

Raja Mushtaq: +923055868956

CS435 Final Term Handouts Highlighted By VU-Gateway

Imp Mcqs + Question Highlighted and explain

❖ **CS435 Final Preparation Video Part A:**

https://youtu.be/sA3ASVZYgZM?si=oymSpxYGFX107N_p

❖ **CS435 Final Preparation Video Part B:**

<https://youtu.be/javSLA4k6Js?si=fkYVu9BvSQ4NbdE>

Join VU-Gateway Whatsapp Group For Imp highlighted Handouts, Notes, Files, Notification and preparation:

<https://chat.whatsapp.com/GecIrau2Nit0D4F5DjDiGM>

Module No – 116: Resource Cluster Mechanism:

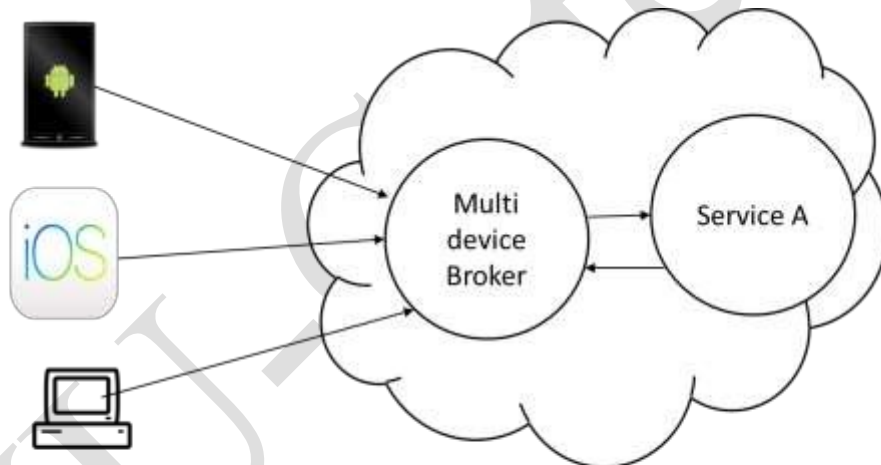
- The Cloud promises virtually unlimited IT resources.
- These IT resources are (although virtualized) but can not be provided through a single physical server.
- It is obvious that the Cloud IT resources are provisioned from multiple physical servers located in a single or multiple data center/s.
- The resource cluster mechanism is used to group multiple IT resources so that they can be used as a single IT resource.
- This increases the computing capacity, load balancing capacity and availability of the clustered IT resources.
- High speed communication links are used to connect the clustered IT resources for:
 - Workload distribution
 - Task scheduling
 - Data sharing
 - System synchronization
- Server clusters may or may not have a shared storage.
- Common types:
 - *Server Cluster*: Consisting of physical or virtual servers. The virtualized clusters support the migration of VMs for scaling and load balancing.

- **Database Cluster:** Is used to keep redundant implementation of databases. It has features to synchronize the data across all the redundant instances.
 - Useful for active-active and active-passive failover systems.
- **Large Dataset Clusters:** This type of cluster is used to partition and distribute large datasets without affecting the data integrity or computing accuracy.
 - Each node processes workloads without any need to depend/communicate with other nodes.
- Additional types:
 - **Load Balanced Cluster:** Implements a load balancer mechanism (discussed before).
 - **HA Cluster:** Implements a failover system (discussed before).

Module No – 117:

Multi-Device Broker: This mechanism is used to transform the messages (received from heterogeneous devices of Cloud consumers) into a standard format before conveying them to the Cloud service.

- The response messages from Cloud service are intercepted and transformed back to the device specific format before conveying to the devices through the multi-device broker mechanism.



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

[This Photo](#) by Unknown Author is licensed under [CC BY](#)

Follow the video lecture to understand fully

- **State Management Database:** It is a device used to temporarily store the state data of software programs.
 - State data can be (for example) the configuration and number of VMs being employed to support a user subscription to a PaaS instance.
 - In this way, the programs do not use the RAM for state-caching purposes and thus the amount of memory consumed is lowered.

like application or software hai
hoti hn apny just work krna hota hn

- The services can then be in a “stateless” condition.
- For example, a PaaS instance (ready-made environment) requires three VMs. If user pauses activity, the state data is saved in state management software and the underlying infrastructure is scaled in to a single VM.
- When the user resumes the activity, the state is restored by scaling out on the basis of data retrieved from state management database.

Lesson No. 25

CLOUD MANAGEMENT

Module No – 118: Remote Administration System

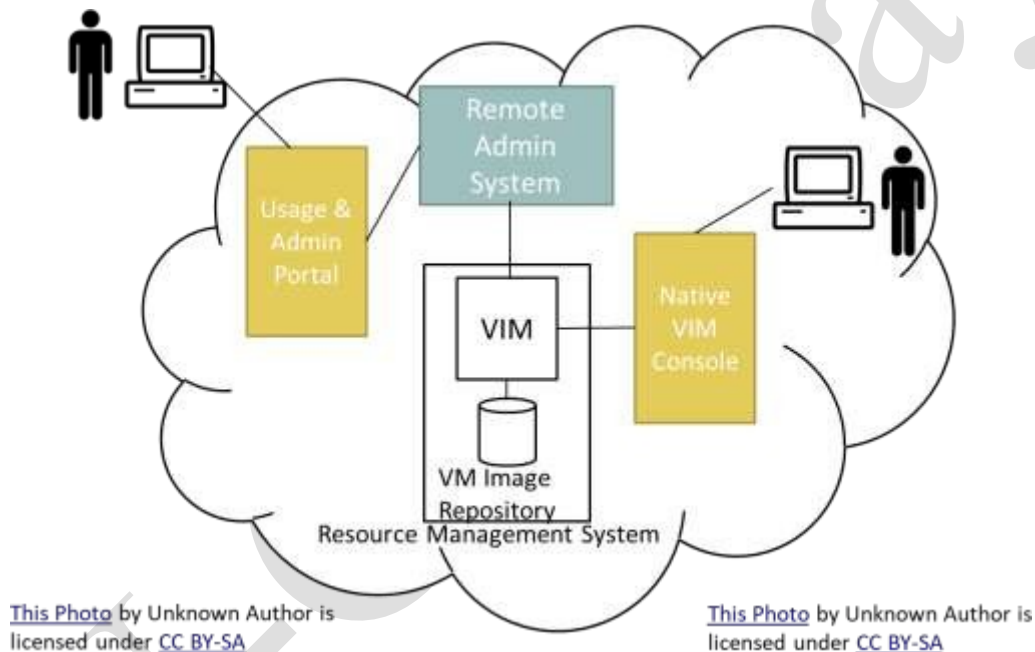
- It is a Cloud mechanism which provides the APIs and tools to the providers to develop and used online portals.
- These portals also provide some administrative controls to the Cloud consumers as well.
- Usage and Administration Portal:
 - Management controlling of Cloud IT resources
 - IT resources usage reports
- Self-Service Portal:
 - The consumer can look at and choose various Cloud services
 - The chosen services/package is submitted to Cloud provider for automated provisioning
- The remote administration console can be used to:
 - Configure and setting cloud services
 - Provision and releasing IT resources for on-demand usage
 - Monitor cloud service status, usage and performance
 - QoS and SLA fulfillment monitoring
 - IT-resource leasing cost and usage fee management
 - Managing user accounts, security credentials, authorization and access control
 - The remote administration console can be used to:
 - Capacity planning
- If allowed, a Cloud consumer can create its own front-end application using API calls of remote administration system.

Module No – 119: Resources Management System

- Utilizes the virtual infrastructure manager (VIM) for creating and managing the virtual IT resources.
- Typical tasks include:
 - Managing the templates used to initialize the VMs
 - Allocating and releasing the virtual IT resources
 - Starting, pausing, resuming and termination of virtual IT resources in response to allocation/release of these resources

Raja Mushtaq: +923055868956

- Coordination of IT resources for resource replication, load balancer and failover system
- Implementation of usage and security policies for a Cloud service
- Monitoring the operational conditions of IT resources
- These tasks can be accessed by the cloud resource administrators (personnel) employed by the cloud provider or cloud consumer.
- The provider (and/or the administrator staff of provider) can access the resource management directly through native VIM console.
- The consumer (and/or administrator staff of the consumer) use the remote administration system(created by the provider and) based upon API calls of resource management system.



Resource Management in Cloud

Module No – 120: SLA & Billing Management Systems

- The SLA management system provides features for management and monitoring of SLA.
- Uses a monitoring agent to collect the SLA data on the basis of predefined metrics.
- The SLA monitoring agent periodically pings the service to evaluate the “down” time if occurs. apka system slow work krna start krta hn tu down time start hot hn forran sy Ping create kr syta hen
- The collected data is made available to the usage and administrative portals so that an external and/or internal administrator can access the data for querying and reporting purposes.
- The SLA metrics monitored are in accordance with the SLA agreement.
- The billing management system collects and processes the data related to service usage.
- This data is used to generate consumer invoice and for accounting purposes provider.

- The pay-as-you-go type of billing specifically require the usage data.
- The billing management system can cater for different pricing (pay-per-use, flat rate, per allocation etc.) models as well as custom pricing models.
- Billing arrangement can be pre-usage or post-usage.

Lesson No. 26

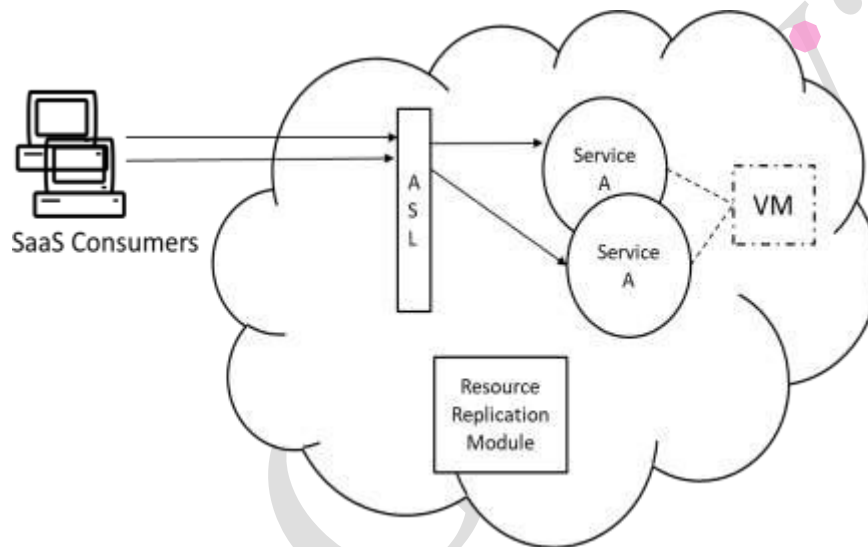
FUNDAMENTAL CLOUD ARCHITECTURES

Module No – 121: Resource Pooling Architecture

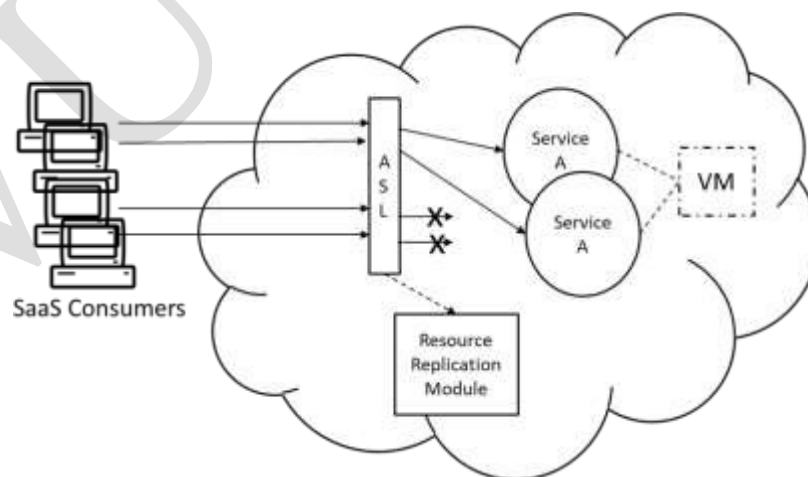
- It is based upon using one or more resource pool in which identical IT resources are grouped and maintained automatically by a system which also ensures that the resource pools remain synchronized.
- A few examples of resources pools are as follows:
 - Physical server pools consisting of (ready to use) networked servers with installed OS and other tools.
 - VM (virtual server) pool/s configured by using one or more templates selected by the consumer during provisioning.
 - Cloud storage pools consisting of file/block based storage structures.
 - Network pools consist of different (preconfigured) network connecting devices that are created for redundant connectivity, load balancing and link aggregation.
 - CPU pools are ready to be allocated to VMs by the multiple of single core.
 - Dedicated pools can be created for each type of IT resources.
 - Individual resource pools can become sub-groups into larger pool.
 - A resource pool can be divided into sibling pools as well as nested pools.
 - Sibling pools are independent and isolated from each other. May have different types of IT resources.
 - Nested pools are drawn from a bigger pool and consist of the same types of IT resources as are present in the parent pool.
- Resource pools created for different consumers are isolated from each other.
- The additional mechanisms associated with resource pooling are:
 - Audit monitor: Tracks the credentials of consumers when they login for IT resource usage.
 - Cloud Usage Monitor
 - Hypervisor
 - Logical Network Perimeter
 - Pay-Per-Use Monitor
 - Remote Administration System
 - Resource Management System
 - Resource Replication

Module No – 122: Dynamic Scalability Architecture:

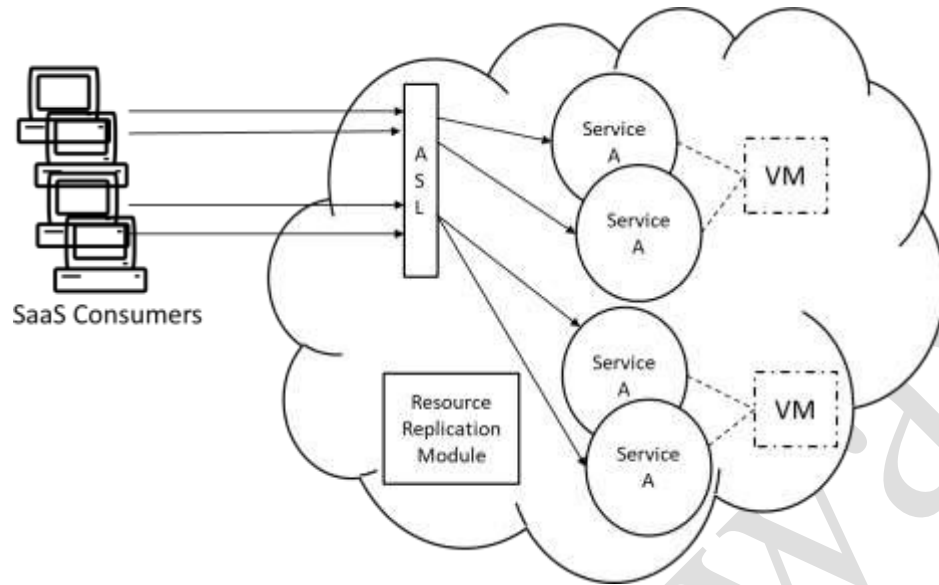
- Dynamic scalability is provided through dynamic allocation of available resources from the resource pool. Allocation ho rae hoti hen diff dynamic resources ki from resource pool
- Scaling can be horizontal & vertical and can also be through dynamic relocation. Scaling (considered in this topic) is preconfigured and according to some preset thresholds.
- To implement this architecture, the automated scaling listener (ASL) and Resource Replication Mechanism are utilized.
- Cloud usage monitor and pay-per-use monitor can complement this architecture for monitoring and billing purposes.



Dynamic Scalability Architecture



Dynamic Scalability Architecture



Dynamic Scalability Architecture

Module No – 123:

- **Workload Distribution Architecture:** The workload distribution is required to prevent the following scenarios:
 - Over-utilization of IT resources to prevent the loss in performance.
 - Under-utilization of IT resources to prevent the over expenditure.
 - The workload is distributed on the basis of a load balancing algorithm with the scope/s of VMs, Cloud storage devices and cloud services.
 - Accompanied by the following mechanisms:
 - Audit monitor
 - Cloud usage monitor
 - Logical network perimeter
 - Resource cluster
 - Resource replication
- **Service Load Balancing Architecture:** This architecture specifically is used for workload distribution for Cloud services. specifically use kia jata hn Workload distribution cloud services ky liye
 - Multiple instances of the Cloud services are deployed with load balancing system.
 - The load balancer can be either deployed as an external module.
 - Alternatively the load balancer can be integrated into the Cloud service. In this case, one of the redundant instances of a service becomes the master or workload distributor to dynamically allocate the workload among service instances.
 - The following modules are additionally required:
 - Cloud usage monitor
 - Resource cluster (with active-active failover system configuration)
 - Resource replication

Module No – 124: Elastic Disk Provisioning Architecture

- Cloud costing model for disk storage may charge on the basis of total volume of allocated storage space instead of total space used.
- The elastic disk provisioning architecture implements a dynamic storage provisioning based billing.
- The user is charged only for the consumed storage.
- The technique of thin-provisioning of storage is used.
- Thin-provisioning allocates the storage space dynamically for the VM's storage.
- Requires some extra overhead when more storage space is to be allocated.
- The thin-provisioning software is required to be installed on VMs to coordinate the thin-provisioning process with the hypervisor.
- Requires the implementation of:
 - Cloud usage monitor
 - Resource replication module (for converting thin-provisioning into thick or static disk storage)
 - Pay-per use monitor tracks and reports the granular billing related to disk usage.
- In order to avoid data loss and service unavailability due to disk failure, redundant storage is applied.
- Additionally, in case of network failure, the disruptions in Cloud services can be avoided through redundant storage incident.
- This is part of failover system (active-passive).
- The primary and secondary storage are synchronized so that in case of a disaster, the secondary storage can be activated.
- A storage device gateway (part of failover system) diverts the Cloud consumers' requests to secondary storage device whenever the primary storage device fails.
- The primary and secondary storage locations may be geographically apart (for disaster recovery) with a (possibly leased) network connection among the two sites.

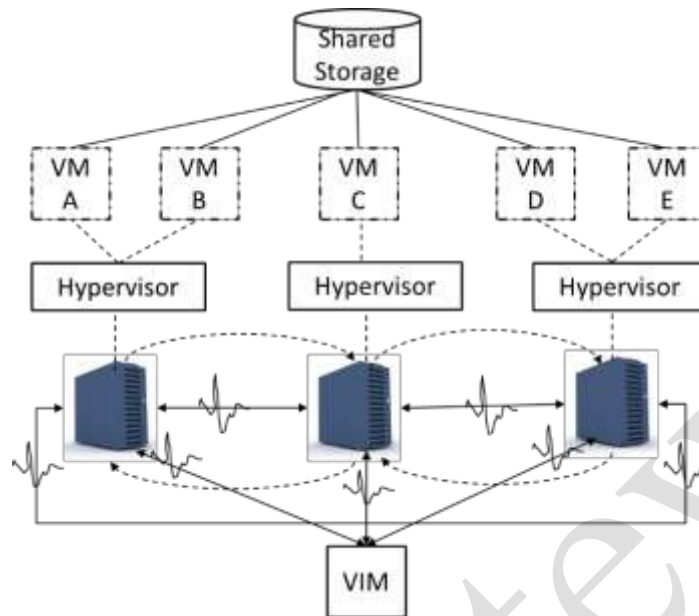
Lesson No. 27

ADVANCED CLOUD ARCHITECTURES

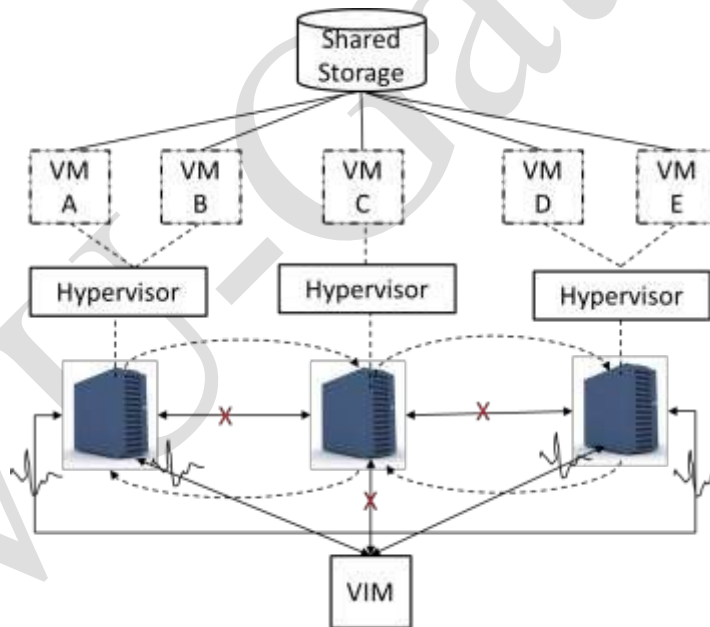
Module No – 125: Hypervisor Clustering Architecture:

- VMs hosted on a physical server are managed by hypervisor.
- The failure of the physical server cripples the hypervisor and therefore the hosted VMs also become unavailable.
- The hypervisor clustering creates a high-availability cluster across multiple physical servers.
- The hypervisor cluster operations such as live VM migration and heartbeat message exchange with hypervisors, are controlled by VIM (virtual infrastructure manager) module.
- The hypervisor cluster uses a shared storage to support a prompt live-migration of VMs.
- The additional modules to be implemented with hypervisor clustering architecture are:
 - Logical network perimeter (to create logical boundary of each hypervisor cluster).

- Resource replication module

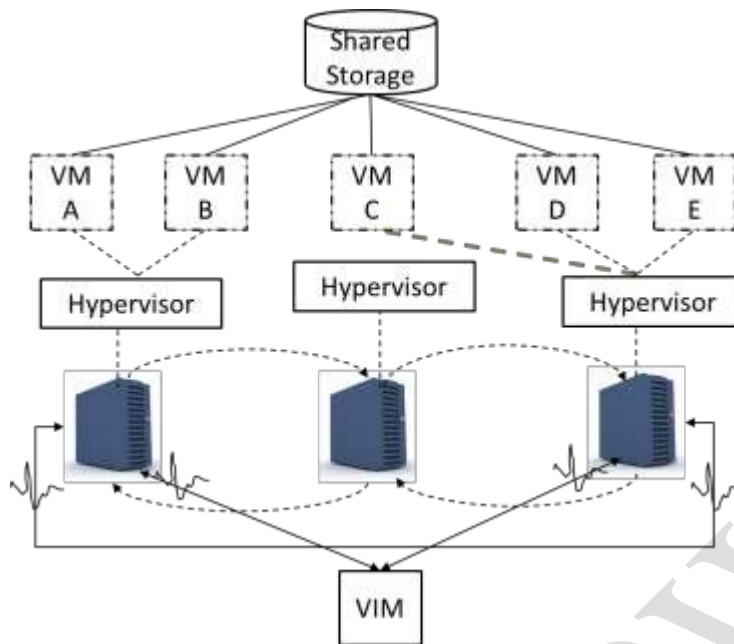


Follow the video lecture to understand fully

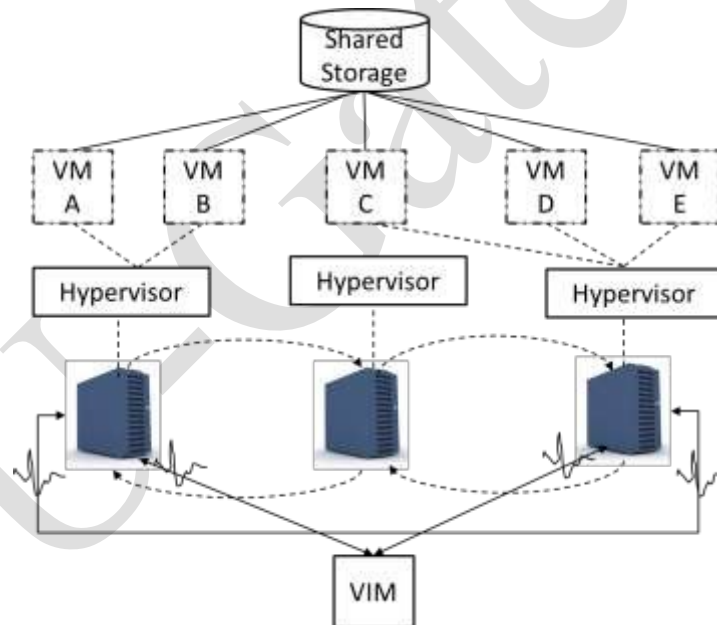


Follow the video lecture to understand fully

Raja Mushtaq: +923055868956



Follow the video lecture to understand fully



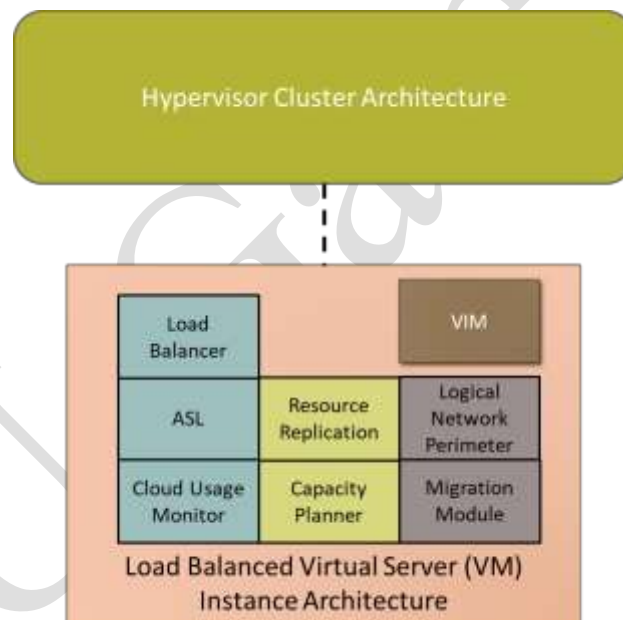
Follow the video lecture to understand fully

Module No – 126: Load Balanced Virtual Server/VM Instances Architecture:

- It balances the physical server utilization through VM migration in the hypervisor cluster architecture.
- Avoids over/under utilization of physical servers.

esy rukh dyta hn physical server so that mazed prob create nah kr sky jb fail ho jata hen wo

- Maintains performance of services hosted on VMs.
- Implements a capacity watchdog/monitor system consisting of:
 - Cloud usage monitor
 - Live VM migration module
 - Capacity planner
- The cloud usage monitor tracks the usage of physical server and VMs hosted on that server. In case of fluctuation in usage, it reports to capacity planner module.
- The capacity planner modules dynamically matches the capacities of physical servers and the resource demands of hosted VMs.
- If any VM is facing resource shortage then the capacity planner initiates the VM migration to the suitable server with sufficient capacity.
- The following modules are integrated into this architecture:
- Automated scaling listener (for monitoring workload over VMs) and load balancer
- Logical network perimeter to comply with privacy requirements of SLA
- Resource replication for load balancing



Load Balanced Virtual Server/VM Instances Architecture

Module No – 127: Non-Disruptive Service Relocation Architecture:

- A Cloud service may become disruptive/unavailable/down due to:
 - Over burden of processing load
 - Scheduled updates
- The requests of service consumers are not processed during the time of unavailability.
- By using the specialized Cloud architectures, the non-disruptive service relocation architecture can be implemented.

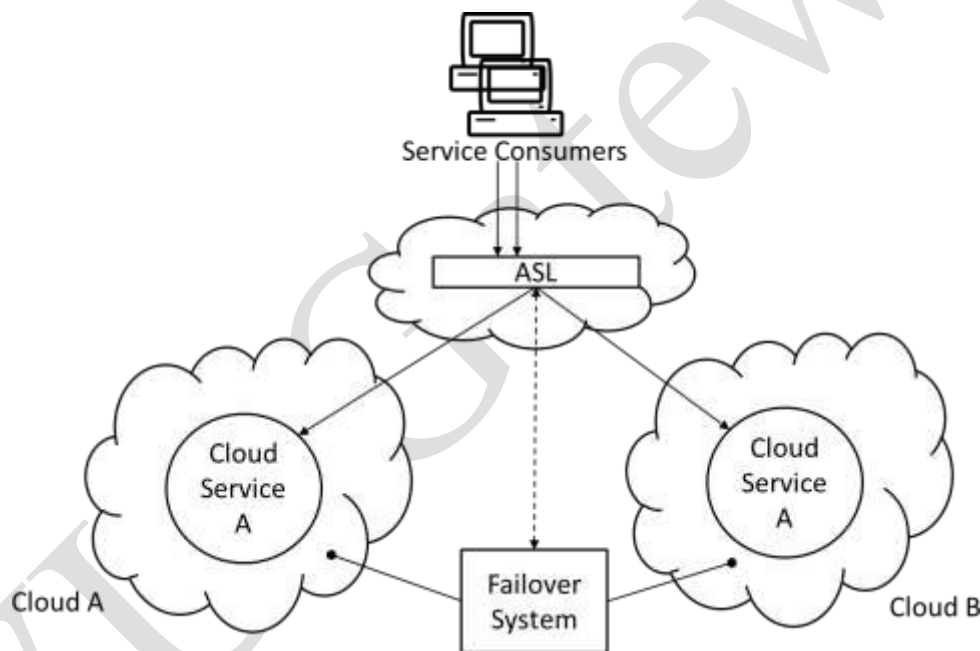
jb service use krna chhta hn us ky liye wo request bhjta hn but mean time failiure ho chuka hn har service unavailable ho gae hri request kabhi bhi proceed ni hoti

- Either the duplication of cloud service or service migration is used to provide a non-disruptiveness in service.
- By using the specialized Cloud architectures, the non-disruptive service relocation architecture can be implemented.
- Either the duplication of cloud service or service migration is used to provide a non-disruptiveness in service.
- In service-duplication implementation, the service run-time is temporarily replicated to another location and then synchronized with the primary deployment.
- The consumers' requests are diverted to the temporary deployment and then the primary deployment is made unavailable for maintenance.
- In case of migration of service to another location (such as on the indication of automated scaling listener), then it is a permanent relocation. Means, the temporary duplicate copy is not made. services ki aik jaga sy 2sri jaga ky jaty hn usy hum permanent relocation provide kr dyty hn temporary services jo kaam krty hn wo copy ni generate kr skti tu y jb automated scalling ko use krty hn yh migrate kr dy ga permanenr es ny temporary ni bny diya usy hataa diyaa
- The service hosting VM's migration procedure depends upon the fact that the VM storage is hosted on shared or local physical server storage is used.
- In later case a replicated copy of to-be-migrated VM is made on the destination server and then powered-on, the consumers' requests are redirected to the duplicated instance through load balancer module. After that, the original VM is deactivated.
- In formal case, the above procedure is not required if the destination server can also access the same shared storage.
- The following are the important modules for the implementation:
 - Automated Scaling Listener
 - Load balancer
 - Hypervisors
 - VMs
 - Cloud storage device
- The additional modules are:
 - Cloud usage monitor
 - Pay per use monitor
 - Resource replication
 - SLA management system
 - SLA monitor

Module No – 128: Zero Downtime Architecture

- The failure of the physical server results in the unavailability of VMs hosted on that server.
- The services deployed over the unavailable VMs are obviously disrupted.
- The Zero downtime architecture implements a failover system through which the VMs (from the failed physical server) are dynamically shifted to another physical server without any interruption. Ques: wo kia chez hn jis ki help sy VM ko shift kr skty hn 2sry physical server py without any interruption????????????? ANs: Zero downtime architecture
- The VMs are required to be stored on a shared storage.
- The additional modules required may include:
 - Cloud usage monitor
 - Logical network perimeter

- Resource cluster group (containing active-active clusters to assure high availability of IT-resources for VM)
- Resource replication
- **Cloud Balancing Architecture:** It is the implementation of failover system across multiple clouds.
 - It improves/increases the following features:
 - Performance and scalability of IT-resources
 - Availability and reliability of IT resources
 - Load balancing
 - Requires an automated scaling listener and failover system.
 - The automated scaling listener redirects the requests of service consumers towards multi-cloud redundant implementations of service instances based on on-going scaling and performance requirements.
 - The failover system (detects any failure/s and) coordinates with automated scaling listener with information regarding the extent of failure so that the automated scaling listener can adjust the relaying of consumers' requests accordingly.



Cloud Balancing Architecture

Module No – 129: Resource Reservation Architecture:

- A situation of *resource constraint* may arise when two or more Cloud-consumers (sharing some IT-resources such as a resource pool) experience a performance loss when the runtime resource demand exceeds the capacity of the provided resources.
- Resource constraint situation may also arise for the IT-resources not configured for sharing such as nested and/or sibling pools when one pool *borrow*s the resources from the other

pool. The lending pool may create resource constraints for its consumers later on if the borrowed resources are not returned sooner.

- If each consumer can be assured the availability of a minimum volume of:
 - Single IT resource
 - Portion of an IT resource
 - Multiple IT resources
 - Then this implements a resource reservation architecture.
- In case of implementation for resource pools, the reservation system must assure that each pool maintains a certain volume of resource/s in *unborrowable* form.
- The resource management system mechanism (studied earlier) can be utilized for resource reservation.
- The resource/s volume in a pool or the capacity of a single IT resource which exceeds the reservation threshold can be shared among the consumers.
- The resource management system manages the borrowing of IT resources across multiple resource pools.
- The additional modules that can be implemented are:
 - Cloud usage monitor
 - Logical network perimeter (for resource borrowing boundary)
 - Resource replication (just in case new IT resources are to be generated)

Module No – 130: Dynamic Failure Detection and Recovery Architecture

cloud environment ko use kr ky hum detect kr skty hn failure kha hn or failure ko recover kr skty hen

- It may be possible to detect and counter some failures in Cloud environment if there is an automated system with failure diagnosis and solution selection intelligence.
- This architecture establishes a resilient watchdog/module containing the definitions of pre-marked events and the runtime logic to select the best (predefined) routine to cope with those events.
- The resilient module generates alarms/reports the events which are not predefined.
- The resilient watchdog module performs the following five core functions:
 - Monitoring
 - Identifying an event
 - Executing the reactive routine/s
 - Reporting
- This architecture allows the implementation of an automated recovery policy consisting of predefined steps and may involve actions such as:
 - Running a script
 - Sending a message
 - Restarting services
- Can be integrated into a failover system along with SLA management system.

Module No – 131: Bare-Metal Provisioning Architecture:

Raja Mushtaq: +923055868956

- This architecture implements the provisioning of bare-metal servers on demand.
- These servers do not have an OS or hypervisor installed when the provisioning process is initiated.
- Therefore these servers are required to contain some mechanism to be accessed through a remote management console to install OS/hypervisor.
- This functionality is either built-in into ROM, contained in the chipset or through an expansion slot.
- These can be accessed through remote administration system through web.
- The IP address of the physical server is required for connectivity.
- The IP address can be configured manually or through DHCP service.
- The bare-metal provisioning can be automated to avoid manual deployment errors and time delays in OS/hypervisor deployment through remote management system.
- The automated bare-metal provisioning allows the consumers to obtain multiple servers by using the management software.
- The automated bare-metal provisioning is centrally controlled.
- The controlling software connects with the server management software for OS installation.
- Following are the steps:
 - Consumer connects to central software through self-service portal.
 - The available servers are shown.
 - The consumer chooses the server and the OS to be installed.
- The resource management system (studied before) is used to install the required chosen OS.
- The consumer starts using the provisioned server.

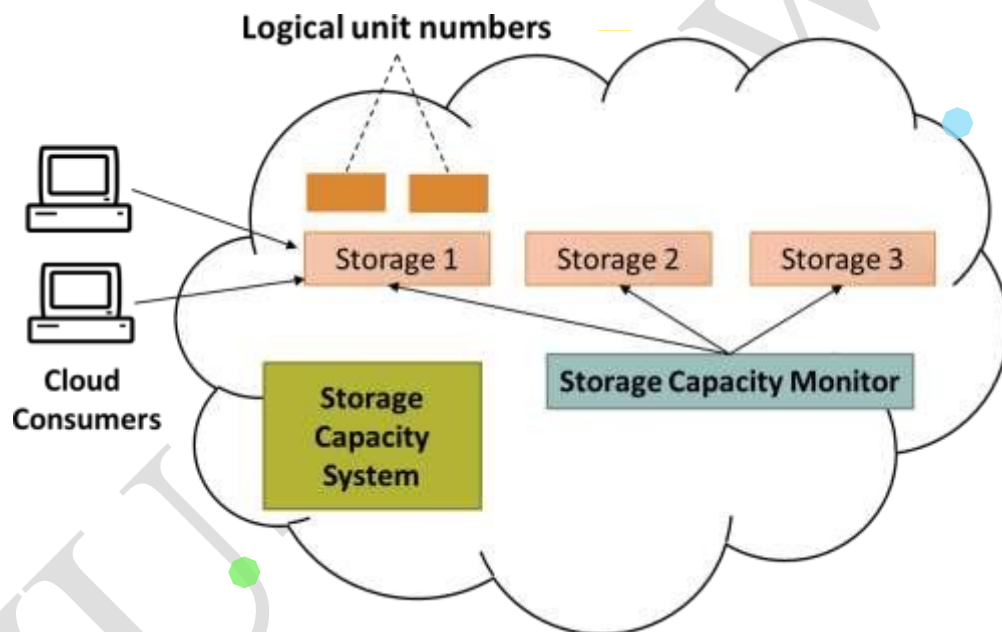
Module No – 132: Rapid Provisioning Architecture:

- The provisioning Cloud IT-resources can be automated to save time, reduce human related errors and to increase the throughput.
- For example a consumer can initiate the automated provisioning of 50 VMs simultaneously instead of waiting for one VM at a time.
- The rapid provisioning architecture has a (centralized) control module complemented by:
 - Server templates
 - Server images (for bare-metal provisioning)
 - Applications and PaaS packages (software and applications & environments)
- OS and Application baselines (configuration templates applied after installation of OS and applications)
- Customized scripts and management modules for smooth procedures
- The following steps can be visualized during the automated rapid provisioning:
 - A consumer chooses a VM package through self-service portal and submits the provisioning request.
 - The centralized provisioning module selects an available VM and initiates it through a suitable template.
 - Upon initiation, the baseline/s templates are applied.
 - The VM is ready to use now.

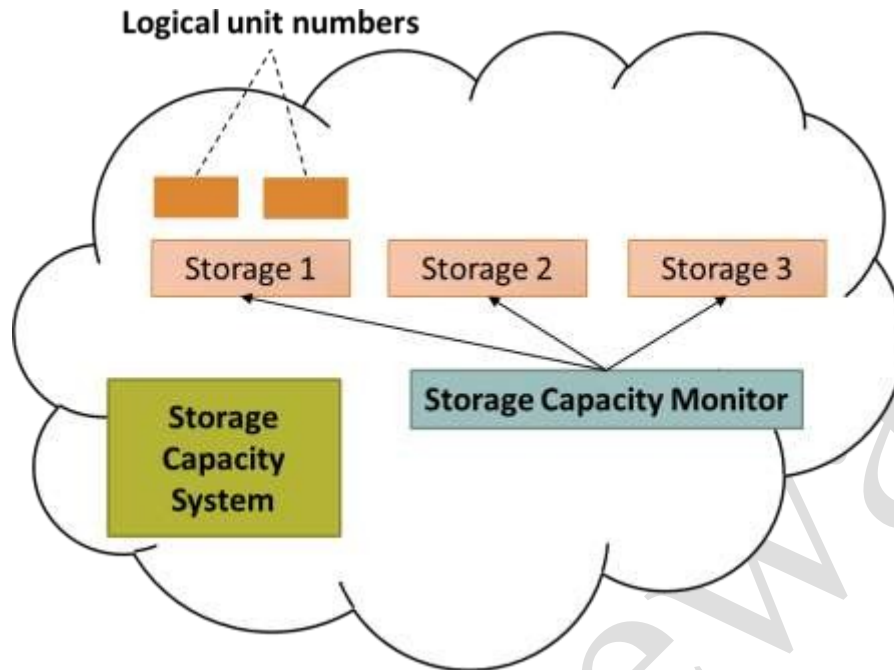
Module No – 133: Storage Workload Management Architecture:

Logical Unit Number jo hn logical drive hen btati hn ku physical derive ky kitny part hn

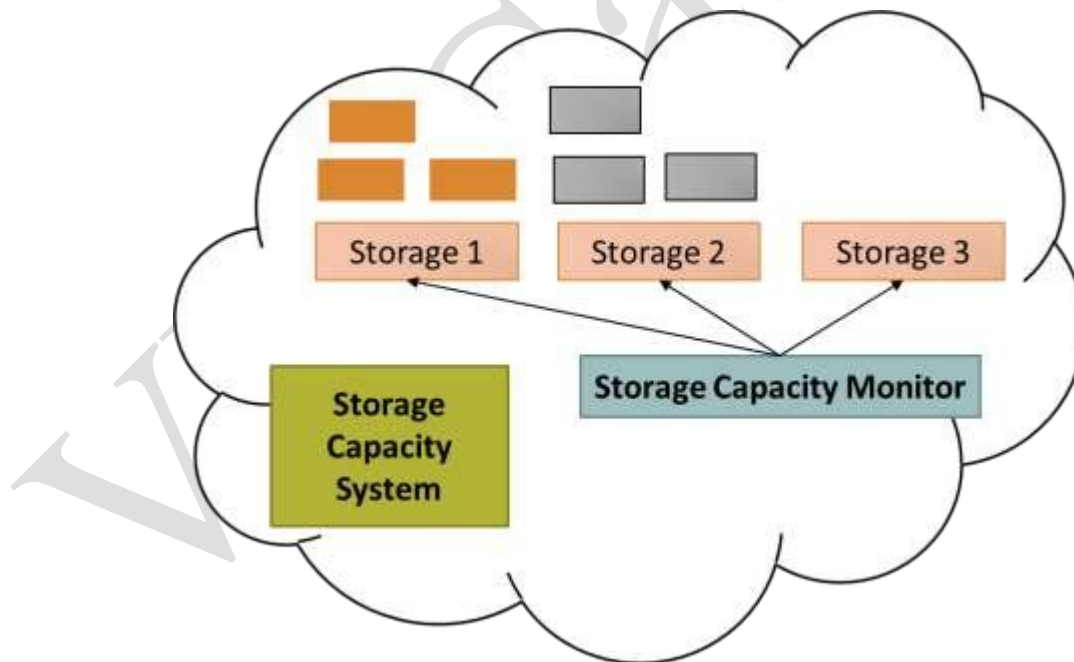
- Logical Unit Number is a logical drive that represents a partition of a physical drive.
- The storage workload management architecture ensures the even distribution of all logical-unit-numbers across the Cloud storage devices.
- The even distribution of logical unit numbers is done through implementation of a storage capacity system and a storage monitoring module.
- The storage capacity monitoring module highlights the overburden storage device.
- The storage capacity system evenly distributes the logical-unit-number drives.
 - Additional modules:
 - Cloud usage monitor
 - Load balancer
 - Logical network perimeter



Initial distribution of logical unit numbers across the Cloud storage devices.

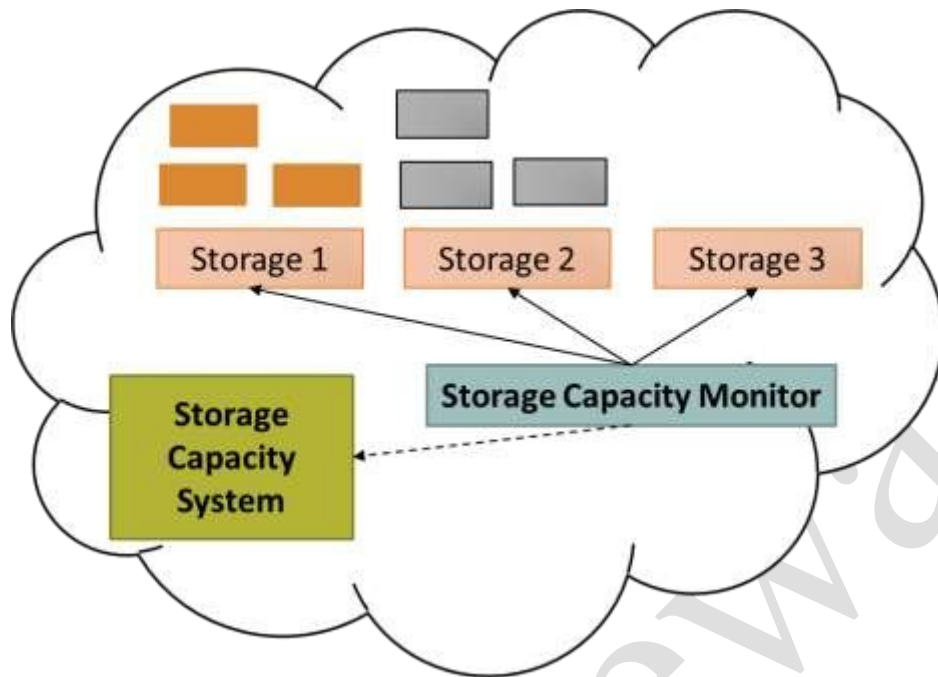


Storage capacity monitoring module checks each storage device.

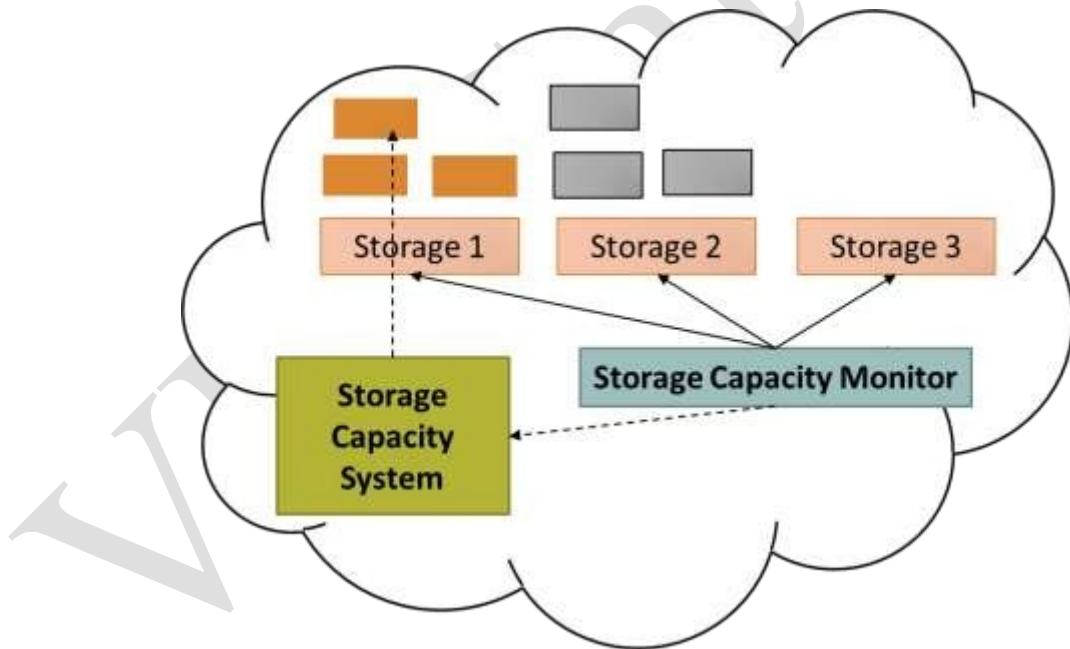


Storage capacity monitoring module highlights the overburden storage device

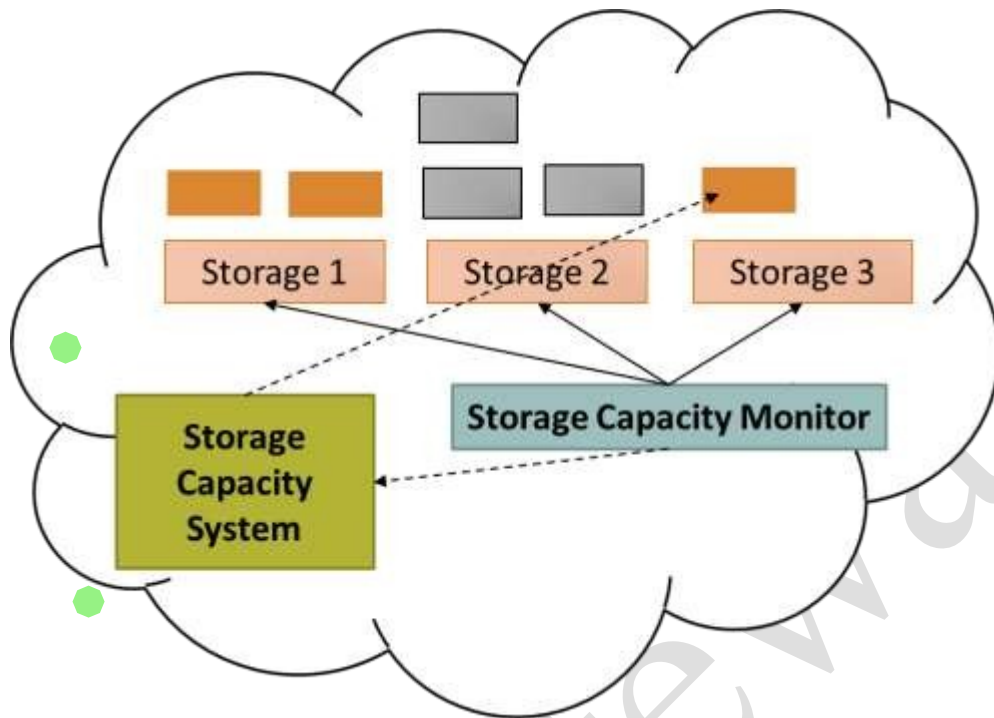
Raja Mushtaq: +923055868956



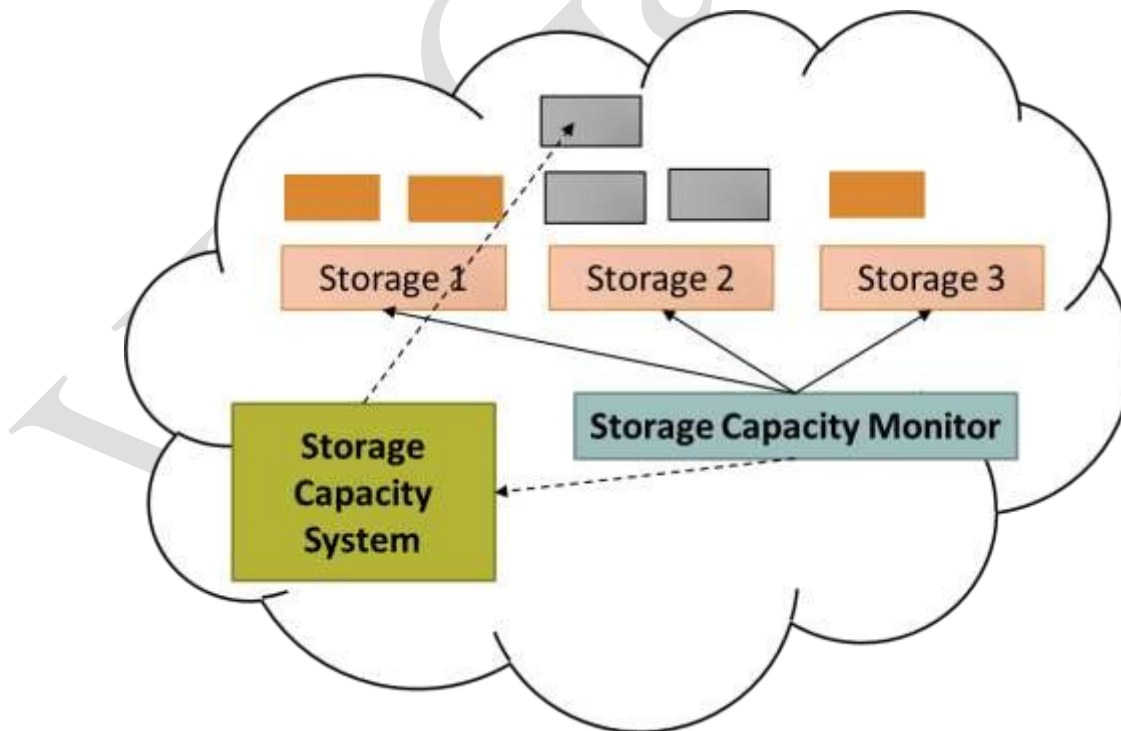
Storage capacity monitoring module indicates the Storage capacity system for migration of logical unit number to another storage device.



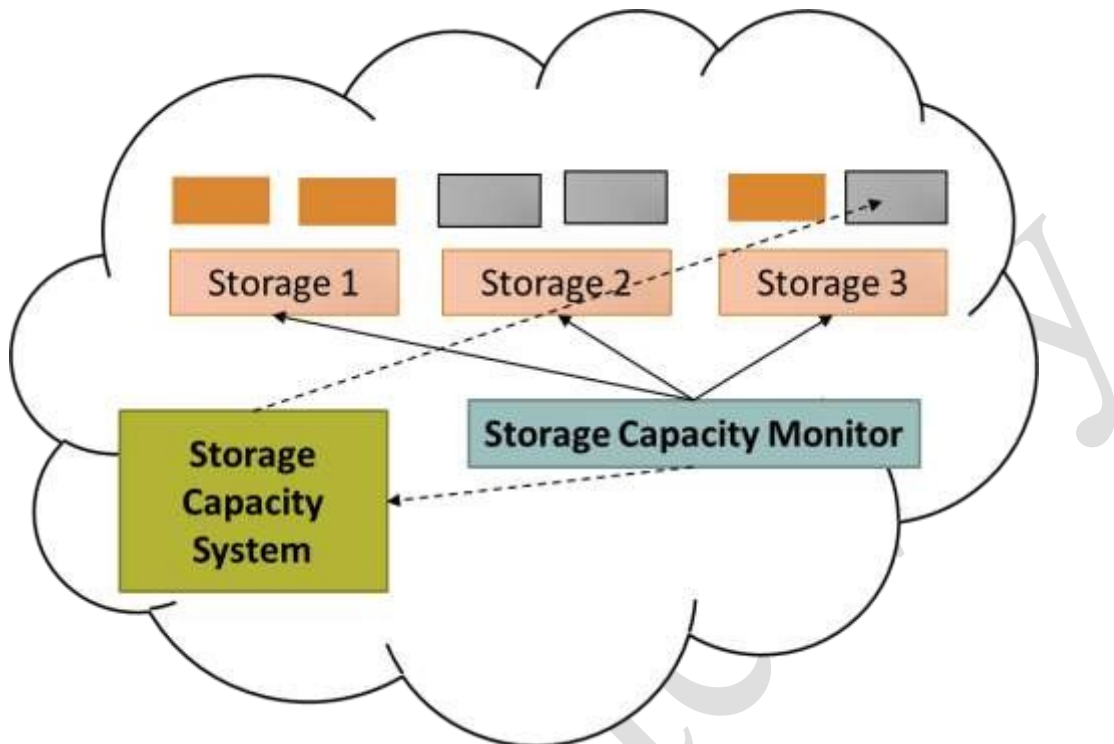
Storage capacity system identifies a logical unit number to migrate.



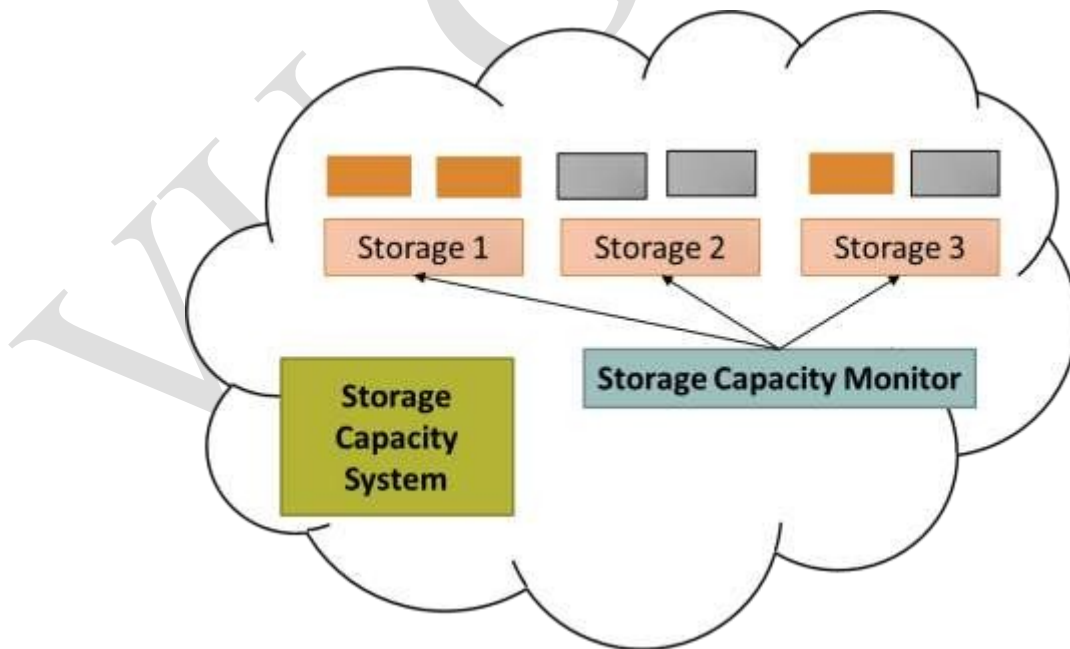
Storage capacity system identifies the destination storage device and shifts the logical unit number to destination device.



Storage capacity monitoring module indicates the Storage capacity system for migration of logical unit number to another storage device.



Storage capacity system identifies the destination storage device and shifts the logical unit number to destination device.

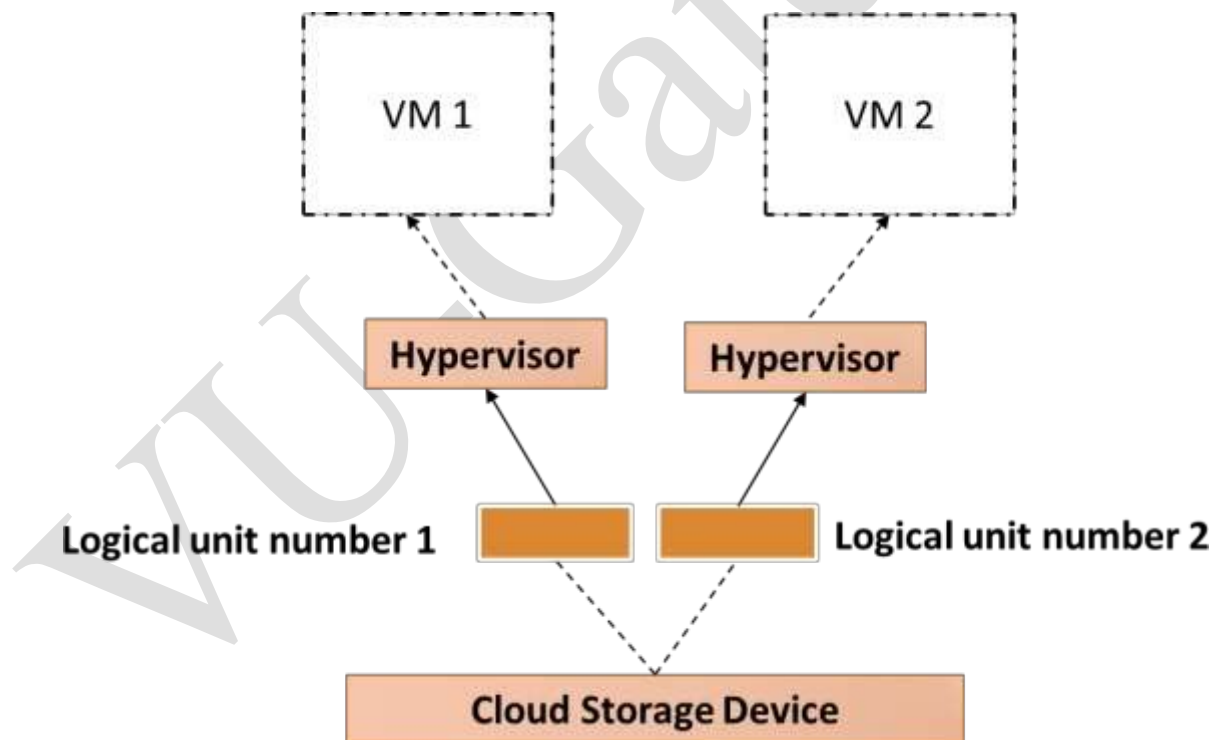


The result is the even distribution of logical unit numbers across all storage devices.

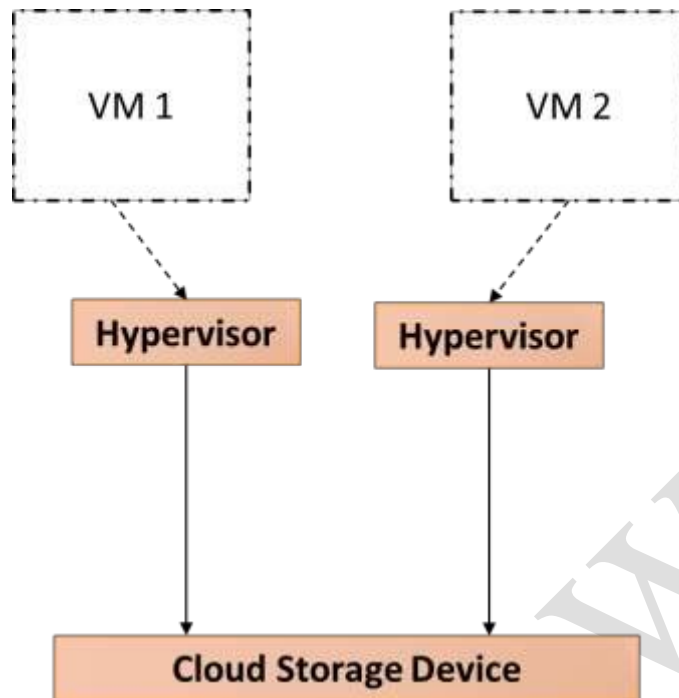
Module No. 134: Direct I/O Architecture:

VM processes ko apni VM Access ki help se host krta hen physical I/O circuit ko jis ki help sy host krta hen physical server ko with the help of Hypervisor

- The VMs access various physical I/O circuits/cards of the hosting physical server through the hypervisor. This is called I/O virtualization.
- However, times may come when the hypervisor assisted access may become a bottleneck for concurrent I/O requests.
- The direct I/O architecture is the possibility of accessing the physical I/O devices from VMs without intervention of hypervisor.
- The physical server's CPU has to be compatible to direct I/O.
- Additional modules required are:
 - Cloud usage monitor
 - Logical network perimeter (to allow only a limited number of VMs to for direct I/O)
 - Pay-per-use monitor
- It is a type of direct I/O in which the VMs access the logical unit numbers directly.
- The VMs can also be given direct access to block level storage.



A type of direct I/O in which the VMs access the logical unit numbers directly.



VMs can also be given direct access to block level storage.

Module No – 135: Dynamic Data Normalization Architecture:

prob jo aattti hen

- The duplication of data over Cloud can cause some problems such as:
- Increase time to store, backup and copy the data
- More space is required
- More cost is to be paid by the consumer
- Data synchronization issues, time consumed in data synchronization and resolving the synchronization related issues.
- The provider has to arrange more storage space and allocate more resources for monitoring and management of replicated data.
- Implements the data de-duplication by preventing the consumers to store replicated data.
- Can be applied to block storage and file based storage.
- Analyzes the received data before sending to storage.
- Each data block is analyzed and a hash code is generated according to the contents.
- The hash code is compared to already stored data blocks
- If a duplicate code is found, the new data block is rejected and a pointer to the already stored block is saved instead.
- The new blocks are saved after the hash code check.
- Can also be applied to backup storage devices.

Module No – 136: Elastic Network Capacity Architecture

- Network bandwidth limit may inhibit the performance and may become a bottleneck.
- It is the software which implements the dynamic scalability of network bandwidth.
- The scalability is provided on per user basis.
- Each user is connected to a separate network port.
- Automated scaling listener, elastic network capacity controller and a resource pool of network ports are used for implementation.
- The automated scaling listener monitors the network traffic and indicates the elastic network capacity controller to enhance the bandwidth and/or number of ports when required.
- When applied to virtual switches, then each virtual switch is configured to induct more physical uplinks.
- Alternatively, the direct I/O can be used to enhance network bandwidth for any VM.

Module No – 137: Cross Storage Device Vertical Tiering Architecture

- The approach is to dynamically shift the logical unit number to another storage device with larger capacity in terms of number of requests processed per second and the amount of data being handled.
 - As compared to traditional approach, it is not constrained by the availability of free space on the physical storage device hosting the logical unit number.
 - Automated scaling listener and storage management modules are required for the implementation.
 - The automated scaling listener monitors the number of requests being sent to the logical unit numbers.
 - When a pre-set threshold of number of requests to a logical unit number is reached, the automated scaling listener signals the storage management module to shift that logical unit number to another device with higher capacity.
 - While moving a logical unit number, the connectivity/availability of data is not interrupted.

Module No – 138: Intra Storage Device Vertical Data tiering Architecture

- Required when there are security and/or legal constraints regarding data migration across different storage devices. jb security require ho tu hum legal coinstraints ko use krty hn data ko migrate krny ky liye
- The data is stored over logical unit numbers.
- This is the implementation of vertical scaling capability over a single cloud storage device.
- The single storage device optimally uses different disks with varying features/capacities.
- Different disks are graded and marked according to capacity.
- Implemented through automated scaling listener and storage management software.
- The automated scaling listener monitors the logical unit numbers.

Raja Mushtaq: +923055868956

- A logical unit number is hosted over a disk. The grade of the disk may be chosen randomly or according to a policy.
- Upon rise of performance requirements for a logical unit number, the automated scaling listener signals the storage management program to move the logical unit number to a disk with higher grade.

Module No – 139: Load Balanced Virtual Switches Architecture

Situations may arise when the consumers' requests may face unlimited delays and packet loss due to network congestion between physical host and network device on uplink.

- The main reason of data packet loss and delays are usually due to single physical uplink.
- This architecture implements a network load balancing mechanism for a physical server (and virtual switch hosted over that server) through the use of multiple physical uplinks.
- This means that more than one NICs are used for each physical server.
- By using *link aggregation* techniques, network traffic can be distributed among multiple physical uplinks.
- The phenomenon of network bottleneck due to single physical uplink can be avoided.
- Can also maintain the availability of the VMs even if any uplink fails.
- The virtual switch has to be configured for compatible and seamless use of multiple physical NICs.

Module No – 140: Multipath Resource Access Architecture

- It is the implementation of multiple access routes/paths to and from a Cloud IT-resource.
- The need for multiple paths arises to provide resiliency when a physical link fails.
- Suppose a Cloud storage device with multiple logical unit numbers deployed over it is connected to (for example) a physical server (hosting multiple VMs with logical unit numbers hosted on that cloud storage).
- If the link to shared storage fails, all the VMs will crash.
- Calling for failover system may take a some time if there are multiple VMs.
- Executing the failover system (when the physical server has not crashed) is expensive.
- An alternative method for resiliency is to provide multiple paths between the physical server and the cloud storage device.

Module No – 141: Persistent Virtual Network Configuration Architecture:

- When a VM is instantiated on a physical host, the network configuration such as the allocated port number (from virtual switch) is set up.
- If the VM is migrated to another physical server, the same port number (of virtual switch of the destination server) may not be available.

jb Vm aik server sy 2sry server ki trf jataa hn uska same port hota hn wo available ni rhtaa

- This will jeopardize the network traffic for the migrated VM because the destination environment does not have the network configuration and port number info regarding the migrated VM.
- This architecture ensures that every VM migration uses a persistent information regarding network configuration and port number.
- Implemented through a central virtual switch spanning over multiple physical servers.
- The network configuration and port setting of the VMs (hosted over servers connected through central virtual switch) is centrally stored.
- Each server is allocated some virtual ports.
- Migration of a VM from one host to another keeps the virtual port number persistent. Thus the connectivity of VM is not lost during and after the migration.

Module No – 142: Redundant Physical Connection for Virtual Servers Architecture

- Redundant hardware devices can be added to a physical server to add resiliency.
- Working in active-passive manner, the redundant device is kept in a waiting state.
- If the primary device fails, the secondary device takes over.
- This architecture implements redundant NICs to provide high availability and connectivity of the VMs hosted on physical server.
- The redundant NIC is connected to the physical switch through separate links.
- The virtual switch is configured to use all the redundant NIC.
- But only one NIC is kept primary and active.
- The secondary NIC does not forward any packets although it receives packets from VMs until the primary NIC fails.
- The process is transparent to the hosted VMs.

Module No – 143: Storage Maintenance Window Architecture

- The Cloud storage devices need to undergo for maintenance process in order to maintain their working potential.
- A Cloud storage device hosts multiple logical unit numbers.
- It is not practical to disconnect the storage device/s and then perform maintenance.
- In order to maintain the availability of data, this architecture temporarily copies the data from a to-be-maintained storage device to a secondary device.
- The data is (for example) arranged/stored in the form of logical unit numbers which in-turn are connected to different VMs and/or accessed by different consumers.
- It is therefore important that the logical unit numbers be migrated live.
- The connectivity and availability of data are maintained.
- ✓ Once the data is migrated, the primary device is made unavailable. The secondary device serves the data requests even during migration.
- The storage service gateway forwards the consumer requests to secondary storage.

- The data is moved back to the primary storage after the maintenance is over.
- The whole process remains transparent.

Lesson No. 28

CLOUD FEDERATION & BROKERAGE

Module No – 144: Cloud Federation:

- VMs It is the interconnection of Cloud computing infrastructures of two or more Cloud providers for load balancing.
- One of the providers buys the services from the other provider.
- The federation agreement may be timely or permanent.
- It provides revenue for the seller and allows the buyer to extend its resources capacity without setting up or acquiring new hardware resources.
- The VMs and data can be migrated across the providers' Clouds.
- The process of Cloud federation remains transparent to the consumers of the buyer.
- Federation can be performed horizontally or vertically on the basis of extending the SaaS, PaaS and IaaS of the federation buyer.
- The SLA of the consumers (of buyer) is followed over the seller's infrastructure as well.

Module No – 145: Workload Placement in Federated Clouds

- Due to the availability of a finite number of physical resources, a single Cloud can handle a certain number of consumers' requests in a unit time.
- We are supposing that a time deadline exists to process a consumer's request.
- If a Cloud infrastructure cannot meet the requests' deadlines, then it is experiencing resource shortage or congestion.
- At this point, the chances of SLA violation start becoming solid.
- The Cloud provider may be heading towards SLA penalties if the situation persists.
- A decision has to be made by the Cloud provider to process the consumer requests that are in excess to the current capacity on the basis of:
 - Revenue to be earned from processing the extra requests
 - The cost to be paid to other provider/s
 - The deadline of the requests vs. latency of remote provider
- A Cloud federation may also be created to fulfill the requests of a remote consumer through the closest provider in that region to reduce network latency.
- Thus federation of Clouds offer a better solution to resource shortage and latency issues in Cloud computing.
- Federation can be horizontal. In this, the Cloud services (IaaS, PaaS and SaaS) are horizontally expanded.

- In **vertical federation**, a Cloud provider *A* (for example) may host a SaaS/PaaS instant of another provider *B* over its own IaaS to fulfil the requests of provider *A*.
- Federation can also be hybrid.

Module No – 146: Cloud Brokerage:

- It is a third party process of finding the appropriate Cloud provider.
- This process is dependent upon the requirements and/or directions of the consumers.
- Performed by a person or individual called **broker**. Acting as intermediary between the consumer and provider of Cloud services.
- Saves the consumer from spending efforts and time to search for Cloud provider.
- Works closely with the consumer to understand the business process, provisioning needs, budget and other requirements.
- The broker then searches for the best options of Cloud providers for the consumer.
- The consumer is then provided with a list of providers according to requirements and budget of the consumer.
- The broker may also be granted rights to negotiate with the providers on behalf of the consumer. The broker can even settle a contract with the most suitable provider.
- A broker may also provide:
 - API and GUI to the consumer for handling the Cloud resources.
 - Encryption and data transfer & management assistance.
 - Advisory service to the consumer for improving the use and benefits of the Cloud.

Lesson No. 29

CLOUD DELIVERY/SERVICE MODELS' PERSPECTIVES

Module No – 147: Cloud Provider's Perspective about IaaS:

- In this and next two modules, we shall discuss the overall perspective of Cloud provider in establishing and managing of **Cloud services**. Namely:
 - IaaS
 - PaaS
 - SaaS
- The two basic IT resources of IaaS are:
 - VMs
 - Cloud storage
- These are offered along with the:
 - OS
 - (virtual) RAM
 - (virtual) CPU
 - (virtual) Storage
- VMs are usually provisioned through VM images which are predefined configurations.
- Bare-metal provisioning is also provided to the consumers with administrative access.
- **Snapshots of VMs can be occasionally taken for failover and replication purposes.**

Raja Mushtaq: +923055868956

- A cloud may be provisioned through multiple data centers spanning at different geographical locations and connected through highspeed networking.
- VLANs and network access control are used to isolate a networked set of VMs (into a network perimeter) which are provisioned to a single consumer/organization.
- Cloud resource pools and resource management systems can be used to provide scalability. *mkta*
- Replication is used to ensure high availability and forming a failover system.
- Multipath resource access architecture is used to provide reliability.
- Resource reservation architecture is used for provisioning of dedicated IT resources.
- Different monitors such as pay-per-use monitor and SLA monitors continuously overlook VM lifecycles, data storage and network usage to establish billing system and SLA management.
- Cloud security (encryption, authentication and authorization systems) are to be implemented.

Module No – 148: Cloud Provider's Perspective about PaaS:

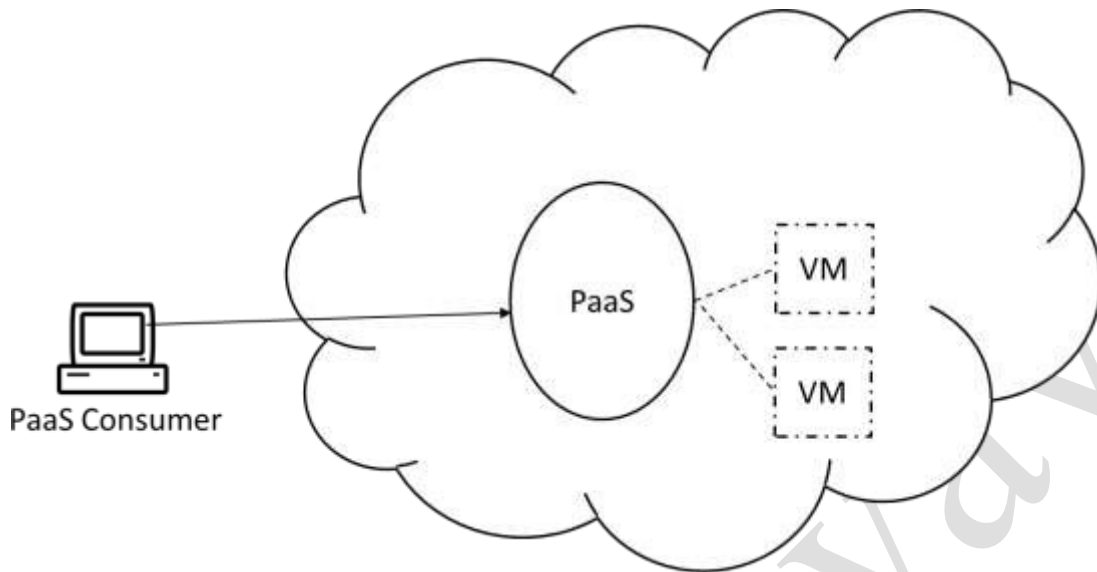
laas mi app consumer ki mrzi sy chal rae hotu hn
Paas mi app developer ki mrzi sy chl rae hoti hn

- PaaS instances are hired by developers who want to develop Cloud applications
- Readymade environments are usually created to provide on-demand access to a pre-configured set of software tools and SDK.
- The PaaS environments can simulate a Cloud environment with security procedures to enable the developer to test the application/s being developed.
- The PaaS environments also help in establishing multitenancy and auto scalability features in developed applications.
- Scalability can be provided to an overloaded application on the recommendation and budget of the PaaS consumer. *consumer buget pass krty hn Scalability ko purchase krty hn khud consumer*
- Automated scaling listener and load balancers are utilized for workload distribution.
- Non-disruptive service relocation architecture and failover systems are utilized to ensure reliability in PaaS instances.
- PaaS instances may comprise of multiple VMs and can be distributed across different data centers.

In Software-as-a-Service (SaaS), the cloud Service Providers (CSP) provide special-purpose software to the cloud users (i.e., consumers) which is deployed and running on cloud Infrastructure. Live Mesh from Microsoft and Customer Relationship Management from Salesforce.com are examples of SaaS services. The online alternative to the Microsoft Office application i.e., a word processor is an example of SaaS services. In SaaS, cloud users are not responsible for the maintenance and management of issues related to the cloud Infrastructure like servers, OS, Networks, development and deployment tools, and other applications.

Platform-as-a-Service (PaaS) is another obstruction level offered by the CSP where consumers (cloud users) deploy their own applications developed in any programming language that is supported by the CSP-provided environment. In PaaS, the cloud user controls the deployment, hosting, and configuration of user-created applications. Microsoft Azure and Google App Engine are examples of PaaS services. However, in PaaS, cloud users are not responsible for maintaining and managing the cloud Infrastructure like managing OS, server configuration, and storage.

In Infrastructure-as-a-Service (IaaS), the Cloud service providers manage and maintain a huge set of computing resources such as processing and storage capacity. Virtualization of these resources enables Cloud service providers to split physical resources and build dynamically resizable ad-hoc computing systems. Moreover, virtualization provides scalability in terms of run-time lease and release of virtual resources and a high level of customization according to the user's requirement



PaaS instances may comprise of multiple VMs and can be distributed across different data centers.

- Pay-per-use monitor and SLA monitor can be used to collect data regarding resource usage and failures.
- The security features of IaaS are usually ample for PaaS instances.

Module No – 149: Cloud Provider's Perspective about SaaS:

- SaaS instances are unique from IaaS and PaaS instances due to the existence of concurrent users.
- The SaaS implementations depend upon scalability & workload distribution mechanisms and non-disruptive service relocation architectures for smooth provisioning and overcoming failures. its provide th best services
- Unlike the IaaS and PaaS, every SaaS deployment is unique from other implementations.
- Every SaaS deployment has different programming logic, resource requirements and consumer workloads.
- The diverse SaaS deployments include: Wikipedia, Google talk, email, Android play store, Google search engine etc.
- The implementation mediums include:
 - Mobile apps
 - REST service
 - Web service
- These mediums also provide API calls. The examples include: electronic payments services such as PayPal, mapping and routing services (Google Maps) etc.
- Mobile based SaaS implementations are usually supported by multi-device broker mechanism for heterogeneous device-based access.
- Therefore, SaaS implementation requires the implementation of:

Raja Mushtaq: +923055868956

- Service load balancing, Dynamic failure detection and recovery, storage maintenance window, elastic resource/network capacity and Cloud balancing architectures.
- Monitoring is usually performed through pay-per-use monitors to collect consumer usage related data for billing
- Additional security features (as already provided by underlying IaaS environment) may be deployed according to business logic.

Module No – 150: Cloud Consumer's Perspective about IaaS

- A consumer accesses the VM through a remote terminal application. The VM has to have an OS installed.
 - Remote desktop client for Windows
 - SSH client for Mac and Linux based systems
- Cloud storage device can directly be connected to the VM or to a local device on-premises.
- The Cloud storage data can be handled and rendered through Networked file system, storage area network and/or object-based storage accessible through Web-based interface.
- **The administrative rights of the IaaS consumer include, controlling of:**
 - Scalability
 - Life cycle of VM (powering-On/Off and restarting)
 - Network setting (firewall and network perimeter)
 - Cloud storage attachment
 - Failover setting
 - SLA monitoring
 - Basic software installations (OS and pre installed software)
 - VM initializing image selection
 - Passwords and credentials management for Cloud IT-resources
 - Costs
- IaaS resources are managed through remote administration portals and/or command line interfaces through execution of code scripts.

Module No – 151: Cloud Consumer's Perspective about PaaS

- **Typically, a PaaS consumer receives the following:**
 - Software libraries
 - Class libraries
 - Frameworks
 - APIs
 - Databases
 - Cloud emulation environment
- **The completed applications are deployed to Cloud**
- **The administrative rights of the PaaS consumer include the control of:**
 - Login management of service/s developed/deployed using PaaS instance
 - Choosing the tools in case of ready-made environment
 - Cloud storage device selection

- IT-resource usage cost
- Deployment of automated scaling listener, load balancer and replication etc.
- SLA monitoring

Module No – 152: Cloud Consumer's Perspective about SaaS

- The SaaS deployments are complemented by APIs.
- The API calls enable the wide spread of the SaaS into webpages and applications. For example Google maps
- Many SaaS are free of charge. Although the service provider may gather background data
- The SaaS consumers have least administrative privileges and the least responsibilities regarding deployment and managing the service.
- A few runtime configurations can be controlled by SaaS consumers. These include:
 - Usage cost control
 - SLA monitoring
 - Security related configurations

Lesson No. 30

INTER-CLOUD RESOURCE MANAGEMENT

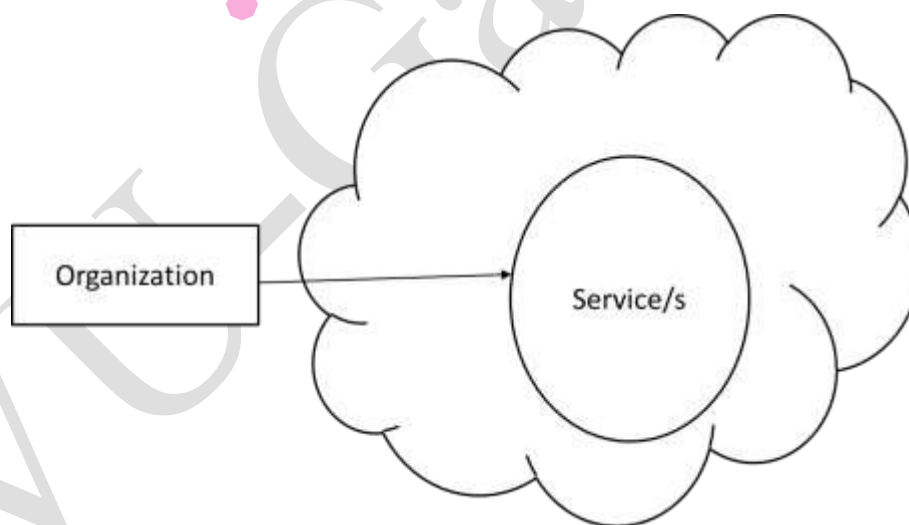
Module No – 153:

- The term **Inter-Cloud** refers to as *Cloud of Clouds* just as **Internet** is regarded as *network of networks*.
- Cloud computing has proliferated throughout the computing world.
- The providers are of two types:
 - With extra (idle) resources
 - With resource shortage
- Many providers look for getting reasonable clients to generate more revenue and to make good use of idle resources.
- Cloud federation gives a solution to this problem.
- But a bigger picture lies in Inter-Cloud where the global federation takes place.
- The Inter-Cloud can be established where each member Cloud is connected to other member Clouds just like Internet connects the networks.
- It is the ultimate future of Cloud federation.
- Technological giants such as IBM, HP, CISCO, RedHat etc. are actively working on establishment of cloud-of-clouds.
- We hope that soon the issues of interoperability, inter-cloud communication, security and workload migration will be addressed.

CLOUD COST METRICS AND PRICING MODELS

Module No – 154:

- In next few modules, we shall discuss different cost metrics and pricing models of Cloud.
- **Business Cost Metrics:** The common types of metrics related to cost benefit analysis of Cloud computing.
- **Upfront Costs:** Related to initial investment regarding IT resource acquiring and installations.
High costs for on-premises installation as compared to leased from Cloud.
- **On-going Costs:** Include the running costs of the IT resources e.g., licensing fee, electricity, insurance and labor.
The long term ongoing costs of Cloud IT-resource can exceed the on-premises costs.
- **Additional Costs:** These are specialized cost metrics. These may include:
 - **Cost of Capital:** It is the cost of raising a capital amount. It is higher if a high capital is to be arranged in short time. The organization may have to bear some costs in raising a large amount. This is important decision for up-front cost metrics.



Organizational perspective of Cloud services.

- **Sunk Costs:** These are the costs already spent by the organization over IT-infrastructure. If the Cloud is preferred then these costs are sunk. Hence should be considered along with up-front cost of Cloud. Difficult to justify the leasing of Cloud IT resources in the presence of high sunk costs.

- **Integration Costs:** The time and labor costs required to integrate a Cloud solution which include the testing of Cloud services acquired.
- **Locked-in Costs:** The costs related to being dependent upon a single Cloud provider due to lack of interoperability among different providers. Affects the business benefits of leasing the Cloud based IT-resources.

Module No – 155:

- **Cloud Usage Cost Metrics:** In this module we shall study different metrics related to cost calculation of Cloud IT resource usage.
 - **Network Usage:** Cumulative of, or separate of outbound and inbound network traffic in bytes over the monitored time. Costing may be cumulative or separate for inbound and outbound traffic. Many Cloud providers do not charge for inbound traffic to promote the consumers to shift their data towards Cloud.
 - May also be based upon the *static IP address usage* and network traffic processed by *Virtual Firewall*.
 - **VM Usage:** Related to the number of VMs and the usage of the allocated VMs. Can be static cost, pay-per-use, or according to the features of VM. Applicable to IaaS and PaaS instances.
 - **Cloud Storage Device Usage:** It is charged by the amount of storage used. Usually the *on-demand storage allocation* pattern is used to calculate bill on time basis for example on hourly basis. Another (scarcely used) billing option is to charge on the basis of I/O operations to and from storage.
 - **Cloud Service Usage:** The service usage can be charged on the basis of duration of subscription, number of nominated users and/or number of transaction served by the service!

Module No – 156: Case Study for Total Cost of Ownership (TCO) Analysis

- The TCO includes the costs of acquiring, installing and maintaining the hardware and software to perform the IT tasks of the organization.
- In this module, we shall perform a case study to evaluate the TCO for on-premises and Cloud based solution.
- Suppose a company wants to migrate a legacy application to PaaS. The application requires a database server and 4 VMs hosted on 2 physical servers.
- Next we perform a TCO analysis for 3 years:

Raja Mushtaq: +923055868956

Upfront Cost	Cloud Environment (Rupees)	On-Premise Environment (Rupees)
Hardware	0	190,000
Licensing	0	200,000
Labor	40,000	40,000
Total Up-Front Costs	40,000	430,000

Follow the video lecture to understand fully

Monthly On-Going Costs	Cloud Environment (Rupees)	On-Premise Environment (Rupees)
Application Servers	120,000	0
Database Servers	30,000	0
WAN Network	4,000	0
Environment	0	40,000
Software Licensing	0	30,000
Hardware Maintenance	0	15,000
Administration	30,000	80,000
Total On-Going Costs	184,000	165,000

Follow the video lecture to understand fully

Raja Mushtaq: +923055868956

	Cloud Environment (Rupees)	On-Premise Environment (Rupees)
Total Upfront Cost	40,000	430,000
3 Months On-Going Costs	$(184000 \times 3) = 552,000$	$(165,000 \times 3) = 495,000$
Gran Total	592,000	925,000

Follow the video lecture to understand fully

Module No – 157: Cost Management Considerations

- Cost management can take place across the lifecycle phases of Cloud services. These phases may include:
 - Design & Development
 - Deployment
 - Service Contracting
 - Provisioning & Decommissioning
- The cost templates used by the providers depend upon:
 - Market competition
 - Overhead occurred during design, deployment and operations of the service
 - Cost reduction considerations through increased sharing of IT resources
- A pricing model for Cloud services can be composed of:
 - Cost metrics
 - Fixed and variable rates definitions
 - Discount offerings
 - Cost customization possibilities
 - Negotiations by consumers
 - Payment options

Module No – 158:

- **Case study:** We shall now see an example case of different price offering from a Cloud provider.

Raja Mushtaq: +923055868956

Instance Name	Configuration	Operating System	Pay-per-use Hourly Rate Rs.
Small VM	1 vCPU, 4GB vRAM, 20GB Storage	Linux	50
		Windows	80
Medium VM	2 vCPUs, 8GB vRAM, 20 GB Storage	Linux	145
		Windows	190
Large VM	8vCPUs, 16GB vRAM, 80GB Storage	Linux	300
		Windows	350
VM with Large VRAM	8vCPUs, 64GB vRAM, 20GB Storage	Linux	800
		Windows	900
VM with Large vCPU	32vCPUs, 16GB vRAM, 20GB Storage	Linux	900
		Windows	1000

Follow the video lecture to understand fully

Instance Name	Configuration	Operating System	1 Year Term Pricing Rs.	
			Up-front	Pay-per-use Hourly
Small VM	1 vCPU, 4GB vRAM, 20GB Storage	Linux	500	30
		Windows	700	45
Medium VM	2 vCPUs, 8GB vRAM, 20 GB Storage	Linux	1200	75
		Windows	1500	90
Large VM	8vCPUs, 16GB vRAM, 20GB Storage	Linux	3000	172
		Windows	3500	200
VM with Large VRAM	8vCPUs, 64GB vRAM, 20GB Storage	Linux	700	400
		Windows	800	450
VM with Large VRAM	32vCPUs, 16GB vRAM, 20GB Storage	Linux	750	400
		Windows	850	450

Follow the video lecture to understand fully

CLOUD SERVICE QUALITY METRICS

Module No – 159:

- These metrics are used to define and monitor the SLA.
- The characteristics of Quality of Service (QoS) can be expressed by these metrics.
- These include:
 - **Availability:** up-time, down-time, service duration
 - **Reliability:** minimum time between failures, guaranteed rate of successful response
 - **Performance:** capacity, response time and delivery time guarantees
 - **Scalability:** Capacity fluctuation and responsiveness guarantees
 - **Resiliency:** Mean time to switchover and recovery
 - Service quality metrics are required to be *quantifiable, repeatable, comparable and easily obtainable*

Module No – 160:Service Availability Metrics

- **Availability Rate Metric:**
 - The value in % of up-time e.g., 100%.
 - Measured as total up-time/total time.
 - Monitored weekly, monthly and/or yearly.
 - Applied to IaaS, PaaS and SaaS.
 - Expressed as cumulative value.
 - E.g., 99.5% minimum
- **Down-time Duration Metric:**
 - Expresses the maximum and average continuous down-time.
 - Covers the duration of outage.
 - Measured whenever the outage event occurs
 - Applied to IaaS, PaaS and SaaS.
 - E.g., 1 hr max, 15 min average

Module No – 161:Service Reliability Metrics

- **Reliability** in context to Cloud IT-resources refers to the probability that an IT-resource can be performing its intended function under predefined conditions without experiencing failure.
 - Focuses on the duration in which the service performs as expected.
 - This requires the service to be operational and available during that time.
- **Mean-Time Between Failures Metric:**
 - Expected time between two consecutive failures.

- Measured as normal operation duration/number of failures.
- Measured as monthly and/or yearly.
- Applicable to IaaS and PaaS.
- E.g., 90 days average
- **Service Reliability Rate Metric:** It is the percentage of successful service outcomes.
 - Measures the non-critical errors during the up-time.
 - Measured as total number of successful responses/total number of requests
 - Measured as weekly, monthly and/or yearly.
 - Applicable to SaaS.
 - E.g. minimum 99.5%

Module No – 162:Service Performance Metrics

- **Service performance** refers to the ability of an IT resource to carryout its functions within expected perimeters.
 - Measured with respect to capacity metrics.
- **Network Capacity Metric:** Measured as bandwidth/throughput in bits per second. Applicable to IaaS, PaaS and SaaS. Measured continuously. Expressed as for example MB/sec.
 - **Storage Device Capacity Metric:** Measured as size in GB. Applicable to IaaS, PaaS and SaaS. Continuously measured.
- **VM Capacity Metric:** Measured as features such as number of CPUs, CPU frequency in GHz, RAM size in GB and storage size in GB. Continuously measured. Applied to IaaS and PaaS.
 - **Web Application Capacity Metric:** The number of requests processed in a minute (for example). Applicable to SaaS

Module No – 163:Service Scalability Metrics

- These are related to the IT resource's elastic capacity, the maximum capacity that an IT resource can reach and the adaptability of an IT resource to workload fluctuations.
- For example a VM can be scaled up to 64 cores and 256 GB of RAM or can be scaled out to 8 replicated instances.
- **Storage Scalability (Horizontal) Metric:** The permissible capacity change of a storage device in accordance with the increase in workload.
 - Measured in GB.
 - Applicable to IaaS, PaaS and SaaS.
 - E.g., 1000 GB maximum (automatic scaling)
- **Server Scalability (Horizontal) Metric:** The permissible server capacity in response to increased workload.
 - Measure in number of VMs in resource pool.
 - Applicable to IaaS, PaaS
 - E.g., 1 VM minimum up to 10 VMs maximum (automated scaling)
- **Server Scalability (vertical) Metric:** Measured in terms of number of vCPUs, vRAM size in GB.
 - Applicable to IaaS and PaaS.
 - E.g., 256 cores maximum and 256 GB od RAM

Module No – 164: Service Resiliency Metrics

- Refers to the ability of an IT resource to recover from operational disturbance.
- When considered with respect to SLA, the resiliency guarantees are based upon redundant implementation, resource replication and disaster recovery systems.
- Can be applied over three phases:
 - **Design phase:** To evaluate the preparation level of systems and service to cope with the known challenge.
 - **Operational phase:** Measure the difference in service levels (in terms of availability, reliability, performance and scalability metrics) before, during and after a downtime event.
 - **Recovery phase:** To measure the rate at which an IT resource recovers from downtime. For example the meantime for a system to record a downtime event and switch over to a new VM.
- Two common metrics related to measuring resiliency are as follows:
 - **Mean-Time to Switchover (MTSO) Metric:** The time to switch over to a replicated instance after the failure of a VM.
 - Measured in terms of time (from time of failure to recovery)
 - Measure as per month and/or year
 - Applicable to IaaS and PaaS
 - E.g., 12 minutes average
 - **Mean-Time System Recovery (MTSR) Metric:** The time expected for a resilient system to perform a complete recovery from a VM failure.
 - Measured as total time spent during recovery/total number of failures
 - Measured as monthly and/or yearly
 - Applicable to IaaS, PaaS and SaaS
 - E.g., 100 minutes average

Module No – 165: Service Quality Metrics and SLA Guidelines

- In this module, we shall discuss some of the best practices of Cloud consumers for dealing with SLAs.
- **Mapping of test-cases to the SLAs:** A consumer should highlight some test cases (disasters, performance, workload fluctuations etc.) and evaluate the SLA accordingly. The SLA should be aligned with the consumer's requirements of the outcome of these test-cases.
- **Understanding the scope of SLA:** A clear understanding of the scope of SLA should be made. It is possible that a software solution may be partially covered by an SLA for example the database may be left uncovered.
- **Documenting the guarantees:** It is important to document all the guarantees at proper granularity. Any particular guarantee requirement should also be properly and clearly mentioned in SLA service agreement document kry note down ky badd

- **Defining penalties:** The penalties and reimbursements should be clearly defined and documented in SLA. jo provider ny guranties di hn wo documented ho
- **SLA Monitoring from independent party:** Consider the SLA monitoring from a third party. jesi 3rd party hn monitor krwa liya jaa dobut clear ho sky
- **SLA monitoring data archives:** The consumer may want the provider to delete the monitored data due to privacy requirement. This should be disclosed as an assurance by the provider in SLA. user ka data clode sy remove kr dyna chae agr wo user quit krta hn tu

Lesson No. 33

CLOUD SIMULATOR

Module No – 166: CloudSim: Introduction

- Cloud computing is an ongoing phenomenon which requires periodic updates in terms of architectures (study before), procedures and services.
- Cloud computing is an ongoing phenomenon which requires periodic updates in terms of architectures (study before), procedures and services.
- For a lot of researchers, it is difficult to test their research and theories on a Cloud computing setup hosted on a real data center.
- It is more suitable to use a simulation environment such as CloudSim for testing various new and updated procedures and hypothesizes related to Cloud computing.
- **CloudSim is free of cost.** data ko directly implement sy phly hum ko es mi check krn chae sae hn koi bugs tu ni us ky baad implement krna chae
- Can be used by IaaS/PaaS users to tune up performance bottlenecks in the Cloud services before deploying on actual Cloud.
- Can be used by the provider to test various policies related to resource leasing, pricing and workload management of the Cloud.
- The documentation, setup and tutorials are available free of cost from the CloudSim webpage: <http://www.cloudbus.org/cloudsim/>

Module No – 167: CloudSim: Configuration

- Some configurations are required for the CloudSim. The important requirements are discussed in this module.
- CloudSim requires Sun's Java 8 or newer version. Older versions of Java are not compatible.
- You can download Java for desktops and notebooks from <https://java.com/en/download/>
- CloudSim requires Sun's Java 8 or newer version. Older versions of Java are not compatible.
- You can download Java for desktops and notebooks from <https://java.com/en/download/>
- CloudSim setup is just needed to be unpacked before using. If you want to remove CloudSim, remove the folder.
- CloudSim setup comes with various coded examples which can be test run for understanding the CloudSim architecture.
- CloudSim site has video tutorial explaining the step-by-step configuration and execution.

Raja Mushtaq: +923055868956

- CloudSim setup is just needed to be unpacked before using. If you want to remove CloudSim, remove the folder.
- CloudSim setup comes with various coded examples which can be test run for understanding the CloudSim architecture.
- CloudSim site has video tutorial explaining the step-by-step configuration and execution.

Module No – 167: CloudSim: Example Code

- CloudSim emulates a virtualized data center environment.
- There are various hosts (physical servers) and VMs mounted on the hosts.
- The workload unit is called *Cloudlet*.
- There is a *broker* entity which gets the Cloudlets executed on Data center just as in real life scenarios.
- A service named as *Cloud Information Service (CIS)* contains the registry of the data center.
- The broker object retrieves the information of all the data centers registered with CIS.
- The broker then contacts a suitable data center and executes the Cloudlet/s over the hosted VMs.
- Each host has properties such as processors and RAM. The hosted VMs share the host.
- Each VM can have multiple Cloudlets scheduled over it.
- Different *policy* objects such as VM-allocation, VM-scheduler and Cloudlet-scheduler exist.
- *VM-allocation policy* is used by data center to allocate VMs to hosts.
- *VM-scheduler policy* is used by host for resource allocation.
- *Cloudlet-scheduler policy* is used by the VM.
- These policies are either space shared or time shared.

Lesson No. 34

COMPUTER SECURITY BASICS

Module No – 169: Computer Security Overview:

- As per NIST, the **Computer Security** is defined as:
- “The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data and telecommunications) “
- **Information System:** It is a software that helps in organize and analyze data.
- **Privacy:** The right of an individual to control or influence about what information can be collected and stored and by whom and to whom that information may be disclosed.

“William Stallings [2013] Computer Security Principles and Practices, Pearson”

- The European Union (EU) definition of *personal data* is:

Raja Mushtaq: +923055868956

- *Personal data shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity.*

European Commission: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- The key terminologies of privacy are:
 - **Data controller:** An individual or a body which individually or jointly determines the purpose and procedure of processing an item of personal information.
 - **Data processor:** An individual or body which processes the personal information on behalf of the data controller
 - **Data subject:** An identified or identifiable individual to whom personal information relates directly or indirectly.
- Privacy is regarded as human right in Europe while in America it traditionally refers to avoiding harm to people in any context.

Module No – 170: Confidentiality Integrity and Availability (CIA):

- **Confidentiality:** Allowing only authorized access and disclosure to the information
 - For example: The student grade information is the asset of students and confidentiality should be imposed by law in the USA. This information is only available to the students, their parents and employees that require the information for routine job purposes. Lesser level of confidentiality is the enrolment information.
- **Integrity:** Guarding against unauthorized modification and/or destruction of information.
 - For example: The information related to patients' allergy requires high integrity because any inaccuracy in this information may lead to serious harm or even death. While a low integrity is required for an online poll where people may choose inaccurate options or reviews.
- **Availability:** Ensuring timely and reliable access to the information.
 - For example: A service providing authentication verification is needed to be highly available otherwise the users/employees can not access the data and organization will suffer monetary losses due to the halt in data processing operations. An online telephone directory may not be required to be highly available.
- **Authentication:** Proving the identity of a user e.g.; through login and password.
- **Authorization:** Verification of the access rights of an authenticated user e.g.; subscription to basic or premium user access to an online gaming website.

Module No – 171: Computer Security & Trust:

Raja Mushtaq: +923055868956

- Trust is a psychological state comprising of intentions to accept the risks on the basis of positive expectations of the behavior of another person or entity.
- Trust is broader term than security because the trust is also based upon experience and criteria.
- Trust has two types:
 - Hard trust: Requires the usage of security-oriented aspects such as authentication, encryption and security (CIA). sec measure ki existing ko require krna prhtaa hn then hard trust aye ga user py
 - Soft trust: Consists of non-security oriented phenomenon such as human psychology, brand loyalty and user friendliness. sec ky liawa 2sry phenomena majood hn
- Usually people find it harder to trust online services than offline services.
- Trust on online services can be enhanced/revived by using security features but it is not a guaranteed solution.
- The trust in Cloud computing is of two types: *Persistent trust* (long term) and *Dynamic trust* (short term). trust
- The trust of Cloud consumer can be enhanced and established through security elements.
- More to come in next modules.

Module No – 172: Cryptography:

communicatio es trah sy ki jae intruder ko pata nagh laag sky es text ka mean kia hn secret info k liye yh use hoti hn sms es trah sy likhy koi 3rd phry usy smj nah aye es kam actual mean kiya hn

- It is a science of providing security for information.
- It is a science of secret communication.
- Has been historically used by the governments and armies for as long ago as 1900 BC.
- It converts the data into a format which is not readable by an un-authorized user.
- Cryptanalysis:** The science of analyzing and breaking the code of encrypted text. data format change kr ky aggy nd kry gy sms
- Cryptology:** Involves both cryptography and cryptanalysis.
- The following are the five primary functions: Cryptography
 - Privacy
 - Authentication
 - Integrity
 - Non-repudiation:** A mechanism to prove the originality of the sender. unauthorised authorize ni bn skta
 - Exchange of **crypto keys** which are the strings of bits used to change the format of the data. wo formuly jis sy sender data ko encrypt krta hn

Module No – 173: Authentication & Access Control:

- Authentication can be performed through:
- Something the user knows: password, **personal identification number (PIN)** or answer to a prearranged question.
- Something the user possesses: **Electronic cards, smart card and physical keys.** Also called *token*.

yh chezy jin ky through user apny ap ko authenticate krta hnnnnnnnn

Raja Mushtaq: +923055868956

- Something the individual is (static biometric): Fingerprint, retina and face scan.
- Dynamic biometric: voice, handwriting and typing pattern.
- The purpose of access control is to limit the actions or operations that an authenticated user of a computer system can perform.
- This includes the privileges of the user as well as the programs executing on behalf of the user.
- Access control is enforced by a software module which monitors every action performed by the user and the programs executing on behalf of the user.
- The authorization of each user is set by the security administrator according to policy of the organization.
- Access control requires authentication.

Module No – 174: Malware or Malicious Software:

- It is a program which is inserted into a system (usually covertly) to compromise the confidentiality, integrity and/or availability of the victim's data.
- **Adware:** Advertisement integrated into the software. It can result in pop-up ads or redirecting of browser.
- **Attack kit:** Set of tools to generate more malware.
- **Auto-rooter:** Hacking tool to remotely break into a machine.
- **Backdoor (trapdoor):** A mechanism that bypass the normal security check and may allow unauthorized access.
- **Flooders (Denial of Service client):** Generates and propagate a flood of packets over a network to perform denial of service attack.
- **Keyloggers:** Capture the keystrokes on a compromised system.
- **Logic-bomb:** A malicious code which executes on the happening of certain event or time.
- **Rootkit:** Set of tools used by a hacker after compromising a system and gaining root level access.
- **Spammer programs:** Used to send large volumes of junk emails.
- **Spyware:** A software that collects keystrokes, screen data, network traffic or stealing sensitive information from the files and transfer them to remote computers.
- **Trojan horse:** A look-as-legitimate program with hidden malicious contents.
- **Virus:** A malware that replicates itself over to other computers in contact with an infected computer.
- **Worm:** An independent program that replicates itself over networked computers and compromises the security.
- **Zombie/bot:** A program which is activated over remote system to make a team attack over a victim computer.

Module No – 175: Denial of Service (DoS) Attacks: bhut sary user ko virus spread kr skty hn

- It floods the servers, systems and networks with traffic.
- Makes it impossible for legitimate users to work on the affected IT-resources.
- Difficult to recover from DoS attack. Restarting is also not helpful most of the times.
- Executed not for ransom but to cause harm to the victim.
- The United States **Computer Emergency Readiness Team (US-CERT)** defines the following symptoms:

- ✓ Degradation in network performance
 - Inability to reach a website
 - Higher than usual volumes of spam email.
- Remedies for DoS attacks:
 - Contact ISP to clarify the reason of downgraded network performance.
 - ISP can help in throttling malicious traffic.
 - Using DoS detection tools.
- Usual victims: Application servers, DNS servers
- Can be in the form of TCP handshake flood, packet flooding with overloaded payload etc.

Module No – 176: Intrusion detection & Firewalls:

- A firewall is a hardware and/or software based module to block unauthorized access (but allowing authorized access) in a networked environment.
 - Stands between a local network and Internet.
 - Filters the harmful traffic.
- Firewall performs packet filtering on the basis of source/destination IP address.
- Firewall checks the packets on the basis of connections (stateful firewall).
- Other types of firewalls also exist.
- Intrusion detection system (IDS) is a software or hardware device installed on a network or a host to detect intrusion attempts, monitors malicious activity or policy violations.
- Intrusion detection system (IDS) is a software or hardware device installed on a network or a host to detect intrusion attempts, monitors malicious activity or policy violations.

Module No – 177: Buffer Overflow Attacks:

- Allows the attacker to control or crash the process or to modify its internal variables. multiple process run ho rhy hn eski occurrence ho skti h user ki traf sy bhi ho ksti hn aur by chance bhi perform ho skti hen
- Can be launched through DoS attack. as prog execute ho rah h execution ki halat mi crash kr
- Can also occur by chance. dyn buffer overflow or stack parameters ki value change kr dyinnn run hoty process ko disturb kr dyn

- It occurs when a program attempts to write more data to a block of memory or buffer than the allowed volume. data process hota hn usy memory ka block addign kia jat hn bs usi mi he process hota hn buffer khty hn prog es sy zyda data nae store or process kry gaaa xyda data agr hn usy destroy kr dia jae gaa or 2sry sath waly buffer or block mi store kr dia jae gaa
- **The overflowed data** is written to the adjacent block/s of the memory. Thus overwriting the adjacent blocks.
- If the adjacent memory buffer is overwritten then the attacker may overwrite a chosen address to a function pointer in that buffer. The chosen address is of a memory location with malicious address.
- Now the function pointer is pointing at the malicious code.
- When the (overwritten) function pointer is executed, the malicious code starts to execute and the attacker gets the system control.
- Can occur wherever direct memory access is allowed such as in C and C++.
- C# and Java have reduced coding errors causing buffer overflow.

WPA wifi protected access

SSL sec socket laye???????
yh browsers or web ka certificate ko verofy krti hn
authentic hn certificate valid hn still ky nae
<https://> authentic and secure web

Module No – 180: Operating System and Virtualization Security

- The installation of operating system requires some security measures such as:
- **Planning:** The purpose, user, administrator and data to be processed on that system.
- **Installation:** The security measures should start from the base.
- BIOS level access should be secured and with a password.
- The OS should be patched/updated with latest critical security patches before installing any applications.
- Remove unnecessary services, applications and protocols.
- Configure the users, groups and authentication according to security policy.
- Configure the resource control/permissions. Avoid the default permissions. Must go through all the permissions.
- Install additional security tools such as anti-virus, malware removal, intrusion detection system, firewall etc.
- Identify the white listed applications which can execute on the system.
- **Virtualization Security:** The main concern should be:
 - Isolation of all guest OSs.
 - Monitoring all the guest OSs.
 - Maintenance and security of the OS-images and snapshots.
- Can be implemented through:
 - Clean install of hypervisor from secure and known source.
 - Ensure only the administrative access to hypervisor, snapshots and OS images.
 - The guest OS should be preconfigured to not to allow any modifications/access to underlying hypervisor by the users.
 - Proper mapping of virtual devices over physical devices.

178 must raed?

- Network monitoring etc.

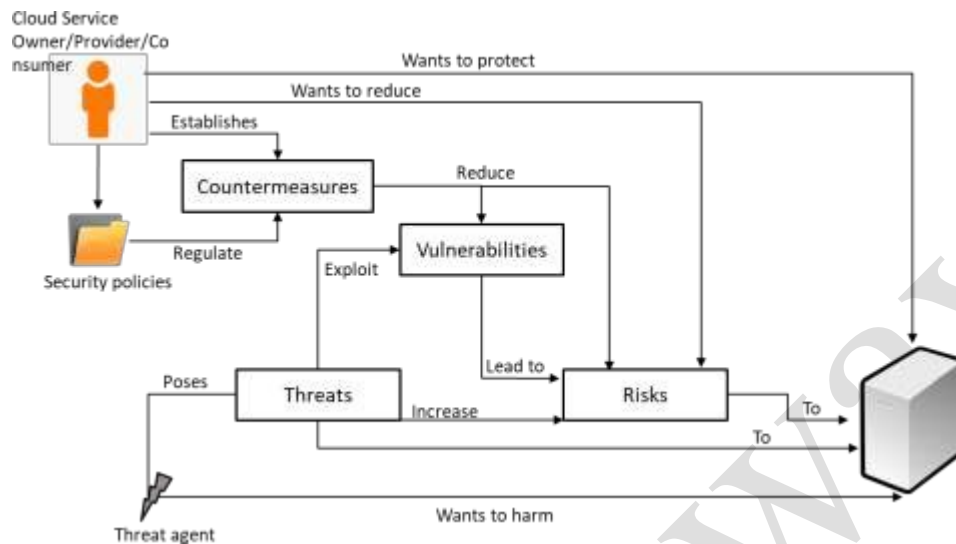
Module No – 181: Threat, Vulnerability & Risk

- **Threat:** It is a potential security breach to affect the privacy and/or cause a harm.
 - Can occur manually and/or automatically.
 - A threat executed results in an *attack*.
 - Threats are designed to exploit the known weaknesses or *Vulnerabilities*.
- **Vulnerability:** It is a (security) weakness which can be exploited.
 - It exists because of:
 - Insufficient protection exists and/or the protection is penetrated through an attack.
 - Configuration deficiencies
 - Security policy weaknesses
 - User error
 - Hardware or firmware weaknesses and software bugs
 - Poor security architecture
- **Risk:** It is a possibility of harm or loss as a result of an activity.
 - Measured according to
 - Threat level
 - Number of possible vulnerabilities
 - Can be expressed as:
 - Probability of occurring of a threat to exploit vulnerabilities
 - The expectation of loss due to compromise of an IT resource

Module No – 182: Threat Agents:

- A threat agent is a factor which is capable of carrying out an attack.
- It can be internal or external and can be human or software.
- **Anonymous Attacker:** A non-privileged service consumer not fully aware of Cloud security measures. Launches network attacks. Can steal user credentials. Can be inhibited by Cloud security measures.
- **Malicious Service Agent:** Can be or acts like a service agent. Has malicious code. Can interpret and forward the network traffic inside Cloud.
- **Trusted Attacker:** Is in the form of legitimate Cloud consumer and launches attacks on other Cloud consumers and the provider to steal information, DoS, hacking of weak authentication processes etc.
- **Malicious Insider:** Typically human threat agent. Can be current or previous employee. Can cause significant damage with administrative rights.

human base hn threat employee hn usy sub chez ka pata hn yh bhut dangerousful ho skta hn



Follow the video lecture to understand fully

Lesson No. 35

NETWORK SECURITY BASICS

Module No – 178: Internet Security:

- It is a branch of computer security which specifically deals with threats which are Internet based.
- The major threats include the possibilities of unauthorized access to any one or more of the following:
 - Computer system
 - Email account
 - Website
 - Personal details and banking credentials
- Viruses and other malware
- Social engineering
- **Secure Socket Layer (SSL):** It is security protocol for encrypting the communication between a web browser and web server.
 - The website has to enable SSL over its deployment.
 - The browser has to be capable of requesting a secure connection to the websites.
 - Upon request, the website shares its security certificate (issued by a Certificate Authority (CA)) with the browser which the browser confirms for validity.

- Upon confirmation of security certificate, the browser generates the session key for encryption and shares it with website, after this the encrypted communication session starts.
- Websites implementing the SSL use HTTPS (https://...) in the URL instead of HTTP (http://...) and a sign of padlock before the URL.

Module No – 179: Wireless Network Security:

- The wireless network security is applied to wireless networks and is also known as **wireless security**.
- It is used to secure the wireless communication from unauthorized access.
- There are a lot of threats for wireless networks. Such as:
 - The packets can be easily eavesdropped and recorded.
 - The traffic can be modified and retransmitted more easily as compared to wired networks.
 - Prone to DoS attacks at access points (APS).
- Some prominent security protocols for wireless security are:
 - **Wired Equivalent Privacy (WEP)**: Designed to provide the same level of security as the wired networks.
 - First standard of 802.11
 - Uses RC4 standard to generate encryption keys of length 40-128 bits.
 - Has a lot of security flaws, difficult to configure and can easily be cracked.
 - **Wi-Fi Protected Access (WPA)**: Introduced as an alternative to WEP while a long-term replacement to WEP was being developed.
 - Uses enhanced RC4 through Temporal Key Integrity Protocol (TKIP) which improves wireless security.
 - Backward compatible with WEP.
 - **Wi-Fi Protected Access 2 (WPA2)**: Standardized release by IEEE as 802.11i the successor to WPA.
 - Considered as the most secure wireless security standard available
 - Replaces the RC4-TKIP with stronger encryption and authentication methods:
 - Advanced Encryption Standard (AES)
 - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
 - Allows seamless roaming from one access point to another without reauthentication.

Lesson No. 36

CLOUD SECURITY MECHANISMS

Module No – 183: Encryption:

- The data by default in human readable format called **plaintext**.
- If transmitted over network, the plaintext data is vulnerable to malicious access.

Raja Mushtaq: +923055868956

- **Encryption** is a digital coding system to transform the plaintext data into a protected and nonreadable format while preserving the confidentiality and integrity.
- The algorithm used for encryption is called **cypher**.
- The encrypted text is also called **cyphertext**.
- The encryption process uses **encryption key** which is a string of characters. It is secretly created and shared among authorized parties.
- The encryption key is combined with the plaintext to create the encrypted text.
- **Encryption helps in countering:**
 - Traffic eavesdropping
 - Malicious intermediary
 - Insufficient authorization
 - Overlapping trust boundaries
- This is because the unauthorized user finds it difficult to decrypt the intercepted messages.
- There are two basic types of encryption:
 - **Symmetric Encryption:** It uses single key for encryption and decryption. Also known as **secret key cryptography**. Simpler procedure. Difficult to verify the sender if the key is shared by multiple users.
 - **Asymmetric Encryption:** Uses two different keys (private and public key pair). Also known as **public key cryptography**. A message encrypted with public key can only be decrypted by the respective private key and vice versa.
 - Any party can acquire a public-private key pair. Only the public key is shared publicly.
 - The senders can use the public key of the receiver to encrypt messages. Only the user with corresponding private key can decrypt the message.
 - Successful decryption can ensure confidentiality but does not assure integrity and authenticity of the sender as anyone can encrypt the message using public key.

Module No – 184:

- **Hashing:** It is a process of deriving a hashing code or *message digest* from a message.
 - The message digest is of a fixed length and is shorter than the original message.
 - Uses a hash function to generate the hashing code.
 - A change in message requires the hashing code to be regenerated.
 - The hashing code is attached with the message and sent to the receiver.
 - The receiver applies the same hash function to verify the integrity of the message.
 - If the message was altered during transmission, the receiver side hashing code computation will mismatch the hashing code received with the message. The receiver rejects such messages.
- **Digital Signatures:** It is a mechanism of verifying the authenticity and integrity of a message, software and/or digital comment.
 - It is a digital equivalent of handwritten signature. Used to prevent the tampering and impersonation in digital communication.
 - In many countries, the digital signatures have a legal value.
 - The hashing function is applied to the original message to generate a message digest.

Raja Mushtaq: +923055868956

- The message digest text is changed through cryptographic mechanism known only by the sender and receiver.
- The encrypted hash code and hashing algorithm is the digital signature.
- Alteration can be detected at receiver end.
- The administrative tools used by Cloud consumers use the digital signatures with every request to prove the authenticity of each consumer.

Module No – 185: Public Key Infrastructure (PKI):

asymmetric encryption keys usko baqyda thoor py run krny ky liyee aur manage ky liye yeh use kia jata hn

- It is a mechanism of issuing, supporting and managing the asymmetric encryption keys systematically.
- An encryption key is a string of bits which is paired with the original data to transform it into encrypted data or cyphertext.
- It is also a system of protocols and data formats etc. to enable the large scale systems to use public key cryptography.
- PKI relies upon digital certificates. Each digital certificate binds the public key to a certificate owner.
- A digital certificate has a validity period and is signed by a certificate authority (CA).
- It is a dependable method to:
 - Implement asymmetric encryption.
 - Managing Cloud consumer and Cloud provider identity information.
 - Defending against malicious intermediary and insufficient authorization threats.

Module No – 186: Identity and Access Management (IAM):

- It is a mechanism comprising of policies and procedures to track and manage the user identities and access privileges for IT resources. it user ki previllages ko manage krta hn aur jo login krty hn unhy ni
- Consist of four main components:
 - **Authentication:** Usernames+passwords, biometric, remote authentication through registered IP or MAC addresses.
 - **Authorization:** Access control and IT resource availability. legal hn usy kis kis type ky control overhand krny chae
 - **User management:** Creating new user-identities, password updates and managing privileges.
 - **Credential management:** It establishes identities and access control rules for defined user accounts.
- As compared to PKI, the IAM uses access control policies and assigns user privileges.
- **Single Sign-On:** Saves the Cloud consumers from signing-in to subsequent services if the consumer is executing an activity which requires several Cloud services. aik he jaga sign ina and login krna pr agai and agai authentication ki need nah pry
 - A security broker authorizes the consumer and creates a security context persistent across multiple services.

Module No – 187:

- **Cloud-based Security Groups:** Cloud IT resources are segmented for easy management and provisioning to separate users and groups.
 - The segmentation process creates Cloud-based security groups with separate security policies.
 - These are logical groups which act as network perimeters.
 - Each Cloud-based IT resource is assigned to at least one logical cloud-based security group.
 - Multiple VMs hosted over same physical server can be allocated to different cloud-based security groups.
 - Safeguard against DoS attacks, insufficient authorization and overlapping trust boundaries threats.
 - Closely related to logical network perimeter mechanism.
- **Hardened Virtual Server Images:** It is a process of removing unnecessary software components from the VM templates.
 - It also includes closing unnecessary ports, removing root access and guest login and disabling unnecessary services.
 - Makes the template more secured than non-hardened server image templates.
un awnated component nikal dy sw sy wo chez bchy gi jo sirf humy pata hn

Lesson No. 37

PRIVACY ISSUES OF CLOUD COMPUTING

Module No – 188: Lack of user control:

- Data privacy issues such as unauthorized access, secondary usage of data without permission, retention of data and data deletion assurance occur in Cloud Computing.
- With the data of a SaaS user placed in Cloud, there is a lack of user control over that data.
- A few reasons are as follows:
 - **Ownership and control of infrastructure:** The user has neither ownership nor the control of underlying infrastructure of the Cloud. There is a threat of theft, misuse and unauthorized sale of user's data.
 - **Access and transparency:** In many cases, it is not clear that a Cloud service provider can/will access the users' data. It is also not clear that an unauthorized access can be detected by the Cloud user/provider.
 - **Control over data lifecycle:** The Cloud user can not confirm that the data deleted by the user is actually been deleted. There is no assurance for the data deletion of terminated accounts as well. There is no regulation to implement a must-erase liability on Cloud provider.
 - **Changing provider:** It is not clear how to completely retrieve the data from previous provider and how to make sure that the data is completely deleted by the previous provider.
 - **Notification and redress:** It is not clear how to determine the responsibility of (user or provider for) an unauthorized access.

koi mechanism ni hn kis py responsibilities daalii jae user or cloud zimadar hnn agr unauthorize acces hoti hn tu

Module No – 189: Lack of Training and Expertise:

- The deployment and running of Cloud service may require the recruitment of highly skilled personals.
- For example the **STEM** skills (Science, Technology, Engineering and Mathematics) should be present in the recruited people.
- The lack of STEM skilled and/or trained persons can be a Cloud security issue.
- Such people may also lack the understanding of the privacy impact of their decisions.
- Due to the rapid speed and spread of computing devices among the employees, now more employees may introduce a privacy threat on average.
- For example multiple employees may leave their laptops unattended with a further possibility of unencrypted sensitive data.
- The employees can access different public Cloud services through self service portals.
- Care and control must be observed regarding public Cloud access to overcome the privacy issues.

Module No – 190: Unauthorized Secondary Usage:

possibility hn ky jo data cloud py rkhty hn uska ownwer or user hn u
ska dta batae beghair use krna read krna yh possibilities ho skti h

- There is a high tendency that the data stored or processed over Cloud may be put to unauthorized usage.
- A legal secondary-usage of Cloud consumers' data is to sell the statistics for targeting the advertisements. us data mi sy kuch data user ka aggy advertysing comp ko sale kr dy wo paisy charge krty yh leagal way hn user ny ijazat di hn
- However an illegal secondary-usage example is the selling of sales data to competitors of the consumer.
- Therefore it may be necessary to legally address the usage of consumer's data by the Cloud provider.
- So far there are no measures and means to verify the illegal secondary-usage of consumers' data by the Cloud provider/s.
- In future, a technological solution may be implemented for checking and preventing the unauthorized secondary usage of consumers' data.

Module No – 191: Complexity of Regulatory Compliance:

cloud cpm all over the world rule ko follow ni kr skti

- The global nature of Cloud computing makes it complex to abide by all the rules and regulations in different regions of the world.
- The legal bindings regarding data location is complex to implement because the data may be replicated on multiple locations at the same time.
- It is also possible that the each replicated copy of the data is managed by different entities for example backup services obtained from two different providers.
- The backup provided by a single provider may be spread across different data centers which may or may not be within the legal location-boundary.

Raja Mushtaq: +923055868956

- The rapid provisioning architecture of the Cloud makes it impossible to predict the location of to-be-provisioned Cloud resource such as storage and VMs.
- The cross border movement of data while in transit is very difficult to control. Specially when the data processing is outsourced to another Cloud provider. Then the location assurance of such Cloud provider is a complex task at runtime.

one country boarder sy dat aout krna us ky kiya rule hn

Module No – 192: Addressing Trans-border Data Flow Restrictions:

- The privacy and data protection regulations in many countries restrict the trans-border flow of personal information of the citizens.
- These countries include EU and European Economic Area (EEU) countries, Australia, Canada etc. yh data citizen ka out ni krti
- From EU/EEU countries, the personal information can flow to countries which have adequate protection. These include the EU/EEU countries and Canada etc.
- The flow of personal information to other countries is restricted, unless some rules/agreements are followed by those countries.
- For example the information can be transferred from EU to USA if the receiving entity has joined the US Safe Harbor agreement. agr us country mi eradicate ho sec about then data dynd kr skty hn
- If the receiving country has signed a model contract with the EU country/ies then the personal information can flow towards the receiving country.
- So far the trans-border regulations are not complied with Cloud computing and there is more to be done to implement these data flow restrictions.

Module No – 193: Litigation:

- A Cloud Service Provider (CSP) may be forced to hand over the consumers' data due to a court writ. order kry gi cloud ko ky user ka jo record hn show kia jae
- For example, in a case handled by the US court of law, with state vs. the defendant, the US govt. was allowed the access to Hotmail service (of Microsoft) through the court orders.
- . The govt. always wants to check the relevance of evidence with the case. For that, the court can allow access to consumers' data.
- But for private entities, this situation can be avoided through the clauses of legal agreement to bind the CSP for disallowing any access (by a non govt. entity) to the data. OR to govern the response of CSP to any writ from such entities.

Module No – 194: Legal Uncertainty:

- Since the Cloud computing moves ahead of the law, there are legal uncertainties about the privacy rights in the Cloud.
- Also, it is hard to predict the outcome of applying the current legal rules regarding trans-border flow of data to Cloud computing.

- One of the areas of uncertainty is about the procedure of anonymizing or encrypting of personal data requires a legal consent from the owner and the processing related to enhancement of data privacy is exempt from privacy protection requirements?
- Also, it is not clear that the anonymized data (which may or may not contain personal data) is also governed by the trans-border data flow legislations or not.
- In short, the legal uncertainty exists regarding the application of legal frameworks for privacy protection upon Cloud computing.

Module No – 195: Conclusions:

- There is uncertainty in privacy protection globally.
- Cloud globalization has invoked new demands of privacy protection from the existing security-frameworks.
- Policymakers are pushing towards the change in security frameworks and placing more emphasis upon accountability for data privacy related violations.
- USA and EU are currently considering the Privacy Bill of Rights and the data protection framework respectively for privacy protection.
- Cloud computing offers complex challenges for entities that need to meet global privacy regulations.
- Complying with trans-border data flow restrictions, the difficulty in knowing the geographic location of data processing and storage location are the major challenges for privacy assurance in Cloud computing.
- Data deletion and discarding of virtual storage device/s must be carefully assured.

Lesson No. 38

SECURITY ISSUES OF CLOUD COMPUTING

● **Module No – 196: Gap in Security:**

- Although the security controls for the Cloud are same as of other IT environments, but the lack of user control in Cloud computing introduces security risks.
- These security risks are due to a possible lack of effort for addressing the security issues by the Cloud service provider.
- SLAs do not include any provision of the security procedures made necessary by the consumer or through any standard.
- The gap in security also depends upon the type of service (IaaS, PaaS & SaaS).
- The more privileges given to the consumer (for example in IaaS), the more responsibility of security procedures lies with the consumer.
- The consumer may need to gain the knowledge of the security procedures of provider.
- The provider gives some security recommendations to IaaS and PaaS consumers.

Raja Mushtaq: +923055868956

- For SaaS, the consumer needs to implement its own identity management system for access security.
- Generally, it is very difficult to implement protection throughout the Cloud. In few cases the Cloud providers are bound by law for the protection of personal data of the citizens.
- It is difficult to ensure the standardized security when a Cloud provider is outsourcing resources from other providers.
- Currently the providers take no responsibility/liability for deletion, loss or alteration of data.
- The terms of service are usually in favor of the provider.

Module No – 197: Unwanted Access:

user ki willingness ky without data access kia jae agrrr

- Cloud consumers may experience unwanted access to their data from the governments. There are many laws in the world (for example the US Patriot Act) which allow the government a privileged access to the Cloud consumers' data.
- The other type of unwanted access is from the lack of adequate security when the Cloud provider is in a supply chain link with other providers.
- A malicious employee may have a privileged access to data (because of being the employee).
- Data thieves and even the other consumers of the same service may break into the consumers' data if the data of each consumer is not adequately separated.
- The damage can be far greater than non Cloud environments due to the presence of various roles in Cloud architectures with administrative level access.
- In general the Cloud storage is more prone to risks from malicious behavior than the Cloud processing
- This is because the data may remain in Cloud storage for longer period of time and hence exposed to more risks.

Module No – 198: Vendor Lock-in:

aik vendor py rely honaa uski mjbhori
bn jana wo 2sry vendor or server
py move nah kr sky

aik cloud server sy 2sry server mi data
synd krny sy phly dat ki format
change krni pry gi bkaz aik server ky
satndard 2sry server ky standard
diff hn

- Cloud computing in today's time lacks interoperability standards.
- There are certain limitations such as
 - Difference between common hypervisors.
 - Gap in standard APIs for management functions.
 - Lack of commonly agreed data formats.
 - Issues with machine-to-machine interoperability of web services.
- The lack of standards makes it difficult to establish security frameworks for heterogeneous environments.
- People mostly depend upon common security best practices.
- Since there is no standardized communication between Cloud providers and no standardized data export format, it is difficult to migrate from one Cloud provider to another or to bring back the data and process it in-house.

Module No – 199: Inadequate Data Deletion:

- So far there is no surety or confirmation functionality for the deleted data being really deleted and non-recoverable by the service provider.
- This is due to lack of consumer control over life cycle of the data (as discussed before).
- This problem is increased with the presence of duplicate copies of the data. back up data agr nah kry del
- It might not be possible to delete a virtual disk completely because several consumers might be sharing it or the data of multiple consumers resides over same disk.
- For IaaS and PaaS, the reallocation of VMs to subsequent consumers may introduce the problem of data persistency across multiple reallocations.
- This problem exists until the VM is completely deleted.
- For SaaS, each consumer is one of the users of a multitenant application. The customer's data is available each time the customer logs-in.
- The data is deleted when the SaaS consumer's subscription ends.
- There is correspondingly higher risk to customers' data when the Cloud IT-resources (such as VM and storage) are reused or reallocated to a subsequent consumer.

Module No – 200: Compromise of the Management Interface:

- As discussed previously, the management interfaces are available through remote access via Internet.
- This poses an increased risk compared to traditional hosting providers.
- There can be vulnerabilities associated with browsers and remote access.
- These vulnerabilities can result in the grant of malicious access to a large set of resources.
- This increased risk is persistent even if the access is controlled by a password.

Module No – 201: Backup Vulnerabilities:

- In order to provide high level of reliability and performance, a Cloud provider makes multiple copies of the data and store them at different locations.
- This introduces many vulnerabilities.
- There is a possibility of data loss from Storage as a Service.
- A simple solution is to place data at consumer's premises and use the Cloud to store (possibly encrypted) backup of data.
- A loss of data may occur before taking backup.
- A subset of the data may get separated and unlinked from the rest and thus becomes unrecoverable.
- The failure/loss of data-keys may significantly destroy the data context.
- Sometimes the consumers of traditional (non-Cloud) backup service suffer a complete loss of their data on non-payment of periodic fee.
- In general, the Cloud service show more resiliency than these traditional (non-Cloud) services.

separate

Module No – 202: Isolation Failure:

multi-tenant multi user work at the same time
data ko 2sry person sy hidden rkhnay ky liye partitioning krty hn

- The multi-tenant SaaS applications developed by Cloud providers use logical/virtual partitioning of the data of each consumer.
- It is possible that such applications be storing the personal and financial data of the consumers on Cloud. sensitive data or personal data inh py store kia jaa rah ho
- This responsibility of securing this data is of the Cloud provider.
- Due to the possibility of the failure of data separation mechanisms, the other tenants can access the sensitive information. failure mi customer aik 2sry ka data bhi get kr skty hn
- Virtualization is widely used in Cloud computing. The VMs although are isolated from each other, yet the virtualization based attacks may compromise the hosting server and hence expose all the hosted VMs to the attacker. isolation failure attack or bugs ki waja sy bhi ho saktaa hain

believe

shafafiat

agr missess hn tu cloud mi kia kia sec issue ho sktyh

Module No – 203: Missing Assurance and Transparency:

cloud provider data loss ki responsibilities kaam sy kaam rkhtaa hain. . .

- As discussed before, the Cloud provider take lesser liabilities in case of data loss.
- Therefore, the consumers should obtain some assurance from the Cloud provider regarding the safety of their data. consumer ko kuch assurance require hoti hn uska data safe rhy gaa cloud py
- Consumers may also demand for getting the warning/s regarding any attack/unauthorized access/loss of data.
- A few frameworks exist for security assurance in Cloud. The Cloud providers offer the assurance on the basis of these frameworks.
- However these assurances may not be applied in case of frequent data accesses and/or in case of some instances such as isolation failure (discussed previously).
- Still, there is no compensation offered by the Cloud providers for the incidents of data loss.
- The best assurance for data security in Cloud computing is achievable through keeping the data in private Cloud.
- Although automated data security assurance evaluation frameworks exist but they still need to evolve in order to comply with all the security issues discussed in this course.

Module No – 204: Inadequate Monitoring, Compliance and Audit:

Audit data process kr krky apni process ko security ky liye check kr kr security krskty

- A Cloud consumer should be able to audit the data processing over Cloud to ensure that the Cloud procedures are in compliance with the security policy of the consumer.
- Similarly the Cloud consumers may want to monitor SLA compliance by the provider but the complexity of Cloud infrastructure makes it very difficult to extract the appropriate information or to perform a correct analysis.
- Cloud providers could implement the internal compliance monitoring controls in addition to external audit process.
- The consumers may even be allowed a 'right to audit' for those particular consumers who have regulatory compliance responsibilities.

- Although the existing procedures for audit can be applied to Cloud computing but the provision of a full audit trail with the public Cloud models is still an unsolved issue.

Module No – 205: Conclusion:

- There are a number of security issues in Cloud computing.
- These issues depend upon the service provision and deployment models.
- Cloud audit is one of the open issues of Cloud security.
- Overall, the adoption of Cloud computing does not necessarily affects the security.
- The security can be outsourced to the experts of security to achieve better security than before.
- The major issue is to find a Cloud provider with suitable controls to assure security, monitoring and audit.

Lesson No. 39

TRUST ISSUES OF CLOUD COMPUTING

Module No – 206: Trust in the Clouds:

- Cloud consumers have to trust the Cloud mechanisms for storing and processing the sensitive data.
- Traditionally, a security perimeter (such as a firewall) is instantiated to setup a trust boundary within which there is a self-control over computing resources and where the sensitive data/information is stored and processed. firewall add ki jae es thk apka data sensitively ap access kr skty hn
- . The network provides trusted links to other trusted end hosts.
- This may work perfectly for the Internet but may not work for public and hybrid Clouds.
- This is because the data may be stored and/or processed beyond the security perimeter such as supply chain issues discussed before.
- The consumers have to extend the trust boundaries to the Cloud provider.
- Therefore, the consumers should only trust the Cloud provider if the information about the reliability of internal mechanisms is provided by trusted entities such as consumer groups, auditors, security experts, reputed companies and established Cloud providers etc.
- The trust relationships can be the decision affecting factors for adopting/accepting a particular security and privacy solution.
- Trust attains a higher level of importance if personal or business critical information is to be stored in Cloud.
- Therefore, the Cloud providers have to have high trust from the consumers.

Module No – 207: Lack of Consumer Trust:

- In the past various surveys in Europe have revealed the lack of consumer trust upon the protection of their data kept online. jo data store hn online user trust ni krty mostly
- Up to 70% of Europeans were concerned about the non authorized secondary usage of their data.
- The survey about trust on Cloud provider showed the following statistics:
 - Reputation: 29%
 - Recommendation from trusted party: 27% loogo ki kaam taadahhd hn jo clouder py trust krty hn
 - Trial experience: 20%
 - Contractual: 20%
 - Others: 4%
- The consumer trust depends upon the compatibility level of data protection provided by the Cloud provider vs. the consumer's expectations. consumer ki expectation ky about clouder data ki sec provide kr rahh hennn
- A few such expectations include the regulatory compliance of data handling procedures and control over data lifecycle even in supply chain Cloud provisioning. rule
- 70% of the business users (in selected regions of the world) are already using private Clouds according to a study.
- However different surveys showed that the enterprises are concerned about:
 - Data security: 70%
 - SLA compliance : 75% consumer ka cloud py weak trust chal rahh hnnnn
 - Vendor lock-in: 79%
 - Interoperability: 63%

Module No – 208: Weak Trust Relationships:

- Although the Cloud provider/s may be using a supply chain mechanism through the IT resources of subcontractors. aik cloud provider 2sry cloud provider sy services ly ky aggy consumer ko provide krr rahhh hnn
- This may jeopardize the security and privacy of the consumers' data (as discussed before) and thus weakens the trust relationships. 3rd party sy contact kr ky provide kr rah hnn dataa
data ko cloud provider ki trf syy aggy subcontractor (3rd person) ko handover krna its cloud be harmful
- Even if the trust relationships are weak in service delivery chain, but at least some trust exists so that the rapid provisioning of the Cloud services can be performed.
- Significant business risks may arise when critical data is placed on cloud and the consumer has lack of control over the passing of this data to a subcontractor.
- So the trust along the service delivery chain from the consumer to Cloud provider is non-transitive.
- There is a lack of transparency for the consumer in the process of data flow. The consumer may even not know the identity of the subcontractor/s.
- In-fact, the 'On-demand' and 'pay-as-you-go' models may be based upon weak trust relationships.
- This is because new providers have to be added on the go to provide the extra capacity on short notice.

Module No – 209: Lack of Consensus About Trust Management Approaches to Be Used:

trust aik concept hn esko number mi represent krna muskal hnn

- The consensus about the use of trust management approaches for Cloud computing is missing.
- Trust measurement is a major challenge due to the difficulty of contextual representation of trust.
- Some standardized trust models are required to be created for evaluating and assurance of accountability.
- Almost all of the existing models for trust evaluation are not adequate for Cloud computing.
- The existing models of trust evaluation in Cloud computing partially cover the trust categories.
- Trust models are lacking a suitable metrics for accountability.
- There is no consensus on type of evidence required for the verification of the effectiveness of trust mechanisms.

Module No – 210: Conclusions:

rule aj ky era mi imp concern hn

- Trust is widely considered as a key concern for consumers, enterprises and regulators.
- Lack of trust is the key factor which inhibits the wide adoption of Cloud services by the end-users.
lack of trust is imp part for consumer
- People are worried about what will happen to their data when it is placed on Cloud.
- There is a fear of unwanted access, unauthorized access and unauthorized secondary usage of the data.
- There is a lack of user control.
- Enterprises shifting to public Cloud are concerned about the confidentiality and security of their data.
- The regulators are worried about illegal trans-border transfer of data.
- Thus the usage of Cloud is a question of trade-offs between privacy, security, compliance, costs and benefits.
- Trust mechanisms have to be propagated along the chain of service provision.
- Trust measurement models are to be developed to cover all aspects of trust in Cloud computing.

Module No – 211: Trust Management in Cloud Computing:

- In order to monitor and evaluate the trust, the systematic trust-management is required.
- There should be a system to manage the trust.
- The trust management system should be able to measure the “trustfulness” of the Cloud services.
- The following attributes can be considered:
 - **Data integrity:** Consisting of security, privacy and accuracy.
 - **Security of consumers’ personal data.**
 - **Credibility:** Measured through QoS.

- Turnaround efficiency: The actual vs. promised turnaround-time. It is the time from placement of consumer's task to the finishing of that task.
- Availability of Cloud service provider's resources and services.
- Reliability or success rate of performing of agreed upon functions within the agreed upon time deadline.
- Adaptability with reference to avoidance of single point of failures through redundant processing and data storage.
- Customer support provided by the Cloud provider.
- The consumer feedback on the service being offered.
- These attributes can be graded and trust computation can be performed. The computed value can be saved for future comparison.

Module No – 218: Approaches to Addressing Privacy, Security and Trust Issues:

- In this module we shall briefly discuss the possible approaches to solve the privacy, security and trust issues in Cloud.
- There are three main dimensions in this regard:
- Innovative regulatory frameworks to facilitate the Cloud operations as well as to solve the possible issues regarding privacy, security and trust.
- Responsible company governance should be exhibited by the provider to show the intension of safeguarding the consumer's data and intension to prove this intension through audit.
- Use of various supporting technologies for privacy enhancement, security mechanisms, encryption, anonymization etc.
- By using a combination of these dimensions, the consumers can be reassured of the security and privacy of their data and the Cloud provider can earn the trust.

Lesson No. 40

OPEN ISSUES IN CLOUD

Module No – 212: Overview:

- Cloud is not a solution for all consumers of IT services.
- Cloud is also not suitable for all applications.
- Cloud computing contains a number of issues which are not necessary unique to Cloud.
- Hardware failures and security compromises are possible in complex computing systems.
- Similarly the software built to fulfill complex requirements of concurrency, dynamic configuration and large scale computations are more prone to bugs and crashes than the commercial scale typical software.
- This should be kept in mind that the Cloud computing(which is based upon complex computing hardware and software) will also exhibit some failures and security compromises.
- But this does not disqualify the Cloud computing from being adopted by the consumers.

Raja Mushtaq: +923055868956

- Instead, it means that there are techniques to address, reduce the effects and isolate these failures and compromises.
- We shall discuss the issues related to Cloud computing in the coming modules as highlighted by NIST USA.

Module No – 213: Computing Performance:

- The real time applications require high performance and high degree of predictability.
- Cloud computing shows some performance issues which are similar to those of other forms of distributed computing.

Latency: As measured through round-trip time (the time from sending a message to receiving a response) is not predictable for Internet based communications.

- **Offline Data Synchronization:** For the offline updates in data, the synchronization with all the copies of data on Cloud is a problem. The solution to this problem requires the mechanisms of version control, group collaboration and other synchronization capabilities.
- **Scalable Programming:** The legacy applications have to be updated to fully benefit from scalable computing capacity feature of Cloud computing.

Data Storage Management: The consumers require the control over data life cycle and the information regarding any intrusion or unauthorized access to the data.

Module No – 214: Cloud Reliability:

- It is a probability that a system will offer failure-free service for a specified period of time for a specified environment.
- It depends upon the Cloud infrastructure of the provider and the connectivity to the subscribed services.
- Measuring the reliability of a specific Cloud will be difficult due to the complexity of Cloud procedures.

Several factors affect the Cloud reliability:

- **Network Dependence:** The unreliability of Internet and the associated attacks affect the Cloud reliability.
- **Safety-Critical Processing:** The critical applications and hardware such as controls of avionics, nuclear material and medical devices may harm the human life and/or cause the loss of property.
- These are not suitable to be hosted over Cloud

Module No – 215:

- **Economic Goals:** Although the Cloud provides economic benefits such as saving upfront costs and elimination of maintenance costs and provides consumers with economies of scale.

- However there are a number of economic risks associated with Cloud computing.

SLA Evaluation: The lack of automated mechanisms for SLA compliance by the provider requires the development of a common template that could cover the majority of SLA clauses and could give an overview of SLA compliance.

- This would be useful in decision making for investing the time and money in manual audit.
- **Portability of Workloads:** The initial barriers to Cloud adoption are the needs of a reliable and secure mechanism for data transfer to Cloud as well as to port the workload to other providers are open issues.

Interoperability between Cloud Providers: The consumers face or are in fear of vendor lock-in due to lack of interoperability among different providers.

- **Disaster Recovery:** The physical and/or electronic disaster recovery requires the implementation of recovery plans for hardware as well as software based disasters so that the provider and consumers can be saved from economic and performance losses.

Module No – 216: Compliance:

es mi rule and regulation & sec procedure implement krna

- It is with respect to any law and preferred security procedures.
- NIST and other US govt agencies are evolving methods to solve the compliance issues between consumers and providers.
- The consumer is although responsible for compliance but the implementation is actually performed by the provider.
- The consumer has a lack of visibility regarding the actual security procedures being adopted and/or applied by the provider. However the consumer may request for the deployment of monitoring procedures.
- The consumers (having their data processed on provider's premises) need to acquire assurance from the provider regarding the compliance with various laws. For example in US: the health information protection act, payment security standard, information protection accountability act etc.
- The forensics support regarding any incidence should be provided. This will evaluate the type of attack, the extent and damage associated and collection of information for possible legal actions in future.
- The forensic analysis for SaaS is the responsibility of the provider while the forensic analysis of IaaS is the responsibility of the consumer.

Module No – 217: Information Security:

- Related to confidentiality and integrity of data.
- It is also linked with the assurance of availability.
- The following measures can be used by an organization for data security:
 - Application of administrative controls for specifying the authority of specific users to create, update, delete, disclose and transport of the data.

- Physical controls for the security of data storage devices.
- Technical controls for Identity and Access Management (IAM), data encryption and data audit-handling requirements according to any regulatory need.
- Public and private Clouds have their own typical security exposures.
- The provider however may also provide physical separation of consumers' data in addition to logical separation.
- According to NIST, the provider should provide the monitoring mechanism to satisfy the consumer regarding the security compliance.

Lesson No. 41

DISASTER RECOVERY IN CLOUD COMPUTING

Module No – 219: Understanding the threats:

- **Disk Failure:** disk drives are electro-mechanical devices which wear out and eventually fail.
- Failure can be due to disaster such as fire and floods. Can also be due to theft.
- All mechanical devices have mean time between failure (MTBF).
- The MTBF values given by the manufacturers are usually generic values calculated for a set of devices. org khti hn yh device 5k hour bad fail hogi zaroori ni hn 5k baad fail ho us sy phly bhi ho skti hn fail. . . dont rely on MTBF
- Therefore, instead of relying upon the MTBF, there must be a disaster recovery plan for the disk failure.
- The following strategies can be utilized:
 - **Traditional approach:** It is to have backup on separate storage. If the disk fails due to any disaster, the data can be recovered on a new disk from the backup. But if the backup is also destroyed or stolen, then there is a complete loss of data. Also, the recovery process is time consuming.
 - **Redundant Array of Independent Disks (RAID):** It is a system consisting of multiple disk drives. Multiple copies of data are maintained and stored in a distributed way over the disks. If one disk fails, simply the disk is replaced and the RAID system copies the data over the new disk. But still backup is required because if the entire RAID is destroyed or stolen, there is a complete data loss.
 - **Cloud based data storage and backup:** Cloud not only provides the facility of data access over the Internet, but it also provides enhanced data replication. The replication is sometimes performed by default without any extra charges. The Cloud based backup is stored at a remote site so it is an extra advantage as compared to onsite backup placement.
 - Further, the Cloud based backup is readily available and thus reduces the downtime as compared to recovery using traditional tape-based backup.

Module No – 220: Understanding the threats:

light failure ki waja sy threat

- **Power Failure or Disruption:** The Computers can be damaged due to a power surge caused by a storm or some fault in power supply system.
- Power surge may permanently damage the disk storage.
- The user loses all the unsaved data when a power-blackout happens.
- A few disaster recovery plans are as follows:
 - Traditionally, the surge protector devices are used. But these devices are not helpful in saving the (unsaved) data in case of a blackout.
 - The in-house data centers can use huge and expensive uninterruptable power supply (UPS) devices and/or generators.
 - Another solution is to shift the data to another site. But this is expensive and time consuming.
 - The best option is to move the data center to Cloud. The Cloud providers have better (and expensive) power backups and their cost is divided among the consumers. Also, the Cloud mechanism may automatically shift the data to a remote site on another power grid (in case of power failures of longer duration).

Module No – 221: Understanding the threats:

- **Computer Viruses:** While surfing the web, the users may potentially be downloading and installing software and/or share the drive such as junk drives over their computing devices.
- These devices are at the risk of attacks through computer virus and spyware.
- Traditionally, the following techniques have been used for safeguarding against the virus attacks:
 - Making sure each computer has anti-virus installed and set to auto-update to get the most recent virus and spyware signatures.
 - Restrict the user privilege to install software.
 - Using a firewall over router or on the computer or around the LAN.
- Cloud computing presents difficulties for non-Cloud based viruses to penetrate. This is because of the complexities of virtualization technologies. Also the Cloud providers ensure reasonable security measures for the consumer's data and software.

Module No – 222: Understanding the threats:

- **Fire, Flood & Disgruntled Employees:** The fire as well as the fire extinguishing practices can destroy the computing resources, data and backup.
- Similarly the heavy and/or unexpected rainfall may cause an entire block or whole city including the computing equipment to be affected by a flood.
- Similarly an angry employee can cause harm by launching a computer virus, deleting files and leaking the passwords.

Raja Mushtaq: +923055868956

- Traditionally the office equipment is ensured to lower the monetary damage. Backup is used for data protection. Data centers use special mechanisms for fire-extinguishing without water sprinkles.
- By residing the data center over Cloud, the consumer is freed from making efforts and expenditures for fire prevention systems as well as for data recovery. The cloud provider manages all these procedures and includes the cost as minimal part of the rental.
- Unlike fire, the floods can not be avoided or put-off.
- The only possibility to avoid the damage due to floods is to avoid setting up the data center in a flood zone.
- Similarly, choose a Cloud provider which is outside any flood zone.
- Companies apply access control and backup to limit the access to data as well as the damage to data due to unsatisfied employees.
- In Cloud, the Identity as a Service (IDaaS) based single sign-on excludes the access privileges of terminated employees as quickly as possible to prevent any damages.

Module No – 223: Understanding the threats:

- **Lost Equipment & Desktop Failure:** The loss of equipment such as a laptop may immediately leads to the loss of data and a possible loss of identity.
- If the data stored on the lost device is confidential then this may lead to even more damage.
- Traditionally the risk of damage due to lost or stolen devices is reduced by keeping backup and to safeguard the sensitive data, login and strong password for the devices are used.
- But even the strong passwords are not difficult to break for the experienced hackers. Yet most of the criminals are still prevented to access the data.
- For the Cloud computing, the data can be synchronized over multiple devices using the Cloud service. Therefore the user can get the data from online interface or from other synced devices.
- In case of desktop failure, the user (such as an employee of a company) becomes offline until the worn out desktop is replaced.
- If there was no backup, the data stored on the failed desktop may become unrecoverable.
- Traditionally, data backup is kept for the desktops in an enterprise. The backup is stored on a separate computer. In case of desktop failure, the maintenance staff tries to provide alternative desktop and restore the data as soon as possible.
- Whereas in Cloud, the employees work on the instances of IaaS or Desktop as a Service by using the local desktops.
- In case of desktop failure, the employee can just walk to another computer and log in to the Cloud service to resume the work.

Module No – 224: Understanding the threats:

- **Server failure & Network Failure:** Just like the desktops, the servers can also fail.

Raja Mushtaq: +923055868956

- The replacement of blade server is relatively simple process and mostly the blade servers are preferred by the users.
- Ofcourse there has to be a replacement server in stock to replace with the failed server.
- Traditionally the enterprises keep redundant servers to quickly replace a failed server.
- In case of Cloud computing, the providers of IaaS and PaaS manage to provide 99.9% up-time through server redundancy and failover systems. Therefore the Cloud consumers do not have to worry about server failure.
- The network failure can occur due to a faulty device and will cause downtime.
- Traditionally, the users keep 3G and 4G wireless hotspot devices as a backup. While the enterprises obtain redundant Internet connections from different providers.
- Since the Cloud consumers access the Cloud IT resources through the Internet, the consumers have to have redundant connections and/or backup devices for connectivity.
- Same is true for the Cloud service provider. The 99.9% up-time is assured due to backup/redundant Network connections.

Module No – 225: Understanding the threats:

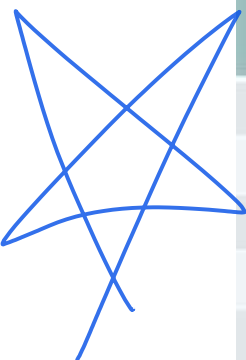
- **Database System Failure & phone system failure:** Most of the companies rely upon database systems to store a wide range of data.
- There are many applications dependent upon database in corporate environment such as customers record keeping, sale-purchase and HR systems etc.
- The failure of data base will obviously makes the dependent application unavailable.
- . Traditionally, the companies either use a backup or replication of database instances. The former case results in downtime of database system while the latter results in minimum downtime or no downtime but is more complicate to implement.
- The Cloud based storage and database systems use replication to minimize the downtime with the help of failover systems.
- Many companies maintain phone systems for conference calling, voice mail and call forwarding.
- Although the employees can switch to using mobile phones in case the phone system fails. But the customers are left unaware of the phone number to connect to the company till the phone system recovers.
- Traditionally, the solutions are applied to reduce the impact of phone failure.
- Cloud based phone systems on the other hand provide reliable and failure safe telephone service. Internally, the redundancy is used in the implementation.

Module No – 226: Measuring Business impact, disaster recovery plan template:

- The process of reducing risks will often have some cost. For example the resource redundancy and backups etc.
- This indicates that investment on risk-reduction mechanisms will be limited.

Raja Mushtaq: +923055868956

- The IT staff should therefore evaluate and classify each risk according to its impact upon the routine operations of the company.
- A tabular representation of the risks, the probability of occurrence and the business continuity impact can be shown.
- The next step is to formally document the disaster recovery plan (DRP).
- A template of DRP can contain the plan overview, goals and objectives, types of events covered, risk analysis and the mitigation techniques for each type of risk identified in earlier step.



Risk	Occurrence Probability	Business Continuity Impact
User disk failure	Medium	Low
Server disk failure	Low	High
Network failure	Low	High
Database failure	Medium	High
Server power failure	High	High
Fire	Low	High
Flood	Low	High

Follow the video lecture to understand fully

- **Standard Programming Languages:** Whenever possible, the consumers should prefer those Clouds which work in standardized programming languages and tools.
- Right from the start, there should be a clearly documented plan of returning of data/resources to the consumer at the time of termination of service usage.
- **Continuity of Operations:** Consumer should assure that the Cloud provider act upon the requested parameters of disaster recovery plan of the consumer for the business-critical software and data hosted on Cloud.
 - In case of service interruption, the consumer should demand compensation in addition to reversal of service charges from provider.
 - Otherwise the consumer should host such critical applications/data/processing locally.
- **Compliance:** The consumer should determine that the provider has implemented necessary procedures and controls to comply with various legal, ISO and audit standards required as a provider and/or for the consumer to fulfill.
- **Administrator Staff:** The consumer should make sure that the internal procedures and policies of the provider are sufficient to protect against malicious insiders.
- **Licensing:** The consumer should make sure that proper licensing is obtained and provided by the provider for the proprietary software.

Module No – 228: Data Governance:

- **Data Access Standards:** Before developing the Cloud based applications, the consumers should make sure that the application interfaces provided in Cloud are generic and/or data adaptors could be developed for portability and interoperability of the Cloud applications can happen when required. jb user ko need ho wo easily all sy 2sry clouder oy shidt ho sky
- **Data Separation:** The consumer should make sure that **proactive measures** are implemented at the provider's end for separation of sensitive and non-sensitive data. koi cheez happen sy phly tadabbeer kr lynn
- **Data Integrity:** Consumers should use checksum and replication technique to ensure the integrity of the data to detect any violations of data integrity. sensitive and unsensitive data 2no process ho rhy hn provider ko cahie ky 2no type ky betwain lodical sepration hoo
- **Data Regulations:** The consumer is responsible to ensure that the provider is complying with all the regulations regarding data which are applicable to consumer regarding data storage and processing. data by rule apply hota hn wo aik region mi data rkh skty hn agr cloud py data rkha hnn tu consumer sure kry clouder bhi wo he rule follow kr rha
- **Data Disposition:** The consumer should make sure that the provider offer such mechanisms which delete the data of consumer whenever the consumer requests for it. Also make sure that the evidence or proof of data deletion is generated. jb consumer data del krta hen tu cloud ny bhi del kiya hn ky nae yh consumer ki zin=mdaari hn confrm kry
- **Data Recovery:** The consumer should examine the data backup, archiving and recovery procedures of the provider and make sure they are satisfactory.

Module No – 229: Security & Reliability:

- **Consumer-side Vulnerabilities:** Consumers should ensure the implementation of proper security and hardening of consumer platforms to avoid browser or other client devices based attacks.
- **Encryption:** Consumer should require that a strong encryption is applied for web sessions, data transfer and data storage.
- **Consumer-side Vulnerabilities:** Consumers should ensure the implementation of proper security and hardening of consumer platforms to avoid browser or other client devices based attacks. jb employee ki trf sy data acces kia jaa rh hn cinsumer ki trf sy koi vulnerabilities nah ayen
- **Encryption:** Consumer should require that a strong encryption is applied for web sessions, data transfer and data storage.
- **Physical:** Consumers should consider the appropriateness of the physical security implementations and procedures of the provider. **There should be a recovery plan for physical attack on provider's site. The providers having multiple installations in different geographical regions should be preferred.** ek palce data loss ho 2sri palce sy get kr sky
- **Authentication:** Consumers should consider the use of advanced procedures for authentications provided by some providers to avoid account hijacking or identity thefts.
- **Identity & Access Management:** Consumers should have the visibility in the capabilities of provider for:
 - Authentication and access management procedures supported by the provider.
 - The tools available for consumers to extract the authentication information.
 - The tools available to consumer for granting authorization to consumer users and other applications without the involvement of provider.

- **Performance Requirements:** Consumers should benchmark the performance scores of an application before deploying it to Cloud in terms of responsiveness and performance regarding the input/output of bulk data.
- These scores should be used to establish key performance requirements after deploying the application over the Cloud.

Module No – 230: VMs, Software & Applications:

- **VM vulnerabilities:** When the provider is offering Cloud IT resources in the form of VMs, the consumer should make sure that the provider has implemented sufficient mechanisms to avoid attacks from other VMs, physical host and network.
- Also make sure the existence of IDS/IPS systems and network segmentation techniques such as VLANs.
- **VM Migration:** The consumers should plan for VM migration across different providers just in case.
- **Time-critical Software:** Since the public Clouds have unreliable response time therefore the consumers should avoid using the Cloud for the deployment of time-critical software.
- **Safety-critical Software:** Due to the unconfirmed reliability of Cloud subsystems, the use of Cloud for deployment of safety-critical software is discouraged.
- **Application development Tools:** When using the application development tools provided by the service provider, preference should be given to the tools which support the application development lifecycle with security features integrated.
- **Application Runtime Support:** Before deploying an application over Clouds, the consumer should make sure that the libraries calls used in application work correctly and all those libraries are dependable in terms of performance and functionality.
- **Application Configuration:** The consumer should make sure that the applications being deployed over the Cloud can be configured to run in a secured environment such as in a VLAN segment.
- Also make sure that various security frameworks can be integrated with the applications according to requirements of security policies of the consumer.
- **Standard Programming Languages:** Whenever possible, the consumers should prefer those Clouds which work in standardized programming languages and tools.

Lesson No. 42

MIGRATING TO THE CLOUD

Module No – 231: Define System Goals and Requirements:

- The migration to Cloud should be well planned. The first step should be to define the system goals and requirements. The following considerations are important:
 - Data security and privacy requirements

- Site capacity plan: The Cloud IT resources needed initially for application to operate.
- Scalability requirements at runtime
- System uptime requirements
- Business continuity and disaster requirements
- Budget requirements
- Operating system and programming language requirements
- Type of Cloud: public, private or hybrid
- Single tenant or multitenant solution requirements
- Data backup requirements
- Client device support requirements such as for desktop, tab or smartphone
- Training requirements
- Programming API requirements
- Data export requirements
- Reporting requirements
- [Jamsa, K. (2012). Cloud computing. Jones & Bartlett Publishers]

Module No – 232: Protect existing data and know your application characteristics:

- It is highly recommended that before migrating to Cloud, the consumer should backup the data. This will help in restoring the data to a certain time.
- The consumer should discuss with provider and agree upon a periodic backup plan.
- The data life cycle and disposal terms and conditions should be finalized at the start.
- If the consumer is required to fulfill any regulatory requirements regarding data privacy, storage and access then this should be discussed with the provider and be included in the legal document of the Cloud agreement.
- The consumer should know the IT resource requirements of the application being deployed over the Cloud.
- The following important features should be known:
 - High and low demand periods in terms of time
 - Average simultaneous users
 - Disk storage requirements
 - Database and replication requirements
 - RAM usage
 - Bandwidth consumption by the application
 - Any requirement related to data caching

Module No – 233: • Establish a realistic deployment schedule, Review budget and Identify IT governance issues:

- Many companies use a planned schedule for Cloud migration to provide enough time for training and testing the application after deployment.
- Some companies use a beta-release to allow employees to interact with the Cloud based version to provide feedback and to perform testing.

Raja Mushtaq: +923055868956

- Many companies use key budget factors such as running cost of in-house datacenter, payrolls of the IT staff, software licensing costs and hardware maintenance costs.
- This helps in calculation of total cost of ownership (TCO) of Cloud based solution in comparison.
- Many Cloud providers offer solutions at lower price than in-house deployments.
- Regarding the IT governance requirements, the following are important point:
 - Identify how to align the Cloud solution with company's business strategy.
 - Identify the controls needed within and outside the Cloud based solution so that the application can work correctly.
 - Describe the access control policies for various users
 - Describe how the Cloud provider logs the errors and system events and how to access the log and performance monitoring tools made available to the consumer.

Module No – 234: Designing Cloud based Solution:

- **Identify functional and non-functional requirements:** Before beginning the design phase of a Cloud application, the system requirements must be obtained and finalized.
- Personal meeting may be very helpful in this regard.
- Identification of errors and omission at early stage will save considerable cost and time later.
- The system requirements are of two types:
 - Functional
 - Non-functional
- **Functional requirements:** Define the specific tasks the system will perform. These are provided by the system analyst to the designer.
- **Non-functional requirements:** These are usually related to quality metrics such as performance, reliability and maintainability.

Module No – 235: Designing Cloud based Solution:

- **Identify Cloud Solution Design Metrics:**
 - **Accessibility:** The Cloud solution should consider either to maximize the user access or to restrict the access to authorized users only.
 - **Audit:** The Cloud solution should contain the logging and exception handling at critical processing points so that the log data can be used for audit later.
 - **Availability:** Identify the uptime requirements of the Cloud application being designed. Use the redundant deployment accordingly.
 - **Backup:** The cost of backup and the time to restore (from backup) should be considered while designing the Cloud based solution. If the data is handled by the provider, the backup policies of the provider should be reviewed and renegotiated if found not appropriate.

Module No – 236: Cloud Solution Design Metrics:

- **Existing & Future capacity:** If the application is being migrated to Cloud, then the current requirement of IT resources should be evaluated and used for initial deployment as well as for horizontal or vertical scaling configuration.
- **Configuration management:** Since the Cloud based solutions are accessed through any OS, browser and device, therefore the interfaces of the application should be able to render the contents with respect to OS, browser and user device.
- **Deployment:** The deployment issues such as related to OS, browser and devices should be addressed for the initial deployment as well as for future updates.
- **Environment (Green computing):** Design consideration for the Cloud based solution should contain considerations for power efficient design in order to reduce the environmental effect of carbon footprint of the Cloud based solution. *power consumption*
- **Disaster recover:** The Cloud solution design should have consideration of disaster recovery mechanisms. The potential risks for business continuity should be identified and cost effective mitigation techniques should be configured for these risks.
- **Interoperability:** The design consideration should contain possibility of interoperability between different Cloud solutions in terms of exchange of data. *data mis match nah during transfer*
- **Maintainability:** The Cloud solution should be designed to increase the reusability of code through loose coupling of the modules. This will lower down the maintenance cost. *esy design kry code usko reus kr lyn*

Module No – 237: Cloud Solution Design Metrics:

- **Performance:** In order to enhance the performance, various considerations should be used such as reduce graphics on key pages, reduce network operations and use of data and application caching. Potential bottlenecks for performance should be identified and addressed.
- **Price:** The design of Cloud solution should be considered with respect to price and budget in short and long term. An inexpensive solution at the time of deployment may prove to be expensive in long run. The scalability, disaster recovery and performance etc. features should be implemented according to budget.
- **Privacy:** Privacy assurance should be implemented. Specifically for healthcare, educational and monitory data related solutions should have privacy assurance for internal as well as external unauthorized access. Same care is to be done for replicated databases and backups.
- **Portability:** The Cloud solution should be designed to be portable to other platforms when required. For that, instead of using the provider specific APIs, the generic or Opensource APIs and programming environments should be proffered for developing the Cloud solution. *2sry platform py synd kr sky*
- **Recovery:** In addition to disaster recovery, the solution should contain features to recover from other events not covered in disaster recovery such as user error, programing bugs, power outage etc.

Module No – 238: Cloud Solution Design Metrics:

- **Reliability:** Design should include the consideration for hardware failure events. The redundant configuration might be applied according to mean time between failure (MTBF) for each hardware device or establish a reasonable downtime.
- **Response time:** The response time should be as less as possible. Specifically for the online form submissions and reports.
- **Robustness:** It refers to the continuous working capability of the solution despite the errors or system failure. This can be complemented with Cloud resource usage monitoring for timely alarm for critical events.
- **Security:** The developer should consider the Cloud based security and privacy issues while designing.
- **Testability:** Test cases should be developed to test the fulfilment of functional and non-functional requirements of the solution.
- **Usability:** The design can be improved for usability by implementing a prototype and getting users' reviews to enhance the ease of usability of the Cloud solution.

Lesson No. 43**CLOUD APPLICATION SCALABILITY AND RESOURCE SCHEDULING****Module No – 239: Cloud Application Scalability:**

- **Review Load Balancing Process:** Cloud based solutions should be able to scale up or down according to demand.
 - Remember, the scaling out and scaling up mean acquiring new resources and upgrading the resources respectively. Scaling in and scaling down are exactly the reverse of these.
 - There should be a load balancer module specially in case of horizontal scaling.
 - Load balancing or load allocating (in this regard) is performed by distribution of workload (which can be in the form of clients' requests) to Cloud IT resources acquired by the Cloud solution.
 - The allocation pattern can be through round robin, random or a more complex algorithm containing multiple parameters. (More on this in later module).
- **Application Design:** Cloud based solutions should neither be having no-scaling nor the unlimited scaling.
 - There should be a balanced design of Cloud application regarding scaling with reasonable expectations.
 - Both horizontal and vertical scaling options should be explored either individually or in combination.

Module No – 240: Cloud Application Scalability:

- **Minimize objects on key pages:** Identify the key pages such as home page, forms and frequently visited pages of Cloud based solution.
 - Reduce the number of objects such as graphics, animation, audio etc. from these pages so that they can load quickly.
- **Selecting measurement points:** Remember a rule that a 20% of code usually performs the 80% of processing.
 - Identify such code and apply scaling to it.
 - Otherwise applying scaling may not have the desired performance improvements.
- **Analyze database operations:** The read/write operations should be analyzed for improving performance.
 - The read operations are non-conflicting and hence can be performed on replicated databases (horizontal scaling).
 - But write operations on one replica database requires the synchronization of all database instances and hence the horizontal scaling becomes time consuming.
 - The statistics of database operations should be used for decision about horizontal scaling.
- **Evaluate system's data logging requirements:** The monitoring system regarding the performance and event logging may be consuming disk space and CPU.
 - Evaluate the necessity of logging operations before applying or periodically afterwards and tune them to reduce disk storage and CPU wastage



capacity aik esi activity jis mi plan kia jata hn khaas tym py kesi app ko kitny resources require ho skty hn
Scalability mui jn work load increase hota hn tu unhy ky under it resources ki taadaad increase ho jati hn

Module No – 241: Cloud Application Scalability:

- **Capacity planning vs Scalability:** Capacity planning is planning for the resources needed at a specific time by the application.
 - Scalability means acquiring additional resources to process the increasing workload.
 - Both capacity planning and scalability should be performed in harmony.
- **Diminishing return:** The scaling should not be performed beyond a point where there is no corresponding improvement in performance.
- **Performance tuning:** In addition to scaling, the application performance should be tuned by reducing graphics, page load time and response time.
 - Additionally the use of caching should be applied. It is the use of faster hard disks, using RAM contents for content rendering and optimizing the code using 20/80 rule.

Module No – 242: Cloud Resource Scheduling Overview:

- **Effective resource scheduling reduces:**
 - Execution cost
 - Execution time
 - Energy consumption

- **Fulfills QoS requirements:**
 - Reliability
 - Security
 - Availability
 - Scalability
- Remember that provider wants to earn more profit and maximize the resource usage.
- **Cloud consumer wants to minimize the cost and time of execution of workload.**
- The Cloud resource scheduling can be performed on various grounds as discussed in coming modules.
 - [Singh, S., & Chana, I. (2016). A survey on resource scheduling in cloud computing: Issues and challenges. Journal of grid computing, 14(2), 217-264.]

Module No – 243: Cloud Resource Scheduling Overview:

- **Cost-Based Resource Scheduling:** This type of resource scheduling is performed on the basis of cost and budget constraints **limited budget**
 - The users' requests are processed in first come first served basis along with QoS and time constraints considerations.
 - The cost constraint may take the priority over other constraints and thus may introduce starvation for some tasks.

Module No – 244: Cloud Resource Scheduling Overview:

within fix tym user ko reply dyna prhta hn

- **Time-Based Resource Scheduling:** This type of resource scheduling prioritizes the processing deadline of the users' requests.
 - The resources are allocated to those jobs with deadline approaching faster than other requests.
 - Evaluated through the statistics such as number of deadlines missed and the overall cost etc.

Module No – 245: Cloud Resource Scheduling Overview:

- **Cost & Time-Based Resource Scheduling:** Time based scheduling may miss some tasks' deadlines or may prove to be expensive if over provisioning of IT resources is used to meet deadlines.
 - The cost based scheduling may miss some deadlines and/or cause starvation to some costs.
 - Better to use a hybrid approach for resource scheduling to gain cost as well as to minimize task deadline violations.

Module No – 246: Cloud Resource Scheduling Overview:

- **Bargain-Based Resource Scheduling:** This type of scheduling considers that a resource market exists with providers making offers to the users.
 - The users can negotiate for the processing cost.
 - The bargain-based scheduling can achieve low cost and meet deadline if negotiation is successful.
 - It is an evolving technique so far

Module No – 247: Cloud Resource Scheduling Overview:

- **Profit-Based Resource Scheduling:** This type of scheduling aims at increasing the profit of Cloud provider.
 - This can be done either by reducing the cost or increasing the number of simultaneous users.
 - The SLA violation is to be considered while making the profit based scheduling decisions.
 - The penalties of SLA violations may nullify the profit gained.

Module No – 248: Cloud Resource Scheduling Overview:

- **SLA & QoS Based Resource Scheduling:** In this scheduling, the SLA violations are avoided and QoS is maintained.
 - The more load put on IT resources, the more tasks may be completed in a unit time.
 - Yet it may cause SLA violation when IT resources are overloaded.
 - Hence the QoS consideration is applied to ensure SLA is not violated.
 - Suitable for homogeneous tasks for which the estimation can be performed for expected workload and expected time of completion.

Module No – 249: Cloud Resource Scheduling Overview:

- **Energy-Based Resource Scheduling:** The objective is to save energy at data center level to decrease the running cost and to contribute towards environment.
 - Energy consumption estimation is required for each scheduling decision. There can be a number of possible task distribution across servers and VMs.
 - Only that distribution is preferred which shows the least energy consumption for a batch of tasks at hand.

Module No – 250: Cloud Resource Scheduling Overview:

- **Optimization-Based Resource Scheduling:** Optimization is the process of perfecting an algorithm to make it more beneficial. Optimized solution to a problem is the best possible option (under some constraints) available for the problem at hand.

- Popular considerations used by researchers are revenue maximization, lowering communication overhead, output efficiency, energy efficiency, reducing completion time of tasks etc.
- Popular techniques used by researchers include Bayesian assumptions, Stochastic Integer Programming etc.
- The only drawback is the computational time of optimal solution. It may result in deadlines missing for some time critical jobs.

Module No – 251: Cloud Resource Scheduling Overview:

task ko preferencw dynaa

- **Priority-Based Resource Scheduling:** In this type of scheduling, the task starvation can be avoided. Specially for the situation of resource contention.
 - If there is a task classification e.g., on the basis of type, user, resource requirement etc., so that the priority of one task can cause the resource scheduler to preempt the other low priority tasks.
 - May cause the low priority tasks to suffer starvation.
 - **Aging factor** can be applied to increase the priority of low-priority tasks to avoid or lower the starvation.

Module No – 252: Cloud Resource Scheduling Overview:

- **VM-Based Resource Scheduling:** Since the VMs can host Cloud based applications and the VMs can be migrated, the resource scheduling can be performed on VM level.
 - The overall demand of all applications hosted on a VM is considered for scheduling. If a VM is facing resource starvation, it can be migrated to another server with available IT resources.
 - The disadvantage is, there is no guarantee that the destination host also runs out of IT resources due to already deployed VMs

Module No – 253: Cloud Resource Scheduling Overview:

- **VM-Based Resource Scheduling:** Resource scheduling may lead to formation of hybrid Cloud in-order to provision additional IT resources.
 - There is going to be a budget issue regarding outsourcing. resources kaam hn tu publik sy resources ly live jae
 - So in order to finish the task/s within deadline and budget, the selection of tasks to reschedule and the Cloud IT resources to be availed are very important.

MOBILE CLOUD COMPUTING**Module No – 254:**

- **Introduction** Mobile devices are frequently being used throughout the world.
 - Over the time, the users have started to rely more and more upon mobile devices due to no constraints of time and location.
 - The applications installed over mobiles are of various types and of various computational requirements.
- **Overview:** The mobile devices are inherently constrained by resources shortage such as processing, memory, storage, bandwidth and battery etc.
 - There might be a number of situations when mobile devices become incapable of processing or running the applications due to resource shortage.
 - On the other hand, Cloud computing offers unlimited IT resources over Internet on-the-go.
- **Definition:** Mobile cloud computing at its simplest, refers to an infrastructure where both the data storage and data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and Mobile Computing to not just smartphone users but a much broader range of mobile subscribers'.
 - [Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18), 1587-1611.]

Module No – 255: Need for Mobile Cloud Computing:

- There are various scenarios which indicate the need of a Mobile Cloud computing environment.
- This module presents a few examples in this regard.
- **Optical character recognition (OCR)** is used to identify and translate the text from one language to another. An OCR application could be installed over a mobile device for tourists.
- But due to resource shortage over the mobile devices, a better solution is to develop a Mobile Cloud application.
- Data sharing such as images form a site of disaster can be performed over Mobile Cloud application to help in developing an overall view of the site.
- The readings from sensors of multiple mobile devices spread across a vast region can not be otherwise collected and processed except through a Mobile Cloud application.

Module No – 256: Applications of Mobile Cloud

- We shall discuss a few example applications of Mobile Cloud computing.

- **Mobile Commerce:** The applications of mobile commerce face the complexities such as **bandwidth limitation**, device configuration and security. In order to address these issues, the mobile commerce applications are integrated into Cloud computing.
- **Mobile Learning:** The mobile learning apps face the limitations in terms of high cost of devices & data plan and network bandwidth. Along with the limitation of storage space over mobile devices, these limitations can be overcome through shifting these applications over Cloud. This results in rendering of larger sized tutorials, faster processing and battery efficiency. **education tutorial**
- **Mobile Healthcare:** The mobile healthcare applications based upon Mobile Cloud computing offer the following benefits in addition to assuring the security and privacy:
 - Remote monitoring of pulse rate, blood pressure etc. for patients over Internet.
 - Timely and effective cautioning and guidance to ambulances in case of medical emergencies.
- **Mobile Gaming:** Rendering of contents over mobile devices while executing the game engine over Cloud. Only the screens of the mobile devices are used, the rest is being done on Cloud.

Module No – 257: Mobile Cloud Computing Architecture

- This module presents a generic architecture of Mobile Cloud computing.
- Mobile devices are connected to mobile networks through base stations such as access point, base transceiver stations or through satellite.
- The base stations establish the link between mobile devices and the mobile networks.
- The base stations convey the ID and location information along with the request to the central processors that are connected to the servers providing mobile network services.
- The mobile networks can provide the authentication, authorization and accounting on the basis of subscribers' data stored in databases.
- The subscribers' requests are then delivered to a Cloud through Internet.
- The Cloud controllers receive the subscribers' requests and provide services accordingly.
- The subscribers' requests are then delivered to a Cloud through Internet.
- The Cloud controllers receive the subscribers' requests and provide services accordingly.

Module No – 258: Mobile Cloud Models

- There are various models of setting up of Mobile Clouds:
- A mobile device accessing an application/service hosted on Cloud servers such as email through 3G connection.
- Some mobile devices can provide resources to other mobile devices in a Cloud setup using mobile peer-to-peer network.
- The mobile devices can be connected to a *cloudlet* which is a set of multi-core computers connected to remotely placed Cloud servers. These cloudlets are usually in closed vicinity of the mobile devices save the network latency.

- [Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. Future generation computer systems, 29(1), 84-106.]

Module No – 259: Advantages of Mobile Cloud Computing

- **Extending battery lifetime:** The offloading of computational workload to Cloud saves battery life and reduces the response time.
- **Improving data storage capacity and processing power:** The storage limitation is overcome through Cloud storage. For example images uploaded to Cloud right after capturing. The running cost (in terms of energy and time) of compute-intensive application is also reduced when the mobile Cloud application is used.
- **Improving reliability:** The backup and disaster recovery features of Cloud computing provide reliability surety of data and applications for mobile Cloud computing as well.
- **Additionally:** The benefits of dynamic provisioning and scalability are also there.

Module No – 260: Cost Benefit Analysis of Mobile Cloud Computing

- Cost benefit analysis proves to be useful for deciding about offloading the workload to Cloud.
- This analysis may consider the total investment (initial and running costs) and compare with the benefits of Mobile Cloud computing.
- Considering the goals of performance, energy conservation and quality to decide which server should receive the offload from mobile devices. Thus the cost benefit analysis in this case is from the point of view of Cloud infrastructure. Prediction can be used to estimate the performance, energy consumption and quality.
- The data related to devices' energy consumption, network throughput and application characteristics can be used to decide for offloading a task (of the profiled application) to Cloud or execute it locally in order to (for example) conserve battery.
- Security and privacy requirements may also be the base of task migration to Cloud.

Module No – 261: Mobile Cloud Computing : Security

- There are a number of data security and privacy issues in Mobile Cloud computing. These are in addition to the security and privacy issues of Cloud computing.
- The following are the key areas for mobile Cloud security:
- Mobile devices themselves: Attacks, Virus and other malwares
- Mobile network: Related to wireless security
- Vulnerabilities in mobile Cloud applications: regarding the security and privacy bugs.

Module No – 262: Mobile Cloud Computing: Issues: Communications

- **There are some communication issues regarding Mobile Cloud computing.** The researchers have also proposed different solutions in this regard.
- **Low Bandwidth:** It is one of the biggest issues for mobile Cloud computing because the radio resource for wireless networks is much scarce as compared with the traditional networks. wifi network
- **Availability:** The availability of the service becomes an important issue when the mobile device has lost contact with mobile Cloud application due to network failure, congestion and loss of signals. radio signal bandwidth ky related hen radio signal carrier signal mi majood ni hoty wo mob device cloud sy connect ho sky
- **Heterogeneity:** The mobile devices accessing a Mobile Cloud Computing application are of numerous types and use various wireless technologies such as 2G, 3G etc and WLAN. An important issue is how to maintain the wireless connectivity along with satisfying the requirements of Mobile Cloud computing such as high-availability, scalability and energy efficiency etc. cloud comp sy connect break ho skta weak of signal

Module No – 263: Mobile Cloud Computing: Issues: Computing

- The mobile device has to make the decision for offloading the computational workload to the Cloud.
- If the offloading is not performed efficiently then the desired performance may not be achieved. Also the battery may get depleted faster than executing the workload locally.
- **There are two main types of computational offloading:**
 - **Static:** In which the offloading decisions (consisting of workload partitioning) are made at the execution start of a task or a batch of tasks. es mi work loading mi predict kia jata hn aany wali work pad
 - **Dynamic:** The offloading decisions depend upon the run-time conditions of dynamic parameters such as network bandwidth, congestion and battery life etc. kaa or aany wali variation ka
- The static offloading decisions may not turn out to be fruitful if the dynamic parameters change unexpectedly.
- Better not to offload if the time/battery consumption (cost) for offloading is higher than the cost of locally processing the task.

Module No – 264: Mobile Cloud Computing: Issues: End User Related

- **Incentives:** In the model of Mobile Cloud computing where a mobile device shares resources with other devices, there should be an incentive to share those resources.
- The incentive can be monetary or non-monetary. The non-monetary incentive can be of a common interest such as visitors of a museum trying to translate the same text on an artifact.
- **Presentation issues:** The mobile devices have a high level of heterogeneity. Developing separate user interface for each type of device is unrealistic.
- **Since the display area on a mobile device is limited, designing a user friendly GUI requires extra effort.**

- **Service Availability and Performance assurance issues:** Mobile devices undergo loss of connectivity due to signal loss, network error, battery depletion etc. and thus service availability and performance assurance turn to become challenges

Module No – 265: Mobile Cloud Computing: Issues: Data Access

- Data access over mobile Cloud applications may be challenging in case of low bandwidth, signal loss and/or battery life.
- Accessing the files through mobile devices may turn out to be expensive in terms of data transmission cost, network delays and energy consumption.
- Data access approaches are needed to be developed/polished to maintain a performance level and to save energy.
- Some approaches have optimized the data access patterns.
- Another approach is to use mobile cloudlets which are intermediate devices acting as file cache.
- Interoperability of data is also a challenge to provision data across heterogeneous devices and platforms. A generic representation of data should be preferred.

Module No – 266: Mobile Cloud Computing: Issues: Miscellaneous

- **Performance:** The performance can be increased by optimally balancing the workload offloading.
 - If the IT resources are being acquired from the surrounding devices, then the performance depends upon the extent of resources available as compared to task at hand.
- **Resource Management:** A mobile Cloud application can acquire all the IT resources from Cloud. Another method is to use the cloudlets which are individual computers or even clusters in the vicinity of the mobile device running the mobile Cloud application.
 - In worst case, the mobile device resources are utilized. All these situations require separate resource management techniques.

Module No – 267: Mobile Cloud Computing Issues: Miscellaneous:

- **Processing Power:** The processing power of a single mobile device is not at all comparable to Cloud.
- The issue is how to efficiently utilize the huge processing power of Cloud to execute the tasks of mobile Cloud applications.
- **Battery Consumption:** Computational offloading becomes more energy efficient if the code size is large and vice versa.

- For example, offloading 500KB of code will take 5% of battery as compared to 10% battery usage if this code is locally processed. Thus 50% of battery is saved when offloading the code.
- But 250KB code is only 30% battery efficient if uploaded.

Module No – 268: Mobile Cloud Computing: Issues and Challenges:

- Support of mobility while assuring connectivity to the Cloud. The network connectivity becomes very important in this case. Cloudlets can support the connectivity but these only exist at certain locations such as cafés and malls.
- The adhoc creation of mobile Cloud over a set of a set of mobiles around a location depends upon the availability of capable devices and cost benefit analysis.
- Assurance of security is an on-going challenge to ensure privacy and security and to establish trust between the mobile device users and the service provider/resource provider.
- The conduct and manage the incentives among the resource lenders (in case of a mobile adhoc Cloud) requires the establishment of trust, payment method and methods to prevent free riders.

Module No – 269: Mobile Cloud Computing vs Cloud Computing:

- Typically, both the Cloud computing and Mobile Cloud computing are dependent upon remote usage of IT resources offered by Cloud.
- Cloud computing traditionally works to provide various Cloud services such as IaaS, PaaS and SaaS etc. to the consumers. cloud comp yh services provide krti hen
- Mobile Cloud computing is however more towards providing Cloud based application over mobile devices and to deal with the connectivity, security and performance issues. individual mob user ko mob cloud app provide ki jae uski access provide ki jae
- Cloud computing deals with user requirements from a single user to an enterprise level.
- Mobile Cloud applications are more accessed by individual users for personal computing purposes.
- There are multiple models of Cloud computing such as Private, Public, Community and Hybrid.
- Mobile Cloud can be setup over Cloud, Cloudlets and on adhoc basis by using the capable and resource rich mobile devices sharing a common location on map.

Lesson No. 45

SPECIAL TOPICS IN CLOUD COMPUTING AND CONCLUSION OF COURSE

Module No – 270: Big Data Processing in Clouds: Overview of Big Data:

- The term “^{popular}Big Data” refers to such enormous volume of data that can not be processed through traditional database technologies.

bhut bara data jo traditionally process ni kr skti database

- The following are the three generic characteristics of big data:
 - Data volume is huge
 - Data may not be categorized into regular relational databases
 - The data is generated, captured and processed at high speed.
- Another definition of Big Data can be: *Big data is a set of techniques and technologies that require new forms of integration to uncover large hidden values from large datasets that are diverse, complex, and of a massive scale.* [Anuar, N.B., Gani, A., Hashem, I.A., Khan, S.U., Mokhtar, S., & Yaqoob, I. (2015). The rise of "big data" on cloud computing: Review and open research issues. Inf. Syst., 47, 98-115]

Module No – 271: Big Data Processing in Clouds: Overview of Big Data:

- The characteristics of big data can be represented by 4vs:
 - **Volume:** The volume of data continues to rise.
 - **Variety:** It refers to the heterogeneous types of data collected through sensors, smartphones, social networks etc. and can be of video, audio, image, text formats. *The data can be structured, semi structured or unstructured.*
 - **Velocity:** It refers to the speed of transfer of data. The contents of the data also change constantly.
 - **Value:** The analysis of Big Data can generate valuable information.

Module No – 272: Relationship between Cloud computing and Big Data:

- Cloud computing infrastructure can fulfill the data storage and processing requirements to store and analyze the Big Data.
- The data can be stored in large fault tolerant databases. Processing can be performed through parallel and distributed algorithms.
- Cloud storage can be used to host Big Data while the processing can be done locally on commodity computers.
- Big data Cloud applications can be built to host and process the big data on Cloud.
- There are three popular models for big data:
 - Distributed Map Reduce model popularized by Hadoop
 - NoSQL model used for non-relational, non-tabular storage
 - SQL RDBMS model for relational tabular storage of structured data.
- Traditional tools for big data processing for example can be deployed over Cloud.
- Top-rated Hadoop options include Apache Hadoop, SAP's HANA/Hadoop combination, Hortonworks, Hadoop and VMware's Cloud Foundry, as well as services provided by IBM, Microsoft and Oracle.
- For NoSQL, consider Cassandra, Hbase or MongoDB. IBM also offers NoSQL for the cloud, and there are plenty of other NoSQL providers.
- [http://searchcloudapplications.techtarget.com/tip/How-to-choose-the-best-cloud-big-data-platform]

Module No – 273: Big Data on Cloud Case Studies:

- In this module we shall cover a few examples of usage of Cloud computing for Big Data hosting and processing as case studies.

SwiftKey: It is a smart prediction technology for mobile device virtual keyboards.

- Terabytes of data is collected and analyzed for active users around the globe for prediction and correction of text through an artificial engine.
- Uses Amazon Simple Storage Service and Amazon Elastic Cloud to host Hadoop.

- Halo Game:** More than 50 million copies have been sold worldwide.

- Collects the game usage data for the players globally for player-ranking in online gaming tournaments.
- Windows Azure HDInsight Service (based on Hadoop) is used for this purpose.

- Nokia:** The well known mobile manufacturer collects terabytes of data for analysis,

- Uses Teradata Enterprise Data Warehouse, Oracle and MySQL data marts, visualization technologies, and Hadoop.

Module No – 274: Big Data Storage and Data processing in Clouds:

- Popular platforms for Big Data processing are:

- **Hadoop:** It is an open-source project of Apache Software Foundation. It is Java based. Used for batch jobs processing. Has two primary components:
 - Hadoop Distributed File System (HDFS)
 - MapReduce programming framework
- **Spark:** It is a data processing framework compatible with Hadoop data sources. Suitable for machine learning tasks. Faster than MapReduce. However it is unable to execute concurrent Reduce methods unlike MapReduce of Hadoop.

- Hadoop MapReduce is however currently a more popular computational model of Cloud providers for Big Data processing.

Module No – 275: Challenges & Issues of Big Data processing on Cloud:

- In this module we shall briefly discuss a few challenges and issues related to Big Data processing on Cloud.
- Scalability assurance for storage of rising volume of Big Data.
- Availability assurance of any data out of Big Data stored on Cloud storage is a challenge.
- Data quality refers to the possibility of data-source verification. It is a challenging task for Big Data (for example) collected from mobile phones.
- Simultaneously handling heterogeneous data is challenging.
- Privacy issues arise when the processing of Big Data (through data mining techniques) may lead to sensitive and personal information. Another issue is the lack of established laws and regulations in this regard.

Module No – 276: Multimedia Cloud Computing: Overview & Introduction:

- Internet multimedia is emerging as a service with the development of Web 2.0.
- Multimedia computing has emerged as a prominent technology to provide rich media contents.
- Millions of subscribers and users worldwide obtain multimedia over heterogeneous devices.
- Thus multimedia rendering can rely upon Cloud computing for providing the processing and storage resources.
- Utilizing multimedia-Cloud can have advantages as well as challenges.
- The advantages include the provision of scalable IT resources and the fault tolerant Cloud infrastructure.
- The challenges include the rendering of a variety of multimedia types, formats and services. Maintaining QoS across heterogeneous devices, users and multimedia contents and services is yet another challenge.
- [Zhu, W., Luo, C., Wang, J., & Li, S. (2011). Multimedia cloud computing. IEEE Signal Processing Magazine, 28(3), 59-69.]

Module No – 277: Multimedia Cloud Computing:

- **Architecture & Processing:** In this module we shall consider the example of **multimedia edge Cloud (MEC)** consisting of cloudlets.
- The multimedia Cloud providers can use the IT resources of cloudlets which are physically placed over the edge (means very close to the multimedia service consumers) to reduce network latencies.
- There can be multiple MECs which are geographically distributed.
- The MECs are connected to central servers through **content delivery network (CDN)**.
- The MECs provide multimedia services and maintain the **QoS**.

Module No – 278: Cloud-aware Multimedia Applications & Rendering:

- The Cloud offers various applications/services for multimedia. Such as:
- **Storage:** There are various providers of multimedia storage services for example IOmega (www.iomega.com) , AllMyData (www.amdwebhost.com) etc.
- **Sharing:** The multimedia contents once uploaded, can be shared to other users. The cloud-client network link is usually more robust, capable and reliable than client-client link.
- **Multimedia authoring:** Refers to the services and tools for editing, merging and enhancing the multimedia contents over Cloud. ^{new}
- **Rendering:** Refers to the creation of images and multimedia to be displayed over the user's device. The multimedia Cloud can perform rendering for less capable devices in order to maintain QoS and minimize the delay. jis ky thorough multi media ko banaya jata hn aik device ky ldisplay ky iye

Module No – 279: Introduction to SDN:

- Network operators often have to configure the devices (switches & routers) separately and by using vendor specific commands.
- Thus, implementing high level network policies is hard and complex in traditional IP networks.
- The dynamic response and reconfiguration is almost non-existent in current IP networks. Enforcing the network policies dynamically is therefore challenging.
- Further, the control plane (the decision making and forwarding rules) and the data plane (which performs traffic forwarding according to the decisions made by control plane) are bundled inside the networking device.
- All this reduces the flexibility, innovation and evolution of the networking infrastructure.
- **Software Defined Networking (SDN)** is the new paradigm of networking that separates the control plane from data plane.
- **It reduces the limitations of traditional networks.**
- The switches become the forwarding-only devices, while the control plane is handled by a software controller.
- The controller and switch have a software interface between them.
- Controller directly exercises direct control over the data plane devices through a well defined application program interface (API) such as OpenFlow.
 - [Jain, R., & Paul, S. (2013). Network virtualization and software defined networking for cloud computing: a survey. IEEE Communications Magazine, 51(11), 24-31.]
 - [Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14-76.]
 - [Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys & Tutorials, 16(3), 1617-1634.]

Module No – 280: History of SDN:

- SDN has its roots in history as long ago as 80s and 90s with the development of **Network Control Point (NCP)** technology.
- **NCP was introduced by AT&T** as probably the first established technique to separate the data plane and control plane.
- **Active Networks** was another attempt to introduce computational and packet modification capabilities to the network nodes. run tym traffic monitoring perform ki jaa sky aur network packt by SW updatw kia jaa sky
- **Network virtualization** is a recent development which allows hypervisor like environment to network infrastructure.
- **OpenFlow based** network operating systems such as ONOS have emerged to make network administration easier and to develop/deploy new protocols and management applications.

Module No – 281: Network Virtualization:

- Each computer system needs at least one L2 NIC (Ethernet card) for communication.
- A physical system must have at least one physical NIC (pNIC).
- Each VM has at least one virtual NIC (vNIC).
- All the vNICs on a physical host (server) are interconnected through a virtual switch (vSwitch).
- The vSwitch is connected to the pNIC.
- Multiple pNICs are connected to a physical switch (pSwitch)
- There are a number of standards available for NIC virtualization.
- A physical ethernet switch can be virtualized by implementing IEEE Bridge Port Extension standard 802.1BR
- The VLANs can span over multiple data centers and there are several approaches to manage the VLANs.
- A VM can be migrated across different data centers by following multiple techniques proposed by researchers.
- The modern processors allow the implementation of software based network devices such as L2 switch, L3 router etc.

Module No – 282: Architecture of SDN:

- SDN has four characteristics:
 - **Separation of control and data planes:** In SDN, the switches are forwarding devices. The network traffic is forwarded by following the forwarding tables. The forwarding tables are created/updated through a controller software.
 - **Centralization of control plane:** SDN relies upon centralized control instead of distributed control.
 - The controller software actually controls a subset of the whole network which is small enough to be controlled by a single controller software.
 - **Programmable control plane:** The controller software is controllable through API calls.
 - This helps in rapid implementation of network policies because the control plane is centralized and not distributed.
 - **Standardized APIs:** There is a southbound API for communication with forwarding devices and a northbound API for communication with network applications.
 - The main southbound API is OpenFlow standardized by the Open Networking Foundation. The northbound APIs have not been standardized yet.

Module No – 283: SDN In Cloud:

- The implementation of SDN in Cloud is an ongoing research work.

- The rise in demand for network virtualization has attracted the virtualization software vendors to integrate SDN features in their products.
- Centralized controllers such as *Beacon* can handle more than 12 million flows per second and can fulfill the requirements of enterprise level networks and data centers for hosting Cloud.
- The SDN can be helpful in monitoring, filtering and managing the network traffic over virtual as well as physical networks inside a Cloud hosting data center.

Module No – 284: Future of SDN:

- In near future, the SDN has to overcome a few challenges.
- Controller and switch design
- Scalability and performance in SDNs
- Controller-service interfacing (specially the northbound interface)
- Virtualization and cloud service applications (the SDN based Cloud infrastructure)
- Information centric networking: The future architecture of Internet aiming at increasing the efficiency of content delivery and availability.
- Enabling heterogeneous networking with SDN: The wired, wireless and adhoc networks.

heterogenous devices apas mi communicate and cooperate kry for the processing aur network storage and other operation task perform krny ky liye APAAS mi tahwaaan kry

Module No – 285: Fog Computing:

jah sy comp device connect ho rae hn cloud ky sath wah py he cloud ki services provide kr si jae

- It is an emerging paradigm of Cloud computing.
- *Fog Computing* or *Fog* extends the Cloud computing and services to the edge of the network.
- Provides data, computing, storage and application services to end-users that can be hosted at the network edge or end devices such as set-top-boxes or access points.
- Fog will support **Internet of Everything (IoE)** applications such as industrial automation, transportation, network of sensors and actuators etc..
- These applications demand real-time/predictable latency and mobility.
- Fog can therefore be considered a candidate technology for beyond 5G networks.
- Fog will result in the defusing of Cloud among the client devices.
- Fog Computing is a scenario where huge number of heterogeneous, ubiquitous and decentralized devices communicate and potentially cooperate among them and the network to perform storage and processing tasks without the intervention of third parties.
- Network virtualization and SDN are going to be the essential parts of Fog computing.
 - [Kitanov, S., Monteiro, E., & Janevski, T. (2016, April). 5G and the Fog—Survey of related technologies and research directions. In Electrotechnical Conference (MELECON), 2016 18th Mediterranean (pp. 1-6). IEEE]

Module No – 286 Cloud Gaming:

- Online gaming consists of four basic building blocks:
- Input module: To receive control information from the player

- Game logic module: To process the game events
- Networking module: To process how the avatars interact with each other
- Rendering module: Formulates the game video and presents it to the players.
- Traditionally, the Internet gaming servers are used to exchange the game information while the input, logic and rendering modules of the game are installed on users' devices.
- Computer games can be hosted as service on Cloud.
- One of the deployment models is to deploy only the I/O module on users' devices and the rest of the modules on Cloud.
- The benefits include the easy deployment, reduced cost and time for the players and formulation of various flexible business models such as pre-pay, post-pay and pay-per-play etc.
 - Cai, W., Chen, M., & Leung, V. C. (2014). Toward gaming as a service. IEEE Internet Computing, 18(3), 12-18.]

Module No – 287: Conclusion & End of Course:

- Cloud computing provides the computing/IT resources to the users over the Internet in a pay-as-you-go type of business model.
- This course has covered almost all the aspects of Cloud computing and the advanced topics related to Cloud.
- We are hopeful that you will find this course interesting, informative and comprehensive.
- We hope that the students of Cloud Computing subject will surely know the importance and ubiquity of Cloud computing.
- We hope that this subject will become the foundation of advanced courses and an initial source of knowledge for all in this regard.

Module No – 288: Short Revision:

- In this course we have had an in-depth study of Cloud computing.
- We came across various technologies forming the building blocks of the Cloud.
- We had detailed study of Cloud deployment and study models.
- We also look at various Cloud mechanisms.
- We also studied some advanced topics related to Cloud computing.
- In particular, the main topics of the course are as follows:
 - Introduction
 - History of Cloud Computing
 - Background (Basics Knowledge)
 - Background (Advanced Knowledge)
 - Cloud Computing in Detail
 - Benefits and Challenges of Cloud Computing
 - Roles and Boundaries of Cloud Computing
 - Cloud Service Models

- Data Storage in Cloud
- Miscellaneous Services of Cloud Computing
- Cloud Deployment Models
- Cloud Security
- Trust Issues in Cloud
- Cloud Infrastructure Basics
- Service Level Agreement
- Cloud Hosting Data Center Design
- Cloud Architectures
- Specialized Cloud Mechanisms
- Cloud Management
- Specialized Cloud Architecture
- Cloud Federation
- Cloud Brokerage
- Cloud Costing Models
- Cloud Metrics
- Privacy Issues for Cloud Computing
- Security Issues for Cloud Computing
- Open Issues in Cloud
- Disaster Recovery in Cloud Computing
- General Recommendations of Cloud Computing
- Migrating to the Clouds
- Designing Cloud based Solutions
- Cloud Applications Scalability
- Cloud Resource Scheduling
- Mobile Cloud Computing
- Special Topics in Cloud Computing
- Advanced Topics
- Cloud Resource Scheduling
- Mobile Cloud Computing
- Special Topics in Cloud Computing
- Advanced Topics
- **Reference Books:**
 - Thomas Erl [2014], Cloud Computing Concepts, Technology and Architecture, Pearson
 - Jamsa, K. (2012). Cloud computing. Jones & Bartlett Publishers
 - Pearson, S., & Yee, G. (Eds.). [2012]. Privacy and security for cloud computing. Springer Science & Business Media.
 - Cloud Computing Synopsis and Recommendations, NIST USA, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf>
- **Instructor's email:** mtayyabch@yahoo.com