely to be more gradual and less linear. Cloud services can easily change and update by the business users. It does not involve any direct involvement of IT department. It is a service provider's responsibility to manage the information and spread it across the organisation. So it is difficult to manage all the complex functionality of cloud computing



17. Dealing with lock-ins: Cloud providers have an important additional incentives to attempt to exploit lock-ins. A prefixed switching cost is always there for any company receiving external services. Exit strategies and lock-in risks are primary concerns for companies looking to exploit cloud computing.

18. Transparency of service provider: There is no transparency in the service provider's infrastructure and service area. You are not able to see the exact location where your data is stored or being processed. It is a big challenge for an organisation to transfer their business information to such an unknown vendor.

19. Transforming the data into virtual set-up: Transition of business data from a premise set up to a virtual set up is a major issue for various organisations. Data migration and network configuration are the serious problems behind avoiding the cloud computing technology.

20. Popularization of cloud computing : The idea of cloud has been famous that there is a rush of implementing virtualization amongst CIOs. This has led to more complexities than solutions.These are some common problems regarding the cloud computing execution in real life. But the benefits of cloud computing are more vast in compare to these hazards. So you should find the perfect solutions and avail the huge benefits of cloud technology in your business. It can take your business to the new heights.

Q. 3. (b) What are the various platforms used in cloud computing? (5)

Ans. Various cloud computing platforms

A. AbiCloud AbiCloud is a cloud computing platform. It can be used to build, integrate and manage public as well as private cloud in the homogeneous environments. Using Abi Cloud, user can easily and automatically deploy and manage the server, storage system, network, virtual devices and applications and so on. Using AbiCloud, user can finish deploying a new service by just dragging a virtual machine with mouse. This is easier and reliable than other cloud platforms. It can also manage Ec2 according to the rules of protocol.

B. Eucalyptus It is an open source private cloud platform for cloud computing that implements infrastructure as a service. Eucalyptus is open source private cloud software

for building private and hybrid clouds that are compatible with AWS APIs. With AWS-compatibility, the open source software pools together existing virtualized infrastructure to create private or hybrid cloud resources for compute, network, and storage. Eucalyptus uses the terminologies like images, instances, and IP addressing, security, networking and access control.

C. Xen Cloud Platform (XCP) The Xen hypervisor is a solution for infrastructure virtualization that provides an abstraction layer between servers hardware and the operating system. A Xen hypervisor allows each physical server to run several "virtual servers" handling the operating system and its applications from the underlying physical server. The Xen solution is used by many cloud solutions such as Amazon Ec2, Nimbus and Eucalyptus. Xen.org invented Xen cloud platform (XCP) as a solution for cloud infrastructure virtualization. But, differently from existent open source cloud solutions, XCP does not provide the overall architecture for cloud services. Their goal is to provide a tool to cope with automatic configuration and maintenance of cloud platforms.

D. Nimbus Nimbus is an open source solution to turn clusters into an infrastructure as a service (IaaS) for cloud computing mainly on scientific applications. To deploy applications, Nimbus offers a "cloud kit" configuration that consists of a manager service hosting and an image repository. Nimbus leaves most of the customization to the administrator and not to the user and has several more components which are constants. Nimbus is very flexible in the number and types of virtual networks that can be set fewer of those options pertain to the nitty-gritty of the underlying software stack.

E. Open Nebula Open Nebula is an open source toolkit to build private, public and hybrid clouds. It has been designed to be integrated with networking and storage solutions and to fix into existing datacenters. It allows user deploy and manage virtual machines on physical resources and it can set users data centers or clusters to flexible virtual infrastructure that can automatically adapt to the change of the service load. The main difference of Open Nebula and Nimbus is that Nimbus implements remote interface based on EC2 or WSRF through which user can process all security related issues, while open nebula does not.The Open Nebula architecture based on the three basic technologies to enable the provision of services on a distributed infrastructure: virtualization, storage and network.

F. Tplatform Tplatform is a cloud solution that provides a development platform for web mining applications, which is inspired in Google cloud technologies and which acts as a platform as a service (PaaS). Their infrastructure is supported by three technologies: a scalable file system called Tianwang File System (TFS) which is similar to the Google File System (GFS), the big table data storage mechanism and the map reduce programming model.

Q.3. (c) What do you mean by high powered cloud ? **(2.5)**

Ans. High-powered cloud computing is a type of cloud computing solution that incorporates standards, procedures and elements from cloud computing. It defines the techniques for achieving computing operations that match the speed of supercomputing from a cloud computing architecture. In this context, HPC cloud computing will provide scientist with access to a massive pool of highly reliable and redundant computing infrastructure that can be provisioned on request and released when not required. The complete solution may include storage, hardware and application software, all of which will be delivered through cloud on an on demand basis.

High powered cloud computing primarily addresses designing large, powerful and robust cloud computing solutions that provide a scalable application runtime environment. The term was first coined by Robert L. Clay of Sandia National Labs to address the challenges faced by scientists who required access to large computing resources.

Q. 4. (a). Define virtualization and what are pros and cons of virtualization. **(5)**

Ans- Refer Q.No. 1(b), End Term Examination-2016.
Refer Q.No. 5(a), End Term Examination, 2016 .

Q.4. (b) What are characterstics of virtualized environments ? **(4)**

Ans. Virtualization has three characteristics that make it ideal for cloud computing:-

Partitioning: In virtualization, many applications and operating systems (OSes) are supported in a single physical system by *partitioning* (separating) the available resources.

Isolation: Each virtual machine is isolated from its host physical system and other virtualized machines. Because of this isolation, if one virtual-instance crashes, it doesn't affect the other virtual machines. In addition, data isn't shared between one virtual container and another.

Encapsulation: A virtual machine can be represented (and even stored) as a single file, so you can identify it easily based on the service it provides. In essence, the encapsulated process could be a business service. This encapsulated virtual machine can be presented to an application as a complete entity. Therefore, encapsulation can protect each application so that it doesn't interfere with another application.

APPLICATIONS OF VIRTUALIZATION

Virtualization can be applied broadly to just about everything that you could imagine:

- Memory
- Networks
- Storage
- Hardware
- Operating systems

Q.4. (c) List and discuss different types of virtualization. **(3.5)**

Ans. Virtualization is the process of creating a virtual environment on an existing server to run your desired program, without interfering with any of the other services provided by the server or host platform to other users. The Virtual environment can be a single instance or a combination of many such as operating systems, Network or Application servers, computing environments, storage devices and other such environments.

While the benefits of virtualization are self-evident, many people are still in the dark when it comes to the many different types of virtualization. Here, we'll show you some of the most common virtualization methods and why they're valuable for your business.

Application Virtualization: This is a process where applications get virtualized and are delivered from a server to the end user's device, such as laptops, smartphones, and tablets. So instead of logging into their computers at work, users will be able to gain access to the application from virtually anywhere, provided an Internet connection is available. This type of virtualization is particularly popular for businesses that require the use of their applications on the go.

Desktop Virtualization: Similar to Application Virtualization mentioned above, desktop virtualization separates the desktop environment from the physical device and configured as a "virtual desktop infrastructure" (VDI). The major advantages of desktop virtualization is that users are able to access all their personal files and applications from any location and on any PC, meaning they can work from anywhere without the need to bring their work computer. It also lowers the cost of licensing for installing

software on desktops and maintenance and patch management is very simple, since all of the virtual desktops are hosted at the same location.

Hardware Virtualization: This is perhaps the most common type of virtualization today. Hardware virtualization is made possible by a virtual machine manager (VM) called the "hypervisor". The hypervisor creates virtual versions of computers and operating systems and consolidates them into one large physical server, so that all the hardware resources can be utilized more efficiently. It also enables users to run different operating systems on the same machine at the same time.

Network Virtualization: Network virtualization is a method that combines all physical networking equipment into a single resource. It is the process of dividing bandwidth into multiple, independent channels, each of which can be assigned to servers and devices in real time. Businesses that would benefit from network virtualization are ones that have a large number of users and need to keep their systems up and running at all times. With the distributed channels, your network speed will increase dramatically, allowing you to deliver services and applications faster than ever before.

Storage Virtualization: This type of virtualization is very easy and cost-effective to implement, since it involves compiling your physical hard drives into a single cluster. Storage virtualization is handy when it comes to planning for disaster recovery, since the data stored on your virtual storage can be replicated and transferred to another location. By consolidating your storage into a centralized system, you can eliminate the hassles and costs of managing multiple storage devices.

Integrating virtualization into your business can be a complex and confusing process. Ideally you will enlist the help of experts to get the job done right. If you're looking for top-quality and reliable virtualization solutions, why not get in touch with our professionals today. We'll make your virtualization experience a quick and painless one.

Q.5. (a) Draw the basic block diagram of cloud computing architecture and also explain it. **(6)**

Ans : Refer Q.No. 5. of First Term exam 2017.

Q.5. (b) What are the various deployment models ? Explain with the diagram. **(6.5)**

Ans. Refer Q.No. 2(b), End term examination, page no.11-2016.

Q.6. (a). What are various service models of cloud computing ? Explain with examples. **(6.5)**

Ans. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Software as a Service (SaaS):

1. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure

2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

3. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Cloud computing providers offer three models as defined by the National Institute of Standards and Technology (NIST), which is a non-regulatory federal agency acting under the U.S Department of Commerce. Service models are defined as the final commodity delivered to a client based on the extent to which the cloud computing ecosystem is partitioned. The different types of service models are the SaaS (Software as a service), PaaS (Platform as a service) and IaaS (Infrastructure as a service) models.

Software as a service (SaaS) is a model in which an application runs directly on the cloud and the user accesses it via the Internet. The service provider is responsible for the infrastructure and the associated maintenance costs. This makes the model extremely cost efficient and flexible for the end user, eliminating hardware and software requirements at the client's end. However, this model has restrictions on the client's application development freedom. Google Docs, Google Sheets are classic examples of SaaS. The SaaS model is most popular and holds the majority of the market share compared to other two models, due to ease of adaptability, good return on investment and reduced time to market.

Platform as a service (PaaS) provides the customer with the development environment including hardware and software tools for various phases of development and network connectivity. The users have the freedom to develop their own applications using the language of their choice without reliance on a web-based console. The caveat with this model is the interoperability of the application between different development environments. Amazon's Relational Database services, Microsoft Azure are examples of this model.

Infrastructure as a Service (IaaS) gives the users the required instance of machine with storage and computational resource tailored to their need. The users have the freedom to provision the network infrastructure, operating system and storage capacity using web based console to meet their application requirements. The users have greater control over the virtual machine and are entirely responsible for the development environment including the installation of the operating system, the required software to develop the application and the timely software updates to the application. Amazon's EC2 is a classic example of this type of service model.

All the three models are extremely efficient for both the cloud service provider and the customer, due to pay per-use model. Since the actual maintenance and the operating costs of the hardware are borne by the service provider, the customers benefit as they do not need to spend capital on maintenance costs while reaping the benefits of the cloud. In the recent times, these basic models have paved the way to newer vertical models like Business Process as a service (BPaaS), which automate certain fixed set of business services that are common across different customers and different departments within

a single organization. In addition, it helps the customers leverage the various APIs in this model in order to customize specific services as per requirement.

Q.6. (b) Describe the fundamental features of the economic and business model behind cloud computing. **(6)**

Ans. The business/economic model is very simple: it's **leasing**.

Essentially the same as a company that rents cars, for example. They distribute the cost of the car among many customers, providing basic services like car maintenance and insurance. They make the cars available for rent by the day(or by the hour).

For the customer, cloud services are based on a few simple principles:

- Metered pricing -Pay for what you use
- On demand - available immediately. Can be turned 'on' or 'off' quickly.
- Operational Expense - instead of the CapEx that would represent a purchase. From an accounting perspective, it hits the books immediately.
- Self service - a customer can consume services on its own.
- Multi-tenancy/resource pooling - the service is shared with other customers

The concept of business model is highly relevant in context of cloud computing. According to Iyer and Henderson , cloud computing is an evolution of the dominant business model for delivering IT-based solutions. Similarly, Zhu argue that cloud computing distinguishes itself from previous computing paradigms with its emerging business model, which creates remarkable commercial value in new use scenarios. The general importance of business model for a firm is demonstrated for example Malone , who find that some business models do have better financial performance than others in a study of over 10,000 US firms. Business model is a concept nowadays widely used in academic and managerial literature as well as in popular discussion. It is used in various domains such as e-business, management, and strategy. The term business model is relatively young: it became popular only towards the end of the 1990s. From the start, the concept of business model has closely related to IT industry; Osterwalder have demonstrated with the stock market data that the surge of the business model term coincidences with the advent of the Internet in the business world. The concept of business model is still relatively poorly understood and there is much confusion in the terminology .Some authors use business model to simply refer the way a company does business whereas other authors emphasize the conceptual model aspect. Nevertheless, previous research agrees on business model's position as a conceptual and theoretical layer between business strategy and business processes . According to Osterwalder and Pigneur business logic triangle model, business model represents the architectural level between planning and implementation.

Q.7(a): What are the various types of specialized cloud architectures? Explain in detail. **(5)**

Ans. Cloud computing is typically classified in the following three ways:

1. Public cloud: In Public cloud the computing infrastructure is hosted by the cWud vendor at the vendora premises. The customer has no. visibility and control over where the computing infrastructure is hosted. The computing infrastructure is shared between any organizations.

2. Private cloud: The computing infrastructure is dedicated to a particular orga/ iization and not shared "with other organizations. Some experts consider that private clouds are not real examples of cloud computing. Private clouds are more expensive and more secure when compared to public clouds.

Private clouds are of two types: On-premise private clouds and externally hosted private clouds. Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. Externally hosted private clouds are cheaper than On-premise private clouds.

3. Hybrid cloud: Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud. A related term is Cloud Bursting. In Cloud bursting organization use their own computing infrastructure for normal usage, but access the cloud using services like Salesforce cloud computing for high/peak load requirements. This ensures that a sudden increase in computing requirement is handled gracefully.

4. Community cloud: Involves sharing of computing infrastructure in between organizations of the same community. For example all Government organizations within the state of California may share computing infrastructure on the cloud to manage data related to citizens residing in California.

Q.7. (b) Explain briefly service management in cloud computing ? **(4)**

Ans. Cloud service management is concerned with aligning both worlds, that is, the world of cloud computing and service management and introducing good cloud management practices among customer, consumer and supplier organisations.

Cloud computing and cloud-based services are not new technology. Cloud principles were followed even for Main frames circa 1950s and 1960s.

There are many frameworks and methods for the management of IT and for service management. In most cases, cloud computing is described as a business model for use of other underlying technologies and not as a technology. Those underlying technologies, such as virtualization, provide the basis for employing cloud computing concepts. Cloud in itself if not a technology.

Cloud Computing-Purpose & Scope

The purpose and scope of cloud service management:

Purpose

- Establish appropriate methods for the management and operation of cloud based services.
- Embed cloud service management practices into existing IT development and support structures.

Scope

- Oversight of the .design, development and transition of cloud based services.
- Management and operation of cloud based services.

Cloud Computing - Features

- Cloud is a style of computing where scalable and elastic IT related capabilities are delivered as a service to consumers using internet technologies.
- Cloud is not defined as a set of technologies, but rather a model for delivering, managing and consuming information technology resources and services.

Cloud Computing - Definition

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing recourses, that is, networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model is composed of five essential characteristics, three service models and four deployment models

The 5 essential Operational Characteristics are:

• **On Demand Self Service** -Automated consumer centric search, selection and provisioning.

• **Measured Service** - Metered resource usage with monitoring, reporting and charging mechanisms.

• **Broad Network Access** - Cloud service accessible connectivity to a range of devices and networks.

• **Resource Pooling** - Shared resources for one or many tenants supporting different demand and supply capacity.

• **Rapid Elasticity** - automated provisioning and scaling for one or many tenants.

The 3 Service Models are:

• **Software as a Service (SaaS)** - Applications which provide business value for users.

• **Platform as a Service (PaaS)** - Applications which provide specialised software components and programming tools.

• **Infrastructure as a Service (IaaS)** -Applications which provide computing infrastructure resources as a service.

The 4 Cloud Deployment Models are:

• **Private Cloud** - This cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers, for example, business units.

• **Community Cloud** — This cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns.

• **Public Cloud** - This cloud infrastructure is provisioned for open use by the general public. It may be owned; managed and operated by a business, academic or government organisation or a combination of these.

• **Hybrid Cloud** — This cloud infrastructure is a composition of two or more distinct cloud infrastructures, such as private and public community that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability.

Q.7. (c) Discuss the benefits of cloud computing. **(3.5)**

Ans. Advantages of Cloud Computing are as follows:

Cost Savings: Perhaps, the most significant cloud computing benefit is in terms of IT cost savings. Businesses, no matter what their type or size, exist to earn money while keeping capital and operational expenses to a minimum. With cloud computing, you can save substantial capital costs with zero in-house server storage and application requirements. The lack of on-premises infrastructure also removes their associated operational costs in the form of power, air conditioning and administration Costs. You pay for what is used and disengage whenever you like - there is no invested IT capital to worry about. It's a common misconception that only large businesses can afford to use the cloud, when in fact, cloud services are extremely affordable for smaller businesses.

Reliability: With a managed service platform, cloud computing is much more reliable and consistent than in-house IT infrastructure. Most providers offer a Service Level Agreement which guarantees 24/7/365 and 99.99% availability. Your organization can benefit from a massive pool of redundant IT resources, as well as quick failover mechanism - if a server fails, hosted applications and services can easily be transited to any of the available servers.

Manageability: Cloud computing provides enhanced and simplified IT management and maintenance capabilities through central administration of resources, vendor managed infrastructure and SLA backed agreements. IT infrastructure updates and maintenance are eliminated, as all resources are maintained by the service provider. You enjoy a simple web-based user interface for accessing software, applications and services - without the need for installation - and an SLA ensures the timely and guaranteed delivery, management and maintenance of your IT services".

Strategic Edge: Ever-increasing computing resources give you a competitive edge over competitors, as the time you require for IT procurement is virtually nil. Your company can deploy mission critical applications that deliver significant business benefits, without any upfront costs and minimal provisioning time. Cloud computing allows you to forget about technology and focus on your key business activities and objectives. It can also help you to reduce the time needed to market newer applications and services.

Q.8. (a). Write a short note on the following: **(3)**

(i) Enterprise software.

Ans. Enterprise Cloud Computing refers to a computing environment residing behind a firewall that delivers software, infrastructure and platform services to an enterprise. Cloud computing also typically delivers Web services, providing access to components that can be easily combined to rapidly create composite web applications to meet the ever changing needs of a business operation. Web services rely on service oriented architecture that provides software developers with interfaces that leverage functionality contained within existing web applications, resulting in reduced web application development time frames and lower software development costs for an enterprise.

ENTERPRISE CLOUD COMPUTING BENEFITS

Enterprise Cloud Computing offers many benefits to an organization, including superior speed and performance for IT resources, more efficient utilization of IT resources, lower IT infrastructure costs, lower IT operational costs and increased capacity to handle peaks in demand for IT resources, like web applications and services. Cloud computing within an enterprise also provides a safer computing environment, through the use of virtual servers, that reduces the threat of an on site intruder attack on the physical storage devices within a data center. Enterprise cloud computing also provides the capacity for flexible data security policies, where security decisions can be made based on a variety of factors including: the user's role within the enterprise, the user's current access location, the type of data or application being accessed by the user and the type of device being used.

IMPLEMENTATION OF CLOUD COMPUTING WITHIN AN ENTERPRISE

With Enterprise Cloud Computing, the bottlenecks that typically occur with the configuration, expansion and replacement of traditional on premise IT systems and components can be eliminated, since the IT infrastructure can be expanded or contracted on demand through virtualization. Cloud computing eliminates the typical challenges presented by localized power grid interruptions, physical data loss due to catastrophic events and malicious on site attacks to the IT infrastructure within an organization. The cloud computing framework provides an optimal environment for faster, safer and cheaper delivery of IT services within an enterprise.

Q.8. (ii) Cloud Security Mechanism **(3)**

Ans. Refer Q.No. 6(a), , end term examination,page no.18-2016.

Q.8. (b) Differentiate between-

(i) Service oriented computing and market oriented cloud computing.

(3.5)

Ans. SOC: Service-oriented computing (SOC) is considered today a key enabler for the development of robust and high-quality intelligent Internet-scale distributed applications. Extensive research and development in the past few years has pushed SOC technology into state-of-the-art applications in emerging areas such as Cloud computing, Internet-of-Things (IoT), Machine-to-Machine (M2M) communication, Cyber-Physical Systems (CPSs), Mobile-Edge Computing, Social computing as well as mobile and enterprise systems. However, many of the critical components on building reliable, robust, and user-centric, cloud-based service-oriented architecture applications and systems are still open for research. Hence, it is time to face new service-oriented architecture (SOA) research opportunities by addressing new research challenges on emerging applications domains like smart cities, smart logistics, smart factories and e-Health, just to mention a few.

Many of the service components are deployed on resource-limited embedded systems and are performance sensitive; others are deployed on cloud servers providing highly parallel services and on edge servers in the middle of resource-limited systems and high-end servers. Edge servers and clouds are connected through various types of networks, including emerging network function virtualization services. These components are part of complex applications and systems that span multiple execution environments. Their capabilities are increasingly being managed and (re)configured via emerging software-defined and elasticity mechanisms. In addition, they have to interact with humans in order to obtain useful human-sensing data and solve complex problems. Thus, on the one hand, SOC may provide effective solutions for managing the ever-increasing complexity while meeting the challenging requirements of services on largely distributed, heterogeneous and dynamic resource environments. On the other hand, the exploitation of emerging trends in such environments to build SOC applications and systems for large-scale service-based systems is an open research challenge.

MOC: As consumers rely on Cloud providers to supply all their computing needs, they will require specific QoS to be maintained by their providers in order to meet their objectives and sustain their operations. Cloud providers will need to consider and meet different QoS parameters of each individual consumer as negotiated in specific SLAs. To achieve this, Cloud providers can no longer continue to deploy traditional system-centric resource management architecture that do not provide incentives for them to share their resources and still regard all service requests to be of equal importance. Instead, market-oriented resource management [7] is necessary to regulate the supply and demand of Cloud resources at market equilibrium, provide feedback in terms of economic incentives for both Cloud consumers and providers, and promote QoS-based resource allocation mechanisms that differentiate service requests based on their utility. Figure shows the high-level architecture for supporting market-oriented resource allocation in Data Centers and Clouds. There are basically four main entities involved:

• **Users/Brokers:** Users or brokers acting on their behalf submit service requests from anywhere in the world to the Data Center and Cloud to be processed.

• **SLA Resource Allocator:** The SLA Resource Allocator acts as the interface between the Data Center/Cloud service provider and external users/brokers. It requires the interaction of the following mechanisms to support SLA-oriented resource management:

• **Service Request Examiner and Admission Control:** When a service request is first submitted, the Service Request Examiner and Admission Control mechanism interprets the submitted request for QoS requirements before determining whether to accept or reject the request. Thus, it ensures that there is no overloading of resources whereby many service requests cannot be fulfilled successfully due to limited resources available. It also needs the latest status information regarding resource availability (from VM Monitor mechanism) and workload processing (from Service Request Monitor mechanism) in order to make resource allocation decisions effectively. Then, it assigns requests to VMs and determines resource entitlements for allocated VMs.

• **Pricing:** The Pricing mechanism decides how service requests are charged. For instance, requests can be charged based on submission time (peak/off-peak), pricing rates (fixed/changing) or availability of resources (supply/demand). Pricing serves as a basis for managing the supply and demand of computing resources within the Data Center and facilitates in prioritizing resource allocations effectively. o Accounting: The Accounting mechanism maintains the actual usage of resources by requests so that the final cost can be computed and charged to the users. In addition, the maintained historical usage information can be utilized by the Service Request Examiner and Admission Control mechanism to improve resource allocation decisions.

• **VM Monitor:** The VM Monitor mechanism keeps track of the availability of VMs and their resource entitlements.

• **Dispatcher:** The Dispatcher mechanism starts the execution of accepted service requests on allocated VMs.

• **Service Request Monitor:** The Service Request Monitor mechanism keeps track of the execution progress of service requests.

• **VMs:** Multiple VMs can be started and stopped dynamically on a single physical machine to meet accepted service requests, hence providing maximum flexibility to configure various partitions of resources on the same physical machine to different specific requirements of service requests. In addition, multiple VMs can concurrently run applications based on different operating system environments on a single physical machine since every VM is completely isolated from one another on the same physical machine.

• **Physical Machines:** The Data Center comprises multiple computing servers that provide resources to meet service demands. In the case of a Cloud as a commercial offering to enable crucial business operations of companies, there are critical QoS parameters to consider in a service request, such as time, cost, reliability and trust/security. In particular, QoS requirements cannot be static and need to be dynamically updated over time due to continuing changes in business operations and operating environments. In short, there should be greater importance on customers since they pay for accessing services in Clouds. In addition, the state-ofthe-art in Cloud computing has no or limited support for dynamic negotiation of SLAs between participants and mechanisms for automatic allocation of resources to multiple competing requests. Recently, we have developed negotiation mechanisms based on alternate offers protocol for establishing SLAs .These have high potential for their adoption in Cloud computing systems built using VMs. Commercial offerings of market-oriented Clouds must be able to:

• support customer-driven service management based on customer profiles and requested service requirements,

• Define computational risk management tactics to identify, assess, and manage risks involved in the execution of applications with regards to service requirements and customer needs,

• Derive appropriate market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain SLA-oriented resource allocation,

• Incorporate autonomic resource management models that effectively self-manage changes in service requirements to satisfy both new service demands and existing service obligations, and

• leverage VM technology to dynamically assign resource shares according to service requirements.

Q.8. (b) (*ii*) Serial computing and Parallel computing. (3)

Ans. The Parallel Computing is evolved from serial computing that attempts to emulate what has always been the state of affairs in natural World .Serial and Parallel Computing Traditionally, software has been written for **serial** computation:n a single computer having a single Central Processing Unit (CPU).Parallel computing is the simultaneous use of multiple compute resources to solve a computational problem: part is further broken down to a series of instructions.

Limits to serial computing : both physical and practical reasons pose significant constraints to simply building ever faster serial computers.

<Transmission speeds : the speed of a serial computer is directly dependent upon how fast data can move through hardware. Absolute limits are the speed of light (30 cm/nanosecond) and the transmission limit of copper wire (9 cm/nanosecond). Increasing speeds necessitate increasing proximity of processing elements.

<Limits to miniaturization : processor technology is allowing an increasing number of transistors to be placed on a chip. However, even with molecular or atomic-level components, a limit will be reached on how small components can be.

<Economic limitations : it is increasingly expensive to make a single processor faster. Using a larger number of moderately fast commodity processors to achieve the same (or better) performance is less expensive.

***While parallel computing*:** is the simultaneous use of multiple compute resources to solve a computational problem:

- A problem is broken into discrete parts that can be solved concurrently.
- Each part is further broken down to a series of instructions.
- Instructions from each part execute simultaneously on different processors.
- An overall control/coordination mechanism is employed.
- The computational problem should be able to:
  - Be broken apart into discrete pieces of work that can be solved simultaneously;
  - Execute multiple program instructions at any moment in time;
  - Be solved in less time with multiple compute resources than with a single compute resource.
- The compute resources are typically:
  - A single computer with multiple processors/coreso
  - An arbitrary number of such computers connected by a network

FIRST TERM EXAMINATION [SEP. 2018]
SEVENTH SEMESTER [B.TECH]
CLOUD COMPUTING [ETIT-407]

Time : 1½ hrs. **M.M. : 30**

Note: *Attempt any three questions including Q. no. 1 which is compulsory.*

Q.1. (a) What is Hypervisor in Cloud Computing and its types? **(2.5)**

Ans. The hypervisor is a virtual machine monitor (VMM) that manages resources for virtual machines. The name hypervisor is suggested as it is a supervisory tool for the virtual machines. There are mainly two types of hypervisors:

Type-1: the guest Vm runs directly over the host hardware, e.g Xen, Hyper-V, VmWare ESXi

Type-2: the guest Vm runs over hardware through a host OS, e.g Kvm, Oracle virtualbox

Q. 1. (b) What are main features of cloud services? **(2.5)**

Ans. Some important features of the cloud service are given as follows:

Accessing and managing the commercial software.

Centralizing the activities of management of software in the Web environment.

Developing applications that are capable of managing several clients.

Centralizing the updating feature of software that eliminates the need of downloading the upgrades.

Q. 1. (c) Explain hybrid and community cloud. **(5)**

Ans. The hybridcloud consists of multiple service providers. This model integrates various cloud services for Hybrid Web hosting. It is basically a combination of private and public cloud features. It is used by the company when a company has requirements for both the private and public clouds. Consider an example when an organization wants to implement the SaaS (Software as a Service) application throughout the company. The implementation requires security that can be provided by the private cloud used inside the firewall. The additional security can be provided by the VPN on requirement. Now, the organization has both the private and public cloud features. The communitycloud provides a number of benefits, such as privacy and security. This model, which is quite expensive, is used when the organizations having common goals and requirements are ready to share the benefits of the cloud service.

Q. 2. (a) Mention what is the difference between elasticity and scalability in cloud computing? **(4)**

Scalability is a typical characteristic of cloud computing which is used to handle the escalating workload by escalating in proportion amount of resource capacity. By the use of scalability, the architecture provides resources on requirement BA is resources as and when the requirement is being raised by the traffic. On the other hand,

Elasticity is a characteristic that provides for the concept of commissioning and decommissioning of thehuge amount of resource capacity dynamically. It is usually measured by the speed by which the resources are coming on demand and the usage of those resources.

Q. 2. (b) what is virtual desktop infrastructure? **(6)**

Ans. Refer Q. 5. (a) End term Examination (Dec. 2018)

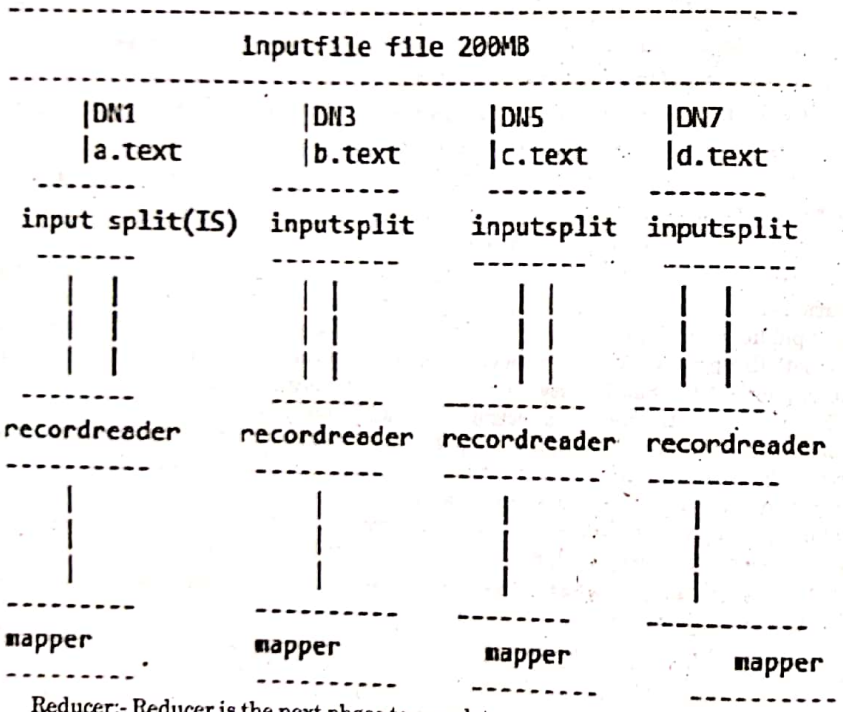
Q. 3. Explain the role of Map and Reduce phase in hadoop. **(10)**

Ans. Actually Map-reduce is a programming model for on Hadoop framework. Map-reduce is not a framework. It is programming model for fast data processing. It can deal with structured, unstructured, semi structured data.

Now, what is Mapper and what is Reducer. So,

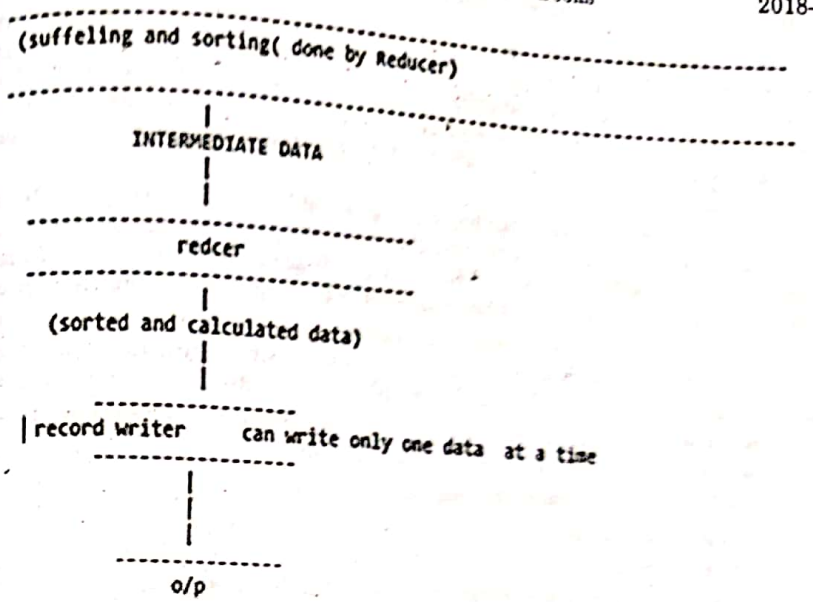
Mapper :- Mapper is a first phase to solve your problem. Most of the time programmer writes 60% to 70% of the logic on Mapper phase only. In this phase all the computation, processing and distribution of data takes place. So this is very very important on the point of designing strategy to deal with the problem. In this phase programmer writes its logic that will deal with the data. Mapper phase works on concept of parallel processing (Hadoop uses divide and conquer approach to solve the problem) for fast execution.

If I talk more logically then, Mapper is not a first step to solve your problem, Input Split is first step but programmers don't write logic/code for this it is already defined on Hadoop framework. ThenRecord Reader comes, that takes input from Input Split and break your problem to more narrow and pass it to Mapper (so ideally Mapper is the third phase of Hadoop framework)

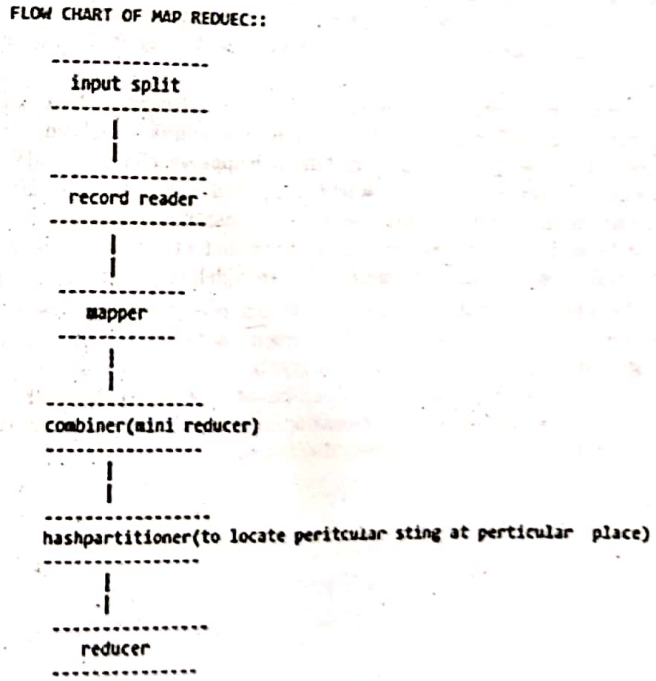


Reducer:- Reducer is the next phase to complete your rest of the 30% logic. It is last phase to design/solve your problem. So whatever your final logic is write on Reducer phase.

There are two sub parts that internally works before your code give its final result, that are shuffle and sort. Shuffle just to collect similar type of works into single unit and Sort for sorting data into some order.



and finally see whole process with combine and Hash partitioner



Q. 4. What are the workflow changes with the use of cloud computing? **(10)**

Ans. Small and medium sized businesses can now compete on an even keel with the big guns, thanks to the way cloud computing has crushed the barriers that were once typical when even the simplest workflows were required. Licensing costs have tumbled, infrastructure headaches have dissipated, clumsy UI is fast becoming a thing of the past, and some configuration and customization can be completed by people with only basic IT expertise.

The benefits also extend to the big end of town, with cloud-based software often far easier to implement. Rolling out new workflows and changing existing ones has become faster in cloud-based applications. Additionally, user adoption can be hastened due to optimisation for mobility devices and accessibility from any internet-enabled device.

Cloud-based computing means less reliance on organisational IT teams. It's becoming increasingly common for executives and business owners to implement integrated cloud-based workflow solutions without the involvement of IT.

This is enabling a new breed of users to leverage the power of workflow tools to automate complex series of business process steps and:

- Solve existing business challenges
- Improve productivity
- Improve compliance
- Reduce the non-value adding activities in their business.

Best of all, cloud-based workflow apps like WorkflowMax save business owners their most precious resource – time. Less time thinking about the process 'stuff', more time thinking about revenue generating goodness. And data integration across mobile devices such as phone and tablets has enabled business owners to seemingly be in two places at one time.

common business processes in technology and consulting organizations have been revolutionised, simplified and drastically improved thanks to cloud. Take expense management. Expense claims can be routed through approval channels and finance teams for processing. However, cloud-based workflow apps like WorkflowMax can incorporate certain business rules and standards, so if the expense claim fails to meet one of those rules it can be auto-rejected, prompting the claimant to fix the issue and resubmit. These types of workflows save significant time and drive a high level of compliance and visibility.

The cloud has also enabled many businesses to become more global in their reach and customer base thanks to improved opportunities to connect with, and service, a worldwide customer base. This is particularly the case for many software companies that have transitioned key functions to cloud-based apps that drive workflows. Typical areas that are prime for workflow automation include technical support requests and access to training and knowledge base information.

END TERM EXAMINATION [DEC. 2018]
SEVENTH SEMESTER [B.TECH]
CLOUD COMPUTING [ETIT–407]

Times: 3 hrs. **M.M. : 75**

Note: Attempt any five questions including Q. no. 1 which is compulsory.

Q.1. (a) Explain issues and challenges in cloud computing. (5)

Ans. Refer Q. 3. (c) End Term Examination 2016.

Q. 1. (b) What is peer to Peer cloud? (5)

Ans. Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or work loads between peers. Peers are equally privileged, equipment participants in the application. They are said to form a peer-to-peer network of nodes.

Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided. Emerging collaborative P2P systems are going beyond the era of peers doing similar things while sharing resources, and are looking for diverse peers that can bring in unique resources and capabilities to a virtual community thereby empowering it to engage in greater tasks beyond those that can be accomplished by individual peers, yet that are beneficial to all the peers.

Q. 1. (c) Explain CRM in detail. (5)

Ans. CRM (customer relationship management) is all aspects of interactions that a company has with its customers, whether it is sales or service-related. While the phrase customer relationship management is most commonly used to describe a business-customer relationship (B2C), CRM is also used to manage business to business (B2B) relationships. Information tracked in a CRM system includes contacts, clients, contract wins and sales leads and more.

CRM tools make the customer-facing functions of business easier. They help you:

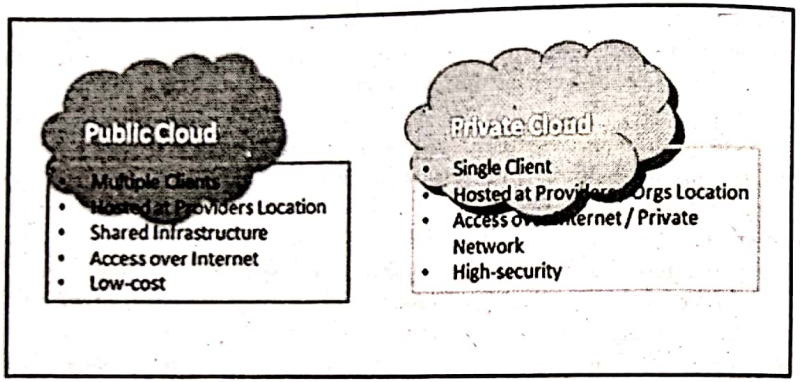
1. Centralize customer information
2. Automate marketing interactions
3. Provide business intelligenc
4. Facilitate communications
5. Track sales opportunities
6. Analyze data
7. Enable responsive customer service

Q. 1. (d) Differentiate between public and private clouds. (5)

Ans. Private Cloud: A private cloud hosting solution, also known as an internal or enterprise cloud, resides on company's intranet or hosted data center where all of your data is protected behind a firewall. This can be a great option for companies who already have expensive data centers because they can use their current infrastructure. However, the main drawback people see with a private cloud is that all management, maintenance and updating of data centers is the responsibility of the company. Over time, it's expected that your servers will need to be replaced, which can get very expensive. On the other

hand, private clouds offer an increased level of security and they share very few, if any, resources with other organizations.

Public Cloud: The main differentiator between public and private clouds is that you aren't responsible for any of the management of a public cloud hosting solution. Your data is stored in the provider's data center and the provider is responsible for the management and maintenance of the data center. This type of cloud environment is appealing to many companies because it reduces lead times in testing and deploying new products. However, the drawback is that many companies feel security could be lacking with a public cloud. Even though you don't control the security of a public cloud, all of your data remains separate from others and security breaches of public clouds are rare.



Q. 1. (e) What is server virtualization in cloud computing? (5)

Ans. Virtualization is a single system file that acts like a real computer, and can be thought of as a logical representation of a server or computer. How do you know if virtualization is the right way to proceed for your business?

Let's look into how virtualization works and what it might add to your enterprise. Multiple virtual computers live on one piece of hardware. You can have a virtual server or virtual desktop. Virtualization is accomplished through software. The concept of virtualization is fairly encompassing and can include devices, servers, operating systems, applications and networks.

Benefits of Virtualization in Cloud Computing:

Dynamic Architecture: Virtualization results in a more dynamic and flexible architecture. Virtual servers are easy to create and maintain. Storage for the virtual machine grows as needed. A virtual machine can run its own operating system. For example, even though the great majority of your programs are Windows based, one aspect of your business might require Linux. Or you may need to run software on an obsolete platform. Virtualization allows many operating systems to co-exist on the same hardware.

Easy Beta Testing Environment: You can also do beta testing in a virtual development environment and avoid corruption of other software. A crash on one virtual computer is confined to that system and other virtual computers on the same hardware are unaffected. If there's one workstation hardware failure, the user can go to a functioning workstation and pick up exactly where she left off.

Quick Back Up and Recovery: Not only does virtualization support the present tense, it's a simple matter to go back in time as well. With the snapshotting function of virtualization, you capture an image of a server at a given moment and can revert to that place anytime. To also prevent downtimes most virtual server environments such as iSySair Cloud Hosting, are equipped with the ability to automatically backup data

at a second data center to ensure maximum data security even if there is a disaster, or technical glitch with one data center.

Cost Reduction: Perhaps the most compelling reason to virtualize is a reduced Total Cost of Ownership (TCO). There is a reduced data center footprint because multiple servers share space on one machine. That consolidation translates into a lower energy bill, and the subsequent reduced energy usage is good for the environment. Virtualized machines reduce downtime, as data can be migrated with minimal interruption, which is known as live migration. Because data is on the server and not spread out over many desktops, virtualization offers increased security, with easier and centralized administration.

Q. 2. (a) What are the different computing service layers involved in cloud computing. (6.5)

Ans. Refer Q. 6. (a) End Term Examination 2017.

Q. 2. (b) Explain characteristics of cloud computing. (6)

Ans. On-demand self-service.

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access.

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling.

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity.

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

Measured service.

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Q. 3. (a) What is community cloud and also discuss its applications. (6.5)

Ans. Refer Q. 2. (b) End term Examination (Dec. 2016)

Media industry. In the media industry, companies are looking for low-cost, agile, and simple solutions to improve the efficiency of content production. Most media productions involve an extended ecosystem of partners. In particular, the creation of digital content is the outcome of a collaborative process that includes movement of large data, massive compute-intensive rendering tasks, and complex workflow executions.

Community clouds can provide a shared environment where services can facilitate business-to-business collaboration and offer the horsepower in terms of aggregate bandwidth, CPU, and storage required to efficiently support media production.

• ***Healthcare industry.*** In the healthcare industry, there are different scenarios in which community clouds could be of use. In particular, community clouds can provide a global platform on which to share information and knowledge without revealing sensitive data maintained within the private infrastructure. The naturally hybrid deployment model of community clouds can easily support the storing of patient-related data in a private cloud while using the shared infrastructure for noncritical services and automating processes within hospitals.

• ***Energy and other core industries.*** In these sectors, community clouds can bundle the comprehensive set of solutions that together vertically address management, deployment, and orchestration of services and operations. Since these industries involve different providers, vendors, and organizations, a community cloud can provide the right type of infrastructure to create an open and fair market.

• ***Public sector.*** Legal and political restrictions in the public sector can limit the adoption of public cloud offerings. Moreover, governmental processes involve several institutions and agencies and are aimed at providing strategic solutions at local, national, and international administrative levels. They involve business-to-administration, citizen-to-administration, and possibly business-to-business processes. Some examples include invoice approval, infrastructure planning, and public hearings. A community cloud can constitute the optimal venue to provide a distributed environment in which to create a communication platform for performing such operations.

• ***Scientific research.*** Science clouds are an interesting example of community clouds. In this case, the common interest driving different organizations sharing a large distributed infrastructure is scientific computing.

Q. 3. (b) Explain the following.

(a) Infrastructure-as-a-service (Iaas)

(b) Platform-as-service (Paas)

(c) Software-as-a-service (Saas) **(6)**

Ans. Refer Q. 6. (a) End term Examination 2017.

Q. 4. (a) Explain the types of cloud and its standard. **(6.5)**

Ans. Cloud computing is typically classified in the following three ways:

1. Public cloud: In Public cloud the computing infrastructure is hosted by the cloud vendor at the vendor premises. The customer has no visibility and control over where the computing infrastructure is hosted. The computing infrastructure is shared between any organizations.

2. Private cloud: The computing infrastructure is dedicated to a particular organization and not shared with other organizations. Some experts consider that private clouds are not real examples of cloud computing. Private clouds are more expensive and more secure when compared to public clouds.

Private clouds are of two types: On-premise private clouds and externally hosted private clouds. Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. Externally hosted private clouds are cheaper than On-premise private clouds.

3. Hybrid cloud: Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud. A related term is Cloud Bursting. In Cloud bursting organization use their own computing infrastructure for normal usage, but access the cloud using services like Salesforce cloud computing for high/peak load requirements. This ensures that a sudden increase in computing requirement is handled gracefully.

4. Community cloud: Involves sharing of computing infrastructure in between organizations of the same community. For example all Government organizations within the state of California may share computing infrastructure on the cloud to manage data related to citizens residing in California.

Classification based upon service provided

Based upon the services offered, clouds are classified in the following ways:

1.Infrastructure as a service (IaaS) involves offering hardware related services using the principles of cloud computing. These could include some kind of storage services (database or disk storage) or virtual servers. Leading vendors that provide Infrastructure as a service are Amazon EC2, Amazon S3,Rackspace Cloud Servers and Flexiscale.

2. Platform as a Service (PaaS) involves offering a development platform on the cloud. Platforms provided by different vendors are typically not compatible. Typical players in PaaS are Googles Application Engine, Microsofts Azure, Salesforce.com force.com .

3. Software as a service (SaaS) includes a complete software offering on the cloud. Users can access a software application hosted by the cloud vendor on pay-per-use basis. This is a well-established sector. The pioneer in this field has been Salesforce.coms offering in the online Customer Relationship Management (CRM) space. Other examples are online email providers like Googles gmail and Microsofts hotmail, Google docs and Microsofts online version of office called BPOS (Business Productivity Online Standard Suite).

The above classification is well accepted in the industry. David Linthicum describes a more granular classification on the basis of service provided. These are listed below:

1. Storage-as-a-service
2. Database-as-a-service
3. Information-as-a-service
4. Process-as-a-service
5. Application-as-a-service
6. Platform-as-a-service
7. Integration-as-a-service
8. Security-as-a-service
9. Management/Governance-as-a-service

10. Testing-as-a-service

11. Infrastructure-as-a-service

Q. 4. (b) How satellite image processing uses cloud computing? **(6)**

Ans. SATELLITE IMAGERY & CLOUD STORAGE

Satellite imagery consists of photographs of Earth or other planets made by means ofartificial satellites.

There are four types of resolution in context of satellite imagery in remotesensing which include the following : (a) Spatial resolution is defined as the pixel size of an image representing the size ofthe surface area (i.e. m2) being measured on the ground, determined by the sensors'instantaneous field of view (IFOV); (b) Spectral resolution is defined by the wavelength interval size (discreet segment ofthe Electromagnetic Spectrum) and number intervals that the sensor is measuring; (c) Temporal resolution is defined by the amount of time (i.e. days) that passesbetween imagery collection periods; (d) Radiometric resolution is defined as the ability of an imaging system to recordmany levels of brightness (contrast for example). Radiometric resolution refers to theeffective bit-depth of the sensor (number of greyscale levels) and is typicallyexpressed as 8-bit (0-255), 11-bit (0-2047), 12-bit (0-4095) or 16-bit (0-65,535). Owing to relatively brobdingnagian and critical requisites of high resolution of thereceived satellite images, further results in demand of large capacity storage requirements of data.

In such scenario's

cloud architectures can come to rescue to easily and conveniently provision larger amounts of storage and computing power; they also offer easy access tocentrally located information reachable through any compatible device a user wishes toimplement; they can provide a back-up to locally stored data; they allow people to easilyshare their data with others. But at the same time there is always going to be an optimum 'balance point' that identifies the 'best' mix of local (PC) processing and storage, on-premise(enterprise data center) processing, storage and networking, as well as 'cloud' processing.That balance point changes would again be dependent on the relative cost-effectiveness of processing power, storage, and data communication changes. The advantages are briefly mentioned below : (a) Investment only for storage that is used and no idle & wasted space. (b) No need to install physical storage devices in their datacenters or offices, whichreduces IT and hosting costs. (c) Storage maintenance tasks, such as backup, data replication, and purchasing additional storage devices are offloaded to the responsibility of a service provider, allowing organizations to focus on their core business only.

Cloud Computing for a Universe of Data

Nebula combines cloud computing and data center containers. It is a new datapowerhouse, which provides on-demand computing power for NASA researchers. The Nebula application lives in a 40-foot container at the NASA Ames Research Center in Mountain View, Calif. The data center in a box was built inside a container fromwhich is filled with Cisco Systems' Unified Computing System and servers from Silicon Mechanics.

Nebula is a self-service platform built from open source software that provides highcapacity computing, storage, and network connectivity for NASA research. It has been designed to automatically increase the computing power and storage available to science-and data-oriented web applications as demand rises. Nebula thus allows for rapid expansion of IT infrastructure, and can provide excellent energy efficiency by offering more precise control of airflow within the container. It provides high-capacity computing, storage, and network connectivity and uses a virtualized, scalable approach to achieve

cost and energy efficiencies. The project began in 2007 and is an open-source project and uses a variety of open-source components, including Eucalyptus, Lustre and RabbitMQ.The Ames Internet Exchange hosts the Nebula Cloud, and also provisions Nebula to connect with 10 GigE-connections. Nebula provides three classes of storage:

(a) Local Storage

Virtual Machines use local storage to run, but the information is localdisk and is not saved by default. Nebula uses hot-swappable commodity drives in a hardware RAID configuration. This allows up to 3 drives to fail before data loss occurs.

(b) Persistent Block Device (iSCSI)

Nebula uses iSCSI to provide a persistent networks torage block device. This storage is always backed up. This type of storage can beused by conventional applications that have not been converted to cloud architectures.This allows highly-reliable and permanent storage, and decouples the storage from the connected server as a single point-of-failure.

(c) Object Store:

With Object Store, it is easy to store petabytes of data and billions offiles. Open-Source implementations of object stores have been used with custom codethat adds in the access control layer (ACL) and management and potentially the API layer

Q. 5. (a) What is virtual desktop infrastructure? **(6.5)**

Ans. Virtual desktop infrastructure (VDI) is virtualization technology that hosts a desktop operating system on a centralized server in a data center. VDI is a variation on the client-server computing model, sometimes referred to as server-based computing. The term was coined by VMware.

There are two main approaches to VDI: persistent and non-persistent. Persistent VDI provides each user with his or her own desktop image, which can be customized and saved for future use, much like a traditional physical desktop. Nonpersistent VDI provides a pool of uniform desktops that users can access when needed. Nonpersistent desktops revert to their original state each time the user logs out.

Benefits of VDI

Virtual desktop infrastructure is a desktop virtualization approach in which a desktop operating system, typically Microsoft Windows, runs and is managed in a data center. The desktop image is delivered over a network to an endpoint device, which allows the user to interact with the OS and its applications as if they were running locally. The endpoint may be a traditional PC, thin client or even a mobile device.

This approach can have many benefits, depending on the type of VDI deployed. Because little actual computing takes place at the endpoint, IT departments may be able to extend the lifespan of otherwise obsolete PCs by repurposing them as VDI clients. And when the time does come to purchase new devices, organizations can buy cheaper, less powerful machines.

Because all data lives in the data center, not on the endpoint, there are significant security benefits of VDI. A thief who steals a laptop that uses VDI can't take any data off the machine, because there is no data on the machine.

Non-persistent VDI also helps when it comes to management. IT has a minimal number of master images to maintain and secure, which is much simpler than managing a complete desktop for each user.

Other benefits of VDI include the ability to more easily support remote and mobile workers.

Drawbacks of VDI

The cost savings associated with endpoint hardware can disappear quickly, however, after factoring in IT infrastructure expenses.

Storage in particular can make VDI cost prohibitive. When a desktop runs locally, the operating system, applications, data and settings are all stored on the endpoint. There is no extra storage cost; it's included in the price of the PC. With persistent VDI, however, the OS, applications, data and settings for every single user must be stored in the data center. Capacity needs, and the cost required to meet them, can quickly balloon out of control.

Converged infrastructure and hyper-converged infrastructure products, which bundle storage, servers, networking and virtualization software — often specifically for VDI deployments — have emerged to help address the scalability and cost challenges associated with virtual desktop infrastructure.

VDI's reliance on network connectivity presents another challenge. Users can't access their virtual desktops without a network connection, and weak connectivity can hinder desktop performance. This problem is especially common with graphics-intensive applications and other software with high processing demands.

In addition, VDI can complicate software licensing and support. Non-persistent VDI especially causes issues, because some licensing and support agreements do not allow for software to be shared among multiple devices and/or users.

Q. 5. (b) How does an unauthorized access can be detected by the help of virtualization techniques. **(6)**

Ans. Virtualization can be used in many ways and requires appropriate security controls in each situation. This article will explore the ways you can use virtualization to increase the security of your Windows environment.

The following are the few ways to minimize risks and improve security using virtualization:

Sandboxing

Sandboxing is a security mechanism for separating running programs that is often used to execute untested code or programs from unverified third parties, suppliers and websites. The main goal of sandboxing is to improve virtualization security by isolating an application to protect it from outside malware, harmful viruses, applications that stop execution, etc. If you have any application that is unstable or untested, simply put it in a virtual machine so that it does not affect the rest of the system.

Sometimes you may get a malicious attack to your application while running it in a browser, so it is always a good practice to run your programs on a virtual machine. Sandbox technology is closely related to virtualization. Virtual computing offers some of the benefits of sandboxes without having to pay premium prices for a new machine. The virtual machine has a connection to the Internet, not to the company LAN, so it protects the operating system and programs from viruses or harmful attacks on the virtual machine.

Server Virtualization

Server virtualization is the masking of server resources, which helps in partitioning the physical server into smaller virtual servers to maximize resources. The administrator divides the physical server into multiple virtual environments. These days, official records are often stolen from servers by hackers. Server virtualization allows small virtual servers to run their own operating systems and reboot independently of one another. Virtualized servers are used to identify and isolate applications that are unstable, as well as compromised applications.

This type of virtualization is mostly used in Web servers, which provide low-cost Web-hosting services. Server utilization manages complicated details of server resources while increasing utilization rates and maintaining capacity. A virtualized server makes it easier to detect malicious viruses or damaging elements while protecting the server, virtual machines and the entire network.

The benefit of using server virtualization is that it creates a hardware abstraction layer between the x86 hardware and the operating system. It also reduces the density of virtual servers to physical server hardware. Server virtualization creates an image of a server, which makes it easy to determine whether the server is acting abnormally.

Network Virtualization

Network virtualization is the combination of hardware and software network resources, and it combines network functionality into a single virtual network. With network virtualization, virtual networks minimize the effect of the malware when infecting the system. Network virtualization creates logical virtual networks from underlying network hardware to better integrate with virtual environments.

An important feature of network virtualization is isolation.It allows the dynamic composition of multiple virtual networks that co-exist in isolation to deploy customized end-to-end services on the fly. They are managed on those virtual networks for the users by sharing and using network resources gained from infrastructure providers.

Another main feature of network virtualization is segmentation, in which the network is divided into sub-networks, a process that leads to boosting performance by minimizing local traffic in the network and improving security by making the internal network structure invisible from the outside. Network virtualization is also used to create a virtualized infrastructure to support complex requirements by creating single instances of software applications serving multiple customers.

Hypervisor Security

The term hypervisor means small software or hardware that creates and runs virtual machines. The machine that contains the hypervisor is called a host machine. Hypervisor security enables virtualization by using hypervisor including development, implementation, provisioning and management. (Learn more in Virtualization Security: Tips to Prevent VM Hyper Jumping.)

There are some key security recommendations for hypervisors:

- Install the hypervisor updates released by the vendor. Most hypervisors will have automatic updating of software and will install updates when found.
- Secure with thin hypervisors, which makes deployment easy and efficient to run with minimal computing overhead. It also reduces the chance of attack by malicious code that could reach the hypervisor.
- Don't connect unused physical hardware to the host system, or unused NICs to any network. Sometimes disk drives are used to back up data, so unused devices should be disconnected when they are not actively being used for backup.
- If you don't need file sharing service or any other service between the guest OS and the host OS, disable any services that aren't needed.
- There must be security between guest operating systems in order for them to communicate. Non-virtualized environments should be handled by security controls such as firewalls, network appliances, etc.

Desktop Virtualization

Desktop virtualization allows for the creation, modification or deletion of images and separates the desktop environment from the physical computer that is used to access it. An administrator can easily manage employees' computers and protect them from unauthorized access or the introduction of viruses. It provides more security to the user by providing a guest OS image for the desktop environment and it doesn't allow copying or saving of data to a disk other than the server, making desktop virtualization a more secure option for networking.

Infrastructure Security

A virtualized information infrastructure allows controlling the access to resources and maintains visibility to ensure proper information handling. All activities within the computing environment need to be tracked though the infrastructure.

Virtual Switches

A virtual switch is a software program that provides security by using isolation, control and content inspection techniques between virtual machines and allows one virtual machine to communicate with another.

It does not allow the execution of inter-switch link attacks. The main purpose of a virtual switch is to provide network connectivity to communicate with virtual machines and applications within the virtual network to physical network.

Guest OS Security

This is the operating system in a virtual machine and it's used to host the main operating system and share resources with other virtual machines on the same host. Virtualization allows the sharing of information with the OS by using disks or folders created by networked disks. It contains some security features, such as updating the guest OS systematically, keeping the backup of virtual drives and applying the same policy for non-virtualized computers.

High Availability and Disaster Recovery

These days, the most important thing is to preserve data and the availability of services in the IT sector. Virtualization reduces the time and cost of disaster recovery by backing up data in a large unique file, which saves time when reinstalling the OS and restoring the data. It allows the restoration of a virtual machine in any host that meets the power requirements and also provides a facility to recover from physical failure quickly.

Server Isolation

Virtualization uses server isolation primarily for business purposes. Multiple servers can be run on one virtual machine without virtualization, but there is a risk when having multiple servers on a single server. Virtualization allows running multiple servers on a single machine while isolating servers from one another because they are running on separate virtual machines.

Q. 6. (a) What is different aspect of cloud management systems? (6.5)

Ans. A solid cloud management strategy helps organizations achieve three main goals.

Self-service capabilities

Self-service capabilities eliminate the traditional processes associated with IT resource provisioning. Users can access a public or private cloud, review current cloud computing instances or create new ones, monitor utilization and costs, and adjust resource allocations. With reporting, users can track cloud budgets and reduce or delete unused instances to cut operating expenses.

Workflow automation

Cloud management enables workflow automation. Through automation, organizations can turn business policies into the actionable steps needed to create and manage cloud computing instances, without the need for human intervention.

In addition to the creation, placement and adjustments of cloud computing instances, workflow automation helps businesses meet their reporting, deployment and compliance needs. For example, cloud management tools can alert a manager when an employee tries to move a private cloud workload to the public cloud, which could potentially violate company compliance or security policies.

Cloud analysis

Cloud management enables the ongoing analysis of cloud computing workloads and user experiences (UX).

In a private cloud environment, organizations can ensure their infrastructure works properly and offer a basis for tasks such as workload balancing and capacity planning. In public clouds, performance metrics for latency or downtime help ensure compliance with public cloud provider service-level agreements (SLAs).

With the use of metrics, organizations can also decide whether it's time to change cloud providers or migrate workloads from public to private clouds.

Cloud management tools

Cloud management requires tools. Public cloud providers typically develop highly specialized tools for monitoring, orchestration, cost management, security and more to suit the capabilities of their services.

For example, Amazon Web Services (AWS) enables users to access and manage cloud instances through a command-line interface (CLI) that runs individual commands and scripts. Google Cloud Platform (GCP) offers a monitoring and logging tool, Google Stackdriver, which provides performance data for applications and virtual machines (VMs) that run on GCP and AWS. Microsoft Azure, as another example, enables administrators to automatically replicate VMs with its Azure Site Recovery tool.

Q. 6. (b) Explain the following cloud security mechanism. (6)

(i) PKI

(ii) SSO

(iii) IAM

Ans. (i) PKI

Refer Q. 6. (a) End term Examination 2016.

(ii) SSO

Refer Q. 1. (e) End Term Examination 2016.

(iii) IAM

An identity management access (IAM) system is a framework for business processes that facilitates the management of electronic identities. The framework includes the technology needed to support identity management.

IAM technology can be used to initiate, capture, record and manage user identities and their related access permissions in an automated fashion. This ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorized and audited.

Poorly controlled IAM processes may lead to regulatory non-compliance because if the organization is audited, management will not be able to prove that company data is not at risk for being misused.

Why you need IAM

It can be difficult to get funding for IAM projects because they don't directly increase either profitability or functionality. However, a lack of effective identity and access management poses significant risks not only to compliance but also an organization's overall security. These mismanagement issues increase the risk of greater damages from both external and inside threats.

Keeping the required flow of business data going while simultaneously managing its access has always required administrative attention. The business IT environment is ever evolving and the difficulties have only become greater with recent disruptive trends like bring-your-own-device (BYOD), cloud computing, mobile apps and an increasingly mobile workforce. There are more devices and services to be managed than ever before, with diverse requirements for associated access privileges.

With so much more to keep track of as employees migrate through different roles in an organization, it becomes more difficult to manage identity and access. A common problem is that privileges are granted as needed when employee duties change but the access level escalation is not revoked when it is no longer required.

This situation and request like having access like another employee rather than specific access needs leads to an accumulation of privileges known as privilege creep. Privilege creep creates security risk in two different ways. An employee with privileges beyond what is warranted may access applications and data in an unauthorized and potentially unsafe manner. Furthermore, if an intruder gains access to the account of a user with excessive privileges, he may automatically be able to do more harm. Data loss or theft can result from either scenario.

Typically, this accumulation of privilege is of little real use to the employee or the organization. At best, it might be a convenience in situations when the employee is asked to do unexpected tasks. On the other hand, it might make things much easier for an attacker who manages to compromise an over-privileged employee identity. Poor identity access management also often leads to individuals retaining privileges after they are no longer employees.

Q. 7. (a) Explain the major cloud features of Google applications engine. **(6.5)**

Ans. Google App Engine (often referred to as GAE or simply App Engine) is a platform as a service (PaaS) cloud computing platform for developing and hosting web applications in Google-managed data centers. Applications are sandboxed and run across multiple servers. App Engine offers automatic scaling for web applications as the number of requests increases for an application, App Engine automatically allocates more resources for the web application to handle the additional demand.

Currently, the supported programming languages are Python, Java (and, by extension, other JVM languages such as Groovy, JRuby, Scala, Clojure), Go, and PHP. Node.js is also available in the Managed VM environment. Google has said that it plans to support more languages in the future, and that the Google App Engine has been written to be language independent.

Python web frameworks that run on Google App Engine include Django, CherryPy, Pyramid, Flask, web2py and webapp2, as well as a custom Google-written webapp framework and several others designed specifically for the platform that emerged since the release. Any Python framework that supports the WSGI using the CGI adapter can be used to create an application; the framework can be uploaded with the developed application. Third-party libraries written in pure Python may also be uploaded.

Google App Engine supports many Java standards and frameworks. Core to this is the servlet 2.5 technology using the open-source Jetty Web Server, along with accompanying technologies such as JSP. JavaServer Faces operates with some workarounds.

Though the datastore used may be unfamiliar to programmers, it is easily accessed and supported with JPA, JDO, and by the simple low-level API. There are several alternative libraries and frameworks you can use to model and map the data to the datastore such as Objectify, Slim 3 and Jello framework. Jello framework is a full-stack Java framework optimized for Google App Engine,that includes comprehensive Data Authorization model and a powerful RESTful engine.

Reliability and Support: All billed High-Replication Datastore App Engine applications have a 99.95% uptime SLA.

App Engine is designed in such a way that it can sustain multiple datacenter outages without any downtime. This resilience to downtime is shown by the statistic that the High Replication Datastore saw 0% downtime over a period of a year.

Paid support from Google engineers is offered as part of Premier Accounts. Free support is offered in the App Engine Groups, Stack Overflow, Server Fault, and GitHub, however assistance by a Google staff member is not guaranteed.

Restrictions

- Developers have read-only access to the filesystem on App Engine. Applications can use only virtual filesystems, like gae-filestore.
- App Engine can only execute code called from an HTTP request (scheduled background tasks allow for self calling HTTP requests).
- Users may upload arbitrary Python modules, but only if they are pure-Python; C and Pyrex modules are not supported.
- Java applications may only use a subset (The JRE Class White List) of the classes from the JRE standard edition.
- Datastore cannot use inequality filters on more than one entity property per query.
- A process started on the server to answer a request can't last more than 60 seconds (with the 1.4.0 release, this restriction does not apply to background jobs anymore).
- Does not support sticky sessions (a.k.a. session affinity), only replicated sessions are supported including limitation of the amount of data being serialized and time for session serialization.

Q. 7. (b) Explain load balanced virtual switches architecture. **(60**

Ans. A load-balanced switch is a switch architecture which guarantees 100% throughput with no central arbitration at all, at the cost of sending each packet across the crossbar twice. Load-balanced switches are a subject of research for large routers scaled past the point of practical central arbitration.

A load-balanced switch has N input line cards, each of rate R, each connected to N buffers by a link of rate R/N. Those buffers are in turn each connected to N output line cards, each of rate R, by links of rate R/N. The buffers in the center are partitioned into N virtual output queues.

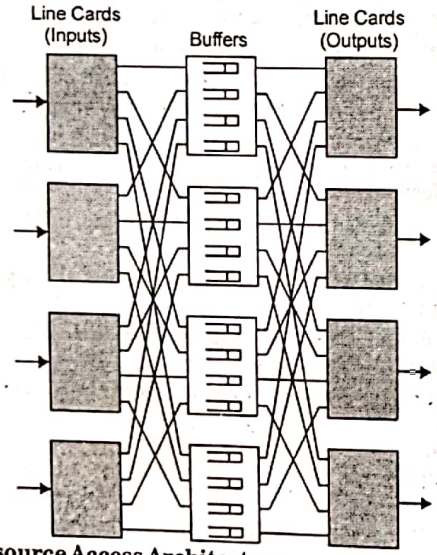
Each input line card spreads its packets evenly to the N buffers, something it can clearly do without contention. Each buffer writes these packets into a single buffer-

local memory at a combined rate of R. Simultaneously, each buffer sends packets at the head of each virtual output queue to each output line card, again at rate R/N to each card. The output line card can clearly forward these packets out the line with no contention.

Each buffer in a load-balanced switch acts as a shared-memory switch, and a load-balanced switch is essentially a way to scale up a shared-memory switch, at the cost of additional latency associated with forwarding packets at rate R/N twice.

The Stanford group investigating load-balanced switches is concentrating on implementations where the number of buffers is equal to the number of line cards. One buffer is placed on each line cards, and the two interconnection meshes are actually the same mesh, supplying rate 2R/N between every pair of line cards. But the basic load-balanced switch architecture does not require that the buffers be placed on the line cards, or that there be the same number of buffers and line cards.

One interesting property of a load-balanced switch is that, although the mesh connecting line cards to buffers is required to connect every line card to every buffer, there is no requirement that the mesh act as a non-blocking crossbar, nor that the connections be responsive to any traffic pattern. Such a connection is far simpler than a centrally arbitrated crossbar.



Multipath Resource Access Architecture

Ans: Cloud service delivery, cloud service management and cloud monitoring toots enable providers to keep up with the continually shifting capacity demands of a highly elastic environment.

Cloud monitoring and cloud service management tools allow cloud providers to ensure optimal performance, continuity and efficiency in virtualized, on-demand environments. These tools — software that manages and monitors networks, systems and applications — enable cloud providers not just to guarantee performance, but also to better orchestrate and automate provisioning of resources.

Cloud monitoring tools, specifically, enable cloud providers to track the performance, continuity and security of all of the components that support service delivery: the hardware, software and services in the data center and throughout the network infrastructure.

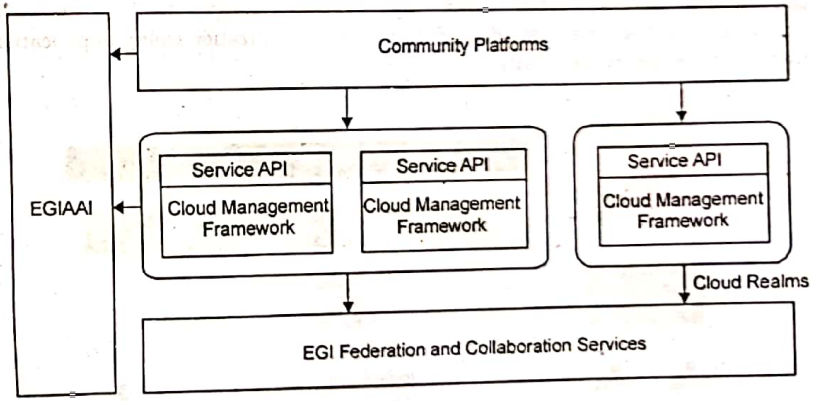
Through successful cloud service management and monitoring, cloud providers can use service quality to differentiate themselves in what remains a crowded and noisy marketplace.

Through successful cloud service management and monitoring, cloud providers can use service quality to differentiate themselves in what remains a crowded and S(bisy marketplace. Effective cloud service management also helps lower the risk 6f frequent cloud outages that can jeopardize security systems. Using these tools also supports greater operational efficiency, helping cloud providers minimize costs aifd maximize profit margins. However, achieving these goals can be difficult in a complex virtual delivery environment where visibility and control are limited.

Q. 8. (a) Describe the architecture of cloud federation stack. **(6.5)**

Ans. The Federated Cloud is a multi-national cloud system that integrates community, private and/or public clouds into a scalable computing platform for research. The Federation pools IaaS, PaaS and SaaS services from a heterogeneous set of cloud providers using a single authentication and authorization framework that allows the portability of workloads across multiple providers and enable bringing computing to data.

Each resource center of the federated infrastructure operates a Cloud Management Framework (CMF) according to its own preferences and constraints and joins the federation by integrating this CMF with components of the Federation and Collaboration Services. All services provided by the CMFs must at least be integrated with AAI so users can access services with a single identity, integration with other components and APIs to be provided are agreed by the community the resource center provides services to.



Federated Cloud Model

Providers are organised into realms, with each realm having homogeneous cloud interfaces and capabilities. Community Platform provide community-specific data, tools and applications, which can be supported by one or more realms. New realms can be defined as needed by the user communities by agreeing with the providers which interfaces to expose and which of the core services to use for the federation, integrates and maintains a flexible solution portfolio that enables various types of cloud federations with IaaS capabilities and seeking to expand to PaaS and SaaS capabilities. FC follows a Service Integration and Management (SIAM) approach to manage the federation with processes that cover the different aspects of the IT Service Management. Providers in

the federation keep complete control of their services and resources. VO OLAs establish a reliable, trust-based communication channel between the Customer and the providers to agree on the services, their levels and the types of support. The VO OLAs are not legal contracts but, as agreements, they outline the clear intentions to collaborate and support research.

Q. 8. (b) Explain the features of following cloud platforms: **(6)**

(i) Cloud SIM

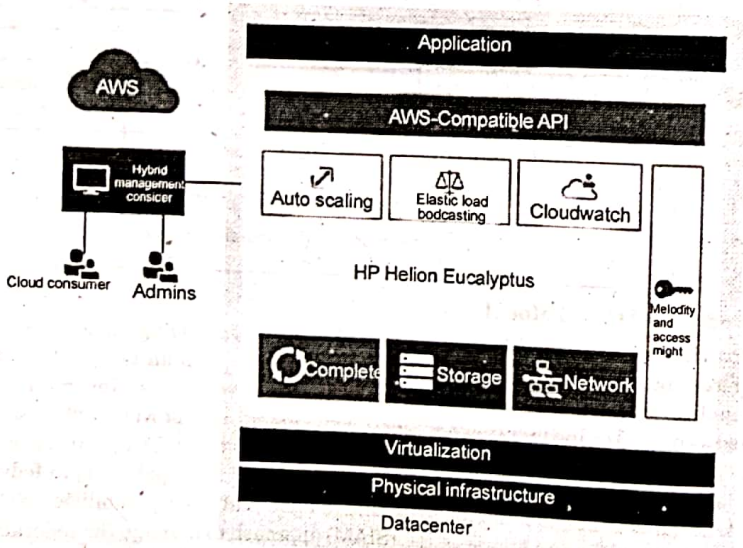
Ans. Cloud sim is a framework for modeling and simulation of cloud computing infrastructures and services. Originally built primarily at the Cloud Computing and Distributed Systems (CLOUDS) Laboratory, The University of Melbourne, Australia, Cloud Sim has become one of the most popular open source cloud simulators in the research and academia. Cloud Sim is completely written in Java.

(ii) Eucalyptus

Ans. Refer Q. 3. (b) End term Examination 2017.

Eucalyptus is free and open-source computer software for building Amazon Web Services (AWS)-compatible private and hybrid cloud computing environments marketed by the company Eucalyptus Systems. Eucalyptus is the acronym for Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems. Eucalyptus enables pooling compute, storage, and network resources that can be dynamically scaled up or down as application workloads change. Eucalyptus Systems announced a formal agreement with AWS in March 2012 to maintain compatibility.

Eucalyptus commands can manage either Amazon or Eucalyptus instances. Users can also move instances between a Eucalyptus private cloud and the Amazon Elastic Compute Cloud to create a hybrid cloud. Hardware virtualization isolates applications from computer hardware details.



Eucalyptus architecture overview

Terminology:

• **Images** - An image is a fixed collection of software modules, system software, application software, and configuration information that is started from a known baseline (immutable/fixed). When bundled and uploaded to the Eucalyptus cloud, this becomes aEucalyptus machine image (EMI).

• **Instances** - When an image is put to use, it is called an instance. The configuration is executed at runtime, and the Cloud Controller decides where the image will run, and storage and networking is attached to meet resource needs.

• **IP addressing** - Eucalyptus instances can have public and private IP addresses. An IP address is assigned to an instance when the instance is created from an image. For instances that require a persistent IP address, such as a web-server, Eucalyptus supplies elastic IP addresses. These are pre-allocated by the Eucalyptus cloud and can be reassigned to a running instance.

• **Security** - TCP/IP security groups share a common set of firewall rules. This is a mechanism to firewall off an instance using IP address and port block/allow functionality. At TCP/IP layer 2 instances are isolated. If this were not present, a user could manipulate the networking of instances and gain access to neighbouring instances violating the basic cloud telnet of instance isolation and separation.

• **Networking** - There are three networking modes. In Managed Mode Eucalyptus manages a local network of instances, including security groups and IP addresses. In System Mode, Eucalyptus assigns a MAC address and attaches the instance's network interface to the physical network through the Node Controller's bridge. System Mode does not offer elastic IP addresses, security groups, or VM isolation. In Static Mode, Eucalyptus assigns IP addresses to instances. Static Mode does not offer elastic IPs, security groups, or VM isolation.

• **Access Control** - A user of Eucalyptus is assigned an identity, and identities can be grouped together for access control.

(iii) Hadoop

Ans. Hadoop is a complete eco-system of open source projects that provide us the framework to deal with big data. Let's start by brainstorming the possible challenges of dealing with big data (on traditional systems) and then look at the capability of Hadoop solution.

Following are the challenges I can think of in dealing with big data:

1. High capital investment in procuring a server with high processing capacity.

2. Enormous time taken

3. In case of long query, imagine an error happens on the last step. You will waste so much time making these iterations.

4: Difficulty in program query building

How Hadoop solves all of these issues :

1. High capital investment in procuring a server with high processing capacity: Hadoop clusters work on normal commodity hardware and keep multiple

copies to ensure reliability of data. A maximum of 4500 machines can be connected together using Hadoop.

2. Enormous time taken : The process is broken down into pieces and executed in parallel, hence saving time. A maximum of 25 Petabyte (1 PB = 1000 TB) data can be processed using Hadoop.

3. In case of long query, imagine an error happens on the last step. You will waste so much time making these iterations : Hadoop builds back up data-sets at every level. It also executes query on duplicate datasets to avoid process loss in case of individual failure. These steps makes Hadoop processing more precise and accurate.

4. Difficulty in program query building : Queries in Hadoop are as simple as coding in any language. You just need to change the way of thinking around building a query to enable parallel processing.

Hadoop works in a similar format. On the bottom we have machines arranged in parallel. These machines are analogous to individual contributor in our analogy. Every machine has a data node and a task tracker. Data node is also known as HDFS (Hadoop Distributed File System) and Task tracker is also known as map-reducers.

Data node contains the entire set of data and Task tracker does all the operations. You can imagine task tracker as your arms and leg, which enables you to do a task and data node as your brain, which contains all the information which you want to process. These machines are working in silos and it is very essential to coordinate them. The Task trackers (Project manager in our analogy) in different machines are coordinated by a Job Tracker. Job Tracker makes sure that each operation is completed and if there is a process failure at any node, it needs to assign a duplicate task to some task tracker. Job tracker also distributes the entire task to all the machines.

A name node on the other hand coordinates all the data nodes. It governs the distribution of data going to each machine. It also checks for any kind of purging which have happened on any machine. If such purging happens, it finds the duplicate data which was sent to other data node and duplicates it again. You can think of this name node as the people manager in our analogy which is concerned more about the retention of the entire dataset.