Cloud Computing Viva Voice Questions

Q.1 What is cloud computing?
Answer - Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software.
Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it.

Cloud computing is a popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance, and security.

Q.2 Explain the characteristics of cloud computing as per NIST?
Answer - There are basically 5 essential characteristics of Cloud Computing.
On-demand self-services:

The Cloud computing services does not require any human administrators, user themselves are able to provision, monitor and manage computing resources as needed.

Broad network access:

The Computing services are generally provided over standard networks and heterogeneous devices.

Rapid elasticity:

The Computing services should have IT resources that are able to scale out and in quickly and on as needed basis. Whenever the user require services it is provided to him and it is scale out as soon as its requirement gets over.

Resource pooling:

The IT resource (e.g., networks, servers, storage, applications, and services) present are shared across multiple applications and occupant in an uncommitted manner. Multiple clients are provided service from a same physical resource.

Measured service:

The resource utilization is tracked for each application and occupant, it will provide both the user and the resource provider with an account of what has been used. This is done for various reasons like monitoring billing and effective use of resource.

Q.3 Explain cloud Ecosystem ?
Answer - A cloud ecosystem is a complex system of interdependent components that all work together to enable cloud services. In nature, an ecosystem is composed of living and nonliving things that are connected and work together. In cloud computing, the ecosystem consists of hardware and software as well as cloud customers, cloud engineers, consultants, integrators and partners.
In a cloud ecosystem, it is also easier to aggregate data and analyze how each part of the system affects the other parts. For example, if an ecosystem consists of patient records, smart device logs

and healthcare provider records, it becomes possible to analyze patterns across an entire patient population.

Q.4. Explain Service Models Of Cloud Computing ?

Answer - Cloud computing makes it possible to render several services, which can be defined according to the roles, service providers and the user companies. Cloud computing models and services are broadly classified as below:

IAAS: Changing Its Hardware Infrastructure on Demand

The Infrastructure As A Service (IAAS) means the outsourcing of the physical infrastructure of IT (network, storage, and servers) from a third party provider. The IT resources are hosted on external servers and users can access them via an internet connection.

The Benefits

Time and cost savings: more installation and maintenance of IT hardware in-house, Better flexibility: On-demand hardware resources that can be tailored to your needs,

- Remote access and resource management.

This cloud computing service model is ideal for large accounts, enterprises or organizations capable of building and managing their own IT platforms. However, they want the flexibility to amend their infrastructure according to their needs.

PAAS: Providing A Flexible Environment For Your Software Applications

Platform as a Service (PAAS) allows outsourcing of hardware infrastructure as well software environment, which includes databases, integration layers, runtimes and more.

The Benefits

- Mastering the installation and development of software applications

- Time saving and flexibility for development projects: no need to manage the implementation of the platform, instant production.

- Data security: You control the distribution, protection, and backup of your business data.

It is ideal for companies wanting to maintain control over their business applications. However, they wish to get rid of constraints to manage the hardware infrastructure and software environment.

SAAS: Releasing The User Experience Of Management Constraints Software as a Service (SaaS) is provided over the internet and requires no prior installation. These services can be availed from any part of the world at a minimal per month fee.

The Advantages

You are entirely free from the infrastructure management and aligning software environment: no installation or software maintenance.You benefit from automatic updates with the guarantee that all users have the same software version.It enables easy and quicker testing of new software solutions.

Q.5 Discuss different type of cloud computing Deployment Model.
Answer - Private Cloud
It is a cloud-based infrastructure used by stand-alone organizations. It offers greater control over security. The data is backed up by a firewall and internally, and can be hosted internally or externally. Private clouds are perfect for organizations that have high-security requirements, high management demands, and availability requirements.

Public Cloud

This type of cloud services is provided on a network for public use. Customers have no control over the location of the infrastructure. It is based on a shared cost model for all the users, or in the form of a licensing policy such as pay per user. Public deployment models in the cloud are perfect for organizations with growing and fluctuating demands. It is also popular among businesses of all sizes for their web applications, webmail, and storage of non-sensitive data.

Community Cloud

It is a mutually shared model between organizations that belong to a particular community such as banks, government organizations, or commercial enterprises. Community members generally share similar issues of privacy, performance, and security. This type of deployment model of cloud computing is managed and hosted internally or by a third-party vendor.

Hybrid Cloud

This model incorporates the best of both private and public clouds, but each can remain as separate entities. Further, as part of this deployment of cloud computing model, the internal, or external providers can provide resources. A hybrid cloud is ideal for scalability, flexibility, and security. A perfect example of this scenario would be that of an organization who uses the private cloud to secure their data and interacts with its customers using the public cloud.

Q.6 Define Cloud Management & Virtualization Technology
Answer - Virtualization in Cloud Computing is making a virtual platform of server operating system and storage devices. This will help the user by providing multiple machines at the same time it also allows sharing a single physical instance of resource or an application to multiple users. Cloud Virtualizations also manage the workload by transforming traditional computing and make it more scalable, economical and efficient.
Virtualizations in Cloud Computing rapidly integrating the fundamental way of computing. One of the important features of virtualization is that it allows sharing of applications to multiple customers and companies. Cloud Computing can also be known as services and application delivered to help the virtualized environment. This environment can be either public or private. With the help of virtualization, the customer can maximize the resources and reduces the physical system which is in need.

Types of Virtualization in Cloud Computing

- Operating System Virtualization
- Hardware Virtualization
- Server Virtualization
- Storage Virtualization

Q.7 Explain VDI (Virtual Desktop Infrastructure)

Answer - Virtual desktop infrastructure (VDI) is defined as the hosting of desktop environments on a central server. It is a form of desktop virtualization, as the specific desktop images run within virtual machines (VMs) and are delivered to end clients over a network. Those endpoints may be PCs or other devices, like tablets or thin client terminals.

How does VDI work?

In all VDI deployments, the following characteristics apply:

- The virtual desktops live within VMs on a centralized server
- Each virtual desktop includes an operating system image, typically Microsoft Windows
- The VMs are host-based, meaning multiple instances of them can housed on the same server within the data center
- End clients must be constantly connected to the centrally managed server in order to maintain access to the virtualized desktops it's hosting
- The VDI implementation's connection broker finds a virtual desktop within the resource pool for each client to connect to upon its successful access of the VDI environment
- Meanwhile, a hypervisor creates, runs and manages the various host machine VMs that encapsulate the individual virtual desktop environments

Q.8 What are third party cloud services

Answer - Third-party services are web-based technologies that are not exclusively operated or controlled by a government entity or that involve significant participation of a nongovernment entity. The FTC uses third-party services to assist it in communicating or interacting with the public.

A cloud service provider is a third-party company offering a cloud-based platform, infrastructure, application or storage services. Much like a homeowner would pay for a utility such as electricity or gas, companies typically have to only pay for the amount of cloud services they use, as business demands require .

Q.9 Explain the benefits of VLAN and VSAN

Answer - A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution .A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes.

The key benefits of implementing VLANs include:

Allowing network administrators to apply additional security to network Communication Making expansion and relocation of a network or a network device easier Providing flexibility because administrators are able to configure in a centralized environment while the devices might be located in different geographical locations Decreasing the latency and traffic load on the network and the network devices, offering increased performance

A virtual storage area network (VSAN) is a logical partitioning created within a physical storage area network. This implementation model of a storage virtualization technique divides and allocates

some or an entire storage area network into one or more logical SANs to be used by internal or external IT services and solutions. A VSAN is identified with a unique ID, which is a number, and is also assigned a name. While creating a VSAN it is mapped to a VLAN which it will use to carry the

Fibre Channel traffic over Ethernet A virtual storage area network is primarily implemented in cloud computing and virtualization environments. A VSAN allows end users and organizations to provision a logical storage area network on top of the physical SAN through storage virtualization.

Q.10 What are the various cloud computing security challenges and different cloud security services

Answer - Cloud security involves the procedures and technology that secure cloud computing environments against both external and insider cybersecurity threats. Cloud computing, which is the delivery of information technology services over the internet, has become a must for businesses and governments seeking to accelerate innovation and collaboration. Cloud security and security management best practices designed to prevent unauthorized access are required to keep data and applications in the cloud secure from current and emerging cybersecurity threats

Cloud computing categories

Cloud security differs based on the category of cloud computing being used. There are four main categories of cloud computing:

Public cloud services, operated by a public cloud provider — These include software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).

Private cloud services, operated by a public cloud provider — These services provide a computing environment dedicated to one customer, operated by a third party.

Private cloud services, operated by internal staff — These services are an evolution of the traditional data center, where internal staff operates a virtual environment they control.

Hybrid cloud services — Private and public cloud computing configurations can be combined, hosting workloads and data based on optimizing factors such as cost, security, operations and access. Operation will involve internal staff, and optionally the public cloud provider.

Q.11 Explain cloud service provider and their components?

Answer - Components in a cloud refers to the platforms, like front end, back end and cloud based delivery and the network that used. All together forms an architecture for cloud computing. With the main components like SAAS, PAAS and IAAS there are 11 more major categories in cloud computing.

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-as-a-service
10. Testing-as-a-Service
11. Infrastructure-as-a-Service

Q.12 Explain the concept of Hadoop ?

Answer - Apache Hadoop is an open source software framework used to develop data processing applications which are executed in a distributed computing environment.

Applications built using HADOOP are run on large data sets distributed across clusters of commodity computers. Commodity computers are cheap and widely available. These are mainly useful for achieving greater computational power at low cost.

Apache Hadoop consists of two sub-projects –

1. Hadoop MapReduce: MapReduce is a computational model and software framework for writing applications which are run on Hadoop. These MapReduce programs are capable of processing enormous data in parallel on large clusters of computation nodes.

2. HDFS (Hadoop Distributed File System): HDFS takes care of the storage part of Hadoop applications. MapReduce applications consume data from HDFS. HDFS creates multiple replicas of data blocks and distributes them on compute nodes in a cluster. This distribution enables reliable and extremely rapid computations.

Q.13 Explain Cloud security challenges ?

Answer - Since data in the public cloud is being stored by a third party and accessed over the internet, several challenges arise in the ability to maintain a secure cloud. These are:

Visibility into cloud data — In many cases, cloud services are accessed outside of the corporate network and from devices not managed by IT. This means that the IT team needs the ability to see into the cloud service itself to have full visibility over data, as opposed to traditional means of monitoring network traffic.

Control over cloud data — In a third-party cloud service provider's environment, IT teams have less access to data than when they controlled servers and applications on their own premises. Cloud customers are given limited control by default, and access to underlying physical infrastructure is unavailable.

Access to cloud data and applications —Users may access cloud applications and data over the internet, making access controls based on the traditional data center network perimeter no longer effective. User access can be from any location or device, including bring-your-own-device (BYOD) technology. In addition, privileged access by cloud provider personnel could bypass your own security controls.

Compliance — Use of cloud computing services adds another dimension to regulatory and internal compliance. Your cloud environment may need to adhere to regulatory requirements such as HIPAA, PCI and Sarbanes-Oxley, as well as requirements from internal teams, partners and customers. Cloud provider infrastructure, as well as interfaces between in-house systems and the cloud are also included in compliance and risk management processes.

Cloud-native breaches – Data breaches in the cloud are unlike on-premises breaches, in that data theft often occurs using native functions of the cloud. A Cloud-native breach is a series of actions by an adversarial actor in which they "land" their attack by exploiting errors or vulnerabilities in a cloud deployment without using malware, "expand" their access through weakly configured or protected interfaces to locate valuable data, and "exfiltrate" that data to their own storage location.

Misconfiguration – Cloud-native breaches often fall to a cloud customer's responsibility for security, which includes the configuration of the cloud service. Research shows that just 26% of companies can currently audit their IaaS environments for configuration errors. Misconfiguration of IaaS often acts as the front door to a Cloud-native breach, allowing the attacker to successfully land and then move on to expand and exfiltrate data. Research also shows 99% of misconfigurations go unnoticed in IaaS by cloud customers. Here's an excerpt from this study showing this level of misconfiguration disconnect:

Disaster recovery – Cybersecurity planning is needed to protect the effects of significant negative breaches. A disaster recovery plan includes policies, procedures, and tools designed to enable the recovery of data and allow an organization to continue operations and business.

Insider threats – A rogue employee is capable of using cloud services to expose an organization to a cybersecurity breach. A recent McAfee Cloud Adoption and Risk Report revealed irregular activity indicative of insider threat in 85% of organizations.

Q.14. How Virtualization Works?

Answer - Virtualization in Cloud Computing is a process in which the user of cloud shares the data present in the cloud which can be application software etc. It provides a virtual environment in the cloud which can be software hardware or any other thing. In virtualization, the server and the software application which are required by the cloud providers maintain by the third party and in this, the cloud provider please some amount to the third party. It is done because it will be costly if a new version of an application is released and it has to be introduced to the customers.

It can be also explained in a way that with the help of Hypervisor which is software the cloud customer can access server. A hypervisor is connectivity between the server and the virtual environment and distributes the resources between different virtual environments.

Q.15 Benefits of Virtualization

Answer –Various benefits are as follows -

1. **Security** - During the process of virtualization security is one of the important concerns. The security can be provided with the help of firewalls, which will help to prevent unauthorized access and will keep the data confidential. Moreover, with the help of firewall and security, the data can protect from harmful viruses malware and other cyber threats.
2. **Flexible operations** - With the help of a virtual network, the work of it professional is becoming more efficient and agile. The network switch implement today is very easy to use, flexible and saves time.
3. **Economical** - Virtualization in Cloud Computing, save the cost for a physical system such as hardware and servers. It stores all the data in the virtual server, which are quite economical.
4. **Eliminates the risk of system failure** - While performing some task there are chances that the system might crash down at the wrong time. This failure can cause damage to the company but the virtualizations help you to perform the same task in multiple devices at the same time.
5. **Flexible transfer of data** - The data can transfer to the virtual server and retrieve anytime. The customers or cloud provider don't have to waste time finding out hard drives to find data. With the help of virtualization, it will very easy to locate the required data and transfer them to the allotted authorities.

Q.16 Benefits of a cloud ecosystem ?

Answer - Companies can use a cloud ecosystem to build new business models. It becomes relatively easy for a medical device manufacturer, for example, to launch a heart-monitoring service on its cloud service provider's cloud infrastructure and then sell the service alongside its main business of manufacturing heart monitors for hospitals.

In a cloud ecosystem, it is also easier to aggregate data and analyze how each part of the system affects the other parts. For example, if an ecosystem consists of patient records, smart device logs and healthcare provider records, it becomes possible to analyze patterns across an entire patient population.

Q.17 What is cloud interoperability?

Answer - Interoperability is the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged. Cloud interoperability is the ability of a customer's system to interact with a cloud service or the ability for one cloud service to interact with other cloud services by exchanging information according to a prescribed method to obtain predictable results

Q.18 What is Cloud Portability ?

Answer - Portability, on the other hand, is moving the data and/or applications from one system to another and having it remain useable or executable. Cloud data portability is the ability to easily move data from one cloud service to another without needing to re-enter the data. Cloud application portability is the ability to migrate an application from one cloud service to another or between a customer's environment and a cloud service.

Q.19 Explain the advantages of cloud computing ?

Answer - Cloud-based software offers companies from all sectors a number of benefits, including the ability to use software from any device either via a native app or a browser. As a result, users can carry their files and settings over to other devices in a completely seamless manner.
Cloud computing is far more than just accessing files on multiple devices
The cloud structure allows individuals to save storage space on their desktops or laptops.

Q.20 Explain Cloud adoption and rudiments?
Answer - **Adoption** term states that accepting the services of new Technology. Adoption means following some kind of new trend or existing trend or a technology.

Cloud rudiments means that the services provided through cloud such as Resource aggregation and integration: - Cloud solution integrates or aggregates the information of virtualization management, physical server provisioning, system management.