



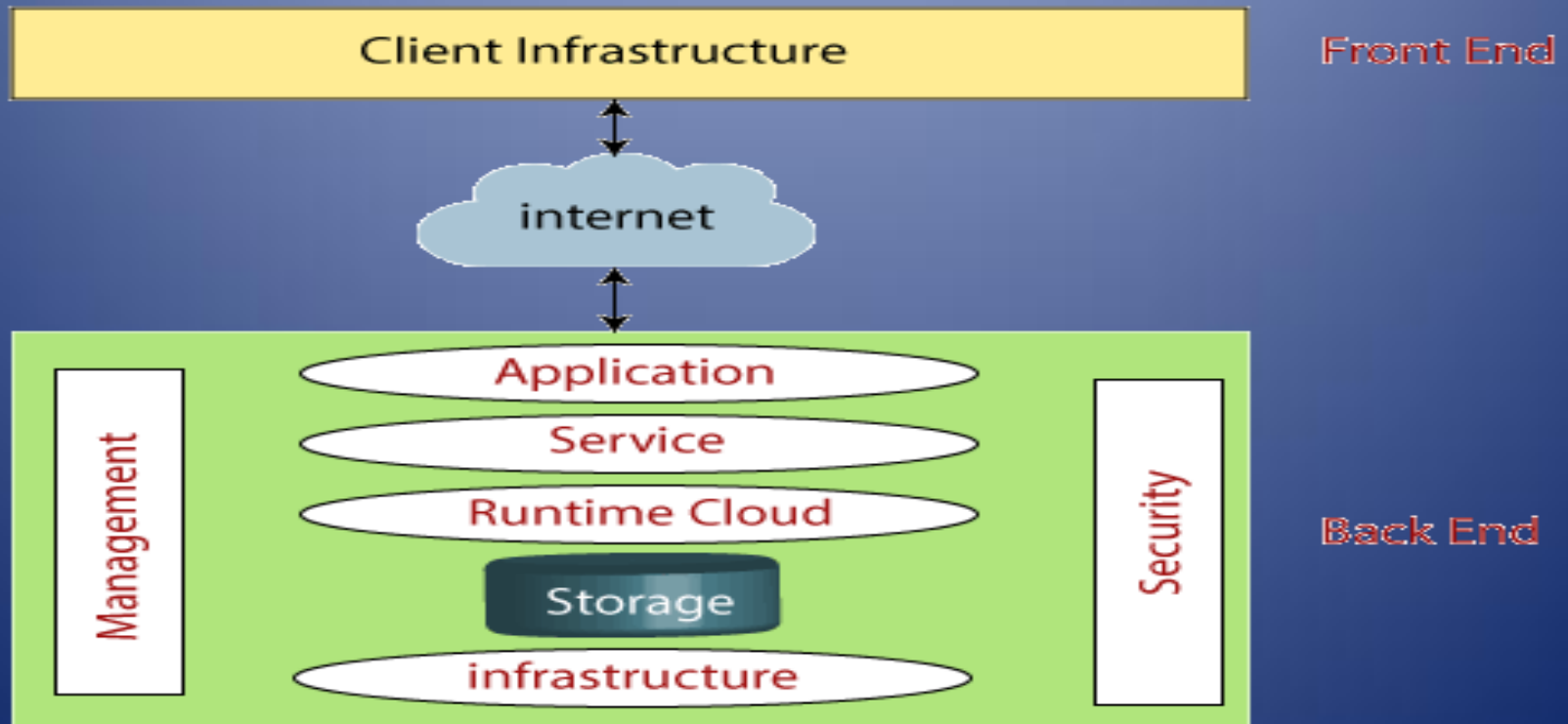
Power Point Presentation On Cloud Computing

**Presented By
Sandhya Vats
Ph.D (Comp Sci &App)
Roll No:20380161003**

Q:1 Explain the architecture of cloud computing in detail.

Cloud computing architecture is a combination of service-oriented architecture and event-driven architecture. Cloud computing architecture is divided into the following two parts –Front End and Back End.

Architecture of Cloud Computing



Components of Cloud Computing Architecture

Front End :-The front end is used by the client. It contains client-side interfaces and applications that are required to access the cloud computing platforms. The front end includes web servers (including Chrome, Firefox, internet explorer, etc.), thin & fat clients, tablets, and mobile devices.

Back End:-The back end is used by the service provider. It manages all the resources that are required to provide cloud computing services. It includes a huge amount of data storage, security mechanism, virtual machines, deploying models, servers, traffic control mechanisms, etc.

Client Infrastructure

Client Infrastructure is a Front end component. It provides GUI (Graphical User Interface) to interact with the cloud.

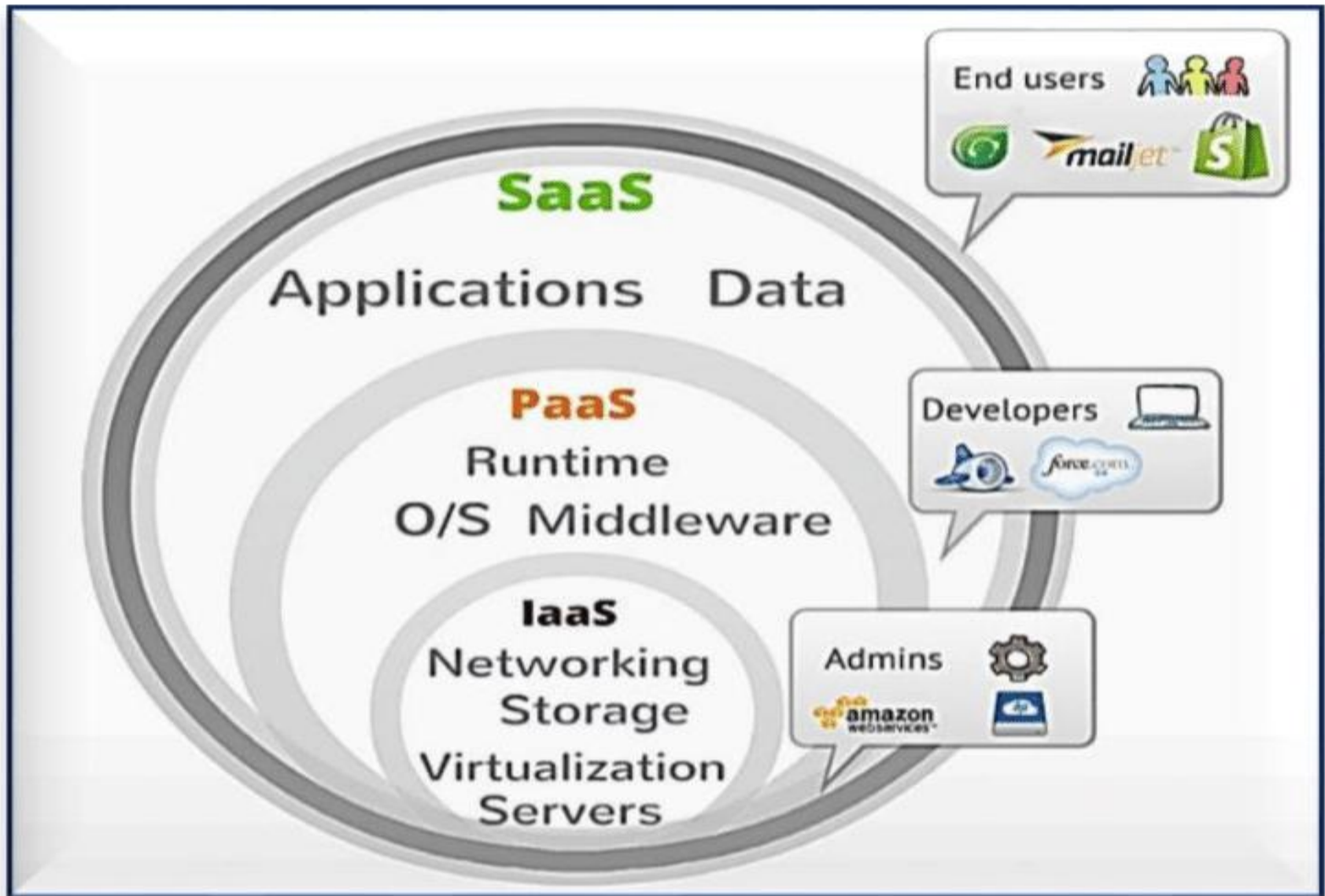
Application

The application may be any software or platform that a client wants to access.

Service

A Cloud Services manages that which type of service you access according to the client's requirement

Diagram of SaaS, PaaS and IaaS



Cloud computing offers three type of services

Software as a Service (SaaS) – It is also known as cloud application services. Mostly, SaaS applications run directly through the web browser means we do not require to download and install these applications.eg Google Apps, Salesforce ,Dropbox , Slack, Hubspot, Cisco WebEx.

Platform as a Service (PaaS) – It is also known as cloud platform services. It is quite similar to SaaS, but the difference is that PaaS provides a platform for software creation, but using SaaS, we can access software over the internet without the need of any platform.eg Windows Azure, Force.com, Magento Commerce Cloud, OpenShift.

Infrastructure as a Service (IaaS) – It is also known as cloud infrastructure services. It is responsible for managing applications data, middleware, and runtime environments.eg Amazon Web Services (AWS) EC2, Google Compute Engine (GCE), Cisco Metapod.

Components of Cloud Computing Architecture

Client Infrastructure

The client infrastructure component is the part of the frontend which provides a graphic user interface for the user to interact with the cloud.

Storage

Storage is one of the most important components of cloud computing. It provides a huge amount of storage capacity in the cloud to store and manage data.

Infrastructure

It provides services on the host level, application level, and network level. Cloud infrastructure includes hardware and software components such as servers, storage, network devices, virtualization software, and other storage resources that are needed to support the cloud computing model.

Components of Cloud Computing Architecture

Runtime Cloud

Runtime Cloud provides the execution and runtime environment to the virtual machines

Management

Management is used to manage components such as application, service, runtime cloud, storage, infrastructure, and other security issues in the backend and establish coordination between them.

Security

Security is an in-built back end component of cloud computing. It implements a security mechanism in the back end.`

Internet

The Internet is medium through which front end and back end can interact and communicate with each other.

Q:2 Explain the concept of cloud computing with its benefits, characteristics, advantages & disadvantages.

Cloud computing is the delivery of computing services including servers, storage, databases, networking, software, analytics, and intelligence over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale.

Benefits of cloud computing

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

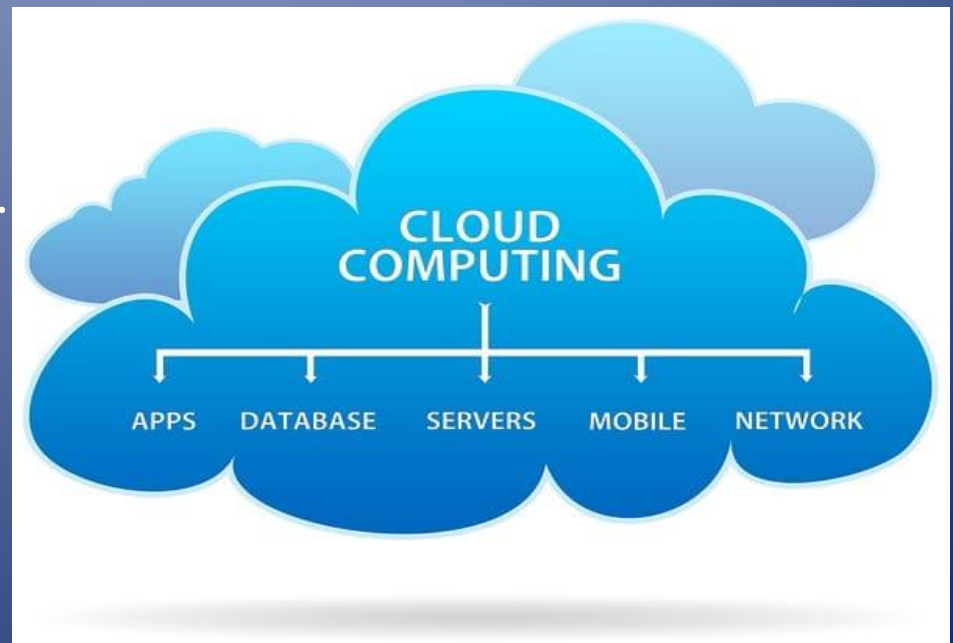
Scalability. ...

Business continuity. ...

Collaboration efficiency. ...

Flexibility of work practices. ...

Access to automatic updates. .



Essential Characteristics of Cloud Computing

On-demand self-service.

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access.

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling.

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. (e.g., country, state, or datacenter)

Rapid elasticity.

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand..

Advantages of Cloud Computing

1.Back-up and restore data

Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud

2.Improved collaboration

Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.

3.Excellent accessibility

Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection.

4.Low maintenance cost

Cloud computing reduces both hardware and software maintenance costs for organizations.

5.Mobility

Cloud computing allows us to easily access all cloud data via mobile.

Disadvantages of Cloud Computing

1. Internet Connectivity

As you know, in cloud computing, every data (image, audio, video, etc.) is stored on the cloud, and we access these data through the cloud by using the internet connection.

2. Vendor lock-in

Vendor lock-in is the biggest disadvantage of cloud computing. Organizations may face problems when transferring their services from one vendor to another

3. Limited Control

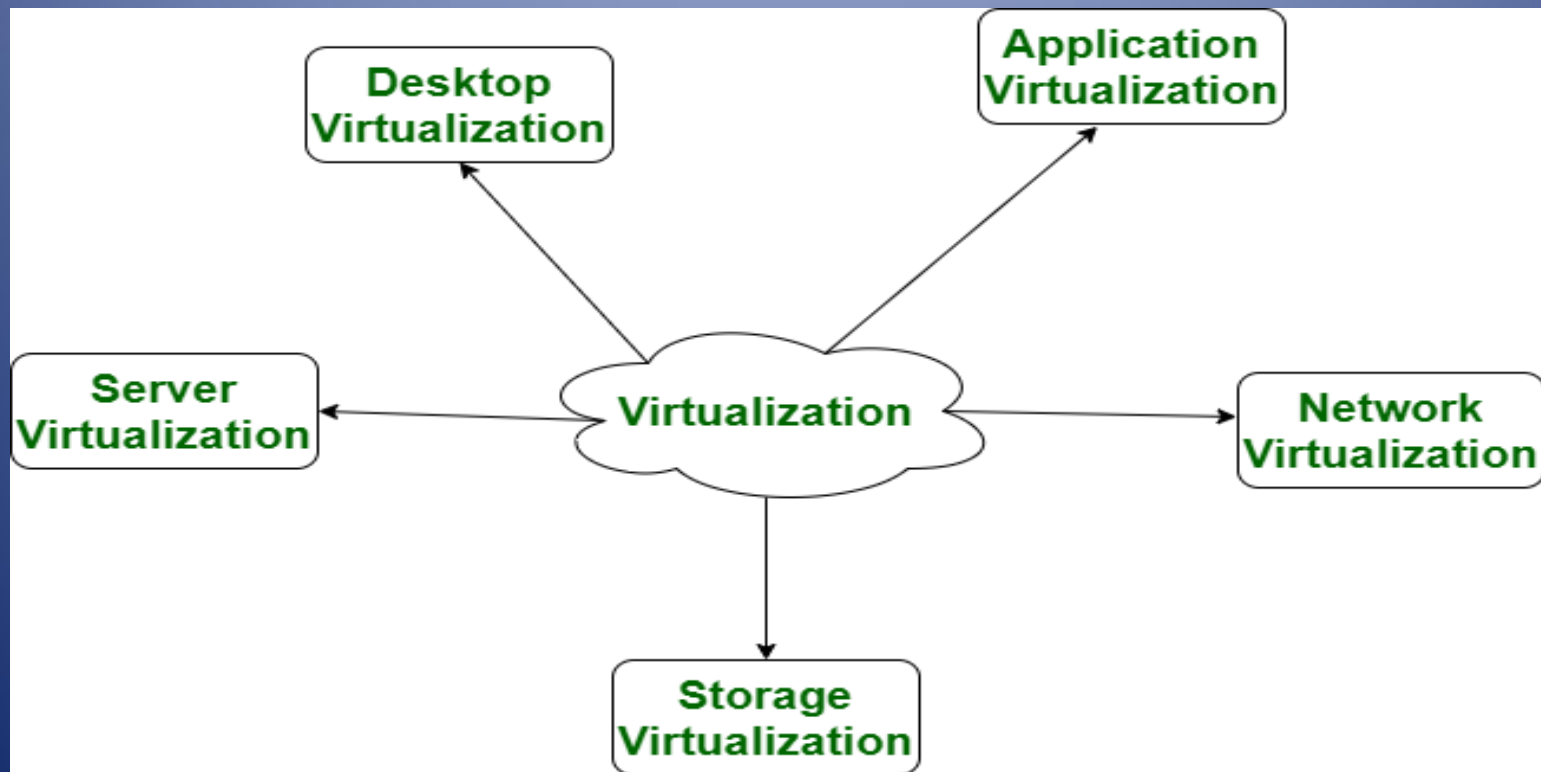
As we know, cloud infrastructure is completely owned, managed, and monitored by the service provider, so the cloud users have less control over the function and execution of services within a cloud infrastructure.

4. Security

Although cloud service providers implement the best security standards to store important information. But, before adopting cloud technology, you should be aware that you will be sending all your organization's sensitive information to a third party

Q:3 Explain the concept of virtualisation in detail with its different approaches.

Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.



Q:3 Explain the concept of virtualisation in detail with its different approaches.

Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.

Server Virtualization

This technique is the masking of server resources. It simulates physical servers by changing their identity, numbers, processors and operating systems. This spares the user from continuously managing complex server resources

Data Virtualization

This kind of cloud computing virtualization technique is abstracting the technical details usually used in data management, such as location, performance or format, in favor of broader access and more resiliency that are directly related to business needs.

Desktop Virtualization

As compared to other types of virtualization in cloud computing, this model enables you to emulate a workstation load, rather than a server. This allows the user to access the desktop remotely.

Q:4 Explain cloud security in detail.

Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion. Methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections.

Infrastructure Security

Cloud computing infrastructure security refers to the entire infrastructure of cloud computing which involves a wide set of policies, applications, technologies. It also includes controls that are used to protect virtualized IP, services, applications and data.

Network level Security

When looking at the network level of infrastructure security, it is important to distinguish between public clouds and private clouds. With private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider.

Infrastructure Security Level

Infrastructure Security – The Host Level

When reviewing host security and assessing risks, the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models (public, private, and hybrid) should be considered. The host security responsibilities in SaaS and PaaS services are transferred to the provider of cloud services.

Infrastructure Security – The Application Level

Application or software security should be a critical element of a security program. Most enterprises with information security programs have yet to institute an application security program to address this realm.

- Application-level security threats;
- End user security;
- SaaS application security;
- PaaS application security;
- IaaS application security
- Customer-deployed application security
- Public cloud security limitations

Data Storage Issues in Cloud Computing

Anonymity: In cloud data storages, anonymity is a technique to obscure the published data and key information preventing the associated identity of the owner of data.

Account or Service Traffic Hijacking: It is usually performed with stolen credentials and remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services.

Availability: The main goal of cloud service is also to provide high availability to the client. Its focus is to ensure that a user can get information anywhere anytime.

Data Loss and Leakage: Data breaches are the result of an intrusive action and data loss may occur when disk drive dies without creating any backup. It is the loss of privacy, trust and has a direct effect on the Service Level Agreement (SLA) policy, which are the main concerns of cloud users.

Cryptography: Often cryptographic mechanisms seem to fail when a security measure is applied. In a cloud, cryptographic techniques are applied to overcome the loopholes in security areas.

Security issues in cloud computing

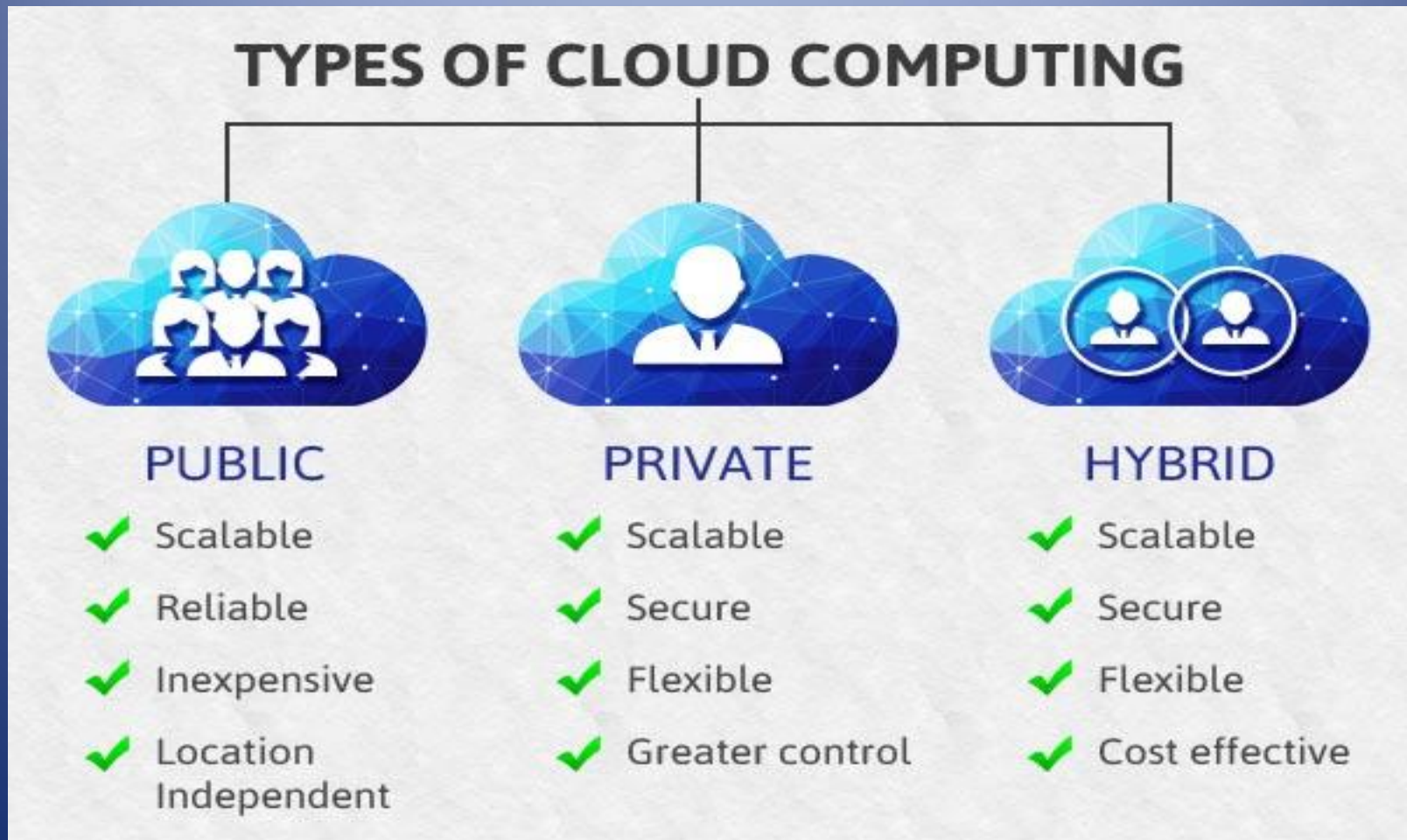
Data breaches: When the safety of data is compromised within the cloud, this can lead to attacks such as leaked data. If the cloud service – or a connected device – is breached, sensitive data has been accessed. When the data in storage is transferred, either electronically or physically, it becomes leaked.

Data loss: Another common cloud storage security risk is data loss. As opposed to information being stolen and distributed, it is erased entirely. This could either be the result of hacking, a virus or a system failure – this poses an issue when data is not backed up, highlighting the importance of securing cloud services.

Crypto jacking: Crypto jacking is a form of threat that uses resources to mine crypto currencies (digital currencies or Bitcoin). The threat can control cloud networks to hack web browsers and compromise endpoints.

Revenue loss: As a direct result of losing clients, businesses may also face revenue loss. This could also be the result of the attack itself – paying compensation to those affected by the leak or loss of their sensitive information, the resources and technology used to fix the problem and updating the security platform

Explain Public cloud vs Private cloud vs Hybrid cloud.



Explain Public cloud vs Private cloud vs Hybrid cloud.

Private cloud provides a high level of security and privacy to data through firewalls and internal hosting. It also ensures that operational and sensitive data are not accessible to third-party providers. HP Data Centers, Microsoft, Elastra-private cloud, and Ubuntu are the example of a private cloud.

Public cloud services are provided by Amazon, Google, Microsoft, IBM, Oracle, and others. Resources are shared by hundreds or thousands of people. Google Cloud Platform public cloud infrastructure is a part of Google cloud storage public services. Gmail, Google Drive are examples of public cloud services.

Hybrid cloud solutions combine public cloud hosting from an IaaS (infrastructure-as-a-service) provider—like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP)—with an internal private cloud.

Explain the process of creating a web cloud with examples.

- There are three varieties of cloud. ...
- Evaluate your applications to identify those that fit the cloud. ...
- Select an application to test out the cloud. ...
- Plan the migration. ...
- Migrate the application to the cloud



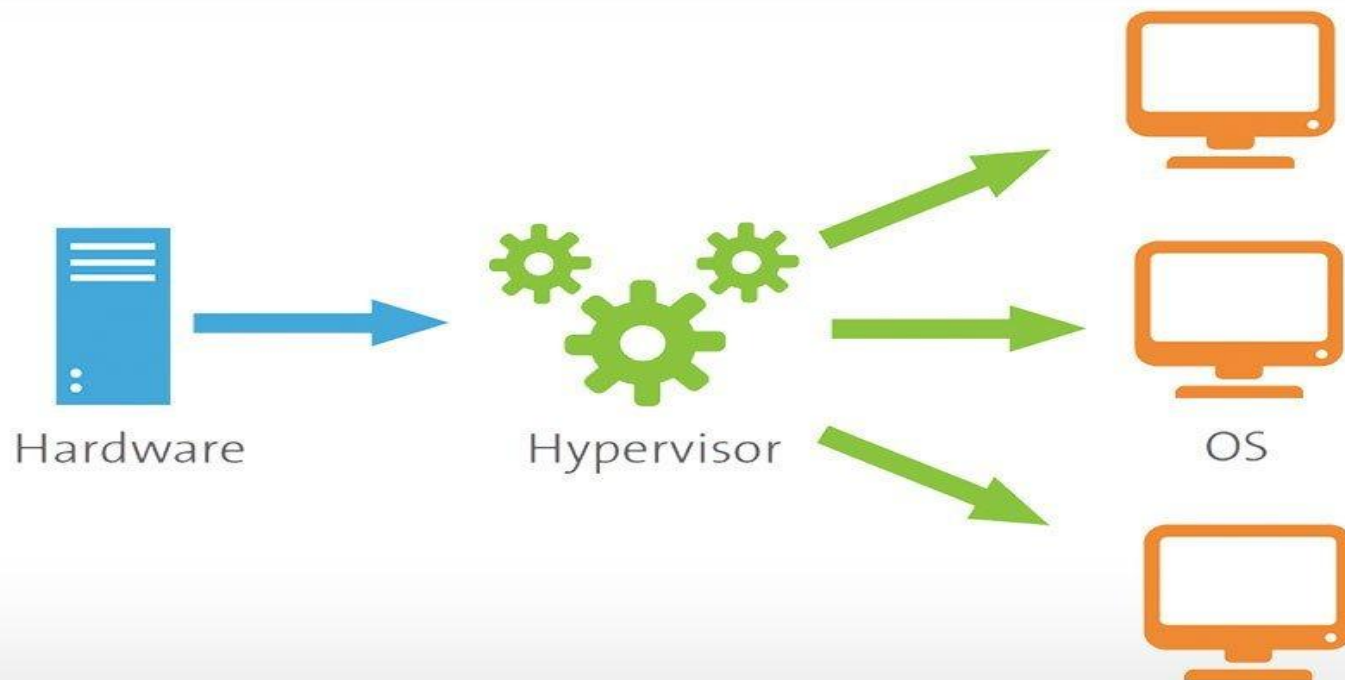
Explain the comparison between SaaS vs PaaS.

PaaS (Platform as a Service) PaaS is the cloud solution where, apart from providing an infrastructure, cloud providers also issue an on-demand computing environment to develop, test, run and collaborate with components such as web servers, database management systems, and software development kits (SDKs) for various programming languages.eg AWS Elastic Beanstalk, Heroku, Windows Azure, Force.com, Google App Engine.

SaaS (Software as a Service) SaaS providers offer fully functional web-based application softwares tailored to a variety of business needs such as project tracking, web conferencing, marketing automation or business analytics.eg Google Apps, Microsoft Office 365, Gmail, Yahoo and Facebook.

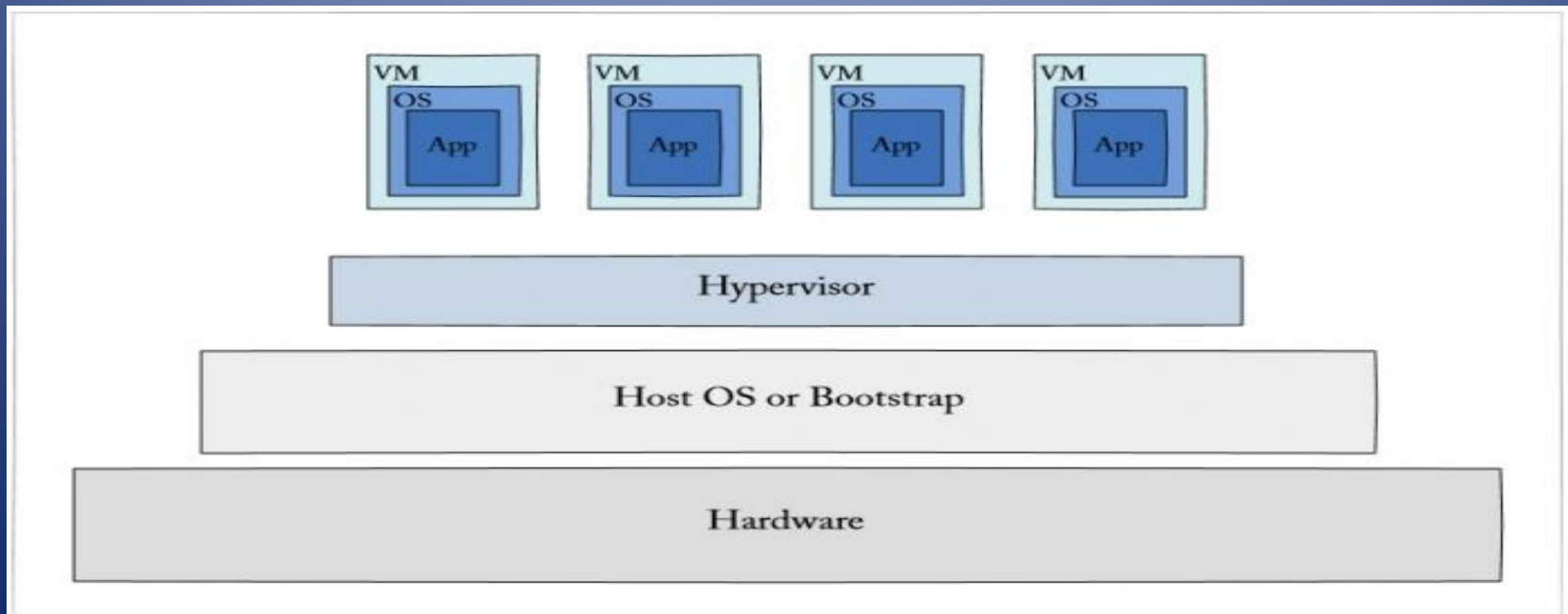
Explain the working principle of Hypervisor & Virtual Machine

Hypervisor:-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. A hypervisor allows you to access several virtual machines that are all working optimally on a single piece of computer hardware.



Explain the working principle of Hypervisor & Virtual Machine

Virtual Machine:- Virtual machines run on a physical machine and access computing resources from software called a hypervisor. The hypervisor abstracts the physical machine's resources into a pool that can be provisioned and distributed as needed, enabling multiple VMs to run on a single physical machine.



What is the role of networks in cloud computing?

- Cloud networking allows users to build networks using cloud-based services. A reliable cloud network provides centralized management, control and visibility, for example, managing devices in different physical locations using the internet. It can be used for connectivity, security, management and control.
- Cloud networking is playing a crucial role in addressing the organization and its infrastructural needs, geographic expanse and other plans like redundancy.
- A cloud network is an IT infrastructure wherein some or all organization's network resources and capabilities are hosted. These can be public, private or hybrid platform.
- Organizations can use on-premises cloud networking resources for building a private network. They can even use the public network on cloud-based networking resources..

Thank You

