1. How grid computing differs from cloud computing? Justify what the provisioning and multi-tenancy properties of cloud computing means?

Grid computing is a computer network in which each computer's resources are shared with every other computer in the system. Processing power, memory and data storage are all community resources that authorized users can tap into and leverage for specific tasks. A grid computing system can be as simple as a collection of similar computers running on the same operating system or as complex as inter-networked systems comprised of every computer platform you can think of. A grid computer is connected through a super-fast network and share the devices like disk drives, mass storage, printers and RAM.

In general, a grid computing system requires:

- At least one computer, usually a server, which handles all the administrative duties for the system
- A network of computers running special grid computing network software
- A collection of computer software called middleware

Cloud is basically an extension to the object-oriented programming concept of abstraction. Here cloud means the Internet. For the end users it is just getting outputs for certain inputs, the complete process that lead to the outputs is purely invisible. Computing is based on virtualized resources which are placed over multiple servers in clusters.

Also within the "cloud computing" family, are what's known as a SPI model SaaS, PaaS and IaaS. These are the services available on the cloud and do all the heavy lifting using someone else's infrastructure. Cloud computing eliminates the costs and complexity of buying, configuring, and managing the hardware and software needed to build and deploy applications; these applications are delivered as a service over the Internet (the cloud).

Cloud vs Grid computing: Conclusion

1. Server computers are still needed to distribute the pieces of data and collect the results from participating clients on grid.
2. Cloud offers more services than grid computing. In fact almost all the services on the Internet can be obtained from cloud, eg web hosting, multiple Operating systems, DB support and much more.
3. Grids tends to be more loosely coupled, heterogeneous, and geographically dispersed compared to conventional cluster computing systems.

2. Describe possible services that can be achieved through infrastructure as a service (IaaS)?

Infrastructure as a Service (IaaS) is one of the three fundamental service models of cloud computing alongside Platform as a Service (PaaS) and Software as a Service (SaaS). Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Clients are able to self-provision this infrastructure, using a Web-based graphical user interface that serves as an IT operations management console for the overall environment. API access to the infrastructure may also be offered as an option. IaaS is usually seen to provide a standardized virtual server. The

consumer takes responsibility for configuration and operations of the guest Operating System (OS), software, and Database (DB). Compute capabilities (such as performance, bandwidth, and storage access) are also standardized

INTERNAL BUSINESS NETWORKS

Utilizing pooled server and networking resources in which a business can store data and run applications. Expanding businesses can scale their infrastructure in accordance with growth

CLOUD HOSTING

Hosting of websites on virtual servers which are founded upon pooled resources from underlying physical servers

VIRTUAL DATA CENTRE'S (VDC)

A virtualized network of interconnected virtual servers which can be used to offer enhanced cloud hosting capabilities, enterprise IT infrastructure or to integrate operations

4. What do you mean by Elastic IP Addressing? Describe how Elastic IPs works in cloud service.

An *Elastic IP address* is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. An Elastic IP address is a public IPv4 address, which is reachable from the Internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address with your instance to enable communication with the Internet; for example, to connect to your instance from your local computer. Elastic IP addresses are used by AWS to manage its dynamic cloud computing services. Within the AWS infrastructure, customers have virtual private clouds (VPCs). Within the VPCs, users have instances. The Elastic IP address is what is used to advertise the data within the instance to the public internet.

Works:

- Each EIP can be assigned to one instance, in which case it replaces the normal dynamic IP address. Remember, by default, each instance starts with a dynamic IP address.
    - Each instance can have only a single external IP address. It starts out with the default dynamic IP address which can be swapped out for an EIP at any time. If the EIP is designed (or assigned to a different instance) then a fresh dynamic IP is allocated for the instance. The limitation of designating a single IP at a time is due to the way NAT (Network Address Translation) works. Remember that each instance has an internal IP address and an external (public) one, which is translated to the internal one. If two external IPs were translated to the same internal IP then inbound packets would arrive fine, but sorting out outgoing packets (i.e. determining which external IP address to assign to outgoing packets) would be very difficult. Hence, the limitation of a single external IP address per instance at any given point in time.
    - EIPs are free while they are assigned to an instance, but they cost $0.01/hr if they are not assigned. The reason for this charge is due to the fact that the number of IP addresses worldwide is very limited. Perhaps in theory, this charge will help prevent users from hogging unused IP addresses that could be dynamically allocated to other users. Yet, in a weird way there is no additional cost to Amazon for an

assigned static IP as opposed to a dynamic IP because while an EIP is assigned to an instance it actually frees-up a dynamic IP.
- Assigning or reassigning an IP to an instance takes a couple of minutes, which is longer than I would have hoped for, but I can imagine that many network devices need to be updated in the infrastructure to make it all happen.

4. Discuss about the planning needed for building the Service Oriented Architecture.

A service-oriented architecture is essentially a collection of services. These services communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity.

The reality in IT enterprises is that infrastructure is heterogeneous across operating systems, applications, system software, and application infrastructure. Some existing applications are used to run current business processes, so starting from scratch to build new infrastructure isn't an option. Enterprises should quickly respond to business changes with agility; leverage existing investments in applications and application infrastructure to address newer business requirements; support new channels of interactions with customers, partners, and suppliers; and feature an architecture that supports organic business. SOA with its loosely coupled nature allows enterprises to plug in new services or upgrade existing services in a granular fashion to address the new business requirements, provides the option to make the services consumable across different channels, and exposes the existing enterprise and legacy applications as services, thereby safeguarding existing IT infrastructure
investments.

5.”Virtualization is the key to cloud computing”, justify this statement with proper arguments. How hypervisor are used in cloud computing service?

Virtualization is one of the key components of the cloud computing paradigm, especially in infrastructure as a service model where the mentioned technology is essential to provide a large set of computing resources. Some experts even define cloud computing as simple as virtualized hardware and software plus advanced monitoring and resource management technologies. Saying it straight and clear, without virtualization, cloud computing would leave the data unstable, uncontrolled and unsafe. It is an important and probably an inseparable element of cloud computing services. Virtualization allows us to consolidate multiple physical components so that they can be managed at one place. With the help of virtualization, organizations have a better visibility and also a greater control of their infrastructure making security management simpler for the cloud. It is due to virtualization that the cloud computing services are so cost-effective. Moreover, it is also responsible for the simplicity of delivering services by providing a platform for optimizing complex IT resources.

A few examples to convince you on the above thought –

- **Intelligent use of single computers**: Virtualization software enables 1 computer to perform as though it were 20 computers. It empowers you to move your data center with thousands of computers to a single one that supports as few as a couple of hundreds.
- **Virtual memory**: Computer systems can use virtual memory to borrow extra memory from the hard disk. Although, it performs slower than the disk spaces, this substitution works considerably well.

- **Efficient use of IT resources**: Cloud data storage services let you optimize your resources/capacity based on your needs. Whenever you need more capacity, you can easily leverage the cloud provider's infrastructure.
- **Easily migrate and balance workload**: When your workloads vary greatly (mostly happens with e-commerce websites), the cloud computing environments can proactively add more capacity in anticipation of the need.

A *hypervisor* is an operating system, which means that it knows how to act as a traffic cop to make things happen in an orderly manner. The hypervisor sits at the lowest levels of the hardware environment. Because in cloud computing you need to support many different operating environments, the hypervisor becomes an ideal delivery mechanism. The hypervisor lets you show the same application on lots of systems without having to physically copy that application onto each system. One twist: Because of the hypervisor architecture, it can load any (or many) different operating system as though it were just another application. Therefore, the hypervisor is a very practical way of getting things virtualized quickly and efficiently. The hypervisor installed on the server hardware controls the guest operating system running on the host machine. Its main job is to cater to the needs of the guest operating system and effectively manage it such that the instances of multiple operating systems do not interrupt one another.

Hypervisors can be divided into two types:

- Type 1: Also known as native or bare-metal hypervisors, these run directly on the host computer's hardware to control the hardware resources and to manage guest operating systems. Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServer and Microsoft Hyper-V hypervisor.
- Type 2: Also known as hosted hypervisors, these run within a formal operating system environment. In this type, the hypervisor runs as a distinct second layer while the operating system runs as a third layer above the hardware.

7. Explain the different types of implementing Network Intrusion Detection System in cloud.

An **Intrusion Detection System** (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies. This article will elaborate on the configuration and functions that define the IDS deployment.

Active and passive IDS

An active Intrusion Detection Systems (IDS) is also known as Intrusion Detection and Prevention System (IDPS). Intrusion Detection and Prevention System (IDPS) is configured to automatically block suspected attacks without any intervention required by an operator. Intrusion Detection and Prevention System (IDPS) has the advantage of providing real-time corrective action in response to an attack.

Network Intrusion detection systems (NIDS) and Host Intrusion detection systems (HIDS)

Network Intrusion Detection Systems (NIDS) usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

A Host Intrusion Detection Systems (HIDS) and software applications (agents) installed on workstations which are to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A

host Intrusion detection systems (HIDS) can only monitor the individual workstations on which the agents are installed and it cannot monitor the entire network.

Knowledge-based (Signature-based) IDS and behavior-based (Anomaly-based) IDS

A knowledge-based (Signature-based) Intrusion Detection Systems (IDS) references a database of previous attack signatures and known system vulnerabilities. The meaning of word signature, when we talk about Intrusion Detection Systems (IDS) is recorded evidence of an intrusion or attack. Each intrusion leaves a footprint behind (e.g., nature of data packets, failed attempt to run an application, failed logins, file and folder access etc.). These footprints are called signatures and can be used to identify and prevent the same attacks in the future. Based on these signatures Knowledge-based (Signature-based) IDS identify intrusion attempts.

8. What can be the impact of disaster in cloud? How geographic redundancy and organization redundancy ensures disaster recovery in cloud services.

9. Discuss how security architecture and trust architecture ensure security of cloud services networks.