Lesson No. 13

CLOUD SERVICE MODELS

Module No – 055: IaaS, PaaS & SaaS Provisioning:

- IaaS: The IT-resources are typically virtualized and packaged in a preplanned way.
  - The IT-resources are usually freshly instanced e.g., VMs.
  - The cloud consumer has a high level of control and configuration-responsibility.
  - The cloud consumer also has the duty of configuring these resources.
  - Sometimes a cloud provider will contract IaaS offerings from other cloud provider to scale its own cloud environment.
  - The VMs can be obtained specifying the hardware requirements such as processor capacity, memory, storage etc.
- PaaS: Delivers a programming environment containing preconfigured tools to support the development lifecycle of custom applications.
  - PaaS products are available with different development stacks such as Google App Engine provides a Python and Java environment.
  - The PaaS is chosen:
    - To enhance or substitute the on-premises software development environment.
    - To create a cloud service in order to provide a cloud service to other cloud consumers.
  - The PaaS saves the consumer from administrative tasks such as installations and configurations to set up the software development infrastructure.
  - On the other hand the cloud consumer has lower level of control over the underlying infrastructure.
- SaaS: Is the software hosted over cloud infrastructure and offered as a utility services.
  - SaaS is provided as a reusable utility service commercially available to different users.
  - A SaaS can be deployed over IaaS and/or PaaS instance. Whereby the cloud consumer (of IaaS/PaaS) becomes the provider.
  - The service consumer has a very limited control over the underlying SaaS implementation.

Module No – 056:IaaS, PaaS & SaaS Comparison

- Control level:
  - SaaS: Usage and usage related configuration
  - PaaS: Limited administrative
  - IaaS: Full administrative
- Functionality provided to cloud consumer:
  - SaaS: Access to front-end user-interface
  - PaaS: Moderate level of administrative control over programming platform
  - IaaS: Full administrative control over virtual resources of the VMs
- Common activities of cloud consumer:
  - SaaS: Use and configure the service
  - PaaS: Develop, debug and deploy the cloud services and cloud based solutions
  - IaaS: Installation and configuration of software, configure the infrastructure of VM

- Common Cloud Provider's Activities:
  - SaaS: Implementation, management and maintenance of cloud service.
  - PaaS: Providing the pre-configured programming platform, middleware and any other IT resource needed.
  - IaaS: Provisions and manages the VMs and underlying physical infrastructure.
- The three cloud models of cloud delivery can be combined in a way that one delivery model is deployed over another. Such as:
  - PaaS over IaaS
  - SaaS over PaaS
  - SaaS over PaaS over IaaS

Module No – 057: Software as a Service (SaaS) Overview:

- NIST definition of SaaS: *"Software deployed as a hosted service and accessed over the Internet."*
- The SaaS is a software solution having the code and data executing and residing on cloud.
- A user accesses the SaaS through browser.
- ~~Remember~~: *The cloud service consumer is a temporary runtime role assumed by a software program when it accesses a cloud service*.
- [Thomas Erl [2014], Cloud Computing Concepts, Technology and Architecture, Pearson]
- ~~For the time being we shall assume that~~ the browser acts as *cloud service consumer* when accessing a SaaS.
- SaaS solutions eliminate the need of on-premises (data center based) applications, application administration and data storage.
- The customer is allowed to adopt pay-as-you-go type of rental.
- SaaS offers scalability and device-independent access to the SaaS solution/s.
- SaaS provider assures that the software provided is solidly tested and supported.
- The notable disadvantage of SaaS is that the data resides off-premises.
- ~~The notable disadvantage of SaaS is that the data resides off-premises~~.
- Therefore the data security is of prime importance because the customers' data may be proprietary and business-sensitive.
- The SaaS provider offers SaaS apps executing over IT-resources. These resources can be from a physical servers or a VM owned/rented by the provider.
- Each instance of a SaaS app (consumed by a user) is allocated separate set of IT-resources.
- Classes of SaaS:
  - Business logic: Connect the suppliers, employees, investors and customers.
    - Example: Invoicing, fund transfer, inventory management, customer relationship management (CRM)
  - Collaboration: Support teams of people work together.
    - Examples: Calendar systems, email, screen sharing, conference management and online gaming.
  - Office productivity: Office environment support.
    - Examples: word processors, spreadsheets, presentation and database software.
  - Software tools: For the support of developing software and solving compatibility problems.

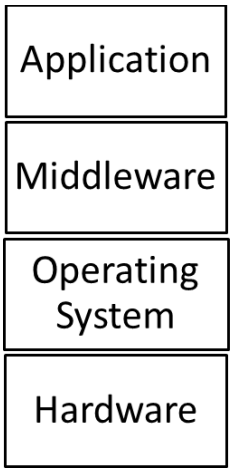
        - Examples: format conversion tools, security scanning, compliance checking and Web development.
- Software that are not suitable for public SaaS offerings (according to NIST):
    - Real-time software: They require precise response time. Due to variable response time and network delays, these software are not suitable to be offered as SaaS. Such as flight control systems and factory robots etc.
    - Bulk-consumer data: When extremely large amount of data is originating physically at the consumer's side such as physical monitoring and patient monitoring data. It is not feasible to transfer this data in real time over WAN to SaaS provider.
    - Critical software: A software is labeled *critical* if its failure or delay in handling can cause loss of life or loss of property. These software are not suitable for SaaS because achieving a continuous acceptable reliability for critical software in public SaaS is quite challenging due to (unreliable) public network based access.
- SaaS billing: Based on
    - Number of users
    - Time in use
    - Per-execution, per-record-processed
    - Network bandwidth consumed
    - Quantity/duration of data stored

Module No – 058:SaaS Examples:

- Salesforce.com SaaS for Customer Relationship Management (CRM)
    - Manage sales contacts and leads.
    - Centralize the contact. information and project details.
    - The sales reports from any place any time.
    - ~~The sales reports from any place any time.~~
    - Manages and syncs sales contacts and meetings with other tools such as Microsoft Outlook.
- Taleo SaaS for Human Resources Management (HRM):
    - Recruitment tools to manage the applicants' data for hiring purposes.
    - Performance management and tracking tools for employees' evaluation.
    - ~~Performance management and tracking tools for employees' evaluation.~~
    - Compensation tools for rewarding the employees according to performance.
    - Workforce training and professional development tools
- ADP SaaS for Payroll Processing and HRM:
    - Cloud solution for time management, employees benefits calculation, worker compensation and HR issues.
- Carbonite SaaS for File Backups:
    - Provides backup services for precious business data and personal data. The data is kept securely and redundantly.
- Microsoft Office 365 SaaS for Document Creation, Editing and Sharing:
    - In order to provide the documentation tools at affordable price and to compete with the freeware solutions, Microsoft offers its flagship software suite on monthly rental basis.

Module No – 059:SaaS Software Stack:

- The provider controls most of the software stack.



SaaS Software Stack

- Application: Email
- Middleware: software libraries, run time environments (Java, Python)
- Service provider has admin control over application and total control over the rest of the layers.
- Service consumer has limited admin control over the application and no control over the rest of the stack.
- A consumer can create, send and manage the emails and even the email accounts.
- But the email provider has absolute control over the SaaS software stack in order to perform its duties such as provisioning, management, updates and billing in email app.

Module No – 060: SaaS Benefits:

- Modest software tool footprint: There is no need for complex installation procedures because the SaaS applications and accessible through web browsers. This is one of the reasons of widespread use of SaaS applications.
- Efficient use of software licenses: The license issuance and management procedure is quite efficient. A single client is issued a single license for multiple computers. This is because the software is running directly on provider's infrastructure and thus can be billed and monitored directly.
- Centralized management and data: The consumer's data is stored in cloud. The provider assures the security and availability of data. The data seems centralized for the consumer may in fact be distributed and replicated by the provider. Data backup is provided at possibly additional charges.
- Platform responsibilities managed by providers: Consumer does not has to bother about operating system type, hardware and software configurations, software installation and upgrades.

- Savings in up-front costs: (~~as discussed before~~) the up-front costs such as equipment acquisition and hardware provisioning etc. are avoided by SaaS consumer.
- The provider is responsible for operational issues such as backups, system maintenance, security software, upgrades, trouble shooting in software, physical security and hardware management etc.

Module No – 061: SaaS: Issues and Concerns:

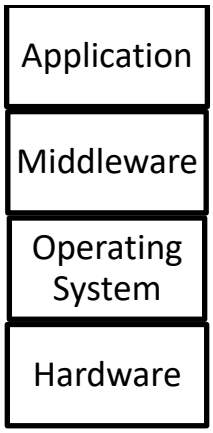
- The NIST has identified few issues and concerns about SaaS.
- Most of these issues are due to network dependency of SaaS.
    - Browser based risks and remedies: Since the SaaS is accessed through browser installed on consumers' device, the inherent vulnerabilities of the web browsers do have impact over SaaS security.
        - Although the browsers apply encryption upon network traffic, yet various network attacks such as brute force and man in the middle attacks are possible upon the SaaS data.
        - The resources leased by a consumer can be hijacked by malicious users due to poor implementation of cryptographic features of browsers.
        - If the consumer's browser is already infected with a security threat (due to a visit to malicious website) then later, the same browser is used for SaaS access, then the SaaS data might get compromised.
        - If a single consumer accesses multiple SaaS services using browser instances, then the data of these SaaS instances may get mixed up.
        - A few suggestions by NIST:
            - Use different browsers to access each different SaaS.
            - Do not use the same web browser for web surfing and SaaS access.
            - Use a VM to access the SaaS.
    - Network dependence: SaaS application depends upon reliable and continuously available network.
        - The reliability of a public network (Internet) can not be guaranteed as compared to dedicated and protected communication links of private SaaS applications.
    - Lack of portability between SaaS clouds:, It may not be trivial to import export data among different SaaS applications deployed over different clouds due to customized development and deployment of SaaS applications and data formats.
    - Isolation vs. Efficiency (Security vs. Cost Tradeoffs): The SaaS provider has to make a trade-off decision as to deploy separate IT-resources (such as VMs) for each client or concurrently server multiple clients through a single deployment of SaaS application.

Module No – 062: NIST Recommendations for SaaS

- Data protection: The consumer should analyze the data protection, configuration, database transaction processing technologies of SaaS provider. Compare them with the confidentiality, integrity, availability and compliance requirement of the consumer.
- Client device/application protection: The consumer's client device (browser running over a computer) should be protected to control the exposure to attacks.
- Encryption: Strong encryption algorithm with key of required strength should be used for each web session as well as for data.
- Secure data deletion: The data deletion through consumer's request should be reliably done.

Module No – 063: Platform As a Service (PaaS) Overview

- According to NIST, PaaS provides a toolkit for conveniently developing, deploying and administering application software which can support a large number of users, process large volumes of data and can be accessed over Internet.
- What does PaaS clouds really provide: a set of software building blocks, a set of development tools (languages and compilers) and supporting environments for run-time of applications developed over PaaS.
- PaaS clouds also provide tools to deploy the developed applications.
- Additionally, the PaaS clouds provide processing, storage and networking resources.
- PaaS consumers:
  - Application developers
  - Application testers
  - Application deployers
  - Application administrators
  - Application end users (SaaS users)
- The consumers are charged according to tools and IT-resources usage.
- PaaS Software stack: The cloud provider fully controls the hardware and OS layers:



PaaS Software stack

- PaaS Provider/ Consumer Scope of Control: The provider has administrative control of middleware.

- The provider has no control over application layer.
- Remember that the application developed by using PaaS is deployed as SaaS and the PaaS consumer has full administrative control over that SaaS.
- The provider however controls the runtime-environment which is necessary for PaaS application.
- PaaS billing: Usually based on:
    - Number of consumers
    - Kind of consumers (e.g., developers vs. application end users)
    - Storage, processing, or network resources consumed by the platform
    - Requests serviced
    - The time the platform is in use.

Module No – 064: PaaS Examples:

- We are going to discuss a few examples of PaaS.
    - Google App Engine (GAE): Allows the users to create and host web based (Java, Python & Go) applications running over the infrastructure and services provided by Google. GAE is a free service until the application grows to a significant size.
    - Force.com as a PaaS: This is a service of Salesforce.com (a SaaS provider). It offers four different programming environments for nonprogrammers, programmers and software vendors.
        - Nonprogrammers can create finance, HR etc. applications and websites without coding by using drag drop of controls.
        - Programmers can develop Java applications and deploy them as SaaS.
        - The software vendors can distribute and update their applications over cloud by using Force.com.
    - LongJump as a PaaS: Supports the entire cycle of software development from requirement gathering to application release and support. It is free of cost.
    - Openshift as a PaaS: It is a PaaS offering from Red Hat which is also the distributor for Red Hat Linux. Openshift PaaS provides the primary development tools for cloud based solutions written in PHP, Python and Ruby.
        - Openshift also provides development tools for Linux-based solutions written in C programming language.
    - Windows Azure and SQL Azure as a PaaS: Provided by Microsoft as a paid service. The users can develop applications in .Net as well as Java, PHP and Ruby.
        - SQL Azure provides database solutions for application developed and running inside Windows Azure.

Module No – 065: Benefits and Disadvantages of PaaS Solutions:

- Benefits:
    - Lower total cost of ownership in terms of hardware and software investment.
    - Lower administrative overhead of system development.

- No requirement of software upgrades of tools.
- Faster application development and deployment.
- Scalable resources available for the applications. The user pays only for the resources used.

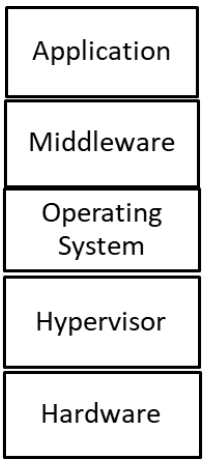
- Disadvantages:
  - The inherent problem of data placed offsite raises the security concerns.
  - The integration of PaaS applications with on-site legacy solutions is not trivial.
  - The PaaS provider has to be trusted for data and application security.
  - The issues of SaaS are also the issues of PaaS such as browser based risks, network dependence and isolation vs efficiency.
  - Portability of PaaS applications across different providers may not be possible sue to incompatibility in coding structures (hash, queue, file etc.).

Module No – 066: PaaS Recommendations:

- Generic interfaces: The consumer should make sure that the interfaces for hash tables, queues and files etc. are generic so that there will be less issues of portability (among PaaS providers) and interoperability (of applications) in future.
- Standard language and tools: Choose a PaaS provider which offers standardized language and tools unless it is absolutely unavoidable to use the proprietary languages and tools.
- Data access: The provider with the standardized data access protocol (such as SQL) should be preferred.
- Data protection: The confidentiality, compliance, integrity and availability needs of the organization should be compared with the data protection mechanisms of the provider.
- Application framework: The PaaS providers which offer the features in application development framework for eliminating security vulnerabilities of the application should be chosen.
- Component testing: The software libraries provided by the PaaS provider should be aiming at providing proper functionality and performance.
- Security and secure data deletion: Ensure that the PaaS applications can be configured to run in a secure manner (e.g., using cryptography during communication) and that a reliable mechanism for data deletion is provided by the PaaS provider.

Module No – 067: Infrastructure As a Service (IaaS) Overview:

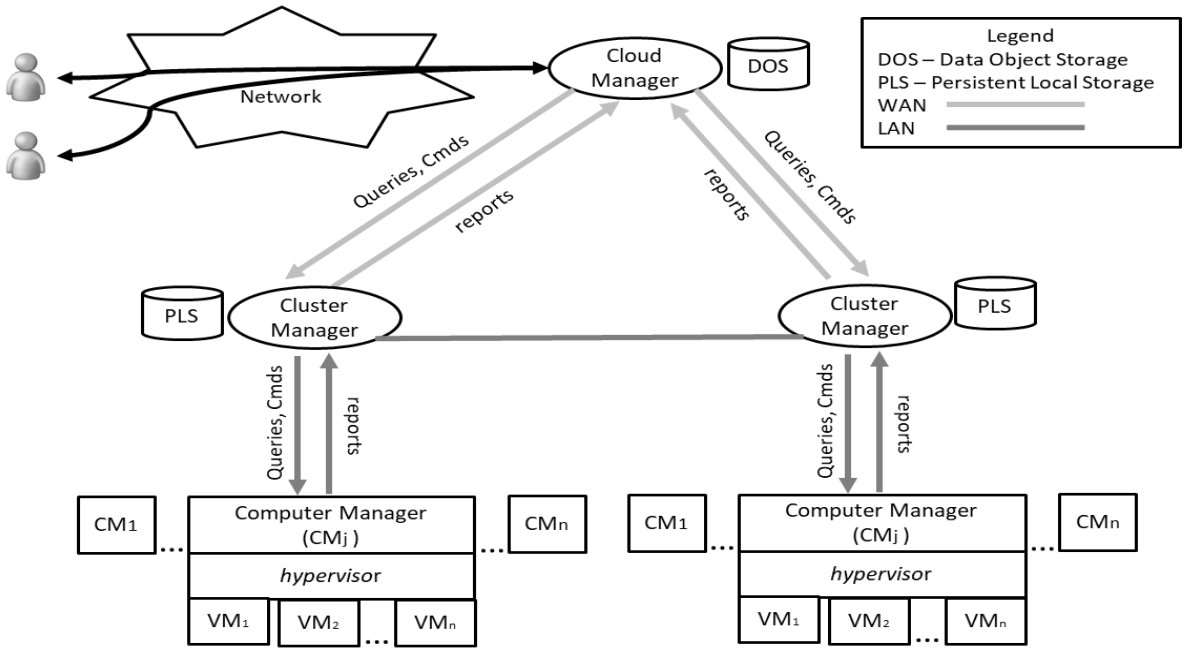
- As an alternative to PaaS, some consumers may prefer to use IaaS in order to have management control over the IT resources.
- The IaaS provider makes available the computing resources in the form of VMs.
- The consumer has the duty of installing OS and software.
- The provider also provides stable network access, network components such as firewalls, and data storage.
- IaaS Provider/Consumer Scope of Control: The provider has no control over top three layers.



IaaS Software Stack

- IaaS Provider/Consumer Scope of Control: The provider has admin control over hypervisor and total control over hardware layer.
- ~~IaaS Provider/Consumer Scope of Control:~~ The consumer has total control over top three layers.
- ~~IaaS Provider/Consumer Scope of Control:~~ The consumer can request the provider to deliver a VM from hypervisor layer.
- The consumer has no control over hardware layer.
- Customer billing:
  - Per CPU hour
  - Data GB stored per hour
  - Network bandwidth consumed, network infrastructure used (e.g., IP addresses) per hour
  - Value-added services used (e.g., monitoring, automatic scaling).

Module No – 068: IaaS Operational Overview:



The operational infrastructure of IaaS

Module No – 069: IaaS Benefits:

- Saving in upfront cost: As in SaaS and PaaS. Although the responsibility of installing OS and software is of the consumer.
- Full administrative control over VM:
  - Start, shut down, pause
  - Installation of OS and applications
  - Accessing VM through network services of VM through a network protocol such as Secure Shell.
  - Flexible and scalable renting: The VMs can be rented in any volume desired by the consumer. The rental for each VM can be on usage (of raw resources such as CPU, memory, bandwidth, storage, firewall, database etc.) basis.
  - Portability and interoperability with legacy applications: Since the consumer has full control over the VM to install OS and other applications, the legacy applications (which are usually installed on consumer owned server/s) can be configured to run with or ported to the VM.

Module No – 070: IaaS Issues and Concerns:

- Network dependence
- Browser based risks (~~same as discussed for SaaS and PaaS~~).
- Compatibility with legacy software vulnerabilities: Since the consumer is allowed to install the legacy applications on VMs rented through IaaS, this exposes the VMs to the vulnerabilities in those legacy software.

- Implementation challenges exist for VM isolation: In order to prevent the VMs from eavesdropping other VMs mounted over same server, the isolation features of hypervisor are utilized. But these features may not withstand a sophisticated attacks.
- Dynamic network configuration for VM traffic isolation: A dynamic network path is provided from VM to consumer when a VM is rented. The provider has to isolate VM consumers from accessing the network traffic of other consumers.
- Data erase practices: When a VM is no longer rented by a consumer, the virtual drive of that VM must be erased/overwritten multiple times to eliminate any chance of residual data access by the next consumer of that VM.
- NIST recommendations for IaaS: The provider should implement data and network traffic isolation for the VM consumers. The features of data security as well as secure deletion of residual data of VM consumer.

Lesson No. 14

DATA STORAGE IN CLOUDS

Module No – 073:Network Storage:

- Computers attached to a local area network (LAN) may require additional storage space to support file sharing, file replication and storage for large files.
- Traditionally this additional space is provided through file servers which have larger disk capacity.
- With the evolution of computer networks, the file server was extended through the use of storage area network (SAN).
- The SAN enabled storage devices are attached to the network.
- The software running over SAN devices allows direct access to these devices throughout network.
- Later on, a class of storage devices emerged to be implemented as network attached storage (NAS).
- Advantages of network storage (particularly of SAN) are:
    - Data reliability and reconstruction through replication.
    - Better performance than file server.
    - Compatibility with common file systems and operating systems.
    - Best choice for backups.

Module No – 074:Cloud Based Data Storage:

- Cloud storage is the next step in the evolution of network storage devices.
- Instead of storing the data locally, the data can be stored on cloud and can be accessed through web.
- The user can have virtually unlimited storage space available at affordable rates.
- There are various modes of data access in Cloud:
    - Using web browser interfaces to move the files to and from the cloud storage.
    - Through a mounted disk drive that appears local to the user's computer.

  - Through API calls to access the cloud storage.
- There are a number of cloud storage providers which offer file storage, sharing and synchronization. Such as:
- Carbonite
- pCloud
- Dropbox
- ElephantDrive
- These providers offer a certain volume of free storage as well as paid storage at low prices.

Module No – 075:Cloud Based Data Storage: Advantages & Disadvantages:

- Advantages:
  - Scalability: The user can scale the storage capacity (up or down) according to requirement.
  - Various convenient costing models are available from one time payment to monthly payment to pay as per use.
  - Reliability: The storage providers provide the assurance for data reliability (through replication).
  - The data can be accessed worldwide by using Internet.
  - Various methods of data access are available (~~as discussed before~~).
- Disadvantages:
  - Performance: Because of the Internet based access, the cloud storage can never be as fast as SAN or NAS based local storage.
  - Security: Not all the users may be able to trust the cloud provider for the users' data.
  - Data orphans: The user has to trust the data deletion policies of the provider. The files (on cloud storage) deleted by the user may not be immediately (or ever) be deleted from the cloud storage.

Module No – 076: Cloud Based Backup Systems:

- The term *backup* refers to the copying of (data and/or database) files to a secondary site for preservation in case of device or software failures.
- Backup is an important part of disaster recovery plan.
- In case of a disaster, the data can be restored to the state of last backup.
- Cloud based backup system comprises of procedures to send the copy of data over a proprietary or public network to a remote server hosted by the cloud service provider.
- The provider charges the user according to number of accesses or data volume or number of users.
- Cloud based backup or online backup system is implemented through a client software installed on the user's computer. The software collects, compresses and sends the data to cloud backup on timely basis.
- Advantages:
  - The data is backed up in encrypted form.

  - Backup can be performed on the convenience of user (daily, weekly, monthly).
  - The user can easily retrieve the backup files from the cloud.
- Disadvantages / Limitations:
  - Due to security concerns, the critical data backup is preferably stored on local storage.
  - The long term data storage in heavy volume over cloud may have humongous cost.
  - Due to network cost, the incremental backup is preferred.

Module No – 077: Database and Block Storage:

- A Cloud database is a database that resides on Cloud platform.
- The Cloud database can be accessed by:
  - The applications hosted on Cloud
  - The application hosted locally (can access through Internet)
- The cloud database is provisioned in either of the following methods:
  - Installed on a rented VM by the user
  - As part of PaaS
  - Provided as a service by cloud provider or the database companies.
- Advantages of Cloud based Database solutions:
  - Cost effective scalability as per use
  - High availability of database software through redundant hardware (minimizes the downtime in case of failure)
  - High availability of data due to replication of database
  - Reduced administration of database provided as service or as part of PaaS.
- Disadvantages of Cloud based database solutions:
  - The user may not trust the cloud provider regarding sensitive data
  - Due to Internet based access, the Cloud based database is not as fast as a locally installed database.
- There are a number of cloud based database providers such as:
  - Oracle
  - Amazon
  - Microsoft

- Cloud based block storage is a sequence of bits and provided as a block on cloud storage.

- It is suitable in the following situations:

  - When the data may not map properly on a file system or on a database

  - The application developer wants to store data in a customized file system

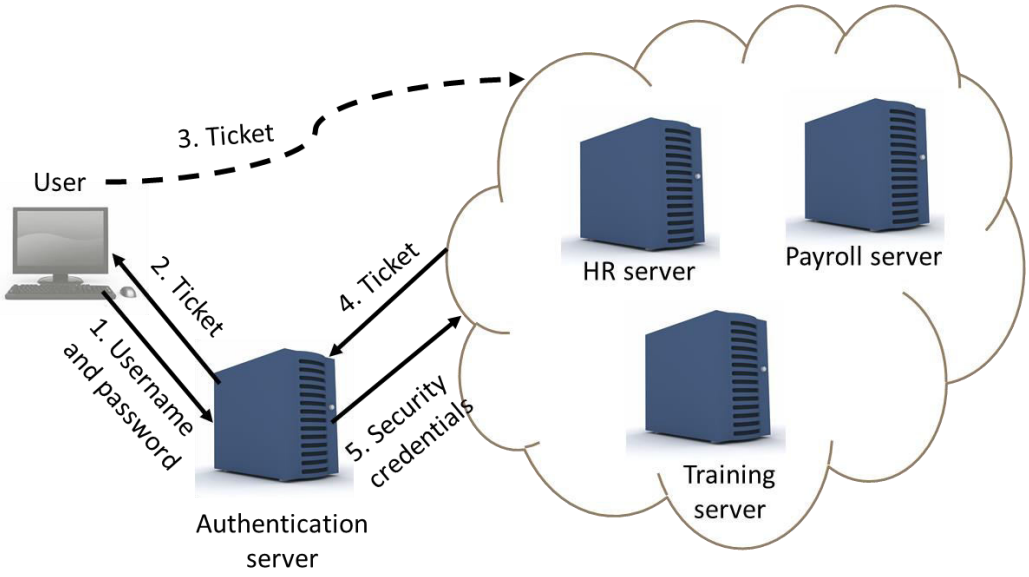
- Amazon Elastic Block Store (EBS) is a highly available, scalable and reliable block storage solution which supports block sizes of up to 1 terabytes.

Lesson No. 15

MISCELLANEOUS SERVICES OF CLOUD COMPUTING

Module No – 071:Identity as a Service (IDaaS):

- Today within most companies, the users may have to log in to several applications servers (on premises and/or cloud) to perform daily tasks. Some of these systems may be cloud based.
- The user has to remember multiple logins and passwords.
- When a user leaves a company, the related logins and passwords must be deleted.
- The identity management is a complex task and therefore provided as a service for cloud consumers.
- For example single sign on (SSO). Single sign on (SSO) software is installed over authentication server.
- Before connecting to application servers, the user connects with the authentication server to obtain a secure ticket.



- The authentication server maintains the user login security credentials required by application servers.
- When the user leaves the company, only the user's login on authentication server is needed to be disabled to block the user's access to all the application servers.
- There are a few examples of IDaaS providers for on-premises and cloud applications such as Ping IDaaS and PasswordBank IDaaS.

Module No – 072:IDaaS: OpenID:

- It is a popular example of Identity as a Service(IDaaS).
- Allows the users to sign-in to multiple websites by using a single account.

- Solves a lot of problems related to multiple log-in accounts per user.
- Why use OpenID:
  - Avoid too many user names and passwords.
  - Overcoming the scarcity of desired user names.
  - Account management is difficult otherwise.
  - Avoid filling long forms for creating logins again and again.
- OpenID is not controlled by any organization and/or person.
- There are a number of companies (providers) which provide OpenID accounts. These include: Google, Microsoft, Yahoo, Amazon, SalesForce etc.
- There are more than 1 billion OpenID accounts which are accepted by over 50,000 websites.
- How does it work:
  - A user creates an OpenID login through a suitable provider.
  - The user visits a website which is compatible with OpenID.
  - The (visited) site prompts the user to sign-in with the OpenID credentials.
  - The user is redirected to the OpenID provider's website.
  - The user opts to share the credentials/token with the (visited) website.
  - The user provides login and password at the OpenID provider's website.
  - If the user is verified, the OpenID provider confirms the (visited) website.
  - The user is redirected to the (visited) website which accepts the user as authenticated user.

Module No – 078: Identity as a Service (IDaaS):

- Collaboration is defined as the process in which two or more people work together to achieve a goal.
- Traditionally, the collaboration has been achieved through face to face meetings in conference rooms.
- Some team members had to travel (from near or far) to attend the meetings.
- Those who could not personally arrive at the meeting had either of the following two choices:
- Phone call to a speaker phone placed at the conference table
- Study the minutes of meeting
- A solution that could reduce the requirements of personal meetings was required to save time and effort and to increase the productivity from the collaborations.
- The web based collaboration began with the web mail.
- Users can compose, send, receive and read the emails by using the web browser and Internet connection.
- A single user can address multiple recipients in a single mail.
- (IM) provide a real time exchange of messages and replies (chat) by using messaging software.
- IM is another form of traditional collaboration. Current tools for IM allow file exchange and audio/video calling.
- Voice over Internet Protocol (VoIP) enables the users to make phone calls over the Internet.
- VoIP tools such as Skype provide a convenient way to perform conference calls by using computers and mobile phones.

Module No – 079: Cloud based Phone & Fax Systems:

- Sending and/or receiving fax traditionally required the fax machine and telephone connection.
- Similarly, phone calling has been dependent upon telephone infrastructure.
- In modern days, many companies have started providing cloud based calling and cloud based fax services.
- These companies have all the calling/fax operations performed over the Cloud and provisioned over the Internet.
- Taking example of Google Voice Phone System: The account holder receives the services of call answering and voice mail.
- The user can even configure the service to forward the incoming phone calls to a cell number.
- Google delivers the voice messages left by the callers as audio messages as well as in the form of text which are receivable anywhere through the Internet.
- Cloud based fax service provided by various companies is provisioned as a separate virtual number to each subscriber. This number corresponds o a virtual fa machine.
- The fax received over the virtual fax machine are delivered through email as PDF attachment.
- Similarly, to send a fax, a simple email (with PDF file) to virtual fax account will send the fax to recipient/s.

Module No – 080: Editing the Shared Files in Cloud:

- ~~As we have seen that~~ data and files can be stored on Cloud storage.
- It is also possible to edit the files (located on Cloud storage) shared among concurrent users.
- Provides another way of collaboration.
- A number of service providers offer the editing of shared files such as text, spreadsheet and presentation files. These include the famous providers:
    - Dropbox
    - Microsoft
    - Google
- Dropbox offers file sharing through public folders among the Dropbox users.
- It is allowed to edit the MSWord, Excel and PowerPoint files in browser and without the MSOffice installed.
- Simultaneous users can edit a shared document.
- Google provided *Google Docs* service offers web-based free access to a word processor, spreadsheet and presentation programs to create, share, edit, print and download the documents stored on Cloud.
- Google Docs can be shared through simple email link.

Module No – 081:Collaboration in the Cloud Through Collaborative Meetings:

- Collaborative meeting can be performed by using the software hosted on Cloud.
- Organizations get a cost effective *virtual meeting* as an alternative to face to face meetings.
- The features of cloud based collaborative meetings are:
  - Streaming video to allow face to face interaction
  - Shared whiteboards to control the presentation
  - Shared applications to demonstrate software in live environment
  - Meeting recordings for playback and sharing
- *GoToMeeting* is one of the leading providers of virtual meetings.
- Can support face to face meetings and web seminars (webinars) with more than 1000 attendees.
- The video recording of virtual meetings and webinars can also be used for virtual training and reference purposes as well.

Module No – 082: Collaboration by Social Media & Video Streaming:

- Social media and streaming video contents provide yet another way for collaboration.
- Cloud hosted social media such as Facebook and SalesForce.com's Chatter tool are available for collaboration among team members.
- The team member can easily exchange updates, comments and reviews regarding different tasks.
- Files can be shared among the team members.
- Photos and videos can be uploaded and shared to demonstrate a situation.
- Live video streaming can also be broadcasted if required.
- YouTube offers a free, reliable and Web accessed cloud storage for video contents worldwide.
- Videos created for collaboration can be shared among team members and publicly as well.
- The collaborative videos may include technical training clips, discussions and/or site coverage etc.
- The viewers can discuss and upload written comments on the video clip.

Lesson No. 16

CLOUD DEPLOYMENT MODELS

Module No – 083: Public Cloud:

- Public cloud is one of the deployment models of Cloud through which the IT resources are publicly available and accessible trough public Internet.
- Characteristics of Public Cloud according to NIST:
  - The consumer is generally not aware of the location of IT resources unless a location restriction is imposed by either of provider or consumer. Still it is difficult for the

consumer to verify the location on map from where the IT resources are being provisioned.
- The consumer workload may be a co-resident of the workload of other consumer (multi-tenancy) which may include the rivals, adversaries and in worst case, the attackers.
- The consumer has limited visibility of the software and procedures of the provider. The consumer has to trust the provider for securing the consumer's data and fully disposing the deleted data.
- The consumer undergoes a limited upfront cost regarding the provisioning of IT resources as compared to in house or locally setting up the IT infrastructure.
- Thanks to the workload management, dynamic collaboration among cloud providers and (generally) large setups, the public clouds can give the illusion of unlimited resources and elasticity to the consumers.
- The provider is in a limited legal Service Level Agreement (SLA) with the consumer. The SLA covers the minimum performance assurance/s by the provider and penalty in case of violation to the assurance/s.

Module No – 084: Private Cloud:

- Characteristics of Private Cloud according to NIST:
  - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).
  - It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
  - The private cloud users depend upon the local area network if the cloud is locally deployed and accessed from a single site.
  - For multi-site access and outsourcing, the dedicated leased secure communication lines should be used.
  - Consumers are needed to be trained for working in Cloud environment.
  - Consumers have no knowledge of the location of their workload. Even in on-site deployment, a consumer can not pinpoint a server for the location of workload.
  - However, in case of outsourced Private Cloud, the consumer organization may have some knowledge of the cluster location and network segment serving the Private Cloud at the provider's end.
  - Consumer workload is vulnerable to cons of multi-tenancy from the insider malicious colleagues.
  - Modest cost for outsourced private Cloud (excludes infrastructure cost): Negotiation with the provider, Upgradation in network equipment, updating of legacy software to work on Cloud, training of staff etc.
  - Significant cost for onsite private Cloud (includes the data center and infrastructure cost): Updating of legacy software to work on Cloud, training of staff etc.
  - Resource limitation in on-site private Cloud but extendible resources available in case of outsourced private Cloud.

Module No – 085: Community Cloud:

- Characteristics of Community Cloud according to NIST:
  - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
  - It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
  - For the onsite Community Cloud, the resource sharing among the participating organizations has to be decided explicitly or implicitly.
  - At least one member of the community should provide Cloud services.
  - Network dependency: In case of on-site deployment, the network dependency is similar to on-site distributed Private Cloud setup. The performance and security can be enhanced through dedicated secured communication lines.
  - ~~Network dependency:~~ The members can also use encryption over Internet for the network access to the Community Cloud resources.
  - IT skills are required to manage the Community Cloud deployment and operations in both the participants (providing Cloud services) and consumer members of the community.
  - Workload locations are generally hidden from the community members unless a participant member decides to outsource the Cloud services (similar to outsourced Private Cloud). In this case, prior approval and documentation should take place.
  - Multi-tenancy cons are similar to onsite Private Cloud scenario.
  - The upfront cost for consumer-only member is same as of outsourced Private Cloud. While for participant members (onsite deployment), the upfront cost is similar to onsite Private Cloud.
  - The onsite deployment of Community cloud suffers from resource shortage as of onsite Private Cloud because each participant organization has limited resources.
  - Extensive resources are available for outsourced Community Cloud just like outsourced Private Cloud.
  - Due to a number of members, there are a number of security perimeters (hence complex cryptography) and dedicated communication lines in a Community Cloud. This offers a better security from external threats.

Module No – 086: Hybrid Cloud:

- Characteristics of Hybrid Cloud according to NIST:
  - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public).
  - The hybrid cloud components infrastructures (private, community, or public) remain unique entities.
  - The hybrid cloud components infrastructures (private, community, or public) are bound together by standardized or proprietary technology that enables data and application portability (for load balancing between clouds).

- Hybrid Clouds are often possible when the phenomenon of *Cloud Bursting* is applied whereby a consumer uses a private cloud in routine but may use the services of other types of clouds for load balancing at peak times.
- Hybrid Clouds are also formed when one type of cloud is used to provide backup to another type of cloud.
- An organization may choose to process sensitive data on outsourced private-cloud but choose new software testing on a public cloud.
- It may be cost effective to put the web requests handling for web applications on a PaaS instance while the background processing of those web applications can be done on on-site community cloud.
- Challenges for hybrid clouds exist in security management, identity management and access control of multiple clouds etc.
- More complex scenario arises when the clouds are dynamically joining and exiting the hybrid cloud.
- Network dependence
- IT skills required
- Workload locations are hidden from consumer
- Security risks due to multi-tenancy

Lesson No. 17

SERVICE ORIENTED ARCHITECTURE

Module No – 087: Web Applications & Multitenant Technology:

- Web Applications: These are the applications which use web technologies (URL, HTTP, HTML, XML) and generally use web browser based interface.
- Can be modeled on the basis of three-tier model.
  - Presentation layer
  - Application layer
  - Data layer
- Web Application Architecture 1:

Layer	Implementation	
	Server side	Client side
Presentation	Web/ Application Server	Web client
Application		
Data	Data storage server	

- Web Application Architecture 2:

Layer	Implementation	
	Server side	Client side
Presentation	Web server	Web client
Application	Application server	
Data	Data storage server	

- Multi-tenant Technology: The multi-tenant applications allow isolated to simultaneous users (tenants).
  - The data and configuration of each user remains private to other users.
  - The tenants can customize the user interface, business process, data model and access control of the multi-tenant application.
- Common Characteristics of Multi-tenant Applications:
  - Usage isolation
  - Data security
  - Backup and restore is separate for each tenant
  - Application upgrades do not negatively effect the existing users
  - Scalability in terms of number of tenants
  - Metered usage
  - Databases, tables and/or schema isolation for each user

Module No – 088: Service Oriented Architecture

- Web Services are independent units of software (code) which allow network based machine-to-machine interaction.
  - Have no user interface.
  - Process data between the computers through API calls.
  - Examples: SOAP and REST based web services
- Service oriented architecture (SOA) is usually a collection of services (web services)
- These services communicate with each other for the exchange of data and processing.
- Two or more services may be coordinating an activity.

- Examples of web services:
  - Return the weather conditions for a specific zip code
  - Return real-time traffic conditions doe a road or highway
  - Return a stock price for a particular company
- Web services are not web pages.
- To use a web service (which resides on a remote server), a program exchanges messages with the service.
- The user program sends parameters (through API call) such as zip code to the web service and waits for the reply.
- Web services are treated as black box by the programmer.
- Web services are interoperable which means that programs written in dissimilar language/s than the web-based service can call the API functions.
- Web Services: The core technologies are:
  - Web Service Description Language (WSDL): A markup language to define the API of the web service including the functions and the input/output messages associated with each function.
  - Message input/output are in the form of XML and defined by XML schema.
  - The message formatting is according to a common messaging format defined by Simple Object Access Protocol (SOAP) or through Representation State Transfer (REST).
  - Universal Description, Discovery and Integration (UDDI) is a standard which regulates the service registries in which WSDL definitions can be published so that they can be discovered by the users.
- Cloud Service & Web Services:
  - These two are not alike.
  - Can be used independent of each other in a SOA.
  - Cloud services are SaaS, PaaS & IaaS
  - Web services are API Calls.
  - Web services can be the front door for the cloud services running at the backend.
  - Cloud services are often provided over web services.
  - For example Amazon Web Service (AWS) based cloud services (e.g., data processing service deployed by a provider) can be accessed over network through API developed (by the same provider) using Amazon API Gateway.

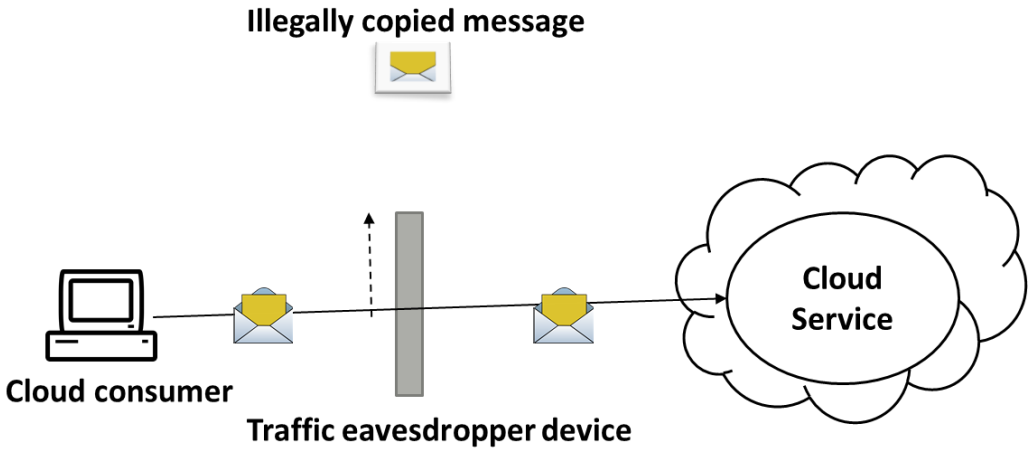
Lesson No. 18

CLOUD SECURITY THREATS

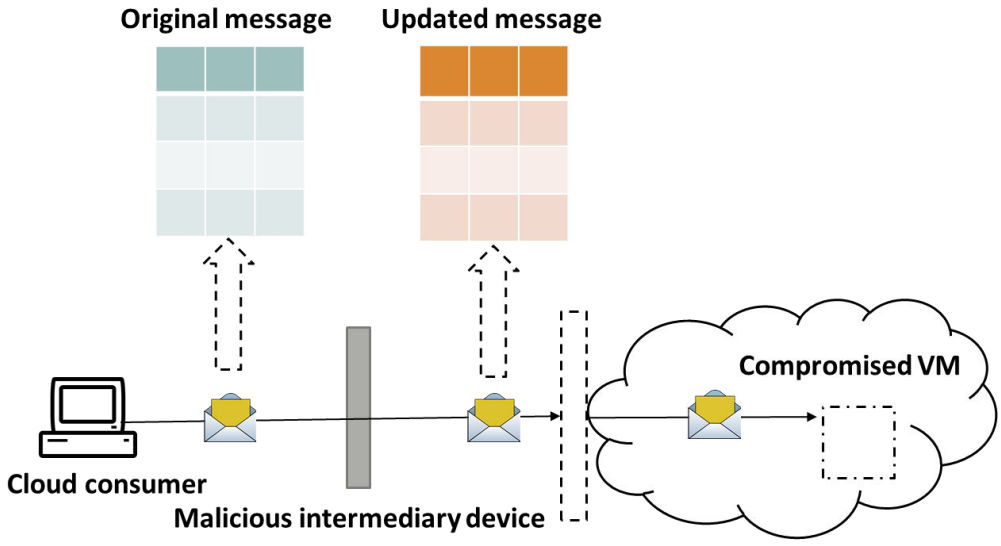
Module No – 089:

- ~~This module is about the prominent security threats to the Cloud computing.~~
- The following are significant threats to Cloud Security:

- Traffic Eavesdropping: ~~This module is about the prominent security threats to the Cloud computing.~~ Compromises the message contents. Can go undetected for extended periods of time.



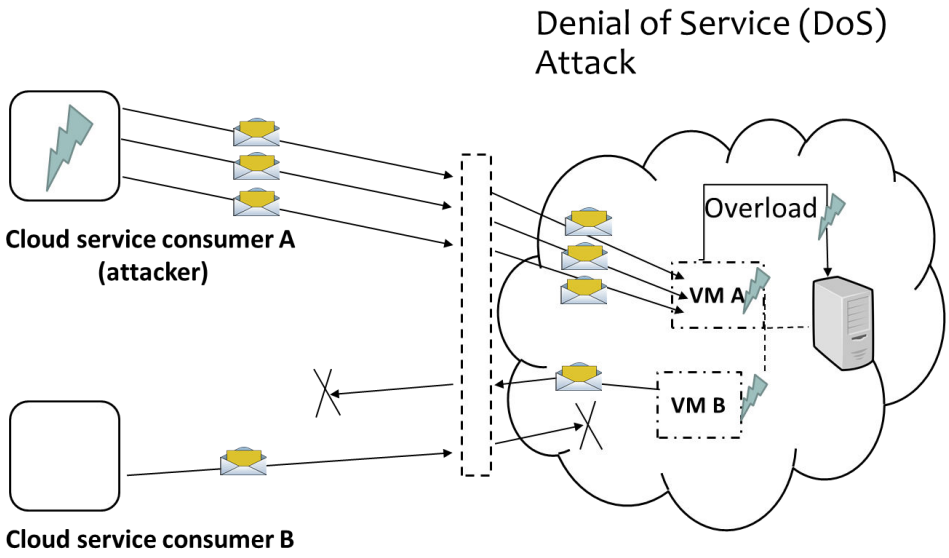
- Malicious Intermediately: The messages are illegally intercepted and then the contents are updated. The updated message is then relayed towards the cloud. ~~The messages are illegally intercepted and then the contents are updated. The updated message is then relayed towards the cloud.~~ The message may be updated with malicious contents which reach the VM hosting the cloud service undetected.



Module No – 090: Cloud Security Threats:

- ~~…continued~~
  - Denial of Service (DoS): The purpose is to overload the IT resources so the sage where they can not work properly. Can be launched in the following ways: Workload on a cloud service is artificially increased through fake messages or repeated

communication requests. Network is overloaded with traffic to cripple the performance and increasing the response time. Multiple cloud service requests are sent. Each request is designed to consume excessive memory and processing resources.



- Insufficient Authorization based attack: It is a situation when a malicious user gets direct access to IT resources which are supposed to be accessed by trusted users only. Happens when a broad access is provided to the IT resources and/or due to erroneously.
- Weak authentication based attacks: Happen when weak passwords or shared (login) accounts are used to protect the IT resources. The impact of attacks due to insufficient authorization and weak authentication depends upon the range of IT resources and the range of access to those IT resources is compromised.

Module No – 091:Cloud Security Threats:

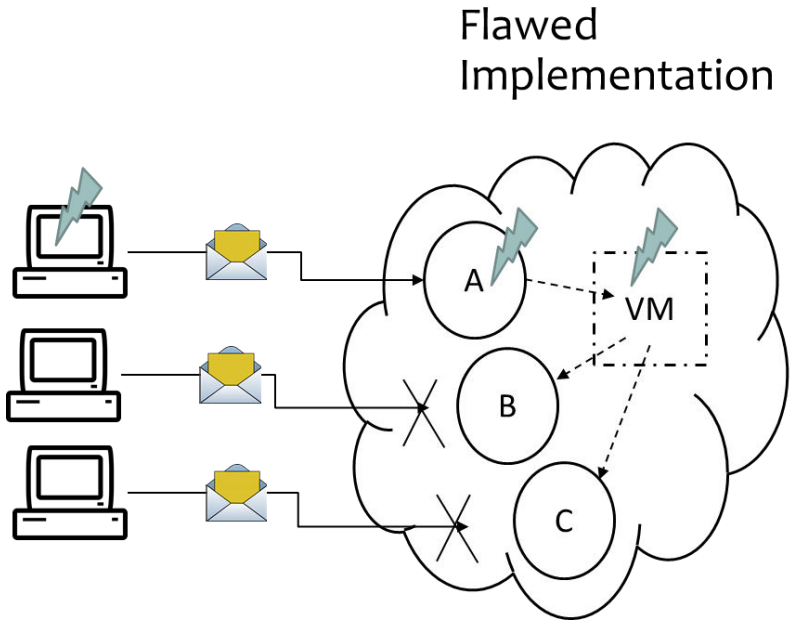
- ~~…continued~~
  - Virtualization Attack: Based upon the administrative privileges provided to the Cloud consumers and multi-tenancy, it is possible to compromise the underlying physical hardware. It is also possible that the security flaws be arising due to *VM sprawl* (a lack of security patches on OS installed on VM). Another possibility is the installation of VM-aware malware to exploit the security flaws of hypervisor. Following are possible sources in which the physical server may be compromised:
    - By an imposter in disguise of a legitimate consumer. The attacker cracks the (weak) password of a consumer.
    - By a trusted but malicious consumer.
    - In either case, the vulnerabilities in the virtualization platform are exploited over a single VM to take control of the physical server hosting the infected VM. Makes all the VMs hosted on the compromised server as vulnerable.

- A more severe scenario arises when the infected VM is migrated to other server for load balancing. In this case, a number of servers may get compromised.

- Overlapping Trust Boundaries: Moving of consumer data to Cloud means that the provider now shares (with the consumer) the responsibilities of availability, confidentiality and integrity of data. The consumer thus extends the trust boundary to include the cloud provider. This is prone to vulnerabilities. When multiple consumers of a cloud share an IT resource, the trust boundaries overlap. The provider may not be able to provider the security features that can satisfy the security requirement of all the consumers of shared IT resource on a Cloud. More complex scenarios arise when the consumer data is replicated and stored on multiple sites.
- Another complexity arises when the Cloud provider handover the business to a new owner. The data integrity becomes threatened in both cases.

Module No – 092:Cloud Security Threats:

- ~~…continued.~~
  - Flawed Implementation: The implementation of Cloud services may have some flaws related to configuration resulting into the occurring of unexpected events. Particularly the security and operational weaknesses in Cloud provider's software/hardware can be targeted by the attackers to put the integrity, confidentiality and/or availability of IT resources of the provider at stake. Equally important point is the implementation flaws of Cloud services may result in the crash of VM and thus will effect all the other services on that VM as well. For example service A has some implementational flaws to crash the hosting VM when a certain message is sent. This will also effect the services B and C and can be exploited by an attacker.



- Disparity of Computer Security Policy : A computer security policy defines the set of rules and mechanisms to ensure the security of the computers of the organization. The computer security policies of the consumer and provider may not match. Before opting of outsourcing and/or public cloud, an organization must evaluate the compatibility of provider's security policy with its own. The lack of administrative privileges provided to the consumer makes the implementation of the consumer chosen computer security policy very difficult. ~~Due to the discussed points,~~ the standardization of securing the IT resources leased by a consumer and the consumer data is a challenging task.

Module No – 093: Cloud Security Threats:

- ~~…continued.~~
  - Contracts: As an additional consideration, the SLA offered by the provider should be carefully examined to clarify the liabilities taken by the provider and the security policy implemented by the provider. This helps in determining the following:
    - If the consumer deploys its own solution over the Cloud resources then it is a situation of consumer's assets deployed over provider's assets. Then how the blame will be determined when a security breach or a runtime failure occurs ?
    - If the consumer can apply its own security policies while the cloud provider keeps the administrative rights to the IT infrastructure. Then how this disparity will be overcome.
  - Risk Management: The cloud consumers should perform a cyclic process of risk management to access the potential threats and challenges related to Cloud adoption. This should be a part of risk management strategy. It is a three stage process.