

Short Questions

1.What is the major revolution introduced by Web 2.0?

Ans: It brought about a change in the architecture of the web which enables features like word press, social media, OTT platforms etc.

2.What is Multi-tenancy?

Ans: In cloud computing, multitenancy means that multiple customers of a cloud vendor are using the same computing resources. Despite the fact that they share resources, cloud customers aren't aware of each other, and their data is kept totally separate. Multitenancy is a crucial component of cloud computing; without it, cloud services would be far less practical. Multitenant architecture is a feature in many types of public cloud computing, including IaaS, PaaS, SaaS, containers, and serverless computing.

3.Give two names of popular Software as a Service solutions.

Ans: 1) Office 365
2) Gmail

4.List some driving factors toward clouds.

Ans: 1)Cloud adoption present scenario
2)Major benefits of cloud adoption
3)Significant factors that influence cloud adoption

5.Define SSL.

Ans: Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remains private and free from attack.

6.What are the benefits of identity management?

Ans: 1)Improved security
2)Information sharing
3)Ease of use
4)Productivity gains
5)Reduced IT Costs

7.How cloud helps to analyse Big Data?

Ans: Cloud Computing providers often utilize a “software as a service” model to allow customers to easily process data. This cloud infrastructure allows for real-time processing of Big Data. It can take huge “blasts” of data from intensive systems and interpret it in real-time.

By using big data analytics in the cloud, businesses are able to derive better analysis from the large amounts of structured and unstructured data in their possession.

8.What is Eucalyptus?

Ans: Eucalyptus is an open source software platform for implementing Infrastructure as a Service (IaaS) in a private or hybrid cloud computing environment.

The Eucalyptus cloud platform pools together existing virtualized infrastructure to create cloud resources for infrastructure as a service, network as a service and storage as a service.

9.What is Virtual private cloud?

Ans: A virtual private cloud (VPC) is a private cloud computing environment contained within a public cloud. Essentially, a VPC provisions logically isolated sections of a public cloud in order to provide a virtual private environment.

Like all cloud environments, VPC resources are available on-demand to scale up as needed and are highly configurable.

10.Write a short note on Microsoft Azure.

Ans: Microsoft Azure, commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

It provides software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) and supports many different programming languages, tools, and frameworks, including both Microsoft-specific and third-party software and systems. Azure is the largest commercial cloud vendor by revenue, although that designation stems in part from the company's "power of incumbency in Office 365 Commercial and Microsoft 365," which may artificially inflate the company's "pure cloud" revenue totals.

11.Write a short note on Community cloud and examples

Ans: Community Cloud is a hybrid form of private cloud. They are multi-tenant platforms that enable different organizations to work on a shared platform.

Community Cloud computing facilitates its users to identify and analyze their business demands better. Community Cloud may be hosted in a data center, owned by one of the tenants, or by a third-party cloud services provider and can be either on-site or off-site.

Example:

1) Example of using a community cloud would be to test-drive some high-end security products or even test out some features of a public cloud environment. This is great for organizations that are driven by compliance and regulatory measures. Government, healthcare, and some regulated private industries are leveraging the added security features within a community cloud environment. Instead of just provisioning space in a public cloud, organizations can test and work on a cloud platform which is secure, "dedicated," and even compliant with certain regulations. The really interesting part is that with a community cloud, the presence can be either onsite or offsite.

12. Write a short note on Virtual Machine

Ans: A virtual machine (or "VM") is an emulated computer system created using software. It uses physical system resources, such as the CPU, RAM, and disk storage, but is isolated from other software on the computer. It can easily be created, modified, or destroyed without affecting the host computer.

As cloud services have grown in popularity, cloud-based VMs have become increasingly popular as well. "Cloud instances," as they are often called, run on a computer that is accessed over the Internet. The VM is often controlled through a web browser or a remote access utility. Cloud-based VMs are a common way for companies to test software deployments since they can test on dozens of machines without hosting the VMs locally.

13. Write a short note on Full Virtualization

Ans: Full virtualization is a virtualization technique used to provide a VME that completely simulates the underlying hardware. In this type of environment, any software capable of execution on the physical hardware can be run in the VM, and any OS supported by the underlying hardware can be run in each individual VM. Users can run multiple different guest OSes simultaneously.

In full virtualization, the VM simulates enough hardware to allow an unmodified guest OS to be run in isolation. This is particularly helpful in a number of situations. For example, in OS development, experimental new code can be run at the same time as older versions, each in a separate VM. The hypervisor provides each VM with all the services of the physical system, including a virtual BIOS, virtual devices, and virtualized memory management. The guest OS is fully disengaged from the underlying hardware by the virtualization layer.

14. Difference between elasticity and scalability in cloud computing

Ans: The purpose of **elasticity** is to match the resources allocated with actual amount of resources needed at any given point in time. **Scalability** handles the changing needs of an application within the confines of the infrastructure via statically adding or removing resources to meet applications demands if needed.

15. Write a short note on Xen Hypervisor.

Ans: Xen is an open source hypervisor based on paravirtualization. Xen has been extended to be compatible with full virtualization using hardware-assisted virtualization. It enables high performance to execute guest operating systems.

16. How does cloud computing differ from the Internet?

Ans:

The Internet is a network of networks, which provides software/hardware infrastructure to establish and maintain connectivity of the computers around the world, while Cloud computing is a new technology that delivers many types of resources over the Internet. Therefore Cloud computing could be identified as a technology that uses the Internet as the communication medium to deliver its services. Cloud services can be offered within enterprises through LANs but in reality, Cloud computing cannot operate globally without the Internet.

17. What is multi-tenancy and its advantage?

Ans: A multi-tenant cloud is a cloud computing architecture that allows customers to share computing resources in a public or private cloud. Each tenant's data is isolated and remains invisible to other tenants.

In a multi-tenant cloud system, users have individualized space for storing their projects and data.

Advantage:

- 1) Helps a great Deal in Cutting the Cost of Investment
- 2) Adding a New Customer is Easy
- 3) It Becomes More Convenient to Maintain the Same Application
- 4) Maximising the Resource Usage
- 5) Holds Multiple Tenants all at the Same Time

18. What is on-demand self-service and resource pooling?

Ans:

On-demand self service:

Cloud computing provides resources on demand, i.e. when the consumer wants it.

For eg:

The consumer's request is then automatically processed by the cloud infrastructure, without human intervention on the provider's side.

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.

Examples of resources include storage, processing, memory, and network bandwidth.

19. Differentiate full-virtualization and para-virtualization.

Ans: . In Full virtualization, virtual machines permit the execution of the instructions with running of unmodified OS in an entirely isolated way. In paravirtualization, virtual machines do not implement full isolation of OS but rather provide a different API which is utilized when OS is subjected to alteration.

20. Write any two characteristics of private and public clouds.

Ans: Private cloud:

- 1) The private cloud offers several advantages of an open cloud computing setting that comprises its service support and flexibility.
- 2) Private clouds allow infrastructure to be accessed only by the members of the organization and granted by third parties .

Public cloud:

- 1) The public cloud is the first deployment model. In this model, users have many options to opt for and decide on any service provider as per requirement.
- 2) This model assists in the reduction of capital expenses and removes equipped IT expenses.

21. What is the role of network manager in the IaaS service layer?

Ans: A TechNote on The Next Generation

Jim Metzler Distinguished Research Fellow and Co-Founder Webtorials Analyst Division.

This is the third in a series of four TechNotes reporting on some of our recent research into the use of cloud-based Infrastructure-as-a-Service (IaaS) solutions. The first and second TechNotes concerned The Growing Use of IaaS and The Drivers and Inhibitors of IaaS.

22. Enlist the services that are provided by Amazon.

Ans:

1. Amazon Elastic Cloud Compute (EC2)
2. Amazon S3 (Simple Storage Service)
3. Amazon Virtual Private Cloud (VPC)
4. Amazon CloudFront

5. Amazon Relational Database Services (RDS)

23. Why is hypervisor important? What is its role?

Ans: A hypervisor is computer software or hardware that enables you to host multiple virtual machines. Each virtual machine is able to run its own programs.

It is important because A hypervisor allows you to access several virtual machines that are all working optimally on a single piece of computer hardware. For the most part, cloud computing entails you being able to access a virtual machine for you to be able to do what you need to do anywhere. A hypervisor manages these virtual machines.

24. Mention the names of phases in SaaS maturity model.

Ans: The SaaS maturity model is broken down into four levels, and each of them brings certain opportunities and challenges you should be aware of when accessing SaaS vendors.

Level 1 (Single-Tenant, Custom Instances)

Level 2 (Single-Tenant, Configurable Instances)

Level 3 (Multi-Tenant, Configurable)

Level 4 (Multi-Tenant Configurable & Scalable)

25. Give any two examples of self-service.

Ans: Self-service cloud computing is a form of private cloud service where the customer provisions storage and launches applications without going through an external cloud service provider. With a self-service cloud, users access a web-based portal, where they can request or configure servers and launch applications.

26. Differentiate Cloud Computing and Internet.

Ans: same as question no 16

27. How do multi-tenancy advantageous to the success of cloud computing?

Ans: In cloud computing, multi-tenancy means that a SaaS (Software as a Service) vendor provides a single version of its software for all its customers. ... Shared infrastructure leads to lower costs: SaaS allows companies of all sizes to share infrastructure and data center operational costs.

28. What is resource pooling and rapid elasticity?

Ans:

Resource pooling:

A given cloud service should be able to serve multiple users simultaneously, using a multi tenant model, with physical and virtual resources dynamically assigned and reassigned according to customer demand.

Rapid elasticity:

The capabilities of the cloud should appear unlimited to the user. These capabilities should be elastically scalable both outward and inward in accordance with demand, whatever the quantity of resources required, and at any time.

29. Is API necessary in cloud computing?

Ans: A cloud API enables end users to access a cloud provider's application or service, such as compute infrastructure, storage resources or monitoring tools. APIs define the possible features and functions of that app or service, along with the details needed to execute them.

30. Write any two characteristics of public cloud and hybrid cloud.

Ans: Two characteristics of public cloud:

Ultimate scalability – vast on demand resources are available so that applications can respond seamlessly to fluctuations in activity.

Cost effective - public cloud brings together a greater level of resources so users can benefit from the largest economies of scale. The centralized operation and management of the underlying resources is shared across all of the subsequent services.

Utility style payment model - public cloud services employ a pay-as-you-go model whereby the consumer is able to access the resource they need, when they need them, and only pay for what they use; avoiding wasted capacity.

Reliability - the sheer number of servers and networks involved in creating a public cloud mean that if one physical component fails, the service would still run unaffected on the remaining components. In some cases, where clouds draw resources from multiple data centers, an entire data center could go offline and individual services would suffer no ill effect. There is, in other words, no single point of failure.

Flexibility - there are a myriad of IaaS, PaaS and SaaS services available on the market which follow the public cloud model and that are ready to be accessed as a service from any internet enabled device. These services can fulfill most computing requirements and can deliver their

benefits to private and enterprise clients alike. Businesses can even integrate their public cloud services with private clouds, where they need to perform sensitive business functions, to create hybrid clouds.

Location independence - the availability of public cloud services through an internet connection ensures that the services are available wherever the client is located. This provides remote access to IT infrastructure (in case of emergencies, etc.) and online document collaboration from multiple locations.

Advantages of the hybrid cloud:

Control: your organisation can maintain a private infrastructure for sensitive assets or workloads that require low latency.

Flexibility: you can take advantage of additional resources in the public cloud when you need them.

Cost-effectiveness: with the ability to scale to the public cloud, you pay for extra computing power only when needed.

Ease: transitioning to the cloud does not have to be overwhelming because you can migrate gradually phasing in workloads over time.

31.What is the role of resource scheduler in the IaaS service layer?

Ans: Resource scheduling assigns the precise and accurate task to CPU, network, and storage. organized scheduling is needed for both cloud providers and cloud users.

32.Enlist the services that are provided by IBM Smart Cloud.

Ans:

Some services offered by IBM Smart Cloud are as follows:

Compute Infrastructure

Compute Services

Storage

Watson (IBM's artificial intelligence and machine learning service)

Data and Analytics

Security

DevOps

Application services

33.What is SSL?

Ans: Secure Sockets Layer (SSL) is a standard protocol used for the secure transmission of documents over a network. Developed by Netscape, SSL technology creates a secure link between a Web server and browser to ensure private and integral data transmission. SSL uses Transport Control Protocol (TCP) for communication.

34.What is the selection criterion for private cloud deployment model?

Ans: A private cloud offers flexibility, cost savings, security, and control benefits. These benefits are particularly valuable for businesses with predictable workloads or customization requirements, and businesses in regulated industries.

35.Give any two examples of self-service.

Ans: same as question no 25

36.What is Cloud Computing?

Ans: Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user.

37.What are the characteristics in cloud computing.

Ans: Characteristics of cloud computing:

- 1.Great Availability of Resources
- 2.On-demand Self-service
- 3.Easy Maintenance
- 4.Large Network Access
- 5.Availability
- 6Automatic System
- 7.Economical
- 8.Security
- 9.Pay as you go

38.What are the different things to be taken into consideration before migrating into a cloud platform?

Ans: <https://whitehatsme.com/factors-consider-when-moving-to-cloud>

39.Roots of Cloud Computing:

Ans: THE CONVERGENCE OF TECHNOLOGY FIELDS THAT SIGNIFICANTLY ADVANCED AND CONTRIBUTED TO THE ADVENT OF CLOUD COMPUTING
HARDWARE (VIRTUALIZATION, MULTI-CORE CHIPS)
INTERNET TECHNOLOGIES (WEB SERVICES, SERVICE-ORIENTED ARCHITECTURES, WEB 2.0)
DISTRIBUTED COMPUTING (CLUSTERS, GRIDS)

SYSTEMS MANAGEMENT (AUTONOMIC COMPUTING, DATA CENTER AUTOMATION)
A SPECIFICATION AND STANDARDIZATION PROCESS FOLLOWED
LEADING TO MATURITY AND WIDE ADOPTION

FROM MAINFRAMES TO CLOUDS
SOA, WEB SERVICES
GRID COMPUTING
UTILITY COMPUTING
HARDWARE VIRTUALIZATION
AUTONOMIC COMPUTING

40.What is the difference between cluster and cloud computing ?

Ans: Cluster computing refers to the process of sharing the computation task to multiple computers of the cluster. The number of computers are connected on a network and they perform a single task by forming a Cluster of computers where the process of computing is called cluster computing.

Cluster Computing is a high performance computing framework which helps in solving more complex operations more efficiently with a faster processing speed and better data integrity. Cluster Computing is a networking technology that performs its operations based on the principle of distributed systems.

Cloud Computing refers to the on demand delivery of the IT resources especially computing power and data storage through the internet with pay per use pricing. It generally refers to the data centers available to the users over internet. Cloud Computing is the virtualized pool of resources. It allows us to create, configure and customize our applications online. The user can access any resource at any time and anywhere without worrying about the management and maintenance of actual resources. Cloud computing delivers both a combination of hardware and software based computing resources over the network.

41.Differentiate between grid and cloud computing.

Ans: <https://www.geeksforgeeks.org/difference-between-cloud-computing-and-grid-computing>

42.What are the benefits in cloud computing.

Ans: Reduced IT costs. Moving to cloud computing may reduce the cost of managing and maintaining your IT systems. ...

Scalability.

Business continuity.

Collaboration efficiency.

Flexibility of work practices.

Access to automatic updates.

43. Discuss the functionality of various components of cloud infrastructure.

Ans: <https://www.javatpoint.com/cloud-computing-architecture>

44. Discuss various cloud service models and prepare a comparative report of these models with example.

Ans:

<https://www.javatpoint.com/cloud-service-models>

https://mrcet.com/pdf/Lab%20Manuals/IT/R15A0529_CloudComputing_Notes-converted.pdf (pg 40)

45. Explain cloud computing architecture and its various components with diagrams.

Ans: <https://intellipaat.com/blog/cloud-computing-architecture/>

46. Explain the NIST cloud reference architecture.

Ans: <https://www.slideshare.net/lersmethasakul/nist-cloud-computing-reference-architecture>

Long Questions

1. What are the major distributed computing technologies that led to cloud computing?

Ans: The major distributed computing technologies which led to cloud computing:-

Cluster Computing:- A computer cluster is a group of linked computers, working together closely so that in many respects they form a single computer. The components of a cluster are commonly, but not always, connected to each other through fast local area networks. Clusters are usually deployed to improve performance and/or availability over that provided by a single computer, while typically being much more cost-effective than single computers of comparable speed or availability.

Grid Computing:- Computing grids are conceptually and logically like electrical grids. In an electrical grid, wall outlet allow us to connect to an infrastructure of resources which generate and distribute the electricity. Likewise, in the IT industry, grid computing uses middleware to coordinate distinct IT

resources over the network, allowing them to function and work as a virtual whole.

The goal of a computing grid, like that of an electrical grid, is to provide users with access to the resources they need, when they need them and to provide remote access to IT assets and aggregating processing power.

Grid provides a series of distributed computing resources via LAN or WAN to the terminal user's application, as if he is using a super virtual computer.

2. Discuss classification of virtualization at different levels.

Ans: 1. Instruction Set Architecture Level

At the ISA level, virtualization is performed by emulating a given ISA by the ISA of the host machine. For example, MIPS binary code can run on an x86-based host machine with the help of ISA emulation. With this approach, it is possible to run a large amount of legacy binary code written for various processors on any given new hardware host machine. Instruction set emulation leads to virtual ISAs created on any hardware machine.

The basic emulation method is through code interpretation. An interpreter program interprets the source instructions to target instructions one by one. One source instruction may require tens or hundreds of native target instructions to perform its function. Obviously, this process is relatively slow. For better performance, dynamic binary translation is desired. This approach translates basic blocks of dynamic source instructions to target instructions. The basic blocks can also be extended to program traces or super blocks to increase translation efficiency. Instruction set emulation requires binary translation and optimization. A virtual instruction set architecture (V-ISA) thus requires adding a processor-specific software translation layer to the compiler.

2. Hardware Abstraction Level

Hardware-level virtualization is performed right on top of the bare hardware. On the one hand, this approach generates a virtual hardware environment for a VM. On the other hand, the process manages the underlying hardware through virtualization. The idea is to virtualize a computer's resources, such as its processors, memory, and I/O devices. The intention is to upgrade the hardware utilization rate by multiple users concurrently. The idea was implemented in the IBM VM/370 in the 1960s. More recently, the Xen hypervisor has been applied to virtualize x86-based machines to run Linux or other guest OS applications. We will discuss hardware virtualization approaches in more detail in Section 3.3.

3. Operating System Level

This refers to an abstraction layer between traditional OS and user applications. OS-level virtualization creates isolated containers on a single physical server and the OS instances to utilize the hardware and software in data centers. The containers behave like real servers. OS-level virtualization is commonly used in creating virtual hosting environments to allocate hardware resources among a large number of mutually distrusting users. It is also used, to a lesser extent, in consolidating server hardware by moving services on separate hosts into containers or VMs on one server. OS-level virtualization is depicted in Section 3.1.3.

4. Library Support Level

Most applications use APIs exported by user-level libraries rather than using lengthy system calls by the OS. Since most systems provide well-documented APIs, such an interface becomes another candidate for virtualization. Virtualization with library interfaces is possible by controlling the communication link between applications and the rest of a system through API hooks. The software tool WINE has implemented this approach to support Windows applications on top of UNIX hosts. Another example is the vCUDA which allows applications executing within VMs to leverage GPU hardware acceleration. This approach is detailed in Section 3.1.4.

5. User-Application Level

Virtualization at the application level virtualizes an application as a VM. On a traditional OS, an application often runs as a process. Therefore, application-level virtualization is also known as process-level virtualization. The most popular approach is to deploy high level language (HLL)

VMs. In this scenario, the virtualization layer sits as an application program on top of the operating system, and the layer exports an abstraction of a VM that can run programs written and compiled to a particular abstract machine definition. Any program written in the HLL and compiled for this VM will be able to run on it. The Microsoft .NET CLR and Java Virtual Machine (JVM) are two good examples of this class of VM.

Other forms of application-level virtualization are known as application isolation, application sandboxing, or application streaming. The process involves wrapping the application in a layer that is isolated from the host OS and other applications. The result is an application that is much easier to distribute and remove from user workstations. An example is the LANDesk application virtualization platform which deploys software applications as self-contained, executable files in an isolated environment without requiring installation, system modifications, or elevated security privileges.

3.What is SaaS in Cloud computing? Explain different categories of SaaS.

Ans: SaaS is a software delivery methodology that provides licensed multi-tenant access to software and its functions remotely as a Web-based service.

– Usually billed based on usage

- Usually multi tenant environment
- Highly scalable architecture.

Different categories of SaaS:-

Packaged software: This is the biggest area of the SaaS market. Packaged software comes in many different flavors: customer relationship management, supply chain management, financial management, and human resources, to name the most common.

These integrated offers focus on a specific process, such as managing employees' benefits, salaries, and annual performance reviews. These products tend to have several characteristics in common: They're designed with specific business processes built in that customers can modify. They have moved in great numbers to the cloud because customers were finding the platforms too hard to manage.

Collaborative software: This increasingly vibrant area of the market is driven by the ubiquitous availability of the Internet, combined with the fact that teams are located all over the world. This area is dominated by software that focuses on all sorts of collaborative efforts including Web conferencing, document collaboration, project planning, instant messaging, and even email. In a sense, it was inevitable that these platforms would move to the cloud: These tasks occur throughout the organization and need to be easily accessed from many locations.

Enabling and management tools: What's in this category? Think about the development tools that developers need when creating and extending a SaaS platform; also think about the testing, monitoring, and measuring that a customer and the developer need. Also consider the compliance issues related to the use of this type of software in the real world. These issues are included in this third category.

4.What are the security risk aspects associated with cloud?Classify the various types of clouds.

Ans:

1. Data Breaches — Data Theft and Data Loss

Risk Factors

A data breach can result in data theft or data loss and damage data confidentiality, availability and integrity.

Causes of cloud data breaches include:

Insufficient identity and credential management

Easy registration systems, phishing and pretexting

Insecure APIs

Best Practices for Risk Mitigation

Develop company-wide cloud usage and permission policies.

Require multi-factor authentication.

Implement data access governance.

Enable centralized logging to make it easy for investigators to access the logs during an incident.

Implement data discovery and classification.

Enable user behavior analytics.

Establish data remediation workflows.

Implement data loss prevention (DLP).

Outsource breach detection by using a cloud access security broker (CASB) to analyze outbound activities.

2) Misconfigurations

Risk Factors

Common types of misconfiguration include:

Human error

Allowing excessive permissions

Maintaining unused and stale accounts

Allowing excessive sharing settings, which can lead to sensitive data being overexposed

Leaving default settings unchanged, including admin credentials and port numbers

Disabling standard security controls

Disabling encryption

Best Practices for Risk Mitigation

Establish baseline configurations and regularly conduct configuration auditing to check for drift away from those baselines.

Use continuous change monitoring to detect suspicious changes and investigate them promptly.

Be sure you know which settings are modified, who made the change, and when and where it happened.

Know who has access to what data and regularly review all users' effective permissions.

Require data owners to periodically attest that permissions match employees' roles. Also validate that all access rights align data protection. Revoke excessive or inappropriate access rights.

3) Insider Threats

Risk Factors

Insider threats can be intentional, such as a disgruntled employee taking revenge, or accidental, like an admin making a mistake. Employees aren't the only insiders either. Contractors, suppliers and partners can also access data inappropriately, expose it or allow it to be stolen.

Many enterprises lack visibility into user and admin activity and application usage across their cloud storage systems.

Specific insider threats include privilege abuse, compromised routers and VPNs, shared accounts, privileged accounts, and service accounts.

Best Practices for Risk Mitigation

De-provision access to resources immediately whenever you have personnel changes.

Implement data discovery and classification technology. Identify all sensitive and business-critical data you have; know which users, contractors and partners have access to it; and track their activities concerning Look for signs of suspicious activity trends, such as an increased number of failed access attempts. Staying on top of user activities around sensitive and business-critical data helps you identify malicious operations before they cause real damage.

Monitor privileged users. Track service and privileged accounts separately from other user accounts. These accounts should be used sparingly for specific tasks that other accounts do not have sufficient rights to perform.

Implement user behavior analytics. Create a baseline behavioral profile of each user and watch for actions atypical for that user or others with the same role. Track attempts to access disabled accounts, along with any other anomalous attempts to access data or gain elevated permissions.

4)Account Hijacking

Account hijacking is the use of stolen credentials for various purposes, such as to gain access to sensitive data.

Risk Factors

Hackers use password cracking, phishing emails and cross-site scripting, among other industry-known tricks, to guess credentials and gain access to staff accounts.

Subscription services and privileged accounts are especially vulnerable.

Best Practices for Risk Mitigation

Implement identity and access control.

Use multi-factor authentication.

Require strong passwords.

Monitor user behavior.

Identify and revoke excessive access to sensitive information.

Remove unused accounts and credentials.

Apply the principle of least privilege.

Control third-party access.

Train employees on preventing account hijacking.

5)Denial of Service Attacks

A denial of service (DoS) attack is an attempt to make it impossible for service to be delivered. A DoS attack is when one system is attacking, and a DDos (distributed denial of service) attack involves multiple systems performing the attack. Advanced persistent denial of service (APDoS) attacks target the application layer, where hackers can directly hit databases or servers.

Risk Factors

In general, a denial of service attack drowns a system with requests, overwhelming bandwidth, CPU or RAM capacity so that other users can't access the system. Botnets are often used to achieve large-scale DDoS attacks that can exceed 1,000 Gbps. Increasingly, hackers rent botnets from their developers.

While the volume of DDoS attacks has declined, new forms of DoS attacks are being discovered that integrate AI and machine learning.

Best Practices for Risk Mitigation

Secure the network infrastructure with a web application firewall.

Implement content filtering.

Use load balancing to identify potential traffic inconsistencies.

6)Malware

Risk Factors

Malware infects a cloud provider's servers just as it does on-prem systems: The attacker entices a user to click on a malicious email attachment or social media link, enabling them to download malware encoded to bypass detection and designed to eavesdrop, steal data stored in cloud service applications or otherwise compromise data security.

Best Practices for Risk Mitigation

Control malware problems and other cloud security issues, including botnets with the tools described above. Be sure to utilize:

Antivirus solutions

Regular comprehensive data backups

Employee training on safe browsing and downloading habits

Advanced web application firewalls

Constant activity monitoring

Other Risks:-

Compliance

Loss of data

Data storage

Business continuity

Uptime

Data integrity in cloud computing

5. Before going for a cloud computing platform what are the essential things to be taken in concern by users?

Ans: <https://whitehatsme.com/factors-consider-when-moving-to-cloud>

6. What are the disadvantages of virtualization?

Ans:- 1. It can have a high cost of implementation.

The cost for the average individual or business when virtualization is being considered will be quite low. For the providers of a virtualization environment, however, the implementation costs can be quite high. Hardware and software are required at some point and that means devices must either be developed, manufactured, or purchased for implementation.

2. It still has limitations.

Not every application or server is going to work within an environment of virtualization. That means an individual or corporation may require a hybrid system to function properly. This still saves time and money in the long run, but since not every vendor supports virtualization and some may stop supporting it after initially starting it, there is always a level of uncertainty when fully implementing this type of system.

3. It creates a security risk.

Information is our modern currency. If you have it, you can make money. If you don't have it, you'll be ignored. Because data is crucial to the success of a business, it is targeted frequently. The average cost of a data security breach in 2017, according to a report published by the Ponemon Institute, was \$3.62 million. For perspective: the chances of being struck by lightning are about 1 in a million. The chances of experiencing a data breach while using virtualization? 1 in 4.

4. It creates an availability issue.

The primary concern that many have with virtualization is what will happen to their work should their assets not be available. If an organization cannot connect to their data for an extended period of time, they will struggle to compete in their industry. And, since availability is controlled by third-party providers, the ability to stay connected is not in one's control with virtualization.

5. It creates a scalability issue.

Although you can grow a business or opportunity quickly because of virtualization, you may not be able to become as large as you'd like. You may also be required to be larger than you want to be when first starting out. Because many entities share the same resources, growth creates lag within a virtualization network. One large presence can take resources away from several smaller businesses and there would be nothing anyone could do about it.

6. It requires several links in a chain that must work together cohesively.

If you have local equipment, then you are in full control of what you can do. With virtualization, you lose that control because several links must work together to perform the same task. Let's use the example of saving a document file. With a local storage device, like a flash drive or HDD, you can save the file immediately and even create a backup. Using virtualization, your ISP connection would need to be valid. Your LAN or Wi-Fi would need to be working. Your

online storage option would need to be available. If any of those are not working, then you're not saving that file.

7. It takes time.

Although you save time during the implementation phases of virtualization, it costs users time over the long-run when compared to local systems. That is because there are extra steps that must be followed to generate the desired result.

7. What is IaaS? Explain its advantages and disadvantages.

Ans: •Infrastructure as a Service (IaaS) – It contains the basic building blocks for cloud IT and provide access to networking features, computers (virtual or physical) and storage space. It provides highest level of flexibility and management control over IT resources.

•Ex -Amazon Web Services, offers IaaS through the Elastic Compute Cloud or EC2.

Advantages of IaaS cloud computing layer

There are the following advantages of IaaS computing layer -

1. Shared infrastructure

IaaS allows multiple users to share the same physical infrastructure.

2. Web access to the resources

IaaS allows IT users to access resources over the internet.

3. Pay-as-per-use model

IaaS providers provide services based on the pay-as-per-use basis. The users are required to pay for what they have used.

4. Focus on the core business

IaaS providers focus on the organization's core business rather than on IT infrastructure.

5. On-demand scalability

On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about upgrading software and troubleshooting issues related to hardware components.

Disadvantages of IaaS cloud computing layer

1. Security

Security is one of the biggest issues in IaaS. Most of the IaaS providers are not able to provide 100% security.

2. Maintenance & Upgrade

Although IaaS service providers maintain the software, they do not upgrade the software for some organizations.

3. Interoperability issues

It is difficult to migrate VM from one IaaS provider to the other, so the customers might face problems related to vendor lock-in.

7. Write short notes on :
Google Cloud platform.
Amazon Web Service

Ans: Amazon Web Services (AWS)

AWS (Amazon Web Services) is a secure cloud service platform provided by Amazon. It offers various services such as database storage, computing power, content delivery, Relational Database, Simple Email, Simple Queue, and other functionality to increase the organization's growth.

Features of AWS

AWS provides various powerful features for building scalable, cost-effective, enterprise applications. Some important features of AWS is given below-

AWS is scalable because it has an ability to scale the computing resources up or down according to the organization's demand.

AWS is cost-effective as it works on a pay-as-you-go pricing model.

It provides various flexible storage options.

It offers various security services such as infrastructure security, data encryption, monitoring & logging, identity & access control, penetration testing, and DDoS attacks.

It can efficiently manage and secure Windows workloads.

AWS Compute Services

Here, are Cloud Compute Services offered by Amazon:

1. EC2 (Elastic Compute Cloud) - EC2 is a virtual machine in the cloud on which you have OS level control. You can run this cloud server whenever you want.

2. LightSail - This cloud computing tool automatically deploys and manages the computer, storage, and networking capabilities required to run your applications.

3. Elastic Beanstalk — The tool offers automated deployment and provisioning of resources like a highly scalable production website.

4. EKS (Elastic Container Service for Kubernetes) — The tool allows you to Kubernetes on Amazon cloud environment without installation.

5. AWS Lambda — This AWS service allows you to run functions in the cloud. The tool is a big cost saver for you as you to pay only when your functions execute.

Migration

Migration services used to transfer data physically between your datacenter and AWS.

1. DMS (Database Migration Service) - DMS service can be used to migrate on-site databases to AWS. It helps you to migrate from one type of database to another — for example, Oracle to MySQL.

2. SMS (Server Migration Service) - SMS migration services allows you to migrate on-site servers to AWS easily and quickly.

3. Snowball — Snowball is a small application which allows you to transfer terabytes of data inside and outside of AWS environment.

Storage

1. Amazon Glacier- It is an extremely low-cost storage service. It offers secure and fast storage for data archiving and backup.
2. Amazon Elastic Block Store (EBS)- It provides block-level storage to use with Amazon EC2 instances. Amazon Elastic Block Store volumes are network-attached and remain independent from the life of an instance.
3. AWS Storage Gateway- This AWS service is connecting on-premises software applications with cloud-based storage. It offers secure integration between the company's on-premises and AWS's storage infrastructure.

Security Services

1. IAM (Identity and Access Management) — IAM is a secure cloud security service which helps you to manage users, assign policies, form groups to manage multiple users.
2. Inspector — It is an agent that you can install on your virtual machines, which reports any security vulnerabilities.
3. Certificate Manager — The service offers free SSL certificates for your domains that are managed by Route53.
4. WAF (Web Application Firewall) — WAF security service offers application-level protection and allows you to block SQL injection and helps you to block cross-site scripting attacks.
5. Cloud Directory — This service allows you to create flexible, cloud-native directories for managing hierarchies of data along multiple dimensions.
6. KMS (Key Management Service) — It is a managed service. This security service helps you to create and control the encryption keys which allows you to encrypt your data.
7. Organizations — You can create groups of AWS accounts using this service to manages security and automation settings.
8. Shield — Shield is managed DDoS (Distributed Denial of Service protection service). It offers safeguards against web applications running on AWS.
9. Macie — It offers a data visibility security service which helps classify and protect your sensitive critical content.
10. GuardDuty — It offers threat detection to protect your AWS accounts and workloads.

Database Services

1. Amazon RDS- This Database AWS service is easy to set up, operate, and scale a relational database in the cloud.
2. Amazon DynamoDB- It is a fast, fully managed NoSQL database service. It is a simple service which allow cost-effective storage and retrieval of data. It also allows you to serve any level of request traffic.
3. Amazon ElastiCache- It is a web service which makes it easy to deploy, operate, and scale an in-memory cache in the cloud.
4. Neptune- It is a fast, reliable and scalable graph database service.
5. Amazon RedShift - It is Amazon's data warehousing solution which you can use to perform complex OLAP queries.

Analytics

1. Athena — This analytics service allows perm SQL queries on your S3 bucket to find files.
2. CloudSearch — You should use this AWS service to create a fully managed search engine for your website.

3.ElasticSearch — It is similar to CloudSearch. However, it offers more features like application monitoring.

4.Kinesis — This AWS analytics service helps you to stream and analyzing real-time data at massive scale.

5.QuickSight —It is a business analytics tool. It helps you to create visualizations in a dashboard for data in Amazon Web Services. For example, S3, DynamoDB, etc.

6.EMR (Elastic Map Reduce) —This AWS analytics service mainly used for big data processing like Spark, Splunk, Hadoop, etc.

7.Data Pipeline — Allows you to move data from one place to another. For example from DynamoDB to S3.

Management Services

1.CloudWatch — Cloud watch helps you to monitor AWS environments like EC2, RDS instances, and CPU utilization. It also triggers alarms depends on various metrics.

2.CloudFormation — It is a way of turning infrastructure into the cloud. You can use templates for providing a whole production environment in minutes.

3.CloudTrail — It offers an easy method of auditing AWS resources. It helps you to log all changes.

4.OpsWorks — The service allows you to automated Chef/Puppet deployments on AWS environment.

5.Config — This AWS service monitors your environment. The tool sends alerts about changes when you break certain defined configurations.

6.Service Catalog — This service helps large enterprises to authorize which services user will be used and which won't.

7.AWS Auto Scaling — The service allows you to automatically scale your resources up and down based on given CloudWatch metrics.

8.Systems Manager — This AWS service allows you to group your resources. It allows you to identify issues and act on them.

9.Managed Services—It offers management of your AWS infrastructure which allows you to focus on your applications.

Internet of Things

1.IoT Core— It is a managed cloud AWS service. The service allows connected devices like cars, light bulbs, sensor grids, to securely interact with cloud applications and other devices.

2.IoT Device Management — It allows you to manage your IoT devices at any scale.

3.IoT Analytics — This AWS IOT service is helpful to perform analysis on data collected by your IoT devices.

4.Amazon FreeRTOS — This real-time operating system for microcontrollers helps you to connect IoT devices in the local server or into the cloud.

Application Services

1.Step Functions — It is a way of visualizing what's going inside your application and what different microservices it is using.

2.SWF (Simple Workflow Service) — The service helps you to coordinate both automated tasks and human-led tasks.

3.SNS (Simple Notification Service) — You can use this service to send you notifications in the form of email and SMS based on given AWS services.

4.SQS (Simple Queue Service) — Use this AWS service to decouple your applications. It is a pull-based service.

5.Elastic Transcoder — This AWS service tool helps you to changes a video's format and resolution to support various devices like tablets, smartphones, and laptops of different resolutions.

Deployment and Management

1.AWS CloudTrail: The services records AWS API calls and send backlog files to you.

2.Amazon CloudWatch: The tools monitor AWS resources like Amazon EC2 and Amazon RDS DB Instances. It also allows you to monitor custom metrics created by user's applications and services.

3.AWS CloudHSM: This AWS service helps you meet corporate, regulatory, and contractual, compliance requirements for maintaining data security by using the Hardware Security Module(HSM) appliances inside the AWS environment.

Developer Tools

1.CodeStar — Codestar is a cloud-based service for creating, managing, and working with various software development projects on AWS.

2.CodeCommit — It is AWS's version control service which allows you to store your code and other assets privately in the cloud.

3.CodeBuild — This Amazon developer service help you to automates the process of building and compiling your code.

4.CodeDeploy — It is a way of deploying your code in EC2 instances automatically.

5.CodePipeline — It helps you create a deployment pipeline like testing, building, testing, authentication, deployment on development and production environments.

6.Cloud9 —It is an Integrated Development Environment for writing, running, and debugging code in the cloud.

Mobile Services

1.Mobile Hub — Allows you to add, configure and design features for mobile apps.

2.Cognito — Allows users to signup using his or her social identity.

3.Device Farm — Device farm helps you to improve the quality of apps by quickly testing hundreds of mobile devices.

4.AWS AppSync —It is a fully managed GraphQL service that offers real-time data synchronization and offline programming features.

Business Productivity

1.Alexa for Business — It empowers your organization with voice, using Alexa. It will help you to Allows you to build custom voice skills for your organization.

2.Chime — Can be used for online meeting and video conferencing.

3.WorkDocs — Helps to store documents in the cloud

4.WorkMail — Allows you to send and receive business emails.

Desktop & App Streaming

1.WorkSpaces — Workspace is a VDI (Virtual Desktop Infrastructure). It allows you to use remote desktops in the cloud.

2.AppStream — A way of streaming desktop applications to your users in the web browser. For example, using MS Word in Google Chrome.

Artificial Intelligence

1. Lex — Lex tool helps you to build chatbots quickly.
2. Polly — It is AWS's text-to-speech service allows you to create audio versions of your notes.
3. Rekognition — It is AWS's face recognition service. This AWS service helps you to recognize faces and object in images and videos.
4. SageMaker — Sagemaker allows you to build, train, and deploy machine learning models at any scale.
5. Transcribe — It is AWS's speech-to-text service that offers high-quality and affordable transcriptions.
6. Translate — It is a very similar tool to Google Translate which allows you to translate text in one language to another.

AR & VR (Augmented Reality & Virtual Reality)

1. Sumerian — Sumerian is a set of tool for offering high-quality virtual reality (VR) experiences on the web. The service allows you to create interactive 3D scenes and publish it as a website for users to access.

Customer Engagement

1. Amazon Connect — Amazon Connect allows you to create your customer care center in the cloud.
2. Pinpoint — Pinpoint helps you to understand your users and engage with them.
3. SES (Simple Email Service) — Helps you to send bulk emails to your customers at a relatively cost-effective price.

Game Development

1. GameLift- It is a service which is managed by AWS. You can use this service to host dedicated game servers. It allows you to scale seamlessly without taking your game offline.

Applications of AWS services

Amazon Web services are widely used for various computing purposes like:

Web site hosting

Application hosting/SaaS hosting

Media Sharing (Image/ Video)

Mobile and Social Applications

Content delivery and Media Distribution

Storage, backup, and disaster recovery

Development and test environments

Academic Computing

Search Engines

Social Networking

Companies using AWS

Instagram

Zoopla

Smugmug

Pinterest

Netflix

Dropbox

Etsy

Talkbox

Playfish

Ftopia

Advantages of AWS

Following are the pros of using AWS services:

AWS allows organizations to use the already familiar programming models, operating systems, databases, and architectures.

It is a cost-effective service that allows you to pay only for what you use, without any up-front or long-term commitments.

You will not require to spend money on running and maintaining data centers.

Offers fast deployments

You can easily add or remove capacity.

You are allowed cloud access quickly with limitless capacity.

Total Cost of Ownership is very low compared to any private/dedicated servers.

Offers Centralized Billing and management

Offers Hybrid Capabilities

Allows you to deploy your application in multiple regions around the world with just a few clicks

Disadvantages of AWS

If you need more immediate or intensive assistance, you'll have to opt for paid support packages.

Amazon Web Services may have some common cloud computing issues when you move to a cloud. For example, downtime, limited control, and backup protection.

AWS sets default limits on resources which differ from region to region. These resources consist of images, volumes, and snapshots.

Hardware-level changes happen to your application which may not offer the best performance and usage of your applications.

Best practices of AWS

You need to design for failure, but nothing will fail.

It's important to decouple all your components before using AWS services.

You need to keep dynamic data closer to compute and static data closer to the user.

It's important to know security and performance tradeoffs.

Pay for computing capacity by the hourly payment method.

Make a habit of a one-time payment for each instance you want to reserve and to receive a significant discount on the hourly charge.

Next

3. Google Cloud Platform

Google cloud platform is a product of Google. It consists of a set of physical devices, such as computers, hard disk drives, and virtual machines. It also helps organizations to simplify the migration process.

Features of Google Cloud

Google cloud includes various big data services such as Google BigQuery, Google CloudDataproc, Google CloudDatalab, and Google Cloud Pub/Sub.

It provides various services related to networking, including Google Virtual Private Cloud (VPC), Content Delivery Network, Google Cloud Load Balancing, Google Cloud Interconnect, and Google Cloud DNS.

It offers various scalable and high-performance

GCP provides various serverless services such as Messaging, Data Warehouse, Database, Compute, Storage, Data Processing, and Machine learning (ML)

It provides a free cloud shell environment with Boost Mode.

Compute Services

Google App Engine: Platform as a Service to deploy Java, PHP, and other applications. It is a Cloud Computing platform for developing and hosting web applications in Google-managed data centers. It offers the automatic scaling feature, i.e., as the number of requests for an application increases, the App Engine automatically allocates more resources for the application to handle additional demand.

Compute Engine: Infrastructure as a Service to run Microsoft Windows and Linux virtual machines. It is a component of the Google Cloud platform which is built on the same infrastructure that runs Google's search engine, YouTube, and other services.

Kubernetes Engine: It aims at providing a platform for automating deployment, scaling, and operations of application containers across clusters of hosts. It works with a wide range of container tools including docker.

Storage Services

Google Cloud Storage: An online file storage web service for storing and accessing data on a Google Cloud platform infrastructure. The service combines the performance and scalability of Google Cloud with advanced security and sharing capabilities.

Cloud SQL: A web service that allows you to create, configure, and use relational databases that live in Google Cloud. It maintains, manages, and administers your databases allowing you to focus on your applications and services.

Cloud Bigtable: A fast, fully managed, and a highly scalable NoSQL database service. It is designed for the collection and retention of data from 1 TB to hundreds of PB.

Networking

VPC: Virtual Private Cloud provides a private network with IP allocation, routing, and network firewall policies to create a secure environment for your deployments.

Cloud Load Balancing: It is a process of distributing workloads across multiple computing resources. This reduces the cost and maximizes the availability of the resources.

Content Delivery Network: A geographically distributed network of proxy servers and their data centers. The goal here is to provide high availability and high performance by spatially distributing the service relating to end users.

Big Data

BigQuery: Google BigQuery Service is a fully managed data analysis service that enables businesses to analyse Big Data. It features highly scalable data storage, the ability to perform ad-hoc queries, and the ability to share data insights via the web.

Google Cloud Datastore: A fully managed, schema less, non-relational datastore. It supports atomic transactions and a rich set of query capabilities and can automatically scale up and down depending on the load.

Google Cloud Dataproc: A fast, easy-to-use and manage Spark and Hadoop service for distributed data processing. With Cloud Dataproc, you can create Spark or Hadoop clusters, sized for your workloads precisely when you need them.

Cloud AI

Cloud Machine Learning Engine: A managed service that will enable you to build Machine Learning models based on mainstream frameworks.

Cloud AutoML: A Machine Learning product that enables developers to provide their data sets and obtain access to quality trained models by Google's transfer learning and Neural Architecture Search.

Management Tools

Google Stackdriver: Provides performance and diagnostics data in the form of monitoring, logging, tracing, error reporting, and alerting it to public cloud users.

Google Cloud Console App: A native mobile application that enables customers to manage the key Google Cloud services. It provides monitoring, altering, and the ability to take actions on resources.

Identity and Security

Cloud Data Loss Prevention API: It helps you manage sensitive data. It provides a fast and scalable classification for sensitive data elements like credit card numbers, names, passport numbers, and more.

Cloud IAM: Cloud Identity and Access Management refers to a framework of policies and technologies for ensuring that proper people in an enterprise have the appropriate access to technology resources. It is also called identity management (IdM).

Check out Intellipaat's GCP Training Course to get ahead in your career!

IoT

Cloud IoT Core: It is a fully managed service that allows you to easily and securely connect, manage, and ingest data from devices that are connected to the Internet. It permits utilization of other Google Cloud services for collecting, processing, analysing, and visualizing IoT data in real time.

Cloud IoT Edge: Edge computing brings memory and computing power closer to the location where it is needed.

Top Users of Google Cloud

Now that we are well aware of the Google Cloud benefits and services, let's now have a look on the top users of this cloud platform.

Twitter: A well-known application, which lets people share information. With people tweeting more and more every day, the data produced is enormously large. Google Cloud is used for storing and computing purpose.

20th Century Fox: Data scientists at 20th Century Fox and Google Cloud have developed a Machine Learning software that can analyse movie trailers and predict how likely people are to see those movies in theaters.

PayPal: PayPal partners with Google Cloud to increase security, build a faster network, and develop services for its customers.

eBay: eBay uses Google Cloud to innovate in image search, improve customer experiences in China, and train translation models.

Chevron: Chevron uses Google AutoML Vision to find information that is always challenging to get when you need it.

HSBC: HSBC brings a new level of security, compliance, and governance to its banks using Google Cloud.

LG CNS: LG CNS data analytics solution, with Google AI and Edge TPU, will provide a great value for LG CNS customers in the smart factory arena.

8.What pros and cons of Cloud computing in comparisons of Distributed Grid computing?

Ans:

Cloud Computing	Distributed Grid Computing
Resources are on-demand.	Resources are pre-reserved.
Rapid elasticity.	Not rapid elasticity.
Client-server architecture.	Distributed architecture.
Used for business and public needs.	Used for specific purposes.
Clouds evolve faster than grid.	Grids evolve slower than cloud.
Level of expertise to use a cloud is lower than grid.	Level of expertise to use a grid is higher than cloud.
Cloud offers more services than grid computing.	It is the base concept of cloud computing
A cloud would usually use cloud or part of a grid.In fact almost all services on the Internet can be obtained from cloud.	Grids tends to be more loosely coupled,heterogeneous, and geographically dispersed compared to conventional cluster computing systems

Pros of Cloud Computing

Disaster Recovery

With many services offering options such as regular backups and snapshots, important data loss is highly unlikely.

Increased Collaboration and Flexibility

Moving to the cloud increases opportunities for collaboration amongst employees. Colleagues can sync documents workflows or share apps with ease. Often these apps will allow collaborators to simultaneously receive updates in real time. Additionally, cloud computing

allows for each team member to work from anywhere, at any time. The cloud centralizes data, meaning that business owners, employees, and clients can access company data from anywhere that has Internet access (this is often referred to as “tunneling-in”, via some sort of Remote Desktop Protocol).

Eco Friendly

Cloud computing can decrease a business’ carbon footprint, reducing energy consumption and carbon emissions by more than 30%. For small companies, the decreased energy usage can reach 90%! It can also help a business project an environmentally sound image.

Cons of Cloud Computing

Internet Connectivity

Running business applications in the cloud is great, as long as a consistent Internet connection is maintained. If a cloud-based service provider loses connectivity, there’s not much to be done until that Internet connection returns. Even the best servers go down occasionally. Because of this, most cloud providers maintain several redundancies to ensure up time. It is important when selecting a cloud provider, to review their SLA.

Learning Curve

Cloud computing platforms are great tools for developers, but for newcomers to the industry, it might not be as simple as it seems. For those unfamiliar with Linux, SSH Key Generation, and other ins-and-outs of basic server administration, cloud computing platforms that deploy virtual machines or dedicated VPS (Virtual Private Servers) may seem much more different than what is anticipated.

Pros and Cons of Grid Computing

Pros of Grid Computing

Cheaper Servers

No need to buy large SMP servers! Applications would be able to break apart and run across smaller servers. Those servers cost far less than SMP servers.

More Efficient

Much more efficient use of idle resources. Idle servers and desktops would be able to accept jobs! Many resources sit idle, especially during off business hours. This is not the case anymore with a grid computing setup.

Fail-safe

Grid computer environments are modular and don’t have just one fail point. Hence if one of the machines within the grid fails, there are plenty of others able to pick the load. Jobs can automatically restart if a failure occurs.

Cons of Grid Computing

May Still Require Large SMP

Will be forced to run on a large SMP for memory hungry applications that can’t take advantage of MPI

Requires Fast Interconnect

You may need to have a fast interconnect between compute resources (gigabit ethernet at a minimum). Infiniband for MPI intense applications

Some Applications Require Customization

Applications would need tweaking to take full advantage of new models.

Licensing

Licensing across many servers may make it prohibitive for some apps.

Advantages and Benefits of Distributed Computing

Scalability and Modular Growth

Distributed systems are inherently scalable as they work across different machines and scale horizontally. This means a user can add another machine to handle the increasing workload instead of having to update a single system over and over again. There is virtually no cap on how much a user can scale. A system under high demand can run each machine to its full capacity and take machines offline when workload is low.

Fault Tolerance and Redundancy

Distributed systems are also inherently more fault tolerant than single machines. A business running a cluster of 8 machines across two data centers means its apps would work even if one data center goes offline. This translates into more reliability as in case of a single machine everything goes down with it. Distributed systems stay put even if one or more nodes/sites stop working (performance demand on the remaining nodes would go up).

Low Latency

Since users can have a node in multiple geographical locations, distributed systems allow the traffic to hit a node that's closest, resulting in low latency and better performance. However, the software also has to be designed for running on multiple nodes at the same time, which can result in higher cost and more complexity.

Cost Effectiveness

Distributed systems are much more cost effective compared to very large centralized systems. Their initial cost is higher than standalone systems, but only up to a certain point after which they are more about economies of scale. A distributed system made up of many mini computers can be more cost effective than a mainframe machine.

Efficiency

Distributed systems allow breaking complex problems/data into smaller pieces and have multiple computers work on them in parallel, which can help cut down on the time needed to solve/compute those problems.

Disadvantages of Distributed Computing

Complexity

Distributed computing systems are more difficult to deploy, maintain and troubleshoot/debug than their centralized counterparts. The increased complexity is not only limited to the hardware as distributed systems also need software capable of handling the security and communications.

Higher Initial Cost

The deployment cost of a distribution is higher than a single system. Increased processing overhead due to additional computation and exchange of information also adds up to the overall cost.

Security Concerns

Data access can be controlled fairly easily in a centralized computing system, but it's not an easy job to manage security of distributed systems. Not only the network itself has to be secured, users also need to control replicated data across multiple locations.

9.What are different types of distributed computing systems before cloud computing?

Ans: Types of Distributed Computing before Cloud Computing:-

Grid computing

Cluster computing

Grid computing is based on the idea of a supercomputer with enormous computing power. However, computing tasks are performed by many instances rather than just one. Servers and computers can thus perform different tasks independently of one another. Grid computing can access resources in a very flexible manner when performing tasks. Normally, participants will allocate specific resources to an entire project at night when the technical infrastructure tends to be less heavily used.

One advantage of this is that highly powerful systems can be quickly used and the computing power can be scaled as needed. There is no need to replace or upgrade an expensive supercomputer with another pricey one to improve performance.

Since grid computing can create a virtual supercomputer from a cluster of loosely interconnected computers, it is specialized in solving problems that are particularly computationally intensive. This method is often used for ambitious scientific projects and decrypting cryptographic codes.

Cluster computing cannot be clearly differentiated from cloud and grid computing. It is a more general approach and refers to all the ways in which individual computers and their computing power can be combined together in clusters. Examples of this include server clusters, clusters in big data and in cloud environments, database clusters, and application clusters. Computer networks are also increasingly being used in high-performance computing which can solve particularly demanding computing problems.

10.What are the advantages of "Software as a Service" (SaaS)? Explain with example

Ans:

SaaS offers many potential advantages over the traditional models of business software installation, including:

Lower up-front cost - SaaS is generally subscription-based and has no up-front licence fees resulting in lower initial costs. The SaaS provider manages the IT infrastructure that is running the software, which brings down fees for hardware and software maintenance.

Quick set up and deployment - SaaS application is already installed and configured in the cloud. This minimises common delays resulting from often lengthy traditional software deployment.

Easy upgrades - The SaaS providers deal with hardware and software updates, deploying upgrades centrally to the hosted applications and removing this workload and responsibility from you.

Accessibility - All you need to access a SaaS application is a browser and an internet connection. This is generally available on a wide range of devices and from anywhere in the world, making SaaS more accessible than the traditional business software installation.

Scalability - SaaS providers generally offer many subscription options and flexibility to change subscriptions as and when needed, eg when your business grows, or more users need to access the service.

If you're considering moving your ecommerce business to the Cloud, here are three important acronyms to wrap your head around:

IaaS.

PaaS.

SaaS.

These are the three main types of cloud computing.

You've probably heard of them before; they're all experiencing a surge in popularity as more businesses move to the Cloud.

SaaS accounts for approximately 24% of all enterprise workloads (up from 14% in 2016)

IaaS is hovering around 12% (up from 6%).

PaaS is currently the most popular model, hovering around 32% and expected to grow in 2020.

With uptake rates like these, cloud computing is becoming the norm, and many businesses are phasing out on-premise software altogether.

The Key Differences Between On-Premise, SaaS, PaaS, IaaS

Not so long ago, all of a company's IT systems were on-premise, and clouds were just white fluffy things in the sky.

Now, you can utilize the Cloud platform for nearly all your systems and processes.

SaaS, PaaS, and IaaS are simply three ways to describe how you can use the cloud for your business.

IaaS: cloud-based services, pay-as-you-go for services such as storage, networking, and virtualization.

PaaS: hardware and software tools available over the internet.

SaaS: software that's available via a third-party over the internet.

On-premise: software that's installed in the same building as your business.

Here's a great visual breakdown from Hosting Advice:

Examples of SaaS, PaaS, and IaaS

Most businesses use a combination of SaaS and IaaS cloud computing service models, and many engage developers to create applications using PaaS, too.

SaaS examples: BigCommerce, Google Apps, Salesforce, Dropbox, MailChimp, ZenDesk, DocuSign, Slack, Hubspot.

PaaS examples: AWS Elastic Beanstalk, Heroku, Windows Azure (mostly used as PaaS), Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud.

IaaS examples: AWS EC2, Rackspace, Google Compute Engine (GCE), Digital Ocean, Magento 1 Enterprise Edition*.

11.How many types of deployment models are used in cloud? Which one is best and why?

Ans: The different deployment models which are used:-

Private Cloud: Cloud services are used by a single organization, so only the organization has access to its data and can manage it.

Public Cloud:Cloud services are accessible via a network like internet and can be used by multiple clients. MS Azure, AWS are some of the examples of public cloud hosting.

Hybrid Cloud:Cloud services are distributed among public and private clouds. Its users can use them as per their requirement i.e.private as well as public cloud services in day to day operations.

A comparison: Private cloud vs Public cloud vs Hybrid cloud

Comparing Cloud Deployment models	Public cloud	Private cloud	Hybrid Cloud
Cloud environment	Multi-Tenancy-Shared environment. Single tenancy-only for single use of an organization.	Both single tenancy and multi –tenancy. When data is stored in the public cloud, it delivers multi- tenant environment meaning the data from multiple organizations is stored in a shared environment whereas when data is stored in private cloud, it is kept private for the use of a single organization.	
Data center location	Anywhere – where the cloud service provider’s services are located.	Inside the organization’s network.	Inside the organization’s network for private cloud services as well as wherever service provider’s services are there for public cloud services.
Resource sharing	Server hardware, network and storage are shared by multiple users in the cloud. No sharing of resources. Hardware, storage and network are dedicated to the use of a single client or company.	Very secure; integration options add an additional layer of security.	
Cloud storage	Public cloud delivers storage as a service on a pay per use basis. Best for backups as a part of a disaster recovery plan as well as archiving email and static non-core application data. OneDrive is an example of public cloud storage.	Private cloud delivers internal cloud storage that runs on a dedicated infrastructure in a data center.	Hybrid cloud manages streamlined storage that uses both local and off-site resources and serves as a gateway between on premise and public cloud storage.
Scalability	Instant and unlimited. Sacrifices scalability but provides greater control and security.	On demand unlimited resources.	
Pricing structure	Prices charged on the usage basis. Comparatively expensive. High but delivers competitive advantage.		
Cloud Security	Good, but depends on the security measures of the service provider.	Most secure.	
Performance	Low to medium.	Very High.	Very High.

Cloud Deployment Models Comparison

There are many things to take into consideration when selecting a cloud deployment model that is right for your company. The table below summarizes each of them, including the various advantages and disadvantages discussed above. Hopefully, this will help you narrow down your selection.

Cloud Deployment Type Summary AdvantagesDisadvantages

Public Cloud It offers companies the ability to consume highly available and scalable services hosted on shared infrastructure, on-demand, maintenance free, at a low cost. This allows companies to grow at scale, while avoiding high up-front capital investments and operational costs. Cloud providers own and operate data centers and are responsible for all management and maintenance of almost infinitely scalable services and platforms. Companies can avoid expenses associated with purchase, management and maintenance of on-premises hardware and focus on deploying and running applications. Operates under a shared responsibility model. Meaning, the provider is responsible for the “security of the cloud” and customers are responsible for “security in the cloud” (applications they deploy and configuration of services they leverage). Misconfigurations are typically the root cause of vulnerabilities and the reason why public clouds are perceived as less secure.

Private Cloud When running a private cloud on-premises, companies have more visibility and control over the physical security controls and data storage. However, these come at the expense of substantial upfront capital expenditure and operating costs. Third party hosted private clouds potentially alleviate these, as companies will not be required to make upfront capital expenses for hardware, nor need to have on-site personnel to run and maintain the hardware. Can be configured to specific requirements needed to run proprietary applications, allows for more direct control of data and integration between public and private clouds allows for extending computing resources to maintain application uptime. Substantial capital investment associated with underutilized purchased hardware or upfront cost associated with third-party hosted hardware. May not scale effectively when demand is in flux, costing more long-term.

Hybrid Cloud All of the benefits of both public and private cloud, but potentially an aggregate of the disadvantages associated with them, too. Companies can still apply specific custom requirements for critical environments and rely on the near infinite scalability of a public cloud provider; thus reducing cost in general. However, this is only possible if a company has the ability to run and manage a complex environment. Companies have increased control over their data, allowing stakeholders to choose environments for each use case. Extending workloads to a public cloud allows for the ability to scale resources on-demand, in a cost effective manner. Lack of tools to manage both on-premise and public cloud resources, creating operational complexity long term.

Multi-Cloud A multi-cloud deployment model is all about choices. It provides companies with more options, making it easier for them to invest in the cloud without fear of single-provider vendor lock-in. Solutions that are cloud provider agnostic could potentially benefit a company financially, as it would be easier to migrate their workloads to a different provider that offers better pricing. This helps reduce vendor lock-in and improve reliability. This is most applicable to companies running containerized workloads. Can be perceived as complex when attempting to leverage traditional tools for governance and compliance. Example, a company’s asset management solution may not be able to provide integration with multiple cloud providers, making it difficult to create a single source of truth of all assets.

How to Choose a Cloud Deployment Model

Bottom line, each company will have to evaluate its own list of unique requirements before they can decide on the best cloud deployment model for them. It is important to point out that they don't have to compromise and choose a single model. There are many companies out there that leverage a combination of models in order to derive different kinds of benefits. These companies tend to have something in common—they're using containers and container tools like Kubernetes.

12.What is AWS? What types of Services does it provide?

Ans: same as question number 7 part 2 (AWS)

13.Describe the architecture of windows Azure.

Ans: The Windows Azure platform is a cloud computing platform supporting the development and deployment of Windows applications that provide services to both businesses and consumers. These applications can be created using the .NET framework in languages such as C# and Visual Basic, or they can be built without the NET framework in C++, Java, PHP, Ruby and Python. Windows Azure is originally a PaaS platform but since November 2010 it is also possible to deploy virtual machine (VM) images of Windows Server (2008), which is a form of IaaS. Notice that Windows Azure provides not necessarily an execution environment for all supported languages. For example, Java APIs are available for the different Azure services, but the developer has to install a JVM and an application server in an Azure VM himself.

The Windows Azure platform is a group of cloud technologies, each providing a specific set of services to application developers.

– Windows Azure: A Windows environment for running applications (Compute) and storing data (Storage) in the cloud. A Windows Azure application can be created using three kinds of compute service types, called roles: (i) a Web role for running web-based applications, (ii) a Worker role for (background) processing, and (iii) a VM role to run VM images. An application is structured as any combination of role instances. Web and worker role instances consist of a Windows Server 2008 R2 VM with the .NET 4.0 framework pre-installed. In a web role, there is also an IIS web server available.

The storage service consists of blob storage (coarse-grained, unstructured data), table storage (set of entities with properties, NoSQL), and queues (asynchronous communication between different roles). All data is accessible via a REST API and the OData query language for tables. The Fabric Controller makes abstraction of the underlying infrastructure and offers a pool of processing power to the compute and storage services.

– SQL Azure: A cloud-based service for relational data, built on Microsoft SQL Server.

Comparing PaaS offerings in light of SaaS development.

– Windows Azure AppFabric: A middleware platform on top of Windows Azure that provides a higher level of abstraction and reduces the complexity of cloud development. The AppFabric Container provides a new programming model and runtime for cloud application development using .NET core language. The AppFabric Container itself is not publicly available and therefore not further discussed in this paper, but Microsoft offers several AppFabric Services on top of this container, for example caching. Recently, the AppFabric Services are renamed to Windows Azure Features.

The Windows Azure platform provides an environment that strongly corresponds to a traditional on-premise setup (cf. Category 1), this especially applies to the Windows Azure Compute service and SQL Azure. In this comparison we focus on Windows Azure using traditional .NET frameworks in the C# programming language and the Ninject dependency injection framework. We also include SQL Azure into the comparison. The case study application is implemented using Azure SDKs 1.2 - 1.6.

14. What is SaaS in cloud computing? Explain the different categories of SaaS.

Ans: Software as a Service (SaaS) – It provides a complete product that is run and managed by the service provider. One need not to worry about how the service is maintained or how the underlying infrastructure is managed.

Ex – Microsoft offering is Office 365, which offers online versions of programs, including Word, Excel, PowerPoint, OneDrive, Outlook, and SharePoint.

Categories:-

The SaaS maturity model is broken down into four levels, and each of them brings certain opportunities and challenges you should be aware of when accessing SaaS vendors.

Level 1 (Single-Tenant, Custom Instances)

At this level of the SaaS maturity model, the only way to support multiple customers (tenants) is to provide each of them a separate copy of the software. Because the provided copies can be customized by writing custom code, each customer is required to run a different instance of the software and scalability is non-existent, even though the software is technically delivered as a service. As such, no economies of scale can be harnessed, making this level the least cost-effective and sustainable when managing a larger number of customers.

Level 2 (Single-Tenant, Configurable Instances)

At level 2, software can be customized by changing its configuration instead of writing custom code. In other words, all tenants interact with the same code configured in different ways, with each tenant running their own copy on a separate virtual or physical machine. Consequently,

scalability and multi-tenancy are still not achieved. What's more, the provider is at a competitive disadvantage because individual instances don't share the same pool of computing power, which would make it possible to achieve economies of scale.

Level 3 (Multi-Tenant, Configurable)

The third level of the SaaS maturity model can be described as being almost the perfect case because it includes both configurability and multi-tenancy, allowing each tenant to quickly and efficiently customize the same shared instance through a self-service tool. The only thing missing is scalability because software can be scaled up only by moving it to a more powerful server, which isn't cost-effective. Still, the inefficient need for server space to accommodate many instances is eliminated and costs can be greatly reduced compared with level 2 of the SaaS maturity model.

Level 4 (Multi-Tenant Configurable & Scalable)

Level 4 is the highest level of the SaaS maturity model. It combines the configurability and multi-tenancy of level 3 with scalability, making it possible to transparently add new software instances to the dynamic pool of instances with the help of a load balancer, whose job is to maximize the utilization of storage, processing power and other resources. Each tenant's data is stored separately, and a virtually infinite number of tenants can be seamlessly accommodated by adjusting the number of servers on the backend to meet the current demand.

If you are planning to make long-term investments in enterprise SaaS applications, think about those investments from a licensing, architecture, security and configuration standpoint. The SaaS maturity model reflects the scalability, multi-tenant efficiency and configurability upon which the licensing and delivery model is built. There are advantages and disadvantages to every model, so be sure to really think it through to figure out if multi-tenancy is necessary for a given business, domain or product.

15. Why is virtualization important? Describe the characteristics of server virtualization and application virtualization.

Ans: same as question number 20

16. What is Service-Level Agreement (SLA)? Explain about the security controls classified in cloud computing.

Ans: A cloud SLA (cloud service-level agreement) is an agreement between a cloud service provider (IaaS, PaaS, SaaS) and a customer (Cloud consumer) that ensures a minimum level of service is maintained.

It guarantees levels of reliability, availability and responsiveness to systems and applications; specifies who governs when there is a service interruption; and describes penalties if service levels are not met.

Service Level Agreements usually specify some parameters which are mentioned below:

- 1.Availability of the Service (uptime)
- 2.Latency or the response time
- 3.Service components reliability
- 4.Each party accountability
- 5.Warranties

Cloud security control primarily helps in addressing, evaluating and implementing security in the cloud. The Cloud Security Alliance (CSA) has created a Cloud Control Matrix (CCM), which is designed to help prospective cloud buyers evaluate a cloud solution's overall security. Although there are limitless cloud security controls, they are similar to the standard information security controls and can be categorized in different domains including:

Deterrent Controls: Don't protect the cloud architecture/infrastructure/environment but serve as warning to a potential perpetrator of an attack.

Preventative Controls: Used for managing, strengthening and protecting the vulnerabilities within a cloud.

Corrective Controls: Help reduce the after-effects of an attack.

Detective Controls: Used to identify or detect an attack.

17.Explain the cloud deployment models in detail. Also, outline their advantages and disadvantages while implementing an application.

Ans: **Private cloud** – It allows systems and services to be accessible within an organization.

- offers higher security.
- managed by the organization or a 3rd party
- Located on or off premise
- Ex - SBI has built own private cloud

Community cloud - It allows systems and services to be accessible by a group of organizations.

- several orgs that have shared concerns
- managed by organization or a 3rd party
- Ex -CityCloud

Public cloud – It allows systems and services to be accessible by the general public.

- A Public Cloud is a huge data centre that offers the same services to all its users.
- It offers lesser security.

- Mega scale infrastructure
- Globally distributed
- Ex -Amazon EC2, Gmail
- Hybrid cloud** - It is a mixture of public and private cloud. The critical activities are performed by private cloud and the non- critical activities are performed by public cloud.
- Ex -Cybercon's Hybrid Cloud Hosting Service.

Advantages of Public Cloud

Benefits of the public cloud include:

Low cost: Public cloud is the cheapest model on the market. Besides the small initial fee, clients only pay for the services they are using, so there is no unnecessary overhead.

No hardware investment: Service providers fund the entire infrastructure.

No infrastructure management: A client does not need a dedicated in-house team to make full use of a public cloud.

Disadvantages of Public Cloud

The public cloud does have some drawbacks:

Security and privacy concerns: As anyone can ask for access, this model does not offer ideal protection against attacks. The size of public clouds also leads to vulnerabilities.

Reliability: Public clouds are prone to outages and malfunctions.

Poor customization: Public offerings have little to no customization. Clients can pick the operating system and the sizing of the VM (storage and processors), but they cannot customize ordering, reporting, or networking.

Limited resources: Public clouds have incredible computing power, but you share the resources with other tenants. There is always a cap on how much resources you can use, leading to scalability issues.

Advantages of Private Cloud

Here are the main reasons why organizations are using a private cloud:

Customization: Companies get to customize their solution per their requirements.

Data privacy: Only authorized internal personnel can access data. Ideal for storing corporate data.

Security: A company can separate sets of resources on the same infrastructure. Segmentation leads to high levels of security and access control.

Full control: The owner controls the service integrations, IT operations, rules, and user practices. The organization is the exclusive owner.

Legacy systems: This model supports legacy applications that cannot function on a public cloud.

Disadvantages of Private Cloud

High cost: The main disadvantage of private cloud is its high cost. You need to invest in hardware and software, plus set aside resources for in-house staff and training.

Fixed scalability: Scalability depends on your choice of the underlying hardware.

High maintenance: Since a private cloud is managed in-house, it requires high maintenance.

Advantages of Community Cloud

Here are the benefits of a community cloud solution:

Cost reductions: A community cloud is cheaper than a private one, yet it offers comparable performance. Multiple companies share the bill, which additionally lowers the cost of these solutions.

Setup benefits: Configuration and protocols within a community system meet the needs of a specific industry. A collaborative space also allows clients to enhance efficiency.

Disadvantages of Community Cloud

The main disadvantages of community cloud are:

Shared resources: Limited storage and bandwidth capacity are common problems within community systems.

Still uncommon: This is the latest deployment model of cloud computing. The trend is still catching on, so the community cloud is currently not an option in every industry.

Advantages of Hybrid Cloud

Here are the benefits of a hybrid cloud system:

Cost-effectiveness: A hybrid solution lowers operational costs by using a public cloud for most workflows.

Security: It is easier to protect a hybrid cloud from attackers due to segmented storage and workflows.

Flexibility: This cloud model offers high levels of setup flexibility. Clients can create custom-made solutions that fit their needs entirely.

Disadvantages of Hybrid Cloud

The disadvantages of hybrid solutions are:

Complexity: A hybrid cloud is complex to set up and manage as you combine two or more different cloud service models.

Specific use case: A hybrid cloud makes sense only if an organization has versatile use cases or need to separate sensitive and non-sensitive data.

How to Choose Between Cloud Deployment Models

To choose the best cloud deployment model for your company, start by defining your requirements for:

Scalability: Is your user activity growing? Does your system run into sudden spikes in demand?

Ease of use: How skilled is your team? How much time and money are you willing to invest in staff training?

Privacy: Are there strict privacy rules surrounding the data you collect?

Security: Do you store any sensitive data that does not belong on a public server?

Cost: How much resources can you spend on your cloud solution? How much capital can you pay upfront?

Flexibility: How flexible (or rigid) are your computing, processing, and storage needs?

Compliance: Are there any notable laws or regulations in your country or industry? Do you need to adhere to compliance standards?

18.What is a middleware? How does it help to achieve compatibility between different software involved in cloud computing?

Ans: Middleware is software which lies between an operating system and the applications running on it. Essentially functioning as a hidden translation layer, middleware enables communication and data management for distributed applications. It is sometimes called plumbing, as it connects two applications together so data and databases can be easily passed between the “pipe.” Using middleware allows users to perform such requests as submitting forms on a web browser or allowing the web server to return dynamic web pages based on a user’s profile.

Middleware helps developers build applications more efficiently. It acts like the connective tissue between applications, data, and users. For organizations with multi-cloud and containerized environments, middleware can make it cost-effective to develop and run applications at scale.

Middleware can help developers transform legacy monolithic applications into cloud-native applications, keeping valuable tools active with better performance and more portability

For all the benefits cloud-native development provides, it also brings added complexity. Applications can be deployed across multiple infrastructures, from on-premises systems to public clouds. Architectures can vary widely. Developers are juggling multiple tools, languages, and frameworks. And the pressure is on to do more in less time and at a lower cost.

Organizations turn to middleware as a way to manage this complexity and to keep application development quick and cost-effective. Middleware can support application environments that work smoothly and consistently across a highly distributed platform.

19.Design the architecture of PaaS and SaaS in cloud computing? Also, explain the different categories of PaaS and SaaS with example.

Ans: To help you make sense of this complicated world, SaaS can be divided into three categories:

Packaged software: This is the biggest area of the SaaS market. Packaged software comes in many different flavors: customer relationship management, supply chain management, financial management, and human resources, to name the most common.

These integrated offers focus on a specific process, such as managing employees' benefits, salaries, and annual performance reviews. These products tend to have several characteristics in common: They're designed with specific business processes built in that customers can modify. They have moved in great numbers to the cloud because customers were finding the platforms too hard to manage.

Collaborative software: This increasingly vibrant area of the market is driven by the ubiquitous availability of the Internet, combined with the fact that teams are located all over the world. This area is dominated by software that focuses on all sorts of collaborative efforts including Web conferencing, document collaboration, project planning, instant messaging, and even email. In a sense, it was inevitable that these platforms would move to the cloud: These tasks occur throughout the organization and need to be easily accessed from many locations.

Enabling and management tools: What's in this category? Think about the development tools that developers need when creating and extending a SaaS platform; also think about the testing, monitoring, and measuring that a customer and the developer need. Also consider the compliance issues related to the use of this type of software in the real world. These issues are included in this third category.

PaaS Types :

Various sorts of PaaS are presently accessible to engineers. They are :

1. Public PaaS 2. Private PaaS 3. Hybrid PaaS 4. Communication PaaS 5. Mobile PaaS 6. Open PaaS

These are explained as follows below.

1. Public PaaS –

Is appropriate for use in public clouds. Public PaaS permits clients to control programming extension, while cloud supplier deals with circulation of all other key IT segments expected to have applications, including working frameworks, databases, workers, and capacity framework systems.

Public dice merchants offer middleware, which permits engineers to introduce, design, and control workers and databases without the need to introduce a framework. Therefore, Public Pass and Infrastructure (IaaS) run all together. PaaS with exercises on merchant's IaaS foundation using public cloud. Tragically, this implies clients will adhere to similar public cloud choices that they would prefer not to utilize.

Some small and medium-sized organizations have received public PaaS, however huge enterprises and associations wouldn't acknowledge it because of their cozy relationship with the public cloud. This is principally a consequence of an enormous number of guidelines and consistency issues on organization application advancement in the public cloud.

2.Private PaaS –

Plans to give dexterity of public pass while keeping up security, consistency, advantages and ease of private security community. A private pass is normally circulated as gadget or programming in a client's firewall, which is regularly kept up in a server farm on an organization's premises. A private PaaS can be created on a framework and works inside an organization's particular private cloud.

Private dice permit an association to all more likely serve designers, improve inside asset usage, and decrease expensive cloud entrance that numerous organizations face. Likewise, private dice permit designers to run and deal with their organization's applications in consistency with severe security and protection necessities.

3.Hybrid PaaS –

Consolidates organizations with Public PaaS and Private PaaS, with accommodation of unbounded limits offered by Public PaaS and cost-adequacy of having inside framework in Private PaaS. Hybrid PaaS utilizes hybrid cloud.

4.Communication PaaS (CPaaS) –

Cloud-based stage that permits engineers to add ongoing communication to their application without requirement for back-end foundation and interfaces. Regularly, ongoing communication happens in applications fabricated explicitly for these assignments. Models are Skype, FaceTime, WhatsApp and conventional telephones.

CPaaS gives a completely evolved system to making ongoing communication highlights without requirement for engineers to assemble their own structure, including standard-based application programming interfaces, programming apparatuses, prebuilt applications, and test code.

CPaaS suppliers help clients in improvement procedures by offering help and item documentation. A few suppliers offer programming advancement packs just as libraries that help assemble applications on different work areas and mobile stages. Improvement groups picking to utilize CPaaS spares time for foundation, HR and market.

5.Mobile PaaS (MPaaS) –

Is an installment incorporated improvement condition for mobile application setup. In MPaaS, coding abilities are not required. MPaaS is circulated through an internet browser and for most part bolsters public cloud, private cloud and on-premises stockpiling. Administration is normally rented at a month to month cost, contingent upon quantity of gadgets and offices bolstered.

MPaaS ordinarily gives an article situated intuitive interface that permits clients to disentangle improvement of HTML5 or local applications through direct access to gadget's highlights, for example, GPS, sensor, camera and amplifier. It frequently underpins different mobile OS.

6. Open PaaS –

Is a free, open-source, business-situated community oriented stage that is alluring on all gadgets and gives a helpful web application including schedule, contacts and mail applications. It is intended to permit clients to immediately run new applications. One of its assets is to create innovation sent for big business synergistic applications, particularly half and half mists.

20. What is virtualization in cloud computing? Outline the characteristics of server virtualization and application virtualization.

Ans: Virtualization is a technique of how to separate a service from the underlying physical delivery of that service. It is the process of creating a virtual version of something like computer hardware. It was initially developed during the mainframe era. It involves using specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource. With the help of Virtualization, multiple operating systems and applications can run on the same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware.

1. Application Virtualization:

Application virtualization helps a user to have remote access to an application from a server. The server stores all personal information and other characteristics of the application but can still run on a local workstation through the internet. Example of this would be a user who needs to run two different versions of the same software. Technologies that use application virtualization are hosted applications and packaged applications.

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.

Advantages of Application Virtualization

No installation required: Installing an application on hundreds or thousands of computers is prone to error. Application virtualization simplifies software deployment.

Application retirement simplified: Getting rid of an app in your whole network is much easier as well. Since virtual apps just have to be deleted, uninstalling them is usually not required.

No more application conflicts: Sometimes installing an app corrupts another app. Application virtualization helps reduce the risks of application conflicts.

No registry and system bloat: The more apps you install on a desktop, the more bloated its registry and system folder will get. This makes the computer slower and increases the risk of failures. Application virtualization lets the registry and the system folder untouched.

Multiple runtime environments: You can deploy the runtime environment together with the application. This enables you to run different versions of a runtime environment on a desktop. For example, you can run different Java versions simultaneously without messing around with environment variables.

Multiple versions of the same application: For instance, end users can run Word 2003 and Word 2007 at the same time.

Deploy apps on unmanaged computers: If clients or partners have to use an app to access the services of your organization, you can just send them an executable where you have already configured everything for them.

Application updates: You can update the virtualized application at a central location on your servers. This means you have to update an app only once and not on all of your desktops.

Rollback: If an app no longer works properly on a user's desktop because he or she changed too many settings or installed incompatible add-ons, you can just reset the app to its original state.

Simplified roaming: Some products allow you to store settings and data belonging to the app in the virtual environment on a server or a memory stick. This way, end users can access their apps with their own settings regardless on which desktop they logon. This is also possible if you are not working with roaming user profiles.

Simplified OS deployment: Deploying a new OS in your network doesn't affect the applications. Also, if you have to reinstall an image on a desktop, you don't have to worry about the apps running on this machine because end users can just access them on the server.

Integration with desktop virtualization: Software virtualization and desktop virtualization perfectly harmonize because these technologies allow you to separate the OS deployment process from software distribution.

Reduced regression testing: Once you know that your app works in the virtual environment, you don't have to make sure that it works on all of the different desktop variations in your network. Changes on desktops usually don't have an effect on the virtualized apps.

Improved security: Virtualized apps are isolated from the operating system and from each other. This way, malware can't infect other parts of the system, easily.

Helpdesk support: Helpdesk personnel can easily access all available apps in your organization and can run the app in the same environment as end users.

Operating system independent: Virtualized apps are often OS independent. If you have apps that are Vista incompatible, then application virtualization might be your solution. Application virtualization also paves the way for Vista x64. Legacy apps that wouldn't work on a

64-bit-system might run without problems on Vista x64 in a virtual environment. Together with Wine and Crossover, you can also run complex Windows apps on Linux and OS X. End users require only minimal privileges: Legacy apps that require admin rights usually work in environments where end-users only have standard rights.

2. Server Virtualization:

Server virtualization is a technology for partitioning one physical server into multiple virtual servers. Each of these virtual servers can run its own operating system and applications, and perform as if it is an individual server. This makes it possible, for example, to complete development using various operating systems on one physical server or to consolidate servers used by multiple business divisions.

Among the various virtualization methods available, NEC primarily focuses on virtualization software solutions. Because the virtualization software, or hypervisor, used by NEC runs directly on bare hardware (physical servers), our virtualized environments have little overhead. NEC's proven, reliable solutions are built upon years of experience with virtualization.

In addition to server virtualization solutions, NEC provides virtual desktop solutions.

Server virtualization features

All the virtualization software provided by NEC have the following features.

Benefits

Benefits

Primary advantages of server virtualization

Reduce number of servers

Partitioning and isolation, the characteristics of server virtualization, enable simple and safe server consolidation.

Through consolidating, the number of physical servers can be greatly reduced. This alone brings benefits such as reduced floor space, power consumption and air conditioning costs. However, it is essential to note that even though the number of physical servers is greatly reduced, the number of virtual servers to be managed does not change. Therefore, when virtualizing servers, installation of operation management tools for efficient server management is recommended.

Reduce TCO

Server consolidation with virtualization reduces costs of hardware, maintenance, power, and air conditioning. In addition, it lowers the Total Cost of Ownership (TCO) by increasing the efficiency of server resources and operational changes, as well as virtualization-specific features. As a result of today's improved server CPU performance, a few servers have high resource-usage rates but most are often underutilized. Virtualization can eliminate such ineffective use of CPU resources, plus optimize resources throughout the server environment. Furthermore, because servers managed by each business division's staff can be centrally managed by a single administrator, operation management costs can be greatly reduced.

Improve availability and business continuity

One beneficial feature of virtualized servers not available in physical server environments is live migration. With live migration, virtual servers can be migrated to another physical server for tasks such as performing maintenance on the physical servers without shutting them down. Thus there is no impact on the end user. Another great advantage of virtualization technology is that its encapsulation and hardware-independence features enhance availability and business continuity.

Increase efficiency for development and test environments

At system development sites, servers are often used inefficiently. When different physical servers are used by each business division's development team, the number of servers can easily increase. Conversely, when physical servers are shared by teams, reconfiguring development and test environments can be time and labor consuming.

Such issues can be resolved by using server virtualization to simultaneously run various operating system environments on one physical server, thereby enabling concurrent development and testing of multiple environments. In addition, because development and test environments can be encapsulated and saved, reconfiguration is extremely simple.

NEC specific advantages on server virtualization

NEC specific advantages on server virtualization

The impact of a failure in a physical server can increase after virtualizing and consolidating servers. To prevent such problems, NEC provides ExpressCluster and other products for improving the availability of virtual servers.

21. Discuss the following concepts in the context of cloud computing:

a) Billing and Metering Services

b) Tooling and automation

Ans: Out of Syllabus

22. Draw the framework of common cloud management platform reference architecture and explain its components.

Ans: Same as Q26. Explain about the transactional process between Data Owner, Third Party Auditor and Cloud Service Provider and Application Users.

23. Write different types of internal security breaches in cloud computing. Also, explain the steps to reduce cloud security breaches.

Ans: out of syllabus

24. Discuss, in detail, the cloud security reference model and explain how cloud security is integrated into the design of application.

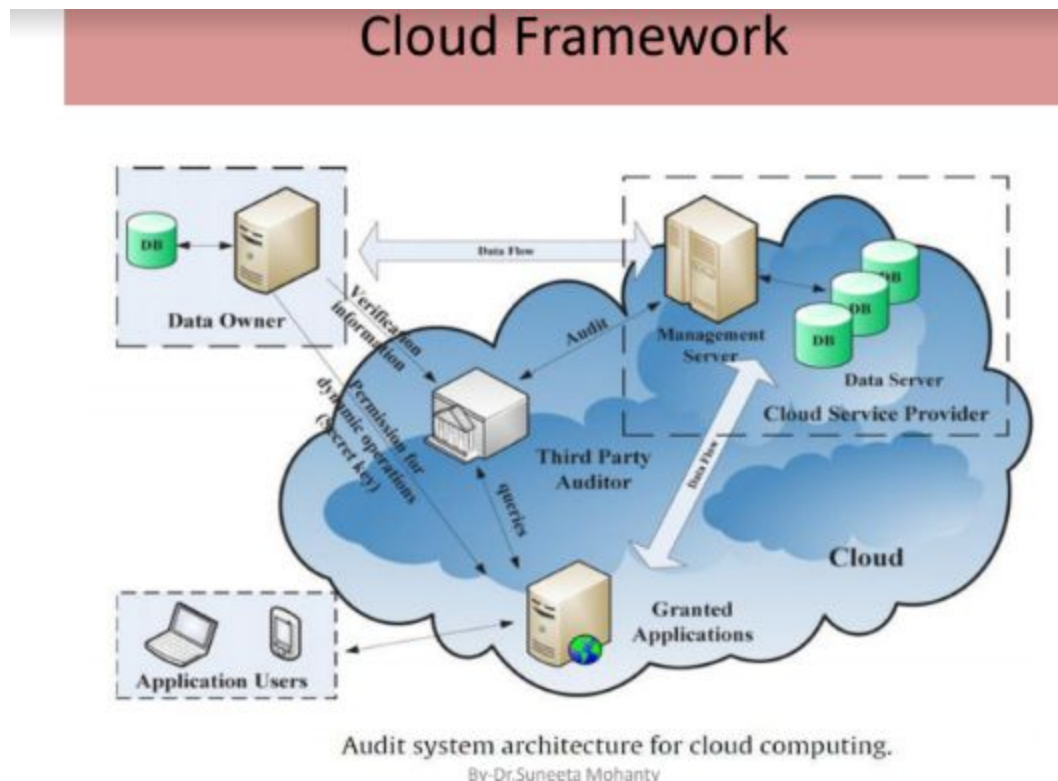
Ans: out of syllabus

25.Explain the cloud deployment models, in detail. Also, outline their benefits and limitations while implementing and applying them.

Ans: same as question number 17

26.Explain cloud computing architecture and its various components with a diagram.

Ans:



27.Discuss the functionality of various components of cloud infrastructure.

Ans: For the end user,CC consists of the following:

- Client-A client is an access device or software interface that a user can use to access cloud services.
- Cloud Network-A network is the connecting link between the user and cloud services. The Internet is the common choice for accessing the cloud.
- Cloud Application Programming Interface (API)- A Cloud API is a set of programming instruction and tool that provides abstractions over a specific cloud provider. API help programmers to have a common mechanism for connecting to a particular cloud service.

28.What are the characteristics in cloud computing.

Ans - Characteristics of cloud computing:-

- i) On demand self services: computer services such as email, applications, network or server service can be provided without requiring human interaction with each service provider. Cloud service providers providing on demand self services include Amazon Web Services (AWS), Microsoft, Google, IBM and Salesforce.com.
- ii) •Broad network access: Cloud Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops and PDAs.
- iii) •Resource pooling: The provider's computing resources are pooled together to serve multiple consumers using multiple-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The resources include among others storage, processing, memory, network bandwidth, virtual machines and email services as mobile phones, laptops and PDAs.
- iv) •Rapid elasticity: Cloud services can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- v) •Measured service: Cloud computing resource usage can be measured, controlled, and reported providing transparency for both the provider and consumer of the utilized service. Cloud computing services use a metering capability which enables to control and optimize resource use. This implies that just like air time, electricity or municipality water IT services are charged per usage metrics – pay per use. The more you utilize the higher the bill.
- vi) •Multi Tenacity: It refers to the need for policy-driven enforcement, segmentation, isolation, governance, service levels, and billing models for different consumer constituencies. Consumers might utilize a public cloud provider's service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities but would still share infrastructure.

29.What are the challenges in cloud computing.

Ans:- Cost :- Cloud computing itself is affordable, but tuning the platform according to the company's needs can be expensive. Furthermore, the expense of transferring the data to public clouds can prove to be a problem for short-lived and small-scale projects.

Scalable and on-demand nature of cloud services makes the assessment of cost difficult. Contracting and budgeting issues arise often with scalable and incremental cloud service procurements. Heavy use of a service for a few days may consume the budget of several months.

Security and Privacy :- The main challenge to cloud computing is how it addresses the security and privacy concerns of businesses thinking of adopting it. The fact that the valuable enterprise data will reside outside the corporate firewall, raises serious concerns. Hacking and various attacks to cloud infrastructure would affect multiple clients even if only one site is attacked. These risks can be mitigated by using security applications, encrypted file systems, data loss software, and buying security hardware to track unusual behaviour across servers.

Interoperability and Portability :- Businesses should have the leverage of migrating in and out of the cloud and switching providers whenever they want, and there should be no lock-in period. Cloud computing services should have the capability to integrate smoothly with the on-premise IT.

Reliability and Availability :- Cloud providers still lack round-the-clock service; this results in frequent outages. It is important to monitor the service being provided using internal or third-party tools. It is vital to have plans to supervise usage, SLAs, performance, robustness, and business dependency of these services.

Performance and Bandwidth :- Businesses can save money on hardware but they have to spend more for the bandwidth. This can be a low cost for smaller applications but can be significantly high for the data-intensive applications. Delivering intensive and complex data over the network requires sufficient bandwidth. Because of this, many businesses are waiting for a reduced cost

before switching to the cloud.

Continuous Monitoring:- Cloud computing often suffers from frequent outages, owing to the lack of round-the-clock service on the part of cloud providers. It is important to monitor the cloud service continuously as well as to supervise its performance, business dependency and robustness.

Vendor lock-in :- Entering a cloud computing agreement is easier than leaving it. “Vendor lock-in” happens when altering providers is either excessively expensive or just not possible. It could be that the service is nonstandard or that there is no viable vendor substitute. It comes down to buyer carefulness. Guarantee the services you involve are typical and transportable to other providers, and above all, understand the requirements.

30.Explain the technologies that work behind the cloud computing platform.

Ans: <https://www.tutorialride.com/cloud-computing/cloud-computing-technologies.htm>

31.Cloud Deployment Model

Ans:- Deployment models define the type of access to the cloud.

This means that deployment types vary depending on who controls the infrastructure and where it's located.

- Private cloud – It allows systems and services to be accessible within an organization. It offers higher security.
- managed by the organization or a 3rd party
- Located on or off premise
- Ex - SBI has built own private cloud
- Community cloud - It allows systems and services to be accessible by group of organizations.
- several orgs that have shared concerns
- managed by organization or a 3rd party
- Ex -CityCloud
- Public cloud – It allows systems and services to be accessible by the general public.
- A Public Cloud is a huge data centre that offers the same services to all its users.
- It offers lesser security.
- Mega scale infrastructure

- Globally distributed
- Ex -Amazon EC2, Gmail
- Hybrid cloud - It is a mixture of public and private cloud. The critical activities are performed by private cloud and the non-critical activities are performed by public cloud.
- Ex -Cybercon's Hybrid Cloud Hosting Service.

32.Discuss the different deployment models of cloud computing.

Ans:- Same as question number 31

33.Discuss various cloud service models and prepare a comparative report of these models with examples.

Ans:- •Infrastructure as a Service (IaaS) – It contains the basic building blocks for cloud IT and provide access to networking features , computers (virtual or physical) and storage space. It provides highest level of flexibility and management control over IT resources.

•Ex -Amazon Web Services, offers IaaS through the Elastic Compute Cloud or EC2.

•Platform as a Service (PaaS) – Such solutions appeal to developers who want to spend more time on coding, testing, and deploying their applications instead of dealing with hardware-oriented tasks such as managing security patches and operating system updates.

•Ex –Microsoft Azure empowers developers to create applications in a variety of languages and frameworks without getting bogged down in infrastructure management.

•Software as a Service (SaaS) – It provides a complete product that is run and managed by the service provider. One need not to worry about how the service is maintained or how the underlying infrastructure is managed.

•Ex –Microsoft offering is Office 365, which offers online versions of programs, including Word, Excel, PowerPoint, OneDrive, Outlook,

and SharePoint.

34. Describe the benefits and drawbacks of the private cloud model.

Ans:- Advantages:-

Controls: Better controls for data, users and information assets.

Security: The cloud belongs to a single client. Hence, the infrastructure and systems can be configured to provide high levels of security.

Superior Performance: Normally private clouds are deployed inside the firewall of the organization's intranet which ensures efficiency and good network performance.

Easy Customization: The hardware and other resources can be customized easily by the company.

Compliance: Compliance is achieved easily in private clouds.

Disadvantages:-

Cost: Costs are substantial in the case of building an on-premise private cloud. The running cost would include personnel cost and periodic hardware upgrade costs. In the case of outsourced private cloud, operating cost will include per resource usage and subject to change at the discretion of the service provider.

Under-utilization: In some instances the resources subscribed can be under-utilized. Hence, optimizing the utilization of all resources is a challenge.

Capacity ceiling: Due to physical hardware limitations with the service provider, there could be a capacity ceiling to handle only a certain amount of servers or storage.

Vendor lock-in: This can be a major impediment in private cloud adoption especially when the hardware and infrastructure is outsourced. This is a service delivery technique where the client company is forced to continue with the same service provider, thus preventing the client to migrate to another vendor.

35. Discuss the benefits and issues of the community cloud model.

Ans:-

<https://www.sectorlink.com/article/pros-and-cons-between-public-private-and-community-cloud>

36. Explain PAAS with its benefits and drawbacks.

Ans:- Platform as a Service (PaaS) – Such solutions appeal to developers who want to spend more

time on coding, testing, and deploying their applications instead of dealing with hardware-oriented tasks such as managing security patches and operating system updates.

- Ex –Microsoft Azure empowers developers to create applications in a variety of languages and frameworks without getting bogged down in infrastructure management.

PaaS provides all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely from the Internet.

- Typically applications must be developed with a particular platform in mind
- Multi tenant environments
- Highly scalable multi tier architecture

Advantages and disadvantages:-

<https://wisdomplexus.com/blogs/advantages-disadvantages-paas/>

37.What is SAAS? Explain its advantages and disadvantages.

Ans:- •Software as a Service (SaaS) – It provides a complete product that is run and managed by the service provider. One need not to worry about how the service is maintained or how the underlying infrastructure is managed.

- Ex –Microsoft offering is Office 365, which offers online versions of programs, including Word, Excel, PowerPoint, OneDrive, Outlook, and SharePoint.

SaaS is a software delivery methodology that provides licensed multi-tenant access to software and its functions remotely as a Web-based service.

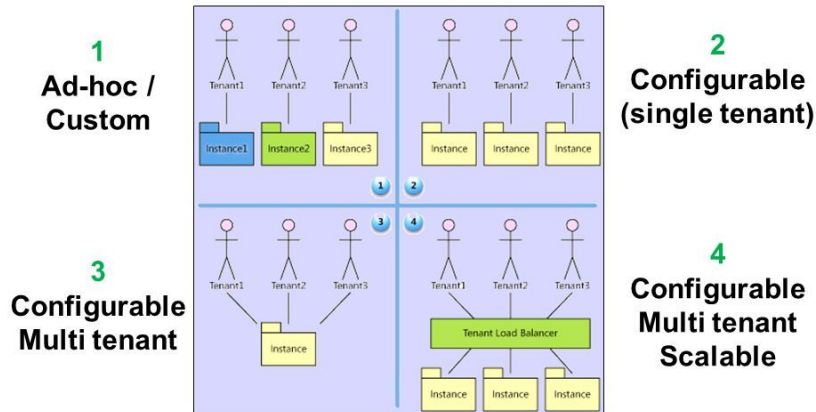
- Usually billed based on usage
- Usually multi tenant environment
- Highly scalable architecture

Advantages and disadvantages:-

<https://www.nibusinessinfo.co.uk/content/advantages-and-disadvantages-software-service-saas>

38.SAAS Maturity Model neat diagram.

“Basic” SaaS Maturity Model



Ans:-

39.Explain the risk from multi-tenancy w.r.t various cloud environments.

Ans:-.Risks in multi tenancy environment:

- Inadequate Logical Security Controls: Physical resources are shared between multiple tenants. That means dependence on logical segregation to ensure that one tenant deliberately cannot interfere with the security of the other tenants.
- Malicious or Ignorant Tenants: If the provider has weaker logical controls between tenants, a malicious or an ignorant tenant may reduce the security posture of other tenants.
- Shared Services can become a single point of failure.
- Performance Risks: One tenant's heavy use of the service may impact the quality of service provided to other tenants.

Uncoordinated Change Controls and Misconfigurations: When multiple tenants are sharing the underlying infrastructure all changes needs to be well coordinated and tested.

40.What is Virtualization? Explain the technique of hardware virtualization.

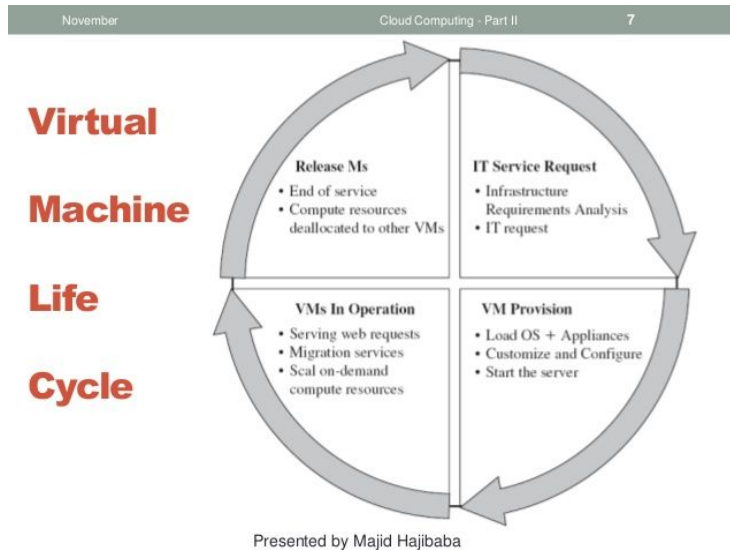
Ans:- Virtualization relies on software to simulate hardware functionality and create a virtual computer system. This enables IT organizations to run more than one virtual system – and multiple operating systems and applications – on a single server. The resulting benefits include economies of scale and greater efficiency.

Hardware Virtualization:- In hardware virtualization, software called hypervisor is used. With the help of a hypervisor virtual machine, software embedded into the hardware component

of the server. The work of hypervisor is that it manages the physical hardware resource which is shared between the customer and the provider.

Hardware virtualization can be done by extracting the physical hardware with the help of the virtual machine monitor (VMM). There are several extensions in the processes, which help to accelerate virtualization activities and boost the performance of hypervisors. If this virtualization is done for a server platform it is known as server socialization.

41.Explain the life cycle of a virtual machine with a suitable diagram.



Ans:-

42.Survey the major features of Google App Engine.

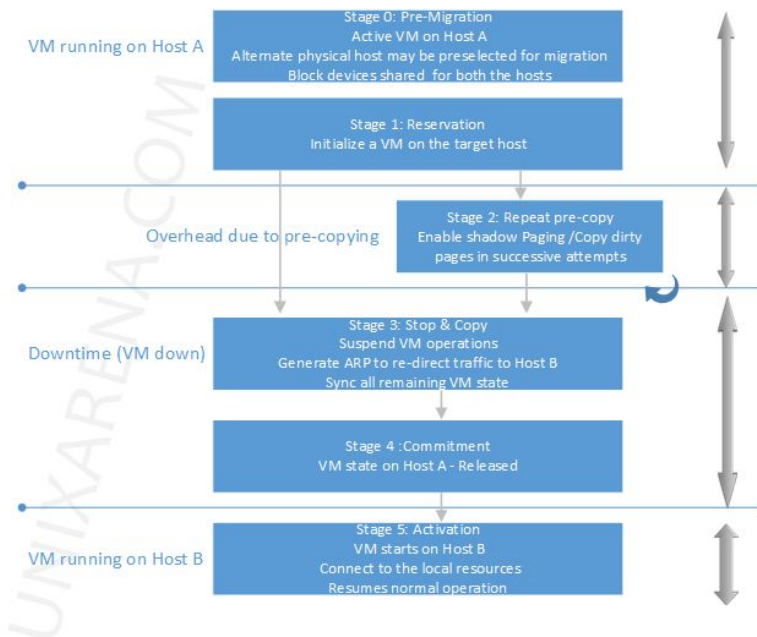
Ans:- https://en.wikipedia.org/wiki/Google_App_Engine

43.Describe the major features of Google App Engine.

Ans:- https://en.wikipedia.org/wiki/Google_App_Engine

44.Identify the stages of live migration of Virtual Machine.

VM Live - Migration Timeline



Ans:-

45.Explain all the necessary stages of live migration of virtual machines.

Ans: same as question number 44

46.Appraise Min-Min scheduling algorithm with suitable examples.

Ans:- Min-min scheduling is based on Minimum Completion Time (MCT) that is used to assign tasks to the resources to have minimum expected completion time. It will work in two Phases. In the first phase, the expected completion time will be calculated for each task in a metatask list. In the second phase, the task with the overall minimum expected completion time from the metatask list is selected and assigned to the corresponding resource. Then this task is removed from the metatask list and the process is repeated until all tasks in the metatask list are mapped to the corresponding resources. However, the Min- min algorithm is unable to balance the load well as it usually does the scheduling of small tasks initially.

47.Explain any two scheduling techniques with suitable examples.

Min-min scheduling is based on Minimum Completion Time (MCT) that is used to assign tasks to the resources to have minimum expected completion time. It will work in two Phases, In the first phase, the expected completion time will be calculated for each task in a metatask list. In the second phase, the task with the overall minimum expected completion time from the metatask list is select and assigned to the corresponding resource. Then this task is removed from metatask list and the process is repeated until all tasks in the metatask list are mapped to

the corresponding resources However, the Min- min algorithm is unable to balance the load well as it usually does the scheduling of small tasks initially

The Max-min algorithm is commonly used in a distributed environment which begins with a set of unscheduled tasks. Then calculate the expected execution matrix and expected completion time of each task on the available resources. Next, choose the task with overall maximum expected completion time and assign it to the resource with minimum overall execution time. Finally recently scheduled task is removed from the metatasks set, update all calculated times, then repeat until meta-tasks set become empty

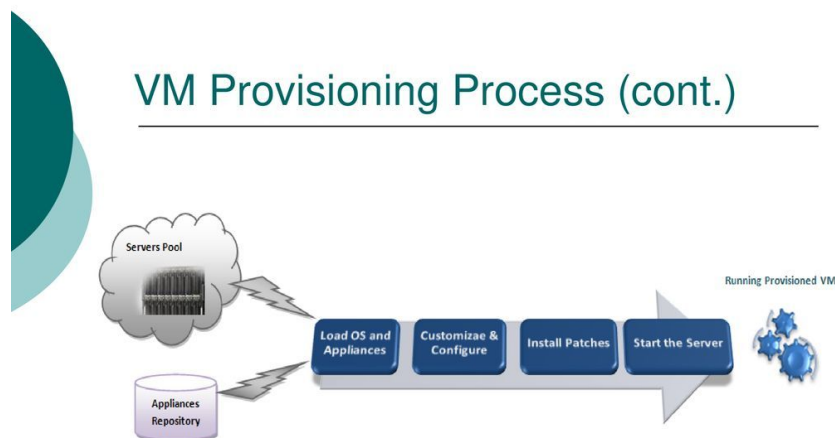
48.Elaborate the Amazon EC2 architecture and its various components.

Ans:-

https://www.tutorialspoint.com/amazon_web_services/amazon_web_services_basic_architecture.htm

49.Appraise the process of VM provisioning with a schematic diagram.

Ans:- Virtual machine provisioning, or virtual server provisioning, is a systems management process that creates a new virtual machine (VM) on a physical host server and allocates computing resources to support the VM. These computing resources typically include CPU cycles (or entire cores) and memory space, but can also involve I/O cycles and storage.



50.What is the concept behind Virtualization? Explain the concept of hardware virtualization in detail with its sub type.

Ans:- Concept:- Virtualization relies on software to simulate hardware functionality and create a virtual computer system. This enables IT organizations to run more than one virtual system – and multiple operating systems and applications – on a single server. The resulting benefits include economies of scale and greater efficiency.

Hardware Virtualization:- In hardware virtualization, software called hypervisor is used. With the help of a hypervisor virtual machine, software embedded into the hardware component of the server. The work of hypervisor is that it manages the physical hardware resource which is shared between the customer and the provider.

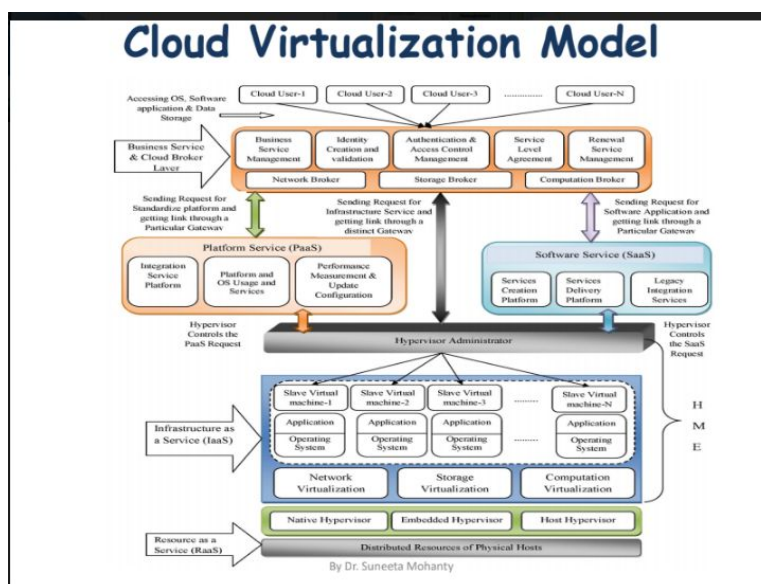
Hardware virtualization can be done by extracting the physical hardware with the help of the virtual machine monitor (VMM). There are several extensions in the processes, which help to accelerate virtualization activities and boost the performance of hypervisors. If this virtualization is done for a server platform it is known as server socialization.

51.Explain the layered virtualization technology architecture with a suitable diagram.

Ans- Virtualization uses software to create an abstraction layer over computer hardware that allows the hardware elements of a single computer—processors, memory, storage and more—to be divided into multiple virtual computers, commonly called virtual machines (VMs). A Virtual Machine is a software implementation of a computing environment where an operating system (OS) or program may be installed and run.

Virtual Machine Monitor (VMM)/ Hypervisor

Virtual Machine Monitor mediates access to the physical hardware presenting to each guest OS a Virtual Machine.



52.Examine the various privacy and security issues of cloud computing.

Ans:- Security and Privacy :- The main challenge to cloud computing is how it addresses the security and privacy concerns of businesses thinking of adopting it. The fact that the valuable enterprise data will reside outside the corporate firewall, raises serious concerns. Hacking and various attacks to cloud infrastructure would affect multiple clients even if only one site is attacked. These risks can be mitigated by using security applications, encrypted file systems, data loss software, and buying security hardware to track unusual behaviour across servers.

Vendor lock-in :- Entering a cloud computing agreement is easier than leaving it. "Vendor lock-in" happens when altering providers is either excessively expensive or just not possible. It could be that the service is nonstandard or that there is no viable vendor substitute. It comes down to buyer carefulness. Guarantee the services you involve are typical and transportable to other providers, and above all, understand the requirements.

Interoperability and Portability :- Businesses should have the leverage of migrating in and out of the cloud and switching providers whenever they want, and there should be no lock-in period. Cloud computing services should have the capability to integrate smoothly with the on-premise IT.

53.Compare and Contrast column oriented and document oriented database.

Ans- A column-oriented DBMS or columnar DBMS is a database management system (DBMS) that stores data tables by column rather than by row. Practical use of a column store versus a row store differs little in the relational DBMS world. Both columnar and row databases can use traditional database query languages like SQL to load data and perform queries. Both row and columnar databases can become the backbone in a system to serve data for common extract, transform, load (ETL) and data visualization tools. However, by storing data in columns rather than rows, the database can more precisely access the data it needs to answer a query rather than scanning and discarding unwanted data in rows.

A document-oriented database, or document store, is a computer program and data storage system designed for storing, retrieving and managing document-oriented information, also known as semi-structured data.

54.Column oriented and document oriented database.

Ans: same as question number 53

55.What is a cloud database? Examine its different classifications based on transaction processing.

Ans:- A cloud database is a database service built and accessed through a cloud platform. It serves many of the same functions as a traditional database with the added flexibility of cloud computing. Users install software on a cloud infrastructure to implement the database.

56.Analyze CAP theorem with necessary explanation.

Ans :- The CAP theorem is called the Brewer's Theorem. It states that a distributed computing environment can only have 2 of the 3: Consistency, Availability and Partition Tolerance – one must be sacrificed.
Consistency implies that every read fetches the last write
Availability implies that reads and writes always succeed. In other words, each non-failing node will return a response in a reasonable amount of time
Partition Tolerance implies that the system will continue to function when network partition occurs.

The CAP theorem categorizes systems into three categories:

CP (Consistent and Partition Tolerant) - a system that is consistent and partition tolerant but never available. CP is referring to a category of systems where availability is sacrificed only in the case of a network partition.

CA (Consistent and Available) - CA systems are consistent and available systems in the absence of any network partition. Often a single node's DB servers are categorized as CA systems. Single node DB servers do not need to deal with partition tolerance and are thus considered CA systems.

AP (Available and Partition Tolerant) - These are systems that are available and partition tolerant but cannot guarantee consistency.

57.Examine the functionalities of mobile cloud computing architecture with schematic diagram.

Ans: same as question number 58

58.Describe the framework of mobile cloud computing architecture with schematic diagram.

Ans:- Mobile Cloud Computing uses computational augmentation approaches (computations are executed remotely instead of on the device) by which resource-constraint mobile devices can utilize computational resources of varied cloud-based resources. In MCC, there are four types of cloud-based resources, namely distant immobile clouds, proximate immobile computing entities, proximate mobile computing entities, and hybrid (combination of the other three models). Giant clouds such as Amazon EC2 are in the distant immobile groups whereas cloudlets or surrogates are members of proximate immobile computing entities. Smartphones, tablets, handheld devices, and wearable computing devices are part of the third group of cloud-based resources which is proximate mobile computing entities.

59.Explain in brief the meaning of Data Integrity, Data confidentiality, Data availability and data privacy.

Ans-. Data Integrity involves maintaining the consistency and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and precautionary steps must be taken to ensure that data cannot be altered by unauthorized people.

Data availability means that information is accessible to authorized users. It provides an assurance that your system and data can be accessed by authenticated users whenever they're needed. Similar to confidentiality and integrity, availability also holds great value.

Confidentiality ensures that data exchanged is not accessible to unauthorized users. The users could be applications, processes, other systems and/or humans. When designing a system, adequate control mechanisms to enforce confidentiality should be in place, as well as policies that dictate what authorized users can and cannot do with the data.

Data privacy or information privacy is a branch of data security concerned with the proper handling of data – consent, notice, and regulatory obligations. More specifically, practical data privacy concerns often revolve around: Whether or how data is shared with third parties.

60.What is a cloud database? Explain SQL based and NoSQL based data model in cloud database.

Ans:- A cloud database is a database service built and accessed through a cloud platform. It serves many of the same functions as a traditional database with the added flexibility of cloud computing. Users install software on a cloud infrastructure to implement the database.

NoSQL, which stands for “not only SQL,” is an approach to database design that provides flexible schemas for the storage and retrieval of data beyond the traditional table structures found in relational databases. While NoSQL databases have existed for many years, NoSQL databases have only recently become more popular in the era of cloud, big data and high-volume web and mobile applications. They are chosen today for their attributes around scale, performance and ease of use. The most common types of NoSQL databases are key-value, document, column and graph databases.

SQL or relational traditional databases. are one type of table based database which can run in the cloud, either in a virtual machine or as a service, depending on the vendor. While SQL databases are easily vertically scalable, horizontal scalability poses a challenge that cloud database services based on SQL have started to address.

61.Explain the risks and security issues that arise in a cloud environment.

Ans:- Security and Privacy :- The main challenge to cloud computing is how it addresses the security and privacy concerns of businesses thinking of adopting it. The fact that the valuable enterprise data will reside outside the corporate firewall, raises serious concerns. Hacking and various attacks to cloud infrastructure would affect multiple clients even if only one site is attacked. These risks can be mitigated by using security applications, encrypted file systems, data loss software, and buying security hardware to track unusual behaviour across servers.

Vendor lock-in :- Entering a cloud computing agreement is easier than leaving it. “Vendor lock-in” happens when altering providers is either excessively expensive or just not possible. It could be that the service is nonstandard or that there is no viable vendor substitute. It comes down to buyer carefulness. Guarantee the services you involve are typical and transportable to other providers, and above all, understand the requirements.

Reliability and Availability :- Cloud providers still lack round-the-clock service; this results in frequent outages. It is important to monitor the service being provided using internal or third-party tools. It is vital to have plans to supervise usage, SLAs, performance, robustness, and business dependency of these services.

Interoperability and Portability :- Businesses should have the leverage of migrating in and out of the cloud and switching providers whenever they want, and there should be no lock-in period. Cloud computing services should have the capability to integrate smoothly with the on-premise IT.