**Cloud computing Mid-term papers**

## Set A

1. Describe cloud based services. What are the challenges in cloud computing?

Cloud Computing can be defined as the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Companies offering such kinds of [cloud computing](https://www.geeksforgeeks.org/architecture-of-cloud-computing/) services are called [*cloud providers*](https://www.geeksforgeeks.org/top-5-cloud-platform-service-providers-in-2020/) and typically charge for cloud computing services based on usage. Grid and cluster are the foundations for cloud computing.

Most cloud computing services fall into three broad categories:

1. Software as a service (Saas)
2. Platform as a service (PaaS)
3. Infrastructure as a service (IaaS)
4. Anything as a service (XaaS)

These are sometimes called the **cloud computing stack** because they are built on top of one another. Knowing what they are and how they are different, makes it easier to accomplish your goals. These abstraction layers can also be viewed as a **layered architecture** where services of a higher layer can be composed from services of the underlying layer i.e, Saas can provide Infrastructure.

[**Software-as-a-Service (SaaS)**](https://www.geeksforgeeks.org/software-as-a-service-saas/)is a way of delivering services and applications over the Internet. Instead of installing and maintaining software, we simply access it via the Internet, freeing ourselves from the complex software and hardware management. It removes the need to install and run applications on our own computers or in the data centers eliminating the expenses of hardware as well as software maintenance.   
SaaS provides a complete software solution that you purchase on a **pay-as-you-go** basis from a cloud service provider. Most SaaS applications can be run directly from a web browser without any downloads or installations required. The SaaS applications are sometimes called **Web-based software, on-demand software, or hosted software.**

**Platform as a service** is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet. PaaS services are hosted in the cloud and accessed by users simply via their web browser.   
A PaaS provider hosts the hardware and software on its own infrastructure. As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application. Thus, the development and deployment of the application take **place independent of the hardware.**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. To make it simple, take the example of an annual day function, you will have two options either to create a venue or to rent a venue but the function is same.

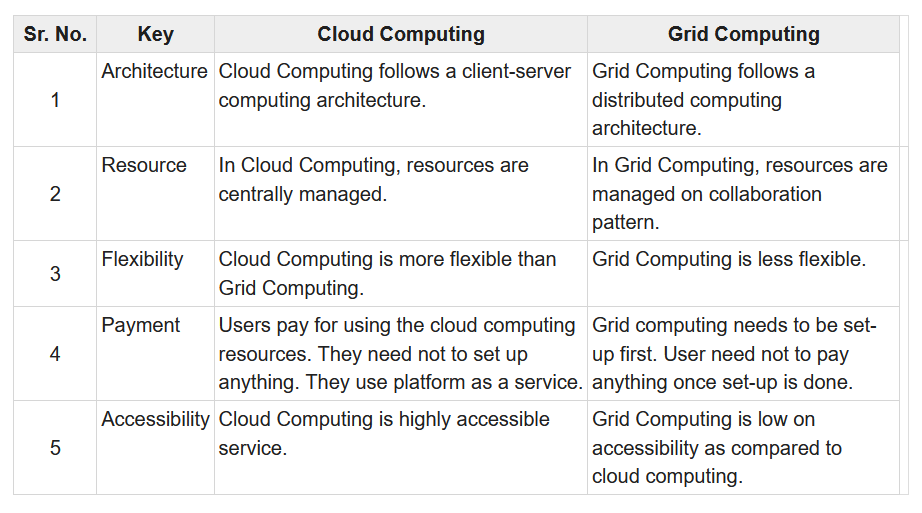
**Infrastructure as a service (IaaS)** is a service model that delivers computer infrastructure on an outsourced basis to support various operations. Typically IaaS is a service where infrastructure is provided as an outsource to enterprises such as networking equipment, devices, database, and web servers.   
It is also known as **Hardware as a Service (HaaS).** IaaS customers pay on a per-user basis, typically by the hour, week, or month. Some providers also charge customers based on the amount of virtual machine space they use.   
It simply provides the underlying operating systems, security, networking, and servers for developing such applications, services, and for deploying development tools, databases, etc.

**Anything as a service:** Most of the cloud service providers nowadays offer anything as a service that is a compilation of all of the above services including some additional services.

1. How grid computing differs from cloud computing? Justify what elasticity and multitenancy properties of cloud computing mean?

Grid computing refers to a network of same or different types of computers whose target is to provide a environment where a task can be performed by multiple computers together on need basis. Each computer can work independently as well. Grid Computing is used internally by organization.

Following are the important differences between Cloud Computing and Grid Computing.



Elastic multitenancy refers to the idea that a system can accommodate multiple client storage resources together ("multitenant") and offer on-demand changes within the system ("elastic").  
  
The term is commonly used in modern cloud computing and network virtualization.

A system that supports elastic multitenancy allows a client’s separate storage resources to be treated completely independently and securitized from one another, even though they may be held in the same servers and hardware pieces, in the same IT room and even on the same sets of drives.

1. What do you mean by virtualization? What is the role of virtualization in cloud computing?

Virtualization is the process of creating a virtual instance of a device, such as a virtual server or virtual operating system. There are several different types of virtualization, which I’ll discuss shortly in more detail.

Most virtualization is performed through virtualization software. These programs have the capability to extend the hardware of the physical machine, network, or storage system, and create virtual versions of these systems.

One example of a virtualization program is called a [hypervisor](https://www.dnsstuff.com/what-is-hypervisor), which can virtualize desktops, applications, network components, and storage. Hypervisors can either be installed directly on the hardware, or work as a layer installed on the operating system between the hardware and the virtual machine.

Cloud computing is possible because of a technology called virtualization. Virtualization allows for the creation of a simulated, digital-only "virtual" computer that behaves as if it were a physical computer with its own hardware. The technical term for such a computer is [virtual machine](https://www.cloudflare.com/learning/cloud/what-is-a-virtual-machine/). When properly implemented, virtual machines on the same host machine are sandboxed from one another, so they do not interact with each other at all, and the files and applications from one virtual machine are not visible to the other virtual machines even though they are on the same physical machine.

Virtual machines also make more efficient use of the hardware hosting them. By running many virtual machines at once, one server becomes many servers, and a data center becomes a whole host of data centers, able to serve many organizations. Thus, cloud providers can offer the use of their servers to far more customers at once than they would be able to otherwise, and they can do so at a low cost.

1. What is the cloud security challenge? How risks can be handled in cloud computing?

Cloud security gives many advantages to an organization such as centralized protection to all the networks, reduction in costs, and a competitive edge to the business. However, cloud computing proffers its challenges, including data protection and security related. This developing cloud technology is facing many technical challenges in various aspects of information management and storage. The below lists the top 10 Cloud Security Challenges that every organization faces:

### **1. Less visibility and Lack of Control**

This is one of the major cloud security challenges that entities face as the lack of perceptibility into the tools and files on the cloud server disturbs the power and ability of the organization to have a check on the effectiveness of the security controls. Further, due to the lack of control, the entity may not able to devise response plans.

Therefore, an entity shall necessarily devise an action plan on the ways to track, the type of data to be accessed, and the kind of security controls the cloud-based technology provider deploys to generally avoid the situation of a data breach when installing a cloud-based technology to the entity’s system.

### **2. Non-compliance with regulatory requirements**

Several regulations need to be followed and complied with by an organization. More so particularly, these regulations are industry-specific and vary from one industry to another. Any non-compliance with the regulations may trigger the penal provisions and result in additional fees, fines, condemnations, and other penalties. This results in the tarnishing of an organization’s image in the industry.

Hence, it is highly imperative to choose and authenticate the cloud service provider on their compliance level with various regulations. A third-party check may also be done to verify if they are compliant as not all cloud service suppliers possess security measures that fulfill every industry-specific regulations. This check on the cloud service providers also rules out the cloud security challenges and risks of observations that may arise in business audits, due-diligence process, and penalties.

### **3. Concerns of Data breach and Data Privacy**

One of the most important challenges of cloud security is the risk of data breaches and issues of data privacy. Before the entry of advanced technologies such as the Cloud, the IT team of every organization had control and hold over the network structure and systems. However, in cloud servers, as the controls are repudiated to the vendor, it is highly necessary to select the right vendor, with a strong track record to avoid the scenarios of exposing data to theft.

### **4. Alerts in situations of Data Breaches**

With Cloud, as there is no total control and with the lack of visibility of the network in a system, in situations when there is a violation of a system’s network, there are immense difficulties to decipher the resources compromised. The security concerns in cloud computing arise as due to the absence of robust visibility features and data of event logs, identifying the customers whose data have been breached, and what data has been compromised becomes difficult.

In such situations, sending out alerts and notifying the security threats to necessary managers, a customer is vital. This should be made part of the security plan and steps should be taken to analyze the solutions that the cloud provider has.

### **5. Access control to users**

It is very essential to evaluate what kind of user access controls are provided with a cloud service. In situations of limited options, it is necessary to check if it is possible to supplement those controls with existing or added tools and integrations to avoid cloud security issues.

### **6. Migration to vendors**

One of the major cloud security challenges is the risk of sole vendor relationships. In situations where a single congruent security solution is deployed, it can be highly restricting. This is because it may lead to complete re-work of security solutions for other business needs. Therefore, it is necessary to check on the comfort of migration from one service to another when preferring cloud-based services to avoid vendor lock.

### **7. Lack of experienced workforce**

As cloud-based technologies are new and evolving, there are immense challenges to find competent security experts in any given environment. This problem is increased with the cloud service, as finding a qualified workforce to run cloud computing security solutions is increasingly complex, and the cost of recruiting and training is costly.

### **8. Vulnerable entry points**

One of the prime security challenges in cloud computing, which is also the main advantage, is that it is easily accessible from any device and any place. This also opens the possibilities for hackers to recognize the vulnerabilities and take advantage of them.

### **9. Loss of data**

Among the many cloud security challenges in cloud computing and cloud storage, the common challenge is the risk of data loss. As critical and significant information of business is transferred into the cloud, the security of the data is one of the major concerns. Some of the threats that arise are data loss from the cloud, inadvertent deletion, Distributed denial of service (DDoS) attacks, or any force majeure events.

For example, A DDoS attack is planned to engulf website servers to render it unresponsive to genuine user requests. If the launch of a DDoS attack becomes successful, it makes a website useless for hours or days. This event can affect the loss of income, customer faith, and brand power.

### **10. Technology vulnerabilities**

Usage of third-party cloud services such as public or hybrid cloud servers can render the system of the organization to many security vulnerabilities from other users of the same cloud server. Further, the risk of negligence of the cloud vendor is always there, and the possibility of security vulnerability due to another user in the same Cloud server is unavoidable, leading to potent cloud computing security issues and challenges.

1. Discuss about disasters in cloud. How intrusions are detected in cloud?

Cloud disaster recovery (CDR) is a cloud-based managed service that helps you quickly recover your organization’s critical systems after a disaster and provides you remote access to your systems in a secure virtual environment.

Cloud disaster recovery is a service that enables the backup and recovery of remote machines on a cloud-based platform.  
  
Cloud disaster recovery is primarily an infrastructure as a service (IaaS) solution that backs up designated system data on a remote offsite cloud server. It provides updated recovery point objective (RPO) and recovery time objective (RTO) in case of a disaster or system restore.

Intrusion detection is the practice of monitoring your network, servers, workstations, and other IT assets for any suspicious activity, malicious actions, or violations of some policy. This practice is an integral component of your company’s infrastructure security.

Intrusion detection systems works by either looking for signatures of known attacks or deviations from normal activity, intrusion detection systems push deviations and anomalies up the stack to be examined at the protocol and application level.

Traditionally, in data center environments, people conduct intrusion detection at the network layer, using tools like Zeek and Snort. These tools process raw network traffic data and then pattern-match for specific signatures, behaviors or anomalies. For example, if you see a login from a different country for the first time, or notice that ten people are logged in simultaneously on the same server, you may recognize it as a suspicious attempt, and you can trigger an alert. Similarly, known signatures for exploits can be matched against network traffic.

However, in the cloud, it’s not as easy to get a copy of the raw network traffic due to the limitations of the environment. The cloud provider typically hosts multiple customers, and is responsible for the physical network, meaning customers do not get direct access to it. Therefore, in the cloud, you must switch to different layers to do intrusion detection.

1. How can you design the security architecture in cloud? Explain.

Cloud security architecture is a security strategy designed around securing an organization's data and applications in the cloud. It is a critical extension of enterprise security, and it requires an architecture to connect it with an overall security approach.

In cloud security architecture, responsibility is shared between the cloud provider and customer. As more organizations shift and share their data in the cloud, the more important it becomes to have a security architecture in place to secure data.

When [developing a cloud security architecture](https://www.guidepointsecurity.com/cloud-security-architecture/) several critical elements should be included:

* Security at Each Layer
* Centralized Management of Components
* Redundant & Resilient Design
* Elasticity & Scalability
* Appropriate Storage for Deployments
* Alerts & Notifications
* Centralization, Standardization, & Automation

The types of service models in use by a business define the types of cloud security architectures that are most applicable. The service models are: Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

Organizations that offer cloud services typically adhere to a shared responsibility model—that is, the cloud service provider is responsible for the security of the components necessary to operate the cloud service (software, computing, storage, database, networking, hardware, infrastructure, etc.). The customer is responsible for protecting the data and information that is stored in the cloud, as well as how they may access that data (identity and access management). Responsibilities vary slightly depending on the type of service (IaaS, SaaS, or PaaS).

**Infrastructure as a Service (IaaS) Shared Responsibility**

With an IaaS, a business purchases the infrastructure from a cloud provider and the business typically installs their own operating systems, applications, and middleware. An example of an IaaS is Azure (Microsoft). In an IaaS, the customer is usually responsible for the security associated with anything they own or install on the infrastructure.

**Software as a Service (SaaS) Shared Responsibility**

With a SaaS, an organization purchases the use of a cloud-based application from a provider. Examples of SaaS include Office 365 or Salesforce. In a SaaS, the customer is typically only responsible for the security components associated with accessing the software, such identity management, customer network security, etc. The software provider manages the security backend.

**Platform as a Service (PaaS) Shared Responsibility**

With a PaaS, a business purchases a platform from a cloud provider to develop, run, and manage applications without developing or managing the underlying platform infrastructure required for the applications. An example of a PaaS would be Amazon Web Services (AWS). In a PaaS, the customer is responsible for the security associated with application implementation, configurations, and permissions.

1. Explain the different approaches for enforcing host security in a cloud environment.

##### Cloud infrastructure entitlement management (CIEM).

This specialized approach uses analytics and machine learning to detect over permissioned identities, spot behavior anomalies and manage entitlements to enforce least privilege, and address the unique challenges created by multi-cloud environments. It’s valuable for complex and highly dynamic cloud environments that rely on IaaS and PaaS. [CIEM](https://www.forbes.com/sites/louiscolumbus/2020/10/25/whats-new-in-gartners-hype-cycle-for-cloud-security-2020/?sh=ebf29a67bd92) shines because it removes manual oversight and instead grants, resolves, enforces, revokes and administers authorizations or privileges in an automated way.

##### Cloud Identity and Access Management (IAM).

Establishing a comprehensive framework for authentication and authorization is at the center of connecting clouds and managing them effectively. The right [IAM](https://www.techopedia.com/definition/23922/identity-and-access-management-iam) solution simplifies account set up and deprovisioning across multiple applications or systems. With robust tools in place to manage identities, perform secure single sign on, reduce passwords, and assign privileges that precisely align with roles, it’s possible to improve and simplify security, and also improve audits and regulatory compliance.

##### Multi-factor authentication.

No cloud framework or software should be without a way to validate the identity of a user. [MFA](https://www.techopedia.com/definition/13657/multi-factor-authentication-mfa) has become a critical component. In the most basic form, an organization should require a text code or the use of an authenticator app that displays rolling codes. More advanced frameworks—which typically rely on a smartphone or wearable—incorporate physical or virtual tokens to automate and further improve the authentication process.

##### Privileged Access Management (PAM).

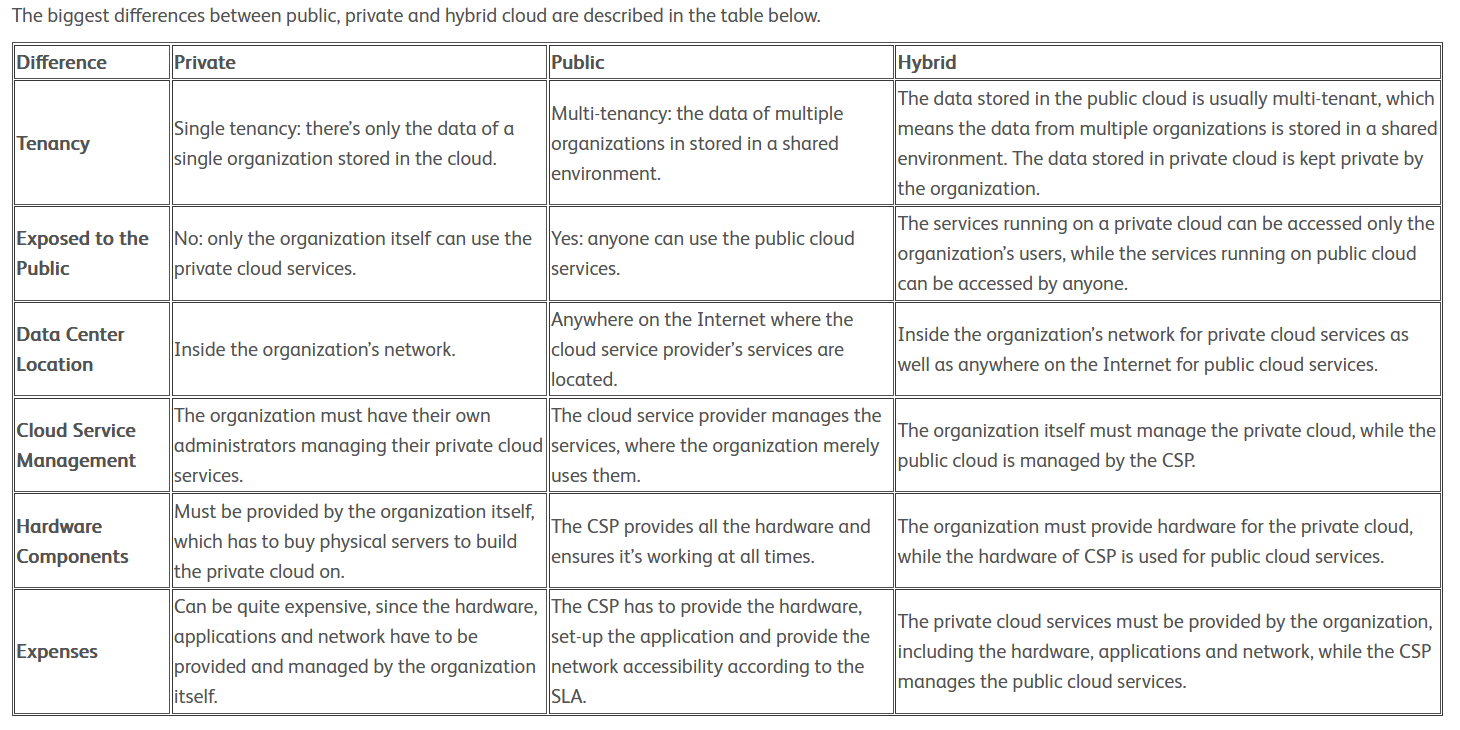
These solutions focus on preventing credential theft and privilege misuse. As the name implies, they provide additional access and protection to privileged groups—though monitoring, visibility and fine grained controls. [PAM](https://www.gartner.com/en/documents/3996969-invest-implications-buyers-guide-for-privileged-access-m) makes it possible to create different classes of accounts. For example, an organization might set up a super-user account for a high level IT administrator, a privileged business user account for an executive that needs to access IT systems, and an emergency account. However, PAM is not natively designed for the cloud or to support DevOps.

##### Zero Trust Network Access (ZTNA).

The concept of zero trust isn’t new. However, [ZTNA](https://www.gartner.com/en/information-technology/glossary/zero-trust-network-access-ztna-) offers an evolving framework to put an organization’s zero trust policies into practice. At a basic level, it ensures that only users who require access to an organization’s network to perform specific tasks obtain permission. The approach replaces virtual private network (VPN) devices, which allow unfettered access to a network.

Better cloud security is achievable. An approach that revolves around securing identities can elevate protection and deliver clear advantages.

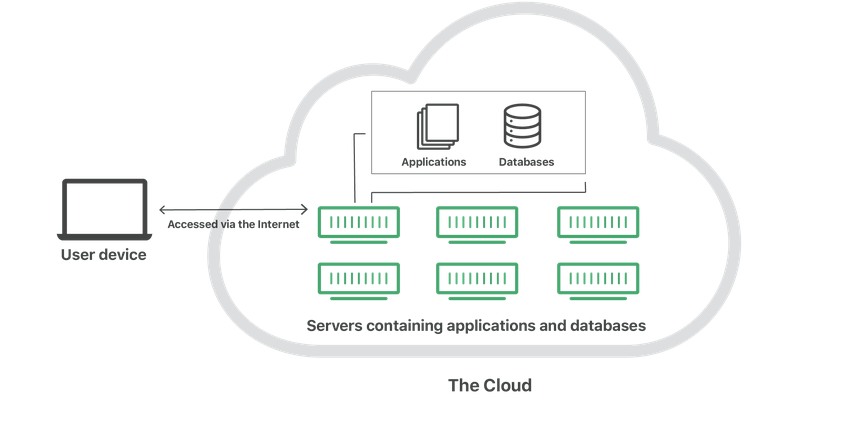
1. Differentiate between each of private, public and hybrid cloud models with suitable examples.



## Set B

1. What do you mean by cloud? Describe the basic characteristics of the cloud.

"The cloud" refers to servers that are accessed over the Internet, and the software and databases that run on those servers. Cloud servers are located in [data centers](https://www.cloudflare.com/learning/cdn/glossary/data-center/) all over the world. By using cloud computing, users and companies do not have to manage physical servers themselves or run software applications on their own machines.



The cloud enables users to access the same files and applications from almost any device, because the computing and storage takes place on servers in a data center, instead of locally on the user device. This is why a user can log in to their Instagram account on a new phone after their old phone breaks and still find their old account in place, with all their photos, videos, and conversation history. It works the same way with cloud email providers like Gmail or Microsoft Office 365, and with cloud storage providers like Dropbox or Google Drive.

For businesses, switching to cloud computing removes some IT costs and overhead: for instance, they no longer need to update and maintain their own servers, as the cloud vendor they are using will do that. This especially makes an impact for small businesses that may not have been able to afford their own internal infrastructure but can outsource their infrastructure needs affordably via the cloud. The cloud can also make it easier for companies to operate internationally, because employees and customers can access the same files and applications from any location.

1. What type of deployment models can be adopted in cloud computing? Describe each of them with a suitable example.

Cloud [deployment models](https://www.sciencedirect.com/topics/computer-science/deployment-model) indicate how the cloud services are made available to users. The four deployment models associated with cloud computing are as follows:

•**Public cloud** As the name suggests, this type of cloud deployment model supports all users who want to make use of a computing resource, such as hardware (OS, CPU, memory, storage) or software (application server, database) on a subscription basis. Most common uses of public clouds are for application development and testing, non-mission-critical tasks such as file-sharing, and e-mail service.

•**Private cloud** True to its name, a private cloud is typically infrastructure used by a single organization. Such infrastructure may be managed by the organization itself to support various user groups, or it could be managed by a service provider that takes care of it either on-site or off-site. Private clouds are more expensive than public clouds due to the capital expenditure involved in acquiring and maintaining them. However, private clouds are better able to address the security and privacy concerns of organizations today.

•[Hybrid cloud](https://www.sciencedirect.com/topics/computer-science/hybrid-cloud) In a hybrid cloud, an organization makes use of interconnected private and public cloud infrastructure. Many organizations make use of this model when they need to scale up their IT infrastructure rapidly, such as when leveraging public clouds to supplement the capacity available within a private cloud. For example, if an online retailer needs more computing resources to run its Web applications during the holiday season it may attain those resources via public clouds.

•**Community cloud** This deployment model supports multiple organizations sharing computing resources that are part of a community; examples include universities cooperating in certain areas of research, or police departments within a county or state sharing computing resources. Access to a community cloud environment is typically restricted to the members of the community.

1. Discuss the capabilities that cloud users can get through Platform-as-a-service (PaaS). Also, mention the key characteristics of PaaS.

**Platform-as-a-Service** offers the runtime environment for applications. It also offers development and deployment tools required to develop applications. PaaS has a feature of **point-and-click** tools that enables non-developers to create web applications.

**App Engine of Google** and **Force.com** are examples of PaaS offering vendors. Developer may log on to these websites and use the **built-in API** to create web-based applications.

But the disadvantage of using PaaS is that, the developer **locks-in** with a particular vendor. For example, an application written in Python against API of Google, and using App Engine of Google is likely to work only in that environment.

Here are the characteristics of PaaS service model:

* PaaS offers **browser based development environment.** It allows the developer to create database and edit the application code either via Application Programming Interface or point-and-click tools.
* PaaS provides **built-in security, scalability,** and **web service interfaces.**
* PaaS provides built-in tools for defining **workflow, approval processes,** and business rules.
* It is easy to integrate PaaS with other applications on the same platform.
* PaaS also provides web services interfaces that allow us to connect the applications outside the platform.

1. How grid computing differs from cloud computing? Justify what the elasticity and multitenancy properties of cloud computing mean?

Done already

1. What do you mean by virtualization? What is the role of virtualization in cloud computing?

Done already

1. What are the Managed Service Providers (MSP)? Discuss the evolution of MSP Model

to Cloud Computing.

A managed service provider (MSP) delivers services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in their MSP's data center (hosting), or in a third-party data center.

A managed service provider (MSP) is a third-party company that remotely manages a customer's information technology (IT) infrastructure and end-user systems.

In the early days of modern business computing, businesses often hired outside support providers, mostly to fix things when they broke. Over time, business computing expanded and both IT leaders and service providers began to shift their focus to more proactive and preventive activities. In addition to fixing what broke, service and support providers began looking for ways to avoid breaks and to improve the performance, reliability, and security of their clients’ IT estates. (The first international computer conference, held in London in 1971, included sessions on making those early time-sharing systems more secure.)

Soon, business technology decision makers began to negotiate “subscription” contracts with their outside providers, for consistent access to their solutions and services. Some providers became sophisticated enough to manage clients’ IT operations, in part or totally. Providers also began to resell hardware, which enabled them to offer more comprehensive solutions and generate additional revenues. Those providers were basically some of the first modern MSPs.

During the 1990s, business decision makers increasingly pursued so-called “lean” and “just-in-time” initiatives. These were largely focused on cutting manufacturing and distribution costs, but many businesses also used these initiatives to pare their IT staffs and costs. Then, the dot-com crash that began in 1995 accelerated the rate at which IT people found themselves unemployed. Meanwhile, IT use was growing, and IT solutions and management tools became more powerful, affordable, easier to use. All these factors led to the growth and evolution of modern MSPs and the services they provide.

Today, MSPs offer a wide range of IT solutions and services, including but not limited to those listed here.

* Anti-virus/anti-spam/anti-phishing/anti-malware services
* Data backup services
* IT estate/network monitoring services
* New software configuration and provisioning services
* New hardware configuration and implementation services
* Network infrastructure configuration, implementation, and enhancement services
* Cloud computing services (applications, services, resources, management)
* Patch/repair/update management services
* On-demand augmentation of incumbent staff/expertise

The growth of business cloud computing has been a major contributor to the growth of the MSP market. An April 2018 Grand View Research study estimates the 2016 cloud managed services market to have been more than $23 billion. That same report predicts the cloud managed services market could be more than $80 billion by 2020.

Today, [managed service providers (MSP)](https://freshservice.com/msp) deliver a broad range of computing services to businesses of all types and sizes. Some estimate that 90 percent of Fortune 1000 companies use MSPs to provide at least part of their IT infrastructures or services. Estimates curated at Statisia .com place the 2018 MSP market at more than $189 billion, and project growth to more than $229 billion by 2020.

1. Discuss about disasters in cloud. How intrusions are detected in cloud?

Done already

1. Explain the different approaches for enforcing host security in a cloud environment.

Done already

## Section c

1.

a. How do the Jericho Cloud Cube model dimensions like parameterized, de-parameterized, and proprietary, open differentiate the cloud formations from each other?

Explained in next….

b. Explain the service provided by the amazon EC2 service from user perspective.

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in [the cloud](https://aws.amazon.com/what-is-cloud-computing/). It is designed to make web-scale computing easier for developers. Just as Amazon Simple Storage Service (Amazon S3) enables storage in the cloud, Amazon EC2 enables “compute” in the cloud. Amazon EC2’s simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon’s proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use.

2. a. Describe the services provided by the Monitoring-as-a-service (MaaS) vendors in cloud service systems.

**Monitoring as a Service (MaaS)** is a security service that provides security to IT assets of any business 24/7. It plays a vital role in securing an enterprise or government clients from any possible cyber threats.

MaaS is a monitoring service that can be outsourced in a flexible and consumption-based subscription model. **Monitoring as a Service** (MaaS) provides you with the security solutions that are essential for the organizations that are reliant on the IT infrastructure. However, for effective and efficient monitoring, the organization must have up to date technology, experts knowing advanced technical skills, scalable security processes and all this come with a tremendous expense.

Prior to the advent of electronic gadgets that are used for providing security services, the human resource was used to perform all these monitoring activities but it was ineffective.

MaaS provides an effective solution to this problem. It provides 24/7 real-time monitoring, reports any issue across the security infrastructure and secures the crucial data of their customers.

If compared to the traditional security operations centre MaaS exceed in two important things:

1. The total cost of ownership was higher in the traditional security operations centre.
2. Traditional security operations are less effective.

### Key Takeaway

* MaaS is a security solution based on cloud computing.
* MaaS lets early detection of threats and reports it to their customer via emails.
* MaaS automates the detection and management of threats.
* MaaS also provides continuous system patching to update the security level and support the newer version of the application installed on the system.
* MaaS provides the forensic analysis of the vulnerability to identify the time effort and cost required to resolve.
* MaaS provide 24/7/365 days of assistance to their customers.

b. Write short notes on (Any Two)

i. Risk Assessment in Cloud

The goal of a cloud risk assessment is to ensure that the system and data considered for migration to the cloud don't introduce any new or unidentified risk into the organization. The focus is to ensure confidentiality, integrity, availability, and privacy of information processing and to keep identified risks below the accepted internal risk threshold.

Risk management needs to be a cyclically executed process comprised of a set of  
coordinated activities for overseeing and controlling risks. This process targets the  
enhancement of strategic and tactical security and includes the execution of a risk  
assessment, the implementation of a risk mitigation strategy, and the employment of risk  
control techniques and procedures for the continuous monitoring of the security state of  
the information system. Cloud-based information systems, as with traditional information  
systems, require that risks be managed throughout the system development life cycle  
(SDLC)

ii. Role of open source software in cloud computing

Open source software (OSS) is software that is distributed with its source code, making it available for use, modification, and distribution with its original rights.

First, most organizations adopt cloud to optimize their IT investment, to improve existing services or to support new business and service models. In this scenario, open-source lowers the barriers for new organizations to build their private cloud.

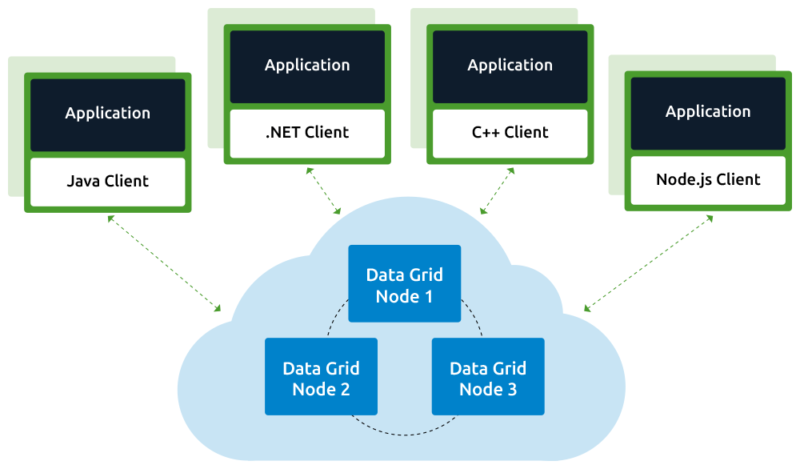
Second, many organizations like the fact that open source allows great customization to meet individual requirements. They can build a differentiated cloud service to meet customers needs.

Third, open-source also encourages and supports innovation in the development of new cloud products. We have seen many examples of how its use lowers the barriers for new ICT players to create their own cloud offerings. Finally, collaboration between technology providers and users is a huge advantage in the open source arena. Until now, small developers did not have the capital to acquire massive compute resources and ensure they had the capacity they needed to handle unexpected spikes in load. Amazon EC2 enables any developer to leverage Amazon’s own benefits of massive scale with no up-front investment or performance compromises. Developers are now free to innovate knowing that no matter how successful their businesses become, it will be inexpensive and simple to ensure they have the compute capacity they need to meet their business requirements.

The “Elastic” nature of the service allows developers to instantly scale to meet spikes in traffic or demand. When computing requirements unexpectedly change (up or down), Amazon EC2 can instantly respond, meaning that developers have the ability to control how many resources are in use at any given point in time. In contrast, traditional hosting services generally provide a fixed number of resources for a fixed amount of time, meaning that users have a limited ability to easily respond when their usage is rapidly changing, unpredictable, or is known to experience large peaks at various intervals.

iii. Grid Computing

**Grid computing** is the practice of leveraging multiple computers, often geographically distributed but connected by networks, to work together to accomplish joint tasks. It is typically run on a “[data grid](https://hazelcast.com/glossary/data-grid/),” a set of computers that directly interact with each other to coordinate jobs. Grid computing works by running specialized software on every computer that participates in the data grid. The software acts as the manager of the entire system and coordinates various tasks across the grid. Specifically, the software assigns subtasks to each computer so they can work simultaneously on their respective subtasks. After the completion of subtasks, the outputs are gathered and aggregated to complete a larger-scale task. The software lets each computer communicate over the network with the other computers so they can share information on what portion of the subtasks each computer is running, and how to consolidate and deliver outputs.



1. Discuss Jericho Cloud Cube Model. How do the Jericho Cloud Cube model dimensions

like parameterized, de-parameterized, and proprietary, open differentiate the cloud

formations from each other?

The Jericho Forum has designed the Cloud Cube Model to help select cloud formations for security cooperation. Their fascinating new cloud model helps IT managers and business tycoons assess the benefits of cloud computing. The Cloud Cube Model looks at the several different "cloud formations". They amount to the cloud service and deployment models. The sourcing dimension addresses the delivery of service. The Cloud Cube Model may be designed to let users show that the traditional notion of network ranges & its boundaries with network firewall no longer applies in Cloud computing.

Cloud Cube model, helps to categorize the cloud network based on the four-dimensional factor. Their main focus is to protect and secure the cloud network. This cloud cube model helps to select cloud formation for secure collaboration.

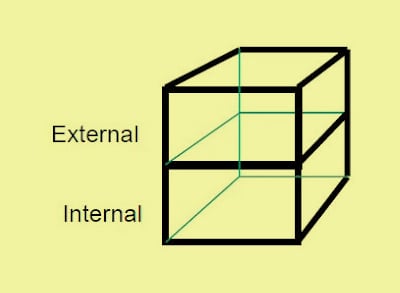
Cloud Cube model has four dimensions to categorized cloud formations:

* Internal/External
* Proprietary/Open
* De-Perimeterized/Perimeterized
* Insourced/Outsourced Dimension

### i. Internal/External

The most basic cloud form is the **external and internal cloud form**. The external or internal dimension defines the physical location of the data. It acknowledges us whether the data exists inside or outside of your organization’s boundary.

Here, the data which is stored using a **private cloud** deployment will be considered internal and data outside the cloud will be considered external.

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2019/01/External-internal.jpg)

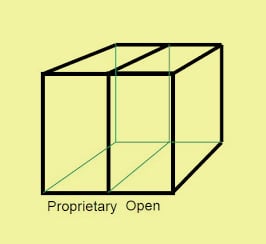
Cloud Cube Model – External/Internal

### ii. Proprietary/Open

The second type of cloud formation is **proprietary and open**. The proprietary or open dimension states about the state of ownership of the **cloud technology** and interfaces. It also tells the degree of interoperability, while enabling data transportability between the system and other cloud forms.

The **proprietary dimension** means, that the organization providing the **service is securing** and protecting the data under their ownership.

The **open dimension** is using a technology in which there are more suppliers. Moreover, the user is not constrained in being able to share the data and collaborate with selected partners using the open technology.

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2019/01/Proprietary-Open.jpg)

Cloud Cube Model – Proprietary/Open

### iii. De-Perimeterized/Perimeterized

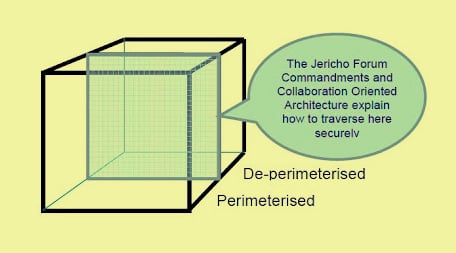
The third type of cloud formation is **De-perimeterized and Perimeterized**. To reach this form, the user needs collaboration oriented architecture and Jericho forum commandments.

The Perimeterised and De-perimeterized dimension tells us whether you are operating inside your traditional it mindset or outside it.

**Perimeterized dimension** means, continuing to operate within the traditional it boundary, orphan signaled by network firewalls.

With the help of VPN and operation of the virtual server in your own IP domain, the user can extend the organizations perimeter into external Cloud Computing domain. This means that the user is making use of the own services to control access.

**De-perimeterized dimension** means the system perimeter is architected on the principles outlined in the Jericho forums commandments. In De-perimeterized dimension, the data will be encapsulated with metadata and mechanisms, which will further help to protect the data and limit the inappropriate usage.

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2019/01/De-Perimeterized-Perimeterized.jpg)

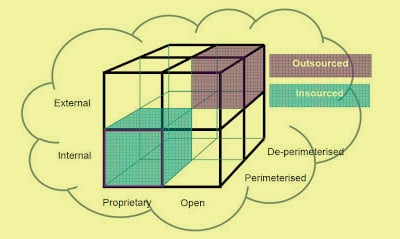
Cloud Cube Model – De-Perimeterized/Perimeterized

### iv. Insourced/Outsourced

The **Insourced and outsourced dimensions** have two states in each of the eight cloud forms. In the outsourced dimension the services provided by the third party, whereas in the insourced dimension the services provided by the own staff under the control.

In this few organizations that are traditional bandwidth software or hardware, providers will run fluently on becoming cloud service providers.

The organizations which are seeking to procedure cloud services must have the ability to set legally binding collaboration agreement. In this, an organization should ensure that data is deleted from the service provider’s Infrastructure.

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2019/01/Cloud-Cube-model-1.jpg)

Insourced/Outsourced Dimension

2. What do you mean by disaster recovery? How recovery point objective differs from

recovery time objective?

Disaster recovery represents the formal planning process through which a business creates its blueprint for responding to disruptive occurrences, which may include anything from natural disasters to cyberattacks to power outages. The disaster recovery process typically results in a disaster recovery plan, a formal document that outlines roles, policies, procedures and resource allocation to help company leaders navigate the aftermath of a cataclysmic event.

The ultimate goal of a disaster recovery plan is to provide a way for companies to minimize the effects of the disaster and return to normal operations as quickly as possible. It is important to remember that disasters can have seismic effects across an organization, including lost productivity, lost revenues, damage to brand reputation and customer dissatisfaction. Through a disaster recovery plan, businesses seek to get back up and running as expediently as possible, ideally minimizing or controlling these ill effects.

Disaster recovery plans must address all possible contingencies. It’s not enough for companies to safeguard against data loss; it’s also necessary to account for building damage or utilities that are out for days at a time. Additionally, successful disaster recovery plans address all aspects of business operations, including telephone and internet outage and the inability to use certain parts of the building.

Disaster recovery (DR) is an organization's ability to respond to and recover from an event that negatively affects business operations.

RTO is used to determine what kind of preparations are necessary for a disaster, in terms of money, facilities, telecommunications, automated systems, personnel, etc. The shorter the RTO, the greater the resources required.

RPO is used for determining the frequency of data backup to recover the needed data in case of a disaster. If your RPO is 4 hours, then you need to perform backup at least every 4 hours; every 24 hours would put you in big danger, but if you did it every hour, it might cost you too much and not bring additional value to the business.

Both Recovery Time Objective and Recovery Point Objective are determined during the business impact analysis (BIA), and the preparations for achieving them are defined in the business continuity strategy.

The main difference is in their purposes – being focused on time, RTO is focused on downtime of services, applications, and processes, helping define resources to be allocated to business continuity; while RPO, being focused on amount of data, has as its sole purpose to define backup frequency.

Another relevant difference is that, in relation to the moment of the disruptive incident, RTO looks forward in time (i.e., the amount of time you need to resume operations), while RPO looks back (i.e., the amount of time or data you are willing to lose).