STYUDY MATRIAL

OF

CLOUD COMPUTING

Prepared by
Smt.Pranati Pattnaik
Sr.Lecturer in CA
Govt.Polytechnic , Bhubaneswar

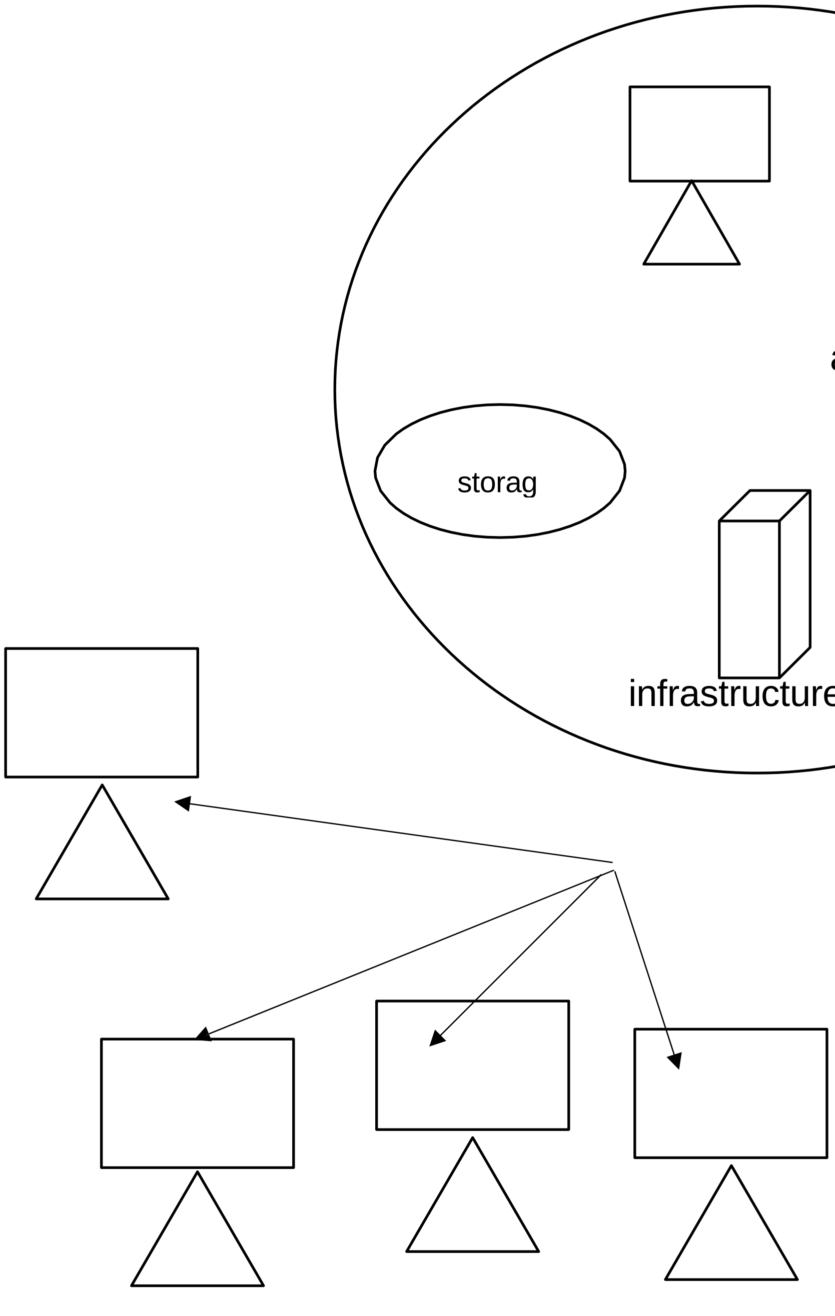
Unit: - 1

INTRODUCTION TO CLOUD COMPUTING

WHAT IS CLOUD?

The cloud refers to a network or internet. Cloud computing is something, which is present at remote location. Cloud can provide services over network i.e., on public network or on private network i.e., WAN, LAN, VPN. Application such as E-mail, web conference.

Cloud computing: - Cloud computing refers to manipulating, configuring and accessing the application online. It offers online data storage, infrastructure and application.



History

The concept of cloud computing came in 1950 with implementation of mainframe computer accessible via static clients. Then evolved dynamic.

The following diagram explains the evolution of cloud computing.

Mainframes	Rise of the pc	c/s architecture	Hosted environment	Cloud computing
• Start of automatic phase • Localized infrastructure	• Rise in demand of pc and FTP • Decentralized computing • Birth of IT services industries	• Virtual private network offered • Demand for high bandwidth	• IT infrastructure management out servicing • Increase use of virtualization	• Emergence of as a service. • Delivery of IAAS, PAAS, SAAS, NAAS. • Collaboration computing • Utilization computing model
1950s	1960s	1990	2000	Beyond 2010

Vision of cloud computing:

1. Cloud computing provides the facility to provision virtual hardware, runtime hardware environment and services to a person having money.
2. These all things can be used as long as they are needed by the user.
3. The whole collection of computing system is transformed into collection of utilities, which can maintenance cost.
4. The long-term vision of a cloud computing is that IT services are traded as utilities in an open market without technological and logical barriers.
5. In future, we can imagine that it will be possible to find the solution for our requirements through cloud computing services.
6. The existence of such digital market will enable the automation of discovery process and its integration onto its existing software systems.
7. Due to existence of global platform for trading cloud services will also help service providers too.
8. A cloud provides can also become a consumer of a competitions services in order to fulfil customers requirement.
9. A cloud provides can also be a buyer a service to fulfil customer’s requirement.

10. In near future we can imagine a solution that suits our needs by applying our application to the global digital market for cloud computing services.

Characteristics of Cloud Computing

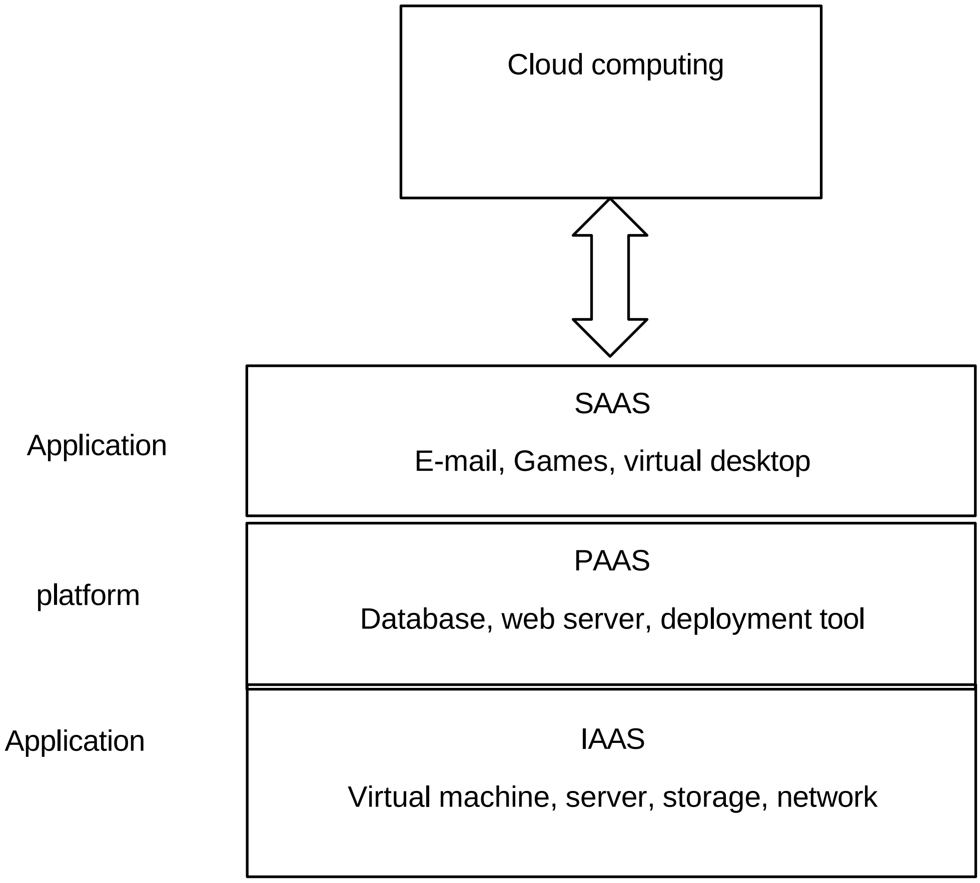
Following are the characteristics of cloud computing.

1. **On-demand self-service: -** Cloud computing allows the user to use web services and resource on demand. One can log on to a website at any time and use them.
2. **Broad network access: -** Cloud computing web based, it can be accessed from anywhere and at any time.
3. **Resource pooling: -** Cloud computing allows multiple tenants to share a pool of resources. One can share single physical instance of hardware, database and basic infrastructure.
4. **Rapid elasticity: -** It is very easy to scale up or down the resources at any time.
5. **Measured service: -** Cloud systems automatically control and optimize resource by using service model and deployment models.

Cloud computing reference model

There are three service model defined by NIST.

1. Cloud software as a service. (SAAS)
2. Cloud platform as a service. (PAAS)
3. Cloud infrastructure as a service. (IAAS)
4. Service model are the reference model on which the CC in based.


Cloud computing
Application
SAAS
E-mail, Games, virtual desktop
platform
PAAS
Database, web server, deployment tool
Application
IAAS
Virtual machine, server, storage, network

IAAS: - IAAS provides access to fundamental resources such as physical machines, virtual storages, etc.

PAAS: - PAAS provides the runtime environment for applications, development & deployment tools, etc.

SAAS: - SAAS allows to use software applications as a service to end users.

Cloud computing environment

CC environment in all about IT and what IT needs. Different kinds of software and hardware, pay-per-use or subscription-based services offered both through the internet and in Realtime.

Cloud services requirements

The vendors providing cloud computing are called cloud services. The cloud in cloud computing refers to the internet. Therefore, cloud computing refers to providing computing services like storage, CPU, networking, RAM, servers, etc. over the internet. So, every successful cloud-computing should follow:

- World class security: provision world class security at every level.
- Trust and transparency: provide transparent, real-time, accurate service performance and availability information.
- True multitenancy: provide software architecture in which a single instance of software runs on a server and servers multiple tenants, a tenant in a group of users.
- Proven scale: support millions of users with proven scalability. (scalability in the measure of system’s ability to increase or decrease in performance.)
- High performance: deliver in the same way overtime, high-speed performance globally.
- Complete disaster recovery: protect customer data by running the service on multiple, data archiving and failure capabilities.
- High availability: equip world- class facilities which proven high availability infrastructure ad application software.

Cloud and dynamic infrastructure:

Dynamic infrastructure refers to a collection of data centre resources, such as computer, networking and storage, that can automatically provision and adjust-itself as workload demands change. IT administration can also choose to manage these resources manually.

Cloud and dynamic infrastructure have following facilities.

1. Service management: This facility includes visibility automation and could to delivering the first-class IT services.
2. Asset management: The property or asset which is involved in providing the cloud services are getting managed.

3. Virtualization and consolidation: consolidation is an effort to reduce the cost of a technology by improving its operating efficiency and effectiveness. It means migrating from large number of resources to fewer one, which is done b virtualization technology.
4. Information infrastructure: It helps the business organizations to achieves the information compliance, availability of resources and security objectives
5. Energy efficiency: hence the IT infrastructure in sustainable. It means it is not likely to damage or effect any other thing.
6. Security: This is responsible for risk management. Risk management refers to the risk involved in the services which are being provided by the cloud service provider.
7. Resilience: This is providing the feature of resilience means the services are resilient it means the infrastructure in safe from all sides. The IT operations will not be easily get affected.

Cloud adaption: It means adapting a services or technology from another cloud services provide.

1. Cloud means the environment of cloud where the cloud services are being operated.
2. Adoption means accepting the services of new technology or new trend.
3. This cloud adoption in suitable for low priority business application.
4. It supports some interactive application that combine two or more data source.
5. Cloud adaption is useful when the recovery management, backup recovery-based implementations and required.
6. It will work will with research and development project.
7. It means the testing of new services, design models, applications that can be adjusted on server.

Cloud application

The major benefits of cloud application are no installations of application, no maintenance required because the software is hosted in a machine, that software is dedicated no worry of external influences. Cloud application are also referred to as software as a service (SAAS), software plus service or data as a service.

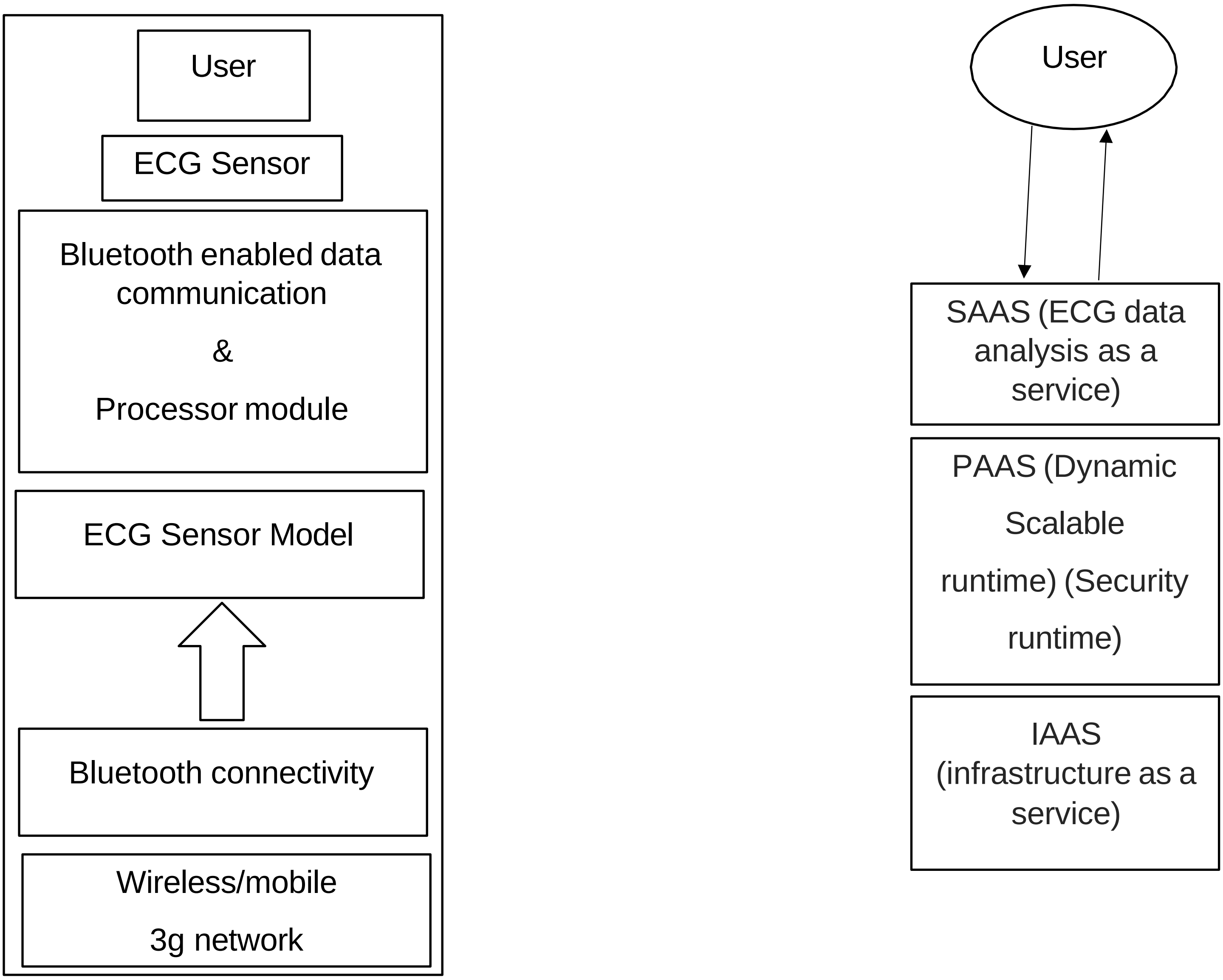
ECG analysis in the cloud

ECG is the elechical activity of the heart. Due to this activity a waveform is produced a specific waveform that is repeated overtime and that represents the heartbeat.

The functionality of an ECG monitoring and analysis involves the following steps:

1. A patient is equipped with a wireless ECG sensor attached to their body and a mobile device that in capable of communicating to the internet.
2. The wireless ECG collects patient’s data and forwards it the mobile device via Bluetooth.

3. A client software in the mobile device transmits the data to the ECG analysis web services, which is hosted by a cloud computing-based software stack.
4. The analysis software received data taking the demographic data, and the patient's historic data.
5. The software records the data in secure cloud-based storage. So authenticated users can access it physician will later interpret the features extract from the ECG wave.


User
ECG Sensor
Bluetooth enabled data communication
&
Processor module
ECG Sensor Model
Bluetooth connectivity
Wireless/mobile
3g network
User
SAAS (ECG data analysis as a service)
PAAS (Dynamic Scalable runtime) (Security runtime)
IAAS (infrastructure as a service)

Above fig. in different type of computing devices equipped with each sensor.

2. Protein structure prediction (PSP)

Protein: - protein are large molecules consisting of amino acids which our bodies add the cells in our bodies need to function properly.

- Protein structure prediction in a computationally intensive task fundamental for different types of research in the life science.
- This prediction of protein structure will help to develop new drugs.
- The computational power required for this prediction can now be online, without owning it.

- Cloud computing grants the access to such capacity on pay per use basis.
- This PSP technique in based on genetic algorithm.
- The GA-based PSP in made as a grid service. (Grid service means web service.)
- The PSP portal submitting the job to GARUDA grid.
- The portal will facilitate for below features.

Features: -

- User can input protein files in two ways.
- Upload protein file from local machine on the PSP server.
- Create the protein file by supplying required parameters.
- Run the PSP web services on GARUDA clusters.
- Download the results.

3. Gene Expression Data Analysis

Gene: - a gene is the basic physical and functional unit of heredity genes are made up of DNA (Deoxyribonucleic acid), act as instructions to make molecules, such as proteins.

Gene expression: - gene expression in the process by which information from gene in used in the synthesis of a functional gene product

- Cloud-coxcs, is a machine learning classification system for gene expression data set on the cloud infrastructure.
- It is composed of three components
  a. Coxcs
  b. Aneka (It is a platform)
  c. Cloud computing infrastructure.
- Gene expression technology, allows for monitoring of the expression levels of thousands of genes at once.
- The gene expression software’s, such as Myrna, uses cloud computing, an internet-based, method of sharing computer resources.

4. Satellite image processing: -

Satellite image processing in CC is an advance application for generating meaningful result. The satellite image sensing generates a lot of raw image that needs to be processed further this requires the high computation in both I/P and O/P manner.

5. CRM and ERP: -

CRM- customer relationship management.

ERP- Enterprise resource planning.

- CRM and ERP both are software. These are powerful tools for a business or enterprise to use.
- CRM handles the sales, marketing and customer service information.
- ERP handles the back-end process and internal information.

Difference between CRM and ERP.	
CRM	ERP
1. This software manages front office services.	1. This software manages back-office activities and tasks.
2. Organise marketing efforts.	2. Distribution process management.
3. Manage the sales pipeline.	3. Supply chain management.
4. Streamline sales process	4. Services knowledge base.
5. Automates customer services.	5. Improve accuracy of financial data
6. Track customer's interactions with business	6. Automate employee life cycle.
7. Share marketing and sales, etc	7. Facilitate before project planning.

6. **Social networking**

   Social networking CC is social CC, also peer-to-peer social CC, is an area of computer science that generalizes CC to include the sharing, and renting of computing resources and operates through social network.

   - The social cloud architecture presented as designed as Facebook application.

UNIT-2

Cloud computing architecture

Cloud reference model:

Cloud reference model consist of for supporting models.

6. Cloud enablement model.
7. Cloud deployment model.
8. Cloud governance and operations model.
9. Cloud ecosystem model.

1. **Cloud enablement model:** it is the core CC reference model. This model. This model describes the fundamental technology tiers of CC capabilities provided by cloud platform.
2. **Cloud deployment model:** it is describing the range of cloud deployment sceneries available. That is internal/private cloud, external/public cloud, hybrid/integrated cloud, community or vertical cloud.
3. **Cloud governance and operations model:** it describes the governance, security operations, support, management, and monitoring requirements force.

4. **Cloud ecosystem model:** it is a complex system of interdependent components that all work together to enable cloud services. In CC the ecosystem consists of hardware, software as well as cloud customers, cloud engineers, consultants and partners.

The components of CC reference model are:

Cloud enablement model:

- Cloud virtualization tier
- Cloud os tire
- Cloud platform tire
- Cloud business tire

Cloud deployment model:

- Internal/private cloud
- External/public cloud
- Hybrid/integrates cloud
- Community/vertical cloud

Cloud governance and operations model:

- Cloud network
- Cloud ecosystem
- Cloud consumers and cloud providers
- Cloud physical access

Type of cloud:

1. Private cloud
2. Public cloud
3. Hybrid cloud

1. **Public cloud:** A public cloud is one in which the services, resources and infrastructure are provided off site over the internet.
   - These clouds offer the greatest level of efficiency with should resources.
   - Public cloud examples are amazon, Microsoft, google these companies provide both services and infrastructures which are shared by all customers.

Pros: This is least expensive CC option considering that only pay for the services and resources that we use.

- There are no hardware and software maintain ace cost.

Cons: security can be a concern, and there is always the risk of data being compromised.

- Network issues can cause performance issues with the amount of data being transferred over the internet.

2. **Private cloud:** private cloud usually resides behind a firewall and one utilized by single organization.
    - these cloud after the greatest level of security

pros: the hardware and cloud software are implemented on a private network offer both security and control.

- The additional control offered by a private cloud makes to restrict access to valuable assets.

Cons: A private cloud solution will not be affected by a public cloud provide system downtime.

- Higher cost is generally associated with private CC because of the hardware, software expenses

Hybrid cloud: Hybrid cloud includes a variety of public and private options with multiple providers.

- They are designed to allow the two platforms, with data and applications moving smoothly from one to the other.

Pros: provides the best of both public and private CC.

- Providing quick access to information and application for public services.
- Providing security to data for private cloud services.

Cons:

- The security, processing and storage between private and public cloud can be technologically challenging today.
- Could cost more than either the private or public cloud options considering the technology and skill required.

Cloud interoperability and standards:

Cloud interoperability is the ability in which a customer's system communication with a cloud service or ability of one cloud service to communicate with other cloud services by sharing information to achieve predictable results according to a specified process.

Interoperability meaning: the ability of computer or software to exchange and make use of information.

Cloud-computing interoperability use case

NIST (National institute of standard technology) defines 21 use classified into three groups.

1. Cloud management
2. Cloud interoperability
3. Cloud security

These use cases are listed below:

1. Cloud management use case:

- ➢ Open an account
- ➢ Close an account
- ➢ Terminate an account
- ➢ Copy data objects into a cloud.
- ➢ Copy data objects out of a cloud.
- ➢ Erase data objects on a cloud.
- ➢ VM (virtual machine) control- allocate VM instruction
- ➢ VM control: manage VM instance state.
- ➢ Query cloud provider capabilities and capacities.

2. Cloud interoperability use case:

- ➢ Copy data objects between cloud-providers.
- ➢ Dynamic operation dispatch to IAAS clouds.
- ➢ Cloud burst from data centre to cloud.
- ➢ Migrate a querying-based application.
- ➢ Migrate (fully-stopped) VMS from one cloud provider to another.

3. Cloud security use cases:

- ➢ User account provisioning.
- ➢ User authentication in the cloud.
- ➢ Data access authorization police management in the cloud.
- ➢ Security monitoring
- ➢ Sharing of access to data in cloud.

Role of standards in cloud-computing environment

Definition: CC standard provides definition of common CC terms, including those for cloud services categories such as software as a service (SAAS), platform as a service (PAAS), and infrastructure as a service (IAAS).

IAAS:

1. IAAS stands for infrastructure as a service.
2. IAAS is the basic layer in CC model.
3. IAAS offers servers, network devices, database, web server etc.
4. IAAS delivers customizable infrastructure on demand.
5. IAAS can be categorized in two categories.
   - ➢ IAAS management layer.
   - ➢ IAAS physical infrastructure.
6. Some services provider provides both services, some provide only one.

7. On virtual machines applications are installed and displayed Example of virtual machine in oracle VM.
8. Hardware virtualization includes workload applications isolation and hardware tuning.
9. Instead of purchasing user can access these virtual hardware's on pay per use basis.
10. Users can take advantage of the fall customization offend by virtualization to deploy their infrastructure in the cloud.

    Ex – amazon web service

    - Microsoft azure.
    - Google complete engine.

PAAS:

1. PAAS stand for platform as a service.
2. PAAS provides a computing platform with a programming language execution environment.
3. PAAS provide a development and deployment platform for running application the channel.
4. PAAS constitute the middleware on top of which applications are built.
5. Application management in the core functionality of the middleware.
6. PAAS provides
    - ➢ Run time environment for the application.
    - ➢ Application deployment
    - ➢ Configuration application.
    - ➢ Configuring supporting technology.
7. PAAS classification
    I. PAAS-I: runtime environment- with web-hosted application development platform.
    II. PAAS-ii: runtime environment for scaling web application.
    III. PAAS-iii: middleware and programming model for develop disturbed application on cloud.
8. Example: google app engine
    - Force.com

SAAS:

1. SAAS stands for software as a service.
2. SAAS allows users to connect to and use cloud-based apps over the internet.
3. SAAS is the service with which and user internet directly.
4. In SAAS customer do not purchase the software they simply access the application website, enter their credentials and billing details, and can instantly use the application.
5. Application is available to the customer on demand.
6. SAAS can be considered as a "one to many software deliveries models."

7. SAAS application are built as per the user needs
   Examples – Gmail
    - Google drive.
    - Dropbox.
    - WhatsApp.

Unit – 3

Scalability and fault tolerance

- cloud scalability is the ability to scale on-demand the facility and services as and when they are required by the user.
- Cloud fault tolerance is tolerating the faults by the cloud that are done by mistake by the users.
- Here the scaling is beyond the limits, it means we cannot even imagine what will be the limit.
- Middleware is designed on the principle of scalability along different dimensions e.g.- performance, size and load.
- The cloud middleware in the software that connects application and devices to other application.
- The cloud middleware manages a huge numbering resources and users.
- So, in this overall scenario the ability to tolerate failure in normal but sometimes it becomes more important than providing an efficient & optimized system.

Cloud solution:

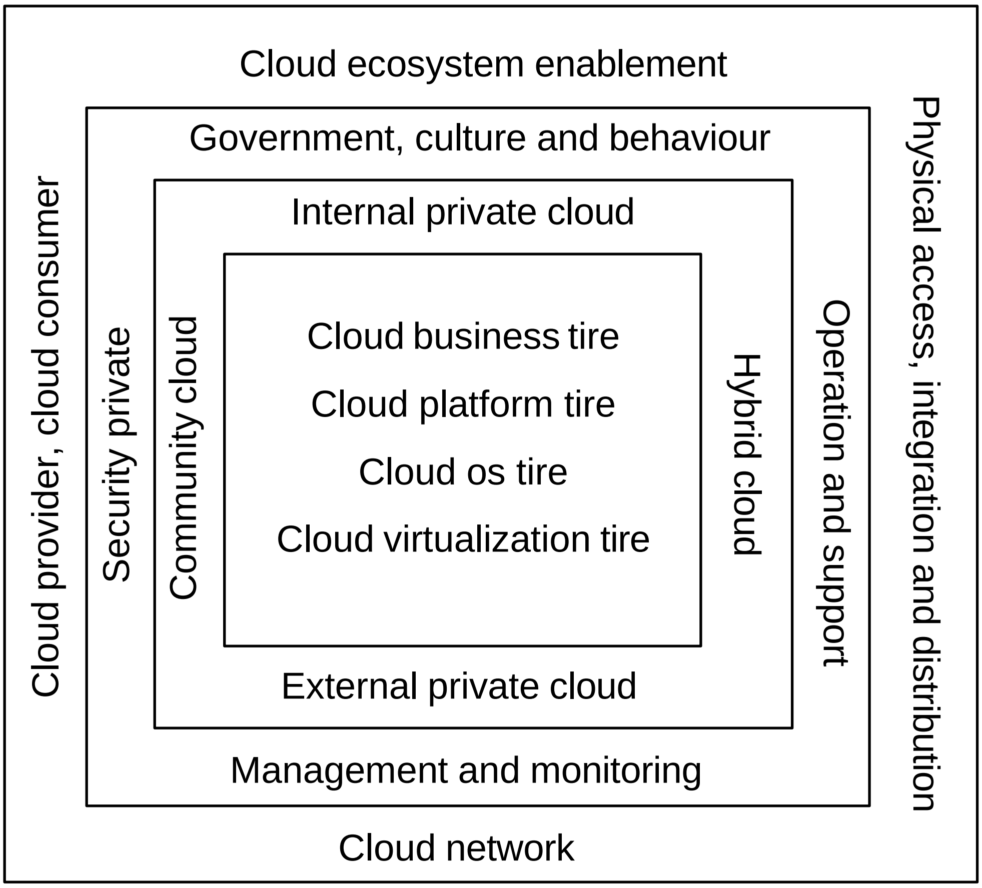
Cloud solution refers to on-demand services computer networks, storage, application, or resources accessed via the internet and through another providers shared cloud computing infrastructure.

Cloud ecosystem:

Cloud ecosystem is a term used to describe the complex system of interdependent components that work together to enable cloud services.

The following elements comprise the cloud ecosystem model.

- Cloud ecosystem enablement.
- Cloud consumers and cloud providers
- Cloud network
- Cloud physical access, integration and distribution.



Cloud ecosystem enablement
Government, culture and behaviour
Internal private cloud
Cloud business tire
Cloud platform tire
Cloud os tire
Cloud virtualization tire
External private cloud
Management and monitoring
Cloud network
Cloud provider, cloud consumer
Security private
Community cloud
Hybrid cloud
Operation and support
Physical access, integration and distribution

Cloud business process management:

Business support: business support in the set of business-related services dealing with clients and supporting process.

It includes the components used to run business operations that are client facing.

- Customer management: manage customer accounts, open/close/terminate accounts, manage user profiles, resolve customer issues and problem.
- contract management: manage services contracts, setup/negotiate/close/terminate/contract etc
- inventory management: setup and mange service catalogues. Etc
- accounting and billing: manage customer billing information, send billing statements, process received payments, track invoices etc.
- Reporting and auditing: monitor user operations generate reports etc.
- Pricing and rating: evaluate cloud service and determine prices.

Provisioning and configuration:

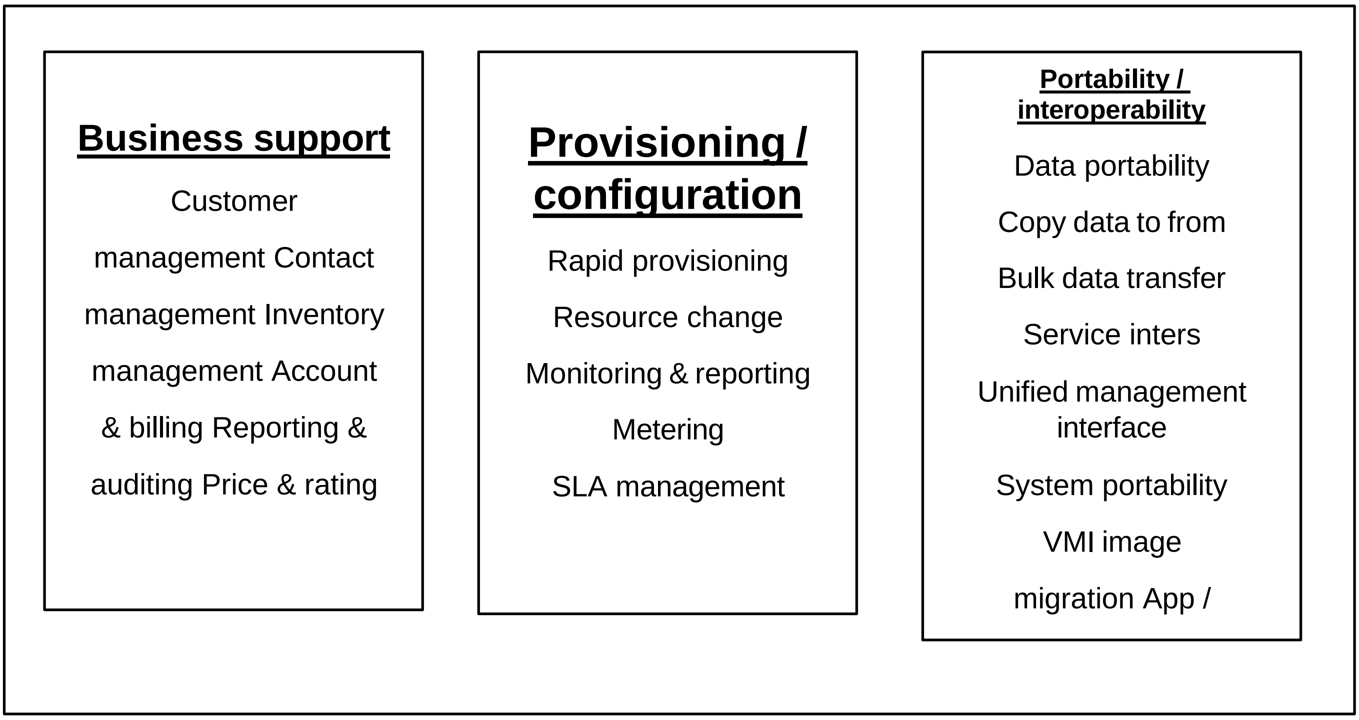
- Rapid provisioning: automatically deploying cloud systems based on the requested services/resource/capabilities.
- Resources changing: adjusting configuration/resource assignment for repairs, upgrades and jointing news nodes into the cloud.
- Monitoring and reporting: discovering and monitoring virtual resources, monitoring cloud operations and generating performance reports.

Portability and interoperability:

- Portability: portability means the ability to move executable software from one cloud system to another, and be able to run, it correctly in the destination system.
- Interoperability: interoperability means the ability of two cloud systems to talk to another i.e., to exchange message and information in a way that both can understand.

Cloud services management:

- It includes all of the services-related functions that are necessary for the management and operation required to cloud consumer.
- Cloud service management can be described from the prospective of business support, providing and configuration and from the prospective of portability and interoperability requirements.



Business support

Customer

management Contact

management Inventory

management Account

& billing Reporting &

auditing Price & rating

Provisioning / configuration

Rapid provisioning

Resource change

Monitoring & reporting

Metering

SLA management

Portability / interoperability

Data portability

Copy data to from

Bulk data transfer

Service inters

Unified management interface

System portability

VMI image

migration App /

Cloud offering

Cloud service refers to wide range of services delivered on demand to compares and customers over the internet. These services are designed to provide easy, affordable access to application and resources, without the need for hardware.

Testing under control

- **Cloud testing** is a type of software testing in which the software application is tested using cloud computing services.
- Load and performance testing conducted on the application and services provided via CC particularly the capability to access these services in order to ensure optional performances and scalability under a wide variety of conditions.

- Cloud testing typically involves monitoring and reporting on real world user traffic condition.

cloud security controls

There are many types of controls behind a cloud security architecture.

- **Deterrent controls:** these controls are to prevent any purposeful attack on cloud system.
- **Preventive control:** these controls upgrade the strength of the system by managing the vulnerabilities. It in the safeguard vulnerabilities of the system.
- **Corrective control:** corrective controls are used to reduce the effect of an attack. The corrective controls take action as an attack in occurring.
- **Defective controls:** detective controls are used to date any attacks that may be occurring to the system the detective control will signal the preventive or corrective controls.

Virtual desktop infrastructure (VDI)

- VDI is defined as the hosting of desktop environments on a central server. It is a form of desktop virtualization.
- VDI in a concept in which a solution based on a server-based computing model, that is similar to traditional terminal server centralized computing model used to deliver application to remote users.
- VDI in the collection of technologies and process that extend the concept of a remote desktop.

VDI benefits:

1. Data security.
2. Reduced hardware expenditure.
3. Easier management.
4. Mobile workforce: users' desktops are portable; users can connect from any location with a variety of devices.
5. Resource pooling.

Unit – 4

Cloud management and virtualization technology

create a virtualization architecture:

- Virtualization in the technology to develop a virtual tension of the resource or device like network, OS, software, etc. It is divided the resource into one or more executable environment.
- Create and deploy end-to-end virtualization helps
    - Reduce cost
    - Provision new application quickly.

    - Maintain high level of application software.
- Cisco provides a comprehensive architectural approach that help reduce cost, protect application and secure the virtualized infrastructure.

Data centre

A data centre is a facility that centralizes an organization shared IT operations and equipment for the purpose of storing, processing and data and application.

Data centre helps:

- Optimized IT productivity and resource utilization.
- Super scale-up and scale-out, storage consolidation & virtualization.
- Lower capital cast and higher utilization.
- Provisioning of pooled resource.

Resilience

Cloud resilience in the capacity to rapidity adopt and respond to risks, as well as opportunities resiliency refers to improve business for handle risk.

Resilience helps:

- Creates an environment to protect valuable applications services information and infrastructure.
- Ensure regulatory compliance by
    - Providing a resistant network infrastructure that supports security, availability.
    - Performance and business goals.
- Improve service table.

Agility:

in cloud computing, agility refers to the ability to rapidly develop, test and launch application that drive business growth in a constantly changing IT environment.

Agility helps:

- Facilities the adoption of new IT strategies, such as
    - Services oriented architecture (SOA)
    - Virtualization and on-demand computing allowing faster response to change.
- Virtualized infrastructure with the ability to respond quickly to new application demands services requirements, attacks based on predefined polices.

The cisco data centre network architecture includes

1. **Network infrastructure:**
    1. Io gigabit ethernet
    2. Fibre channel switching on intelligent server farm.

3. Server fabric (The term fabric is used to describe data or storage area networks; vendors are using the terms to describe the servers high speed connection and switches that make up CC platform.)
4. Storage networking platforms.
5. DWOM, SONET and SDH optical transport platforms

DWOM in dense wavelength division multiplexing (DWOM) delivers data on optical fibres, DWDM can deliver up to 80 separate channels of data into a single stream of light transmitted over an optical fibre each channel can carry from 2.5 GBPS (billion bits per second) up to 200 GBPS by the optical fibre system.

SONET (Synchronous optical network) is a standard for connecting fibre-optic transmission system. SONET defines interface standards at the physical layer of OSI model.

SDH (synchronous digital hierarchy) is a standard technology for synchronous data transmission on optical media. This technology provides faster and less expensive network.

2. Interactive services:

- Storage fabric services.
- Compute services.
- Security services.
- Application delivery and integration services.

3. Management framework:

- Configuration
- Security
- Provisioning
- Change and fault management services.

Storage:

Net app commercial benefits

- Store the maximum amount of data for lowest cost.
- 50% lower capacity requirements without sacrificing.
- Achieving 100% utilization.
- Maximize the value of existing storage system.

Technical benefits:

Single architecture means seamless scaling. Net application storage architecture allows, customers the flexibility to manage, support and scale their environment using knowledge and tools. Net app customers use these products from the remote office the data centre, collecting, distributing and managing data from all locations and application at the same time.

Examples of cloud storage are googled docs, x drivers, media max and storage space. Most private computer users are familiar with backup service in cloud. Backup requires storage and when storage in available over the internet.

Cloud provisioning

- Cloud provisioning in the allocation of a cloud provider's resource to a customer.
- When a cloud provider accepts a request from a customer, it must create the appropriate number of virtual machines (VMS) and allocate resources to support them. The process is conducted in several ways.
  - Advance provisioning
  - Dynamic provisioning
  - Self-provisioning.

The word provisioning means to provide.

- Cloud provisioning defines how, what and when an organization will provision cloud services. These services can be internal, public or hybrid cloud products and solutions.
- Cloud providers deliver cloud solution through on-demand, pay-as-you use.

Cloud Asset management

CAM is primarily absent managing the challenges of cloud application, platforms and infrastructure (SAAS, PAAS, IAAS)

Benefits of CAM:

1. Accurate tracking of key application delivered cloud.
2. Overtime the limitations of cloud by providing access to single centralized view.
3. Expanded access to data.
4. Combine cloud and deployment data for complete end-to-end view of IT ecosystem.
5. Access all the information needed to ensure a successful migration to the cloud.

Concepts of map reduce.

Map reduce in a programming model designed for processing language volumes of data in parallel by dividing the work into a set of independent tasks.

The work into a set of independent tasks.

The whole process of map reduce go through four phases of execution.

1. Splitting
2. Mapping
3. Shutting
4. Reducing

The process of map reduces in:

1. Splitting: I/P divided into fixed size pieces called input splits.
2. Mapping: In this phase data in each split in passed to a mapping function to produce O/P value.
3. Shuffling: The same words are clubbed together along with their respective frequency.
4. Reducing: This phase summarizes the complete data set.

Cloud governance

- Cloud governance is a general term for applying specific polices or principal to the use of CC services.
- We can say that cloud governance refers to the decision-making processes, criteria and policies involved in the planning, architecture, deployment, operation, management of CC capabilities.
- The goal of cloud governance is to secure application and data when they are located remotely.

Reasons of cloud governance:

- Enable business of cloud speed and establish a cloud centric IT operating model based on speed, agility and cost of CC.
- Enable appropriate cloud decision making without friction.
- Proactive to anticipate and prevent clouds an unauthorized cloud activity that expose organizational risk.

The cloud governance and operations model consist of the following elements.

- Governance
- Security and privacy
- Management and monitoring
- Operations and support.

High availability and disaster recovery:

High availability:

- High availability refers to the availability of resources in a computer system.
- In term of CC, it refers to the availability of cloud services.
- It provides the idea of anywhere, anytime access to service of cloud environment.
- Availability in also related to reliability.
- Availability in technology issues as well as business issue.
- High availability can be defined by
- HA = MTBF/MTBF*MTTR
- MTBF – mean time between failure.
- MTTR – mean time to repair.
- HA – high availability.

Disaster recovery: (DR)

- DR is the process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure which are organization after a natural or human induced disaster.
- A DR is the process by which an organization can recover and access their software, data and hardware.
- It is necessary for faster disaster recovery to have an infrastructure supporting high availability.
- The failure of DR plan mainly due to lack of high availability preparation, planning and maintenance to occurrence of the disaster.

Strategies of DR

1. RTO, 2. RPO

RTO – recovery time objective. The maximum acceptable length of time required for an organization to recover lost data and get back up and running.

RPO – Recovery point objective. The maximum acceptable age of the data that can be restored, RPO can be thought the time between the time of data loss and the last useful backup.

Load balancing:

Cloud load balancing is the process of distributing workload across multiple computers, resources, network links, to active optimal resource utilization, maximum throughput and maximums availability of resources.

These are at least two reasons for load balancing in deployed.

1. The required capacity is too large for a single machine.

In this case a single server in upgraded to a higher performance server, the new server may also be overloaded soon, demanding another upgrade moreover the upgrading process is expensive.

2. Looking for more reliability and flexibility in solution deployment:

In this case multiple server solution in which a scalable service system on a cluster of servers in built that’s why it in more cost effective as well as more scalable to build a server cluster system for network services.

Unit – 5

Virtualization

Definition:

CC virtualization is a technique for creating a virtual platform of storage devices and the forever OS virtualization helps the user make use of multiple machines sharing one single physical instance of any resource across the network.

Cloud storage: The first form of web-based data storage is called cloud storage. This is a form of networked data storage where data file is stored on multiple virtual servers.

The serves used for cloud storage are hosted by third party companies who operates large data centres.

- The best know cloud storage service today is amazon. Can's simple storage service (S_3), google chrome if offers unlimited storage space. It also has the ability to rescue.
- There are three primary benefits to cloud storage.
    - Scalability.
    - Reliability.
    - Lower cost.
- The risk of string data in cloud in.
    - Security.
    - User error.
    - Access problem.
- Some popular cloud storage services are
    - Amazon's.
    - Egnyte.
    - Elephant drive.
    - My data bus.
    - Microsoft office live workspace.
    - Widows live sky drive.

Advantages of cloud storage:

- File accessibility: The files can be accessed at any time from any place as long as we have internet access.
- Office backup: cloud storage provides organizations with offsite / remote backups data.
- Effective use of bandwidth: cloud storage uses the bandwidth effectively i.e., instead of sending files to recipients, a web link can be sent through mail.
- Security of data: Helps in protecting the data against malware as it is secured and needs proper authentication to access the storage data.

Disadvantages of cloud storage:

- Depending on internet speed:
- Dependency on a third party: A third party stored and hence it becomes important in selecting a vender to examine the security standards prior investing.
- High cost for Huge data: organizations that required a large amount of storage may also find cost increase after the first few gigabytes of a data stored.
- No/minimal control over data storage framework: since the cloud storage framework is entirely managed and monitored by the service provider, the customer has minimal control over it.

Network virtualization:

Definition: Network Virtualization is the process of combining hardware and software network resources and network, functionality into a single, software based administrative entity.

Components of virtual network:

- Network hardware, such as switches and network adopters, also known as (NIC) network interface cords.
- Network elements such as firewalls and load balances.
- Networks, such as virtual LANs (VLANs) and containers such as Virtual machines (VMs).
- Network storage devices.
- Network mobile elements such as laptops, tablets and cell phones.
- Network media, such as ethernet and fibre channel.

External network virtualization:

External network virtualization combines or subdivides one or more LANs into virtual networks to improve a large networks or data centre’s efficiency.

Internal network virtualization:

Internal network virtualization consists of one system using virtual machines or zones whose network interfaces are configured over at least one physical NIC.

Internal network virtualization provides network functionality purely based on software.

Combined internal and external network virtualization:

Some vendors offer both internal and external network virtualization software in their product line.

Example: M2MI

Machine to machine intelligence (M2MI) technology can both internal, external and multivendor software and hardware-based technologies.

Desktop and application virtualization:

Desktop and application virtualization is a software technology that publish end user’s desktops and applications in a data centre.

Benefits of desktop and application virtualization:

- Improve security: Data and application never leave the datacentre, eliminating leakage at the endpoint.
- Increase productivity: deliver business critical application to any device, with any os to any location.
- Ensure complication: granular controls help enforce compliance in regulated industries.
- Boost the bottom line: low-cost endpoints and pooling compete, graphics and storage resources in the data centre to increase utilization.
- Simplify management: centralize, simplify and speed management and delivery with a modern approach, avoiding traditional pc management tools.

Virtual desktop infrastructure (VDI):

VDI is defined as the hosting of desktop environment on a central server, it is a form of desktop virtualization, as the specific desktop images run within virtual machines (VMs) and delivered to clients over a network.

Example of VDI: VM Ware horizon 8.8

Parallels remote application server 8.8 etc.

- The VDI live within VMs on a centralized server.
- Each virtual desktop includes os typically Microsoft windows.

Remote desktop services:

In the cloud we can access our files from any devices at any time, with remote desktop software, we can access a specific desktop, the files, the application, and everything related to that desktop from a remote location.

Application virtualization:

App virtualization is a technology that allow users to access and use an application from a separate computer than the one on which the application in installed. For the users, the experience of the virtualized app in the same as using the installed app on a physical machine.

User virtualization:

This will help the users by providing multiple machines at the same time it also allows sharing a single physical instance of resources on an application multiple user.

Desktop as a service (DAAS)

DAAS is a cc offering where a services provider delivers virtual desktop to end users over the internet, licensed with a per user subscription. Cloud service provides may also handle security and application for the desktop or users may manage these service aspects individually.

Local desktop virtualization

- Local desktop virtualization implementation run the desktop environment on the client device using hardware virtualization.
- Local desktop virtualization means the os runs on a client device using hardware virtualization, and all processing and workload occur on local hardware.
- This type of desktop virtualization works well when users do not need a continues network connection and can meet application computing requirements with local system resources. However, because this requires processing to be done locally, we cannot use local desktop virtualization to share VMs or resources access a network.

Virtualization Benefits:

1. Save energy: Reducing the number of physical servers through virtualization cuts power and cooking costs and provides more computing power in less space. As a result, energy consumption typically decreases by 80%.
2. Reduce the data centre footprint: it results in the requirement of lesser number of servers, lesser networking hardware.
3. QA/Lab environments: Virtualization allows to easily build out a self-contained lab or test environment, operating on its own isolated network.

   Ex- VM ware machine.

4. Faster server provisioning: Faster server provisioning enables system provisioning and deployment within minutes, allowing an existing virtual machine with the laws and costs normally spent processing and installing a new physical server.
5. Reduce hardware vendor lock in: Server virtualization abstracts away the underlaying hardware and replaces it with virtual hardware, data centre manages and owners gain a lot more flexibility when it comes to the server equipment they can choose from.
6. Increase uptime: These technologies keep virtual machines chugging alone or give them the ability to quickly and easily move a virtual machine from one server to another in one of the greatest single benefits of virtualization with far-reaching uses.
7. Improve disaster recovery: Virtualization greatly simplifies disaster recovery, since it does not require rebuilding a physical server environment, instead we can move virtual machines over to another system and access them as normal.

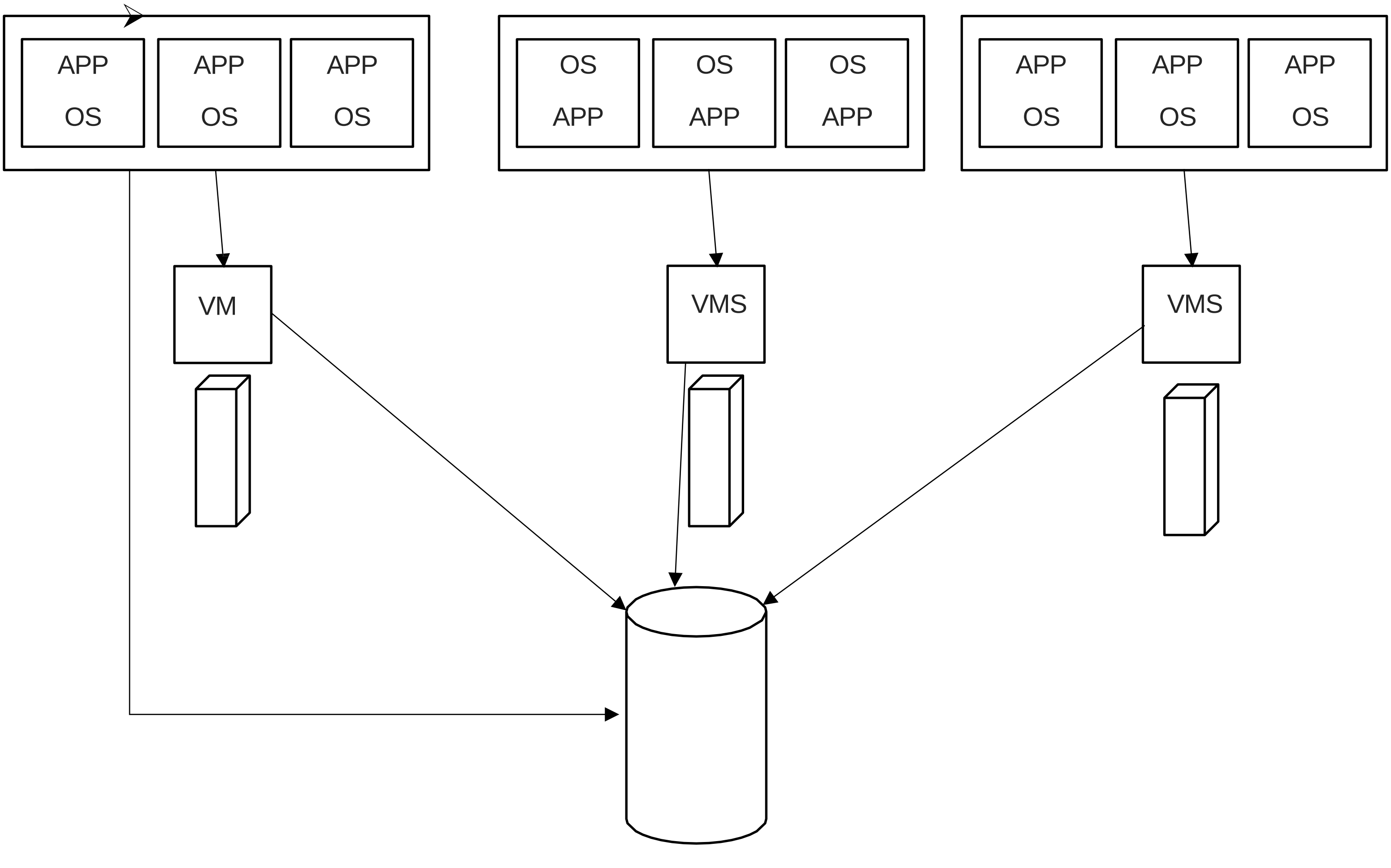
8. Isolate Application: Server virtualization provides application isolation and removes application compatibility issues by consolidating many of these virtual machines across physical server.

It allows incompatible application to run side by side, at the same time and with minimal regression testing against one another. Isolating application from the OS has security benefits as well, as the exposer of the application does automatically entail the exposure of the entire OS.

9. Extend the life of older application: by virtualizing and encapsulating the application and its environment we can extend its life, maintain uptime, and finally get rid of that old Pentium machine hidden in the data centre.

Server virtualisation:

- Server virtualization is the partitioning of physical server into smaller virtual server.
- In server virtualization the resources of the server itself are hidden from user.
- A software is uses to divide the physical server into virtual environment called virtual or physical server.
- One common usage of this tech is in web server.
- Server virtualization is also known as system virtualization.
- The software providing the virtualization is call VMM (virtual machine monitor) or hypervisor.
  - Server virtualization can also be defined as partitioning of a single physical machine into multiple execution environment each of which can host a different server. This type of virtualization is also known as consolidation.



Advantages:

1. Flexibility for non-disruptive migration.
2. Easy of management.
3. Each virtual server can also be independent.
4. Reduce cost.
5. High availability.
6. Disaster recovery.
7. Efficient utilization.

Block level virtualization:

- Block level virtualization means that storage capacity in made available to the os or the application in the form of virtual disk.
- The task of file system management in the responsibility of the os or the application.
- The task of the virtualization entity in to map these virtual blocks to the physical blocks of the real storage devices.

Meta data:

The virtualization software or device is responsible for maintaining the mapping information for the virtualized information for the virtualized storage. This mapping information is called metadata and is stored as a mapping table.

I/O redirection:

The virtualization software or device uses the meta data to re-direct I/O request. It will receive an incoming I/O request certain information about the location of the data of the logical disk (Vdisk) and translate into a new I/O request to the physical disk location.

Capabilities: capabilities are not limited to a single vender's device and are in fact possible across different vendor's devices.

Replication: replication involves sharing information so as to ensure consistency between redundant resources, such as software or hardware components to improve reliability, fault-tolerance or accessibility replication provides

- Remote data replication for DR.
- Synchronous mirroring – is an approach to data protection that involves data being written to a remote site and local disk at the same time. Each time data in written to local disk. It is also written to disk at a remote site and the write is not considered complete until confirmation is sent from the remote site applicable for shorter distance. (200kms)
- Asynchronous mirroring – same as synchronous but remote site and the write in complete before ACK from the remote site. Applicable for greater distance (>200kms).

Pooling: The physical storage resource is aggregated into storage pool, from which logical storage in created micro storage system can be added as and when needed and the virtual storage space will scale up by the same time.

Disk management:

The software providing storage virtualization becomes a common disk manager in the virtualized environment, Vdisk are created by the virtualization software or device and are mapped (made visible) to the required host or server. Enhanced features are easy to provide in this environment.

- Provisioning to maximum storage utilization
- This is relatively easy to implement.
- Disk expansion and shrinking.
- More physical storage can be allocated.
- Disk can be reduced by some physical storage.

File virtualization:

In CC, file virtualization is a field of storage virtualization operating on computer file level. It involves uniting multiple storage devices into a single logical pool of file. Network file. Network file management (NFM) in the concept of creating a virtualization layer between the clients and the file server.

NFS: It a client/server application that lets a computer as though they were on the user's own computer.

Virtual machine monitor

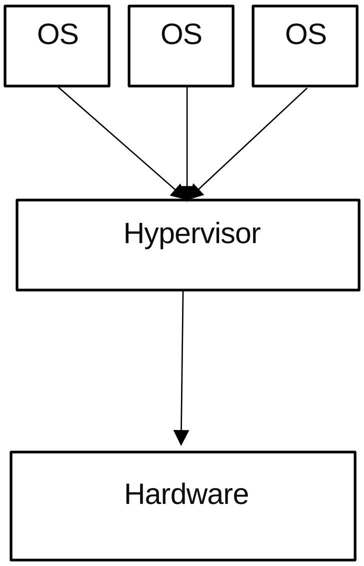
In CC hypervisor or VMM is a piece of computer software, firmware or hardware that creates and run virtual machines.

A computer on which a hypervisor is running one or more virtual machines is defined as host machine. Each virtual machine is called guest machine.

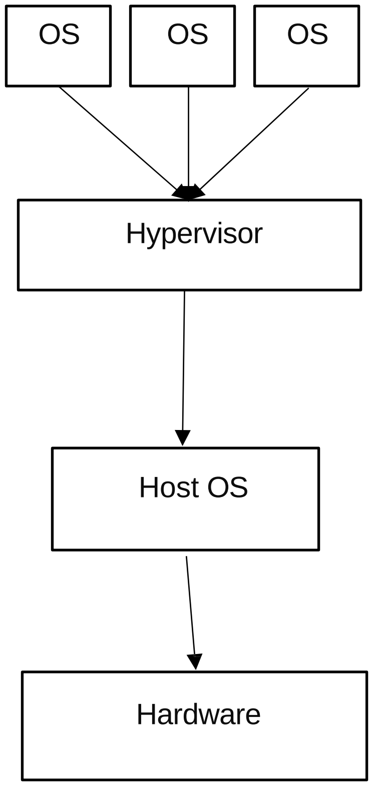
A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources such as memory and processing.

Benefits of hypervisor:

- The main benefit of running VMs is if one of them crashes, it does not affect the other virtual machines, or the main physical hardware or OS. Although they use the same physical hardware. They are logically separate from each other.
- Hypervisor used for security purpose. It creates another layer between OS and we might be downloading or accessing from the internet. Even if the download causes a problem in our virtual machine, our OS will be protected by the hypervisor.



Type – 1



Type – 2

Native or Bare metal runs directly on the hardware.

Hosted or embedded host run within and uses the host os.

There are two main types of hypervisor.

1. Native or “bane metal” hypervisor.
2. Hosted or “embedded” hypervisor.

Example: Two key example of hypervisor are

- VMware and Hyper-V

VMware owned by Dell.

Hyper-V created by Microsoft.

Both software one made for CC and virtualization and it can install a hypervisor on physical server to allow multiple VMs to runs at the same time.

Hyper – v does the same thing but can also virtualize servers. Hyper – v comes pre-installed with windows – 10 both are bane metal hypervisors. Oracle Vm, virtual Box is a hosted hypervisor.

Type – 1 hypervisor	Type – 2 hypervisor
It run directly on the host hardware to control the hardware and to manage guest OS.	It run on a conventional OS
Called a native or base metal hypervisor	Called host OS hypervisor
Runs directly on the hardware	Runs through host os

Example: VM ware, hyper – v	Oracle VM, virtual box.

Infrastructure requirements:

There are server infrastructure items required for planning for the cloud.

1. Heterogeneous system support.
2. Service management.
3. Dynamic workload and resource management.
4. Reliability, availability and security.
5. Integration with data centre management tools visibility and reporting.
6. Visibility and reporting.
7. Administrator, developer and End user interface.

1. Heterogeneous system support:

Not only should cloud management solutions leverage the talent hardware, virtualization and software solutions, but they should also support a data centres existing infrastructure cloud management provider must integrate with traditional IT systems in order to meet the requirement of data centre.

2. Service management:

A service offering is a set of services and application that user can consume through that provider. Whether the cloud in private or public service offering should include resource guarantee, resource management etc.

3. Dynamic workload and resource management:

In order for a cloud to be truly on- demand and elastic to meet consumer service. The cloud must be workload and resource aware. CC raise the level of abstraction to make all components of the data centre virtualized.

4. Reliability, availability and security:

To be fully reliable and available, the cloud needs to be able to continue to operate while data remains intact in the virtual data centre. If a failure occurs in one or more components, most cloud architectures deal with shared resource pool.

5. Integration with data centre management tools:

Many components of traditional data centre management still require some level of integration with new cloud management solution within most data centres a variety of tools are used for provisioning, customer cause, billing system management, security and much more.

6. Visibility and reporting:

Without string visibility and reporting mechanisms the management of customer service levels, system performance, compliance and billing become difficult data centre operations have the requirement of having real-time visibility and reporting capabilities within the cloud environment to ensure compliances, security, billing as well as other instruments, which requires high level of granular visibilities and reporting.

7. Administrator, Developer and End user interface:

One of the primary attributes and success of existing cloud-based services on the market comes from the fact that self – service portal and deployment model shield the complexity of the cloud service from the end user within the self – service portal consumer able to manage their own virtual data centre, create and launch templates, manage their virtual storage, compute and network resources and access image libraries to get their service up and running quickly

VLAN (VIRTUAL LAN)

A VLAN is a logical group of workstations, server and network that appear to be on the same LAN.

Computer networks can be segmented into LANs and WANs, network devices such as switches, hubs, bridges, workstations and servers connected to each other in the same network at a specific location are generally known as LANs.

A LAN is also considered a board cast domain. A VLAN allow several networks to work virtually as one LAN. One of the best beneficial elements of VLAN is that it removes latency in the network which saves network resources and increases network efficiency. VLANs are created to provide segmentation and assist in issues like security, network management and scalability. Traffic can also easily control by using VLANs.

Advantages:

- Allowing network administrator to apply additional security to network communication.
- Making expansion and relocation of a network or a network device easier.
- Providing flexibility because administration is able to configure in a centralized environment while the device might be located in different geographical location.
- Decreasing the latency and traffic load on the network and the network devices, offering increased performance.

Disadvantages:

- High risk of virus issues because on infected system may spread a virus through the whole logical network.
- Equipment limitations in very large networks because additional routers might be needed to control the workload.
- More effective at controlling latency than a WAN, but less efficient than a LAN.

VSAN (Virtual storage area network)

VSAN is primarily implemented in CC and virtualization environments.

- VSAN allows end users and organizations to provision a logical storage are network.
- The VSAN can be used to build a virtual storage pool for multiple services.
- A VSAN provides similar services and features as a SAN, but because it is virtualized, it allows for the addition and relocation of subscribers without having to change the network's physical layout.
- It also provides flexible storage capacity that can be increased or decreased over time.
- VSAN allows traffic to be isolated within specific portions of the network.
- If a problem occurs in one VSAN, that problem can be handled with a minimum of disruption to the rest of network.
- VSAN can also be configured separately and independently.

VLAN	VSAN
VLAN is a network technology used to logically separate large broadcast domain using layer 2 devices.	VSAN is a logical partition in a SAN.
It divides the network into different virtual sub-network reduces traffic and improve performance.	The use of multiple VSAN's can make a system easier to configure and scale out.
VLANs are implemented to achieve scalability, security and difficult of network management	VSAN allow traffic to be isolated within specific portions of a SAN
VLANs can quickly adopt to change in network requirement and relocations of workstations and server node	In this subscriber can be added or relocated without the need for changing the physical layout.
Improve the performance of a network	VSANs minimizes vulnerability security in improvement

Unit – 6

Cloud security

Cloud security fundamental:

Cloud security in defending the confidentiality, integrity and availability of assets (data, application, infrastructure), using cloud services, from outside or inside threat.

Security in cloud computing in a major concern, data in cloud should be stored in encrypted from, to restrict client from direct accessing the shaved data, proxy and brokerage services should be employed.

Since all the data in transferred using internet data security in of a major concern in cloud. Here is the key mechanism for protecting data.

- Access control
- Auditing
- Authentication
- Authorization.

Security concern of CC: top 10 security concerns for cloud-based services.

1. Where in the data?
2. Who has access?
3. What are your regulatory requirements?
4. Do you have the right to audit?
5. What type of training does the providing offer their employees?
6. What type of data classification system does the provider use?
7. What are the service level agreement (SCA) terms?
8. What is the long-term ability to work successfully of the provider?
9. What is the disaster recovery/business continuity plan (DR/BCP)?

Cloud security services:

- Authentication
- Authorization
- Auditing

Authentication: authentication is the testing of a user's identity. The computer system authenticates the user by verifying the password.

Authorization: authorization refers to rights and privileges granted to an individual or process that enable access to computer resources and information once authentication established then user permitted to access a resource.

[Authentication confirms that users are who they say that are.

Authorization gives those users permission to access a resource.]

Auditing: these are two basic method of auditing in CC:

1. System audit: system audit is a one-time or periodic event to evaluate security.
2. Monitoring: monitoring refers to an ongoing activity that examines either the system or users such as displacement detection.

Its auditors are two types,

- Internal auditor: work for given organisation.
- External auditor: are certified public account (CPAs)

Its auditors typically audit the following functions.

- System and transaction controls.
- System development standards.
- Backup control
- Data library procedure

- Data centre security

An audit log is a set of records that provide documentary evidence of processing. Audit logs should record the following.

- The transactions data and time.
- Who processed the transaction?
- At which terminal the transaction was processed.
- Various security events relating to the transaction.

In addition, an auditor should examine the audit long for the following:

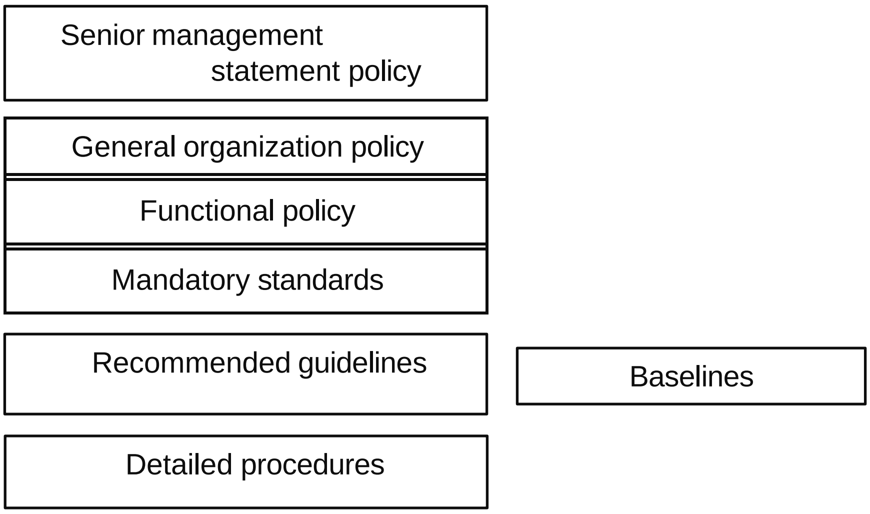
- Amendments to production jobs.
- Production job returns.
- Computer operator practices
- All commands directly initiated by the user.
- All identification and authentication attempts.
- Files and resources accessed.

Design principles:

The security design principal is considered while designing any security mechanism for a system. These principals are review to develop a secure system which prevents the security flows and also prevents unwanted access to the system. The following security design principles

- **Least privilege:** it means that you ensure people only have enough access that they need to do their jobs. This approach reduces the opportunity for unauthorized access to sensitive information.
- **Separation of duties:** This is different from the concept of least privilege. While that focuses on moving sense that people only have the privileges, they need to do their job, making secure their job is not too big. When someone does too big job, need lots of permissions to do that job.
- **Defense in depth:** It is about preventing access to the System Defense in the application of multiple layers of protection where is subsequent layer will provide protection if a previous layer in breached.
- **Fail safe:** fail safe means that if a cloud system fails it should fail to a state in which the security of the system and its data are not compromised.
- **Economy of mechanism:** It promotes simple and comprehensible design and implementation of protection mechanism, so that not planned access path do not exist or can be readily identified and eliminated.
- **Complete mediation:** In complete mediation, every request undergoes a valid and effective authorization procedure. Complete mediation involves the following:
  - Identification of the entity making the access request.
  - Verification that the request has not changed since its initiation.
  - Application of the appropriate authorization procedures.

    - Re-examination of previously authorized requests by the same entity.
- **Open design:** This security principal suggest that the security mechanism design should be open to the public. The encryption key in kept secret while the encryption algorithm in opened for a public investigation.
- **Least common mechanism:** This principal state that a minimum number of protection mechanisms should be common to multiple users, as shared access least common mechanism promotes the last possible sharing of common security mechanism.
- **Psychological acceptability:** It refers to the difficulty of use and ability to knew the user interface that controls and interacts with the cloud access control mechanisms.
- **Weakest link:** The security of a cloud system is only as good as its weakest component; thus, it is important to identify the weakest mechanisms in the security chain and layers of Defense and improve them.
- **Leveraging existing components:** The security mechanism of a cloud implementation might not be configured properly or used to their maximum capability, reviewing the state and setting of the extant security mechanism and ensuring that they are operating at their optimum design points will greatly improve that security.
- **Secure cloud software requirements**
  The requirement for secure cloud software is concerned with non-functional issues such as minimizing, eliminating, vulnerabilities and ensuring that the software will perform as required, even under attack.
  Software requirements in the process of determining customer software expectations and needs.
- **Policy Implementation:** a policy is one of those terms that can mean several things. Cloud policies are the guidelines under which companies operate in the cloud. Often implemented in order to ensure the integrity and privacy of company owned information cloud policies can also be used for financial management, cost optimization, performance management, and network security.



Senior management statement policy

General organization policy

Functional policy

Mandatory standards

Recommended guidelines

Baselines

Detailed procedures

Policy types

Senior management statement of policy:

- This policy in the first policy of any policy creation process.
- This is general, high level policy that acknowledges the importance of computing resources to the business model.
- It states supports for information security throughout the enterprise and commits to authorizing.

Regulatory policy:

- It is a security policy.
- An organization must implement due to compliances regulation or other legal requirements.

Advisory policy:

- It is a security policy that are not mandated but strongly suggested, perhaps with serious consequences defined for failure (such as termination, a job action warning.)

Informative policies:

- These policies exist simply to inform the reader.
- There are not implied or specified requirements.

Cloud computing security challenges:

When an organization consuming cloud services and especially public cloud services, much of the computing system infrastructure will now be under the control of third-party cloud services provider (CSP) some general management processes will be required.

Security policy implementation:

Security policies are the foundation of a sound security implementation.

Computer intrusion detection and response:

Response includes notifying the appropriate parties to take action in order to determine the extent of an incidents fact and to remediate the incident effects.

Virtualization security management:

Virtualization security: virtualized security or security virtualization, refers to security solutions that are software based and designed to work within a virtualized IT environment. This differs from traditional hardware-based network security, which is static and runs on devices such as firewalls, routers and switches.

How does virtualized security work?

Virtualized security can take the functions of traditional security hardware application (such as firewall and antivirus protection) and deploy them via software. In additional security functions. These functions are only possible dare to the advantages of virtualization.

Some common management solutions to threats.

The virtual machine (VM), virtual memory management (VMM) and hypervisor or host os are the minimum set of components needed in a virtual environment.

Virtual threats:

Shared clipboard:

Shared clipboard technology allows data to transferred between VMs and the host, providing a means of moving data between malicious programs in VMs of different security realms.

Keystroke logging:

Creating records of everything you type on a computer or mobile keyboard. These are used to quietly monitor your computer activity while you use your devices as normal.

Keyloggers are software or hardware devices that tracks the activities of keyboard. Keylogger software store your keystrokes in a small file, which in either accessed later or automatically emailed to the person monitoring you action.

VM monitoring from the host:

Because all network packets coming from or going to a VM pass through the host, the host may be able to affect the VM by the following

- Starting, stopping, passing and restart VMs.

Virtual machine monitoring from another VM:

If the VM platform uses a virtual hub or switch to connect the VMs to the host, then intruders as “ARP positioning” (Address resolution protocol) to redirect packets going to from the other VM for sniffing. (Sniffing in a process of monitoring and capturing all data pkts. Passing through given network.)

Virtual machine backdoors:

A backdoor cover communications channel between the guest and host could allow intruders to perform potentially dangerous operations.