Cloud Computing [131P15C302]

~ Asst. Prof. Shivkumar Chandey
M.Sc. Computer Science

Objectives

At the end of Cloud Computing course, the students will:

1. Have an insight into the basics of cloud computing along with virtualization.
2. Have a conceptual understanding of cloud computing and will be in the position to assess their application objectives and decide how to deploy their application in the cloud with ease.
3. Understand the security aspects in cloud.

Unit III Syllabus

Unit III	Recent Trends in Cloud Computing and Standards Host Security in the Cloud Data Security in the Cloud Application Architecture for Cloud

Text Books and References

- **Textbooks:**

1. Cloud Computing Black Book, Dreamtech Press, 2014
2. Mastering Cloud Computing - Technologies and Applications Programming, 2014

- **Reference Books:**

1. Cloud Computing: Concepts, Technology & Architecture, Pearson, 2013
2. Cloud and Distributed Computing: Algorithms and Systems, Wiley

Course Learning Outcomes

1. Student will have basic understanding about cloud and virtualization along with it how one can migrate over it.
2. Students can identify the various levels of services that can be achieved by cloud
3. Student can understand the issues related to Cloud Computing.
4. Students will recognize the administrative challenges in Cloud Computing.

List of Practicals

1. Implementation of Bare-metal and hosted virtualization
2. Implementation of containerization using docker
3. Demonstration of IaaS cloud
4. Demonstration of PaaS cloud
5. Demonstration of SaaS cloud
6. Implementation of Cloud services on Open stack cloud platform
7. Implementation of Cloud services on Amazon web services
8. Demonstration of data analytics in Cloud

Recent Trends in Cloud Computing and Standards

Recent Trends : Conflict of Interest for Public Cloud and IT Product Providers

- Established software and hardware product vendors are finding themselves at the crossroads .
- They are not sure if they want to welcome the cloud or if they ought to ignore it . The vendors know that the customers are aware of and are evaluating cloud options .
- At the same time , they see cloud services as cannibalizing their traditional product markets .

Recent Trends : Conflict of Interest for Public Cloud and IT Product Providers

- They want to shun the cloud option as it tends to replace their more lucrative product sales .
- As a result , there have been cases recently where product vendors who had rolled out but later withdrawn their cloud services . Nonetheless , many vendors are rushing to offer more cloud services and it seems certain there will be more pullbacks .

Recent Trends in Cloud Compliance

- One of the recent advancements has been the various regulatory compliances that cloud providers must meet .
- Most of the public clouds are mindful of regulatory requirements such as PCIDSS , HIPAA , ECPA , GLBA , etc.
- They have taken onerous measure to make sure their cloud complies with industry regulations .
- Sometimes , start - ups or SMEs using public clouds are unaware of all compliance requirements .
- But the cloud providers are attentive to the compliance needs and are willing to work with consumers to meet the regulatory requirements .

Recent Trends in Security : BYOD and Encryption Exposures

- An increasing number of employees are bringing and using their personal wireless devices into offices .
- Since they are very familiar with the user interface , they use their smart phones and tablets to access corporate data .
- This has led to the development of the concept of Bring Your Own Device BYOD) .

Recent Trends in Security : BYOD and Encryption Exposures

- Encryption is considered important in enhancing data security.

Recent Trends in Cloud Standards

- This section discusses the adoption and implementation of standards by cloud providers .
- It is important to have a set of standards and norms that can be implemented by many cloud providers
- This will help build uniformity and enable inter - cloud communication and migration .

Recent Trends in Cloud Standards

- The trend for adopting cloud services has introduced new risks , rollout problems , and vendor lock-ins.
- In order to mitigate these , you need to make sure that the provider follows certain common standards.
- They are a critical element for adoption and later migration to another provider , when needed.
- There are several emerging and established cloud standards. Several global organizations are working on cloud standards.

Some of these organizations are as follows

- Cloud Standards Customer Council (CSCC)
- Open Grid Form (OGF)
- Open Cloud Consortium (OCC)
- Distributed Management Task Force (DMTF)
- Storage Networking Industry Association (SNIA)
- The Open Group (TOG)
- Organization for the Advancement of Structure Information Standards (OASIS)
- Cloud Security alliance (CSA)

Some of these organizations are as follows

- These are consortiums of IT product companies and cloud providers .
- They are trying to establish standards that would be used by more and more providers .
- The following is a description of the organizations mentioned above

Cloud Standards Customer Council (CSCC)

- CSCC is an end - user advocacy group , dedicated to improving cloud's successful adoption , and drilling down into the standards , security , and interoperability issues with migration of new services to the cloud .
- It allows cloud users to drive client requirements into standards development .
- Its founding enterprise members include IBM , CA Technologies , Kaavo , and Rackspace . Since then , more than 100 of the world's leading enterprises such as Lockheed Martin , Citigroup , State Street and North Carolina State University have joined the Council .

Open Grid Forum (OGF)

- OGF develops standards to champion architectural blueprints related to cloud and grid computing and associated software development .
- It helps to build pervasive adoption of advanced distributed computing techniques for business and research worldwide .

Open Cloud Consortium (OCC)

- OCC supports the development of standards and benchmarks for cloud computing.
- It also develops frameworks for interoperation between different clouds .
- It supports reference implementations for cloud computing , commonly using open source software .
- It is particularly focused on large data clouds and related reference models .

Distributed Management Task Force (DMTF)

- DMTF has a group called Open Cloud Standards Incubator (OCSI) dedicated to developing standards and specifications for cloud architecture and implementation so as to make it easy for cloud providers to interact and share data .
- DMTF has another taskforce called Cloud Management Working Group (CMWG) , which is now developing a set of prescriptive specifications to deliver architectural semantics and deployment details .
- The goal of CMWG is also to help achieve interoperable clouds management between providers , consumers and developers .

Distributed Management Task Force (DMTF)

- Another DMTF working group is Cloud Auditing Data Federation (CADF) , which develops standards for federating cloud audit information .
- The specifications will federate different audit event data , such as interface definitions and compatible interaction models .
- These models , in turn , will help describe interactions between different cloud resources .
- This will help cloud providers to produce and share specific audit for events and logs , and report information for each cloud tenant that they have .
- The reports and logs will help users classify and tag events as being relevant to different compliance controls and frameworks (such as COBIT , ISO 27002 , PCI DSS , etc.) .

Storage Networking Industry Association (SNIA)

- A key SNIA taskforce named Cloud Storage Initiative (CSI) is working towards identifying and developing standards for cloud storage .
- The specifications will help providers implement consistency of messages , interface , and protocols for cloud storage .
- SNIA has set up a cloud storage standard called Cloud Data Management Interface (CDMI) to lay out a practical interface that storage providers can use to create , retrieve , update , and delete data .

The Open Group (TOG)

- TOG has a taskforce called the Cloud Work Group , with some of the industry's leading cloud providers and end - user enterprises as its members .
- The taskforce collaborates on standard models and frameworks to eliminate vendor lock - in and help realize the benefits of scalability , cost savings , data security , and implementation agility

Organization for the Advancement of Structure Information Standards (OASIS)

- OASIS has several technical committees (TCs) for cloud standards .
- Important standards are being formed by various OASIS TCs , such as :
- OASIS Cloud Application Management for Platforms (CAMP) TC
- OASIS Identity in the Cloud (IDCloud) TC
- OASIS Symptoms Automation Framework (SAF) TC
- OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) TC
- OASIS Cloud Authorization (CloudAuthZ) TC
- OASIS Public Administration Cloud Requirements (PACR)

Cloud Security Alliance (CSA)

- The primary role of CSA is to identify and formulate measures to mitigate security threats .
- CSA has a unit called the Secretariat , which provides technical and advisory support , primarily related to security and information management for other clouds CSA has Standards Developing Organizations (SDOs) that represent the CSA to form standards with other peer SDOs such as the International Standardization Council (ISC) .

More on emerging standards

- An emerging standard , specific to security for cloud computing , is ISO 27017.
- The proposed working title for ISO 27017 is " Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002 " .
- ISO 27017 is centered on the popular ISO 27002 (Information Security Management Systems or ISMS) standards .
- ISO 27017 standards are expected to be a guideline for recommending relevant data security controls for cloud providers .

More on emerging standards

- ISO 27017 will help specify security controls and will add to the ISO 27002 requirements .
- The status of ISO 27017 standards is under development . All these standards have been developed by independent organizations .
- Most are being implemented by providers .
- Users need to , however , know about the standards adopted by the provider and how it will help them in migration to another cloud .

Approaches to Implement Interoperability between Clouds

- The goal of the various standards is to facilitate interoperability .
- One way to do this is to create and provide an orchestration layer .
- This layer will help to enhance the usage of various clouds by forming a federated cloud environment .
- The cloud orchestration mechanism was initiated by various cloud service providers to form a single management platform , where the services of a federated cloud can be centrally assembled and managed .

Approaches to Implement Interoperability between Clouds

- The interoperability features can resolve the problem of vendor lock - in , and accelerate the integration amongst cloud service providers .
- The end result is a set of integrated cloud services where data can be easily interchanged .
- However , the service providers need to implement standards in their services . Without interoperable features and the ability to exchange data , the use of cloud services would be significantly reduced .

Host Security in the Cloud

Host Security in the Cloud

- Security for the Virtualization Product
- Host Security for SaaS
- Host Security for PaaS
- Host Security for IaaS

Host Security

- Host security describes how your server is set up for the following tasks:
  - Preventing attacks.
  - Minimizing the impact of a successful attack on the overall system.
  - Responding to attacks when they occur.

Security for the Virtualization Product

- The cloud provider is responsible for the security of the virtualization software in all the public cloud deployments .
- It is the software that sits on top of the bare metal and enables the provider or the customer to create and delete virtual machines .
- It enables several virtual machines or instances to share the same underlying server resources (CPUs , network cards , bandwidth , memory and connected storage) .
- The OS and user data is located on a SAN , NAS or iSCSI storage device connected to the server . Some common hypervisors used by cloud providers are vSphere from VMware , Hyper - V from Microsoft , and Xen from Citrix .

Security for the Virtualization Product

- In PaaS and SaaS , the virtual machines are shared by several customers .
- In an IaaS environment , each virtual machine is owned by a customer .
- The virtual machines come with an operating system such as Microsoft Windows , Linux or a Unix variant .
- Customers have no access or control of the virtualization software .
- Nonetheless , since virtualization is used by all cloud providers and is critical to host security , users should ask for details on mechanisms implemented to keep the virtualization layers secure .

Host Security for SaaS

- For SaaS services , the provider owns and manages the servers , network and applications .
- As a SaaS customer , if you ask the provider for host information , you will get little or no data .
- The applications run on a number of virtual machines with Linux , Windows or other operating systems .
- The provider will often refuse to provide details on OS , patches , implemented security measures , hypervisor , etc.

Host Security for SaaS

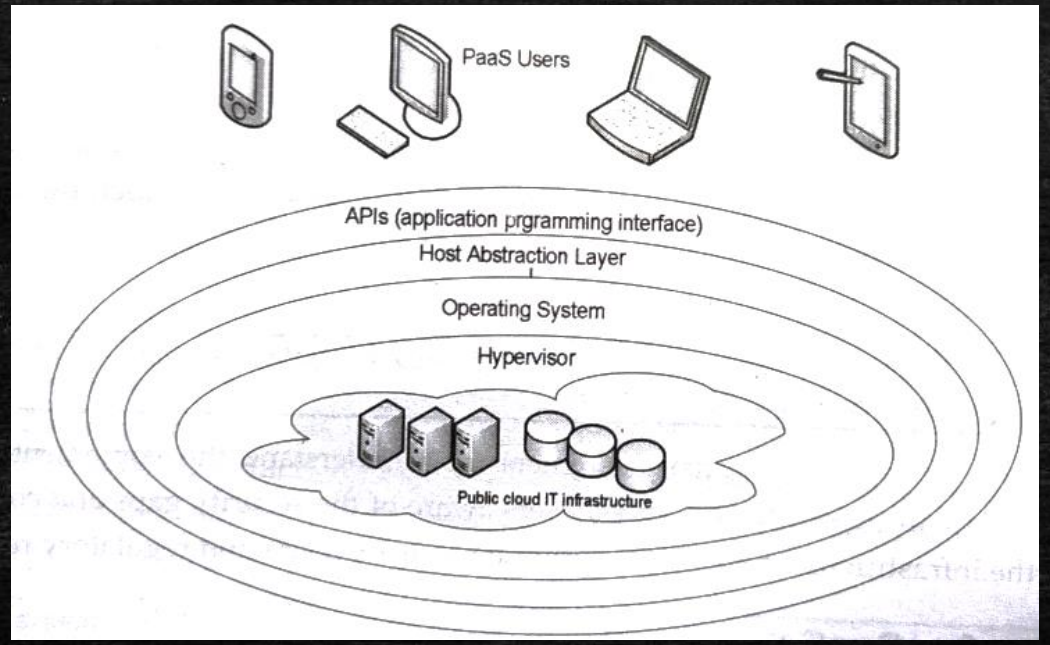
- This is partly to keep the information away from hackers who might then exploit the data to intrude into hosts .
- SaaS access hides the operating system from the user .
- The following are some ways to get assurance of the degree of security implemented by the SaaS provider :
  1. Customers can ask for detailed security status after signing a Non - Disclosure Agreement (NDA) with the provider .
  2. Customers can ask if the provider has security assessment report such as SAS 70 or SysTrust report .
  3. Customers can also ask for security certifications such as ISO 27002 .
- However , SaaS providers are not obligated to give customers details of the environment but will give a high - level SLA for the service availability or for the type of data backups and disaster recovery .

Host Security for PaaS

- The access , control and amount of information customers can get for servers in a PaaS environment is similar to that for SaaS .
- Since PaaS provides an environment to develop products , customers do have access to libraries and kernel - level parameters .
- However since the server is shared by other developers , customers don't have root or administrator - level privileges .
- Like SaaS , PaaS access also hides the operating system from the user . However , in case of PaaS , the user at least has the access to the abstraction layer over the OS .

Host Security for PaaS

- The cloud provider gives a number of Application Programming Interfaces (APIs) which in turn are used by the PaaS users to indirectly access the abstraction layer that hides the operating system .
- Figure shows how PaaS users utilize APIs to access the host abstraction layer :



Host Security for IaaS

- Host Security for IaaS In Iaas , users have complete access to the server OS , its resources such as the CPU , memory , network ports , bandwidth and storage , along with root or administrator password .
- Users need to decide the OS modules to be installed and services to be activated on the server .

Precautionary measures

- To protect from attacks , it is important to understand that t virtual hosts in the cloud are accessible to everyone .
- Hence users must implement strategies to limit the access .
- Users must open only one port at a time , as and when required .
- One port to open for Unix virtual hosts is port 22 that is to be used with sFTP (secure FTP) , SSH (Secure Shell) and SCP (Secure Copy) .

Precautionary measures

- The encryption used by SSH provides confidentiality and integrity to data over an unsecured network .
- Another attack surface (attack surface are different points that an unauthorized user can use to extract data illegally from an environment) is the APIs , along with programs based on the APIs .

Precautionary measures

The following are some ways to tighten the host - level security in an IaaS cloud :

- Each IaaS provider offers the OS a user can install . However , users should create their own OS image to be installed on virtual servers . This protects the integrity of users OS image .
- Every time a user installs an OS on a virtual host , it is important to customize the hosts to run services required by the application on the host . In this way , the users will be able to decrease the attack surface and the number of patch updates needed to install on the host.

Precautionary measures

- Block ports that are not used such as FTP (ports 20 and 21) , telnet (port 23) and NetBIOS (port 139) , SMTP (port 25) . According to Internet Security Systems (ISS) , Port 139 is the single most dangerous port on the Internet . All file and printer sharing on a Windows machine runs over this port . About 10 % of all users on the Internet leave their hard disks exposed on this port . This is the first port hackers want to connect to , and the port that firewalls block .
- Install host - based IPS and IDS services to monitor and analyze the OS and log files. It records the object attributes (such as modification dates , size and permissions) and creates a check - sum database for later comparison . Examples are tripwire , OSSEC (Open Source Security) and Verisys .

Precautionary measures

- Enable event logging for all security and user activities to a dedicated log server . Setup automated alerts for malicious events . Review log files regularly for security breaches .
- Protect the encryption keys . Keep the keys separate from the cloud where the data is stored the service or data processing requires keys , users need to co - locate them . After the processing is over , it is best to remove the keys from the cloud .
- Users are required to type passwords for sudo access to gain root - level rights for Unix hosts .
- Enforce strong passwords for users .

Precautionary measures

- Several vendors have products for cloud host and data security .
- Trend MicroTM has a product called SecureCloudTM that encrypts and controls data in public and private cloud environments with a simple , policy - based key management .
- It lets users to manage how and where data is accessed . Another product Deep Security (again from Trend MicroTM) provides security for virtual hosts in a private or public cloud .

Precautionary measures

- It combines intrusion detection and prevention , firewall , integrity monitoring , log inspection and agent - less anti - malware capabilities in a single , centrally - managed solution .
- Deep Security also checks for compliance with several standards and regulations such as PCI DSS , FISMA and HIPAA .
- It has strong data encryption for confidentially and protects hosts from Cross - Site Scripting (CSS) attacks , SQL injection and other vulnerabilities .

Data Security in the Cloud

Data Security in the Cloud

- Challenges with Cloud Data
- Challenges with Data Security
- Data Confidentiality and Encryption
- Data Availability
- Data Integrity
- Cloud Data Management Interface
- Cloud Storage Gateways (CSGs)
- Cloud Firewall
- Virtual Firewall

Data stored in cloud , faces the following crucial threats

Data Availability

- A software or hardware fault or data integrity problem in one part of the infrastructure or data storage unit impacts not only that part of the database but also the entire environment .
- Hence , data availability and integrity are critical for the cloud to function .

Data Performance

- Data is located at various datacenters owned by the cloud provider .
- Data far from the users , has higher distance - induced latency , and has low performance with synchronous writes , mirroring , and parallel read and write operations .
- To resolve these issues providers must configure caching techniques such as storage in memory and pre - emptive read ahead .

Price

- Price for storage space and bandwidth to access the data must be low.

Flexibility

- In a multi - tenant cloud , some tenant applications or activity causes high that impacts other user groups , unless storage access speed is adjusted in real time to meet load requirements .

Underlying Complexity

- The underlying storage hardware can be heterogeneous , but it must be presented as a simple storage device and as a virtual storage pool to the end user.

Data Security

- The data must be encrypted (while at rest and in - motion) and kept safe with a highly - monitored and regulated access.

Data Integrity

- With ease of access by varied user types , it is critical to manage data integrity.
- It is important for the cloud provider to understand the challenges and build in measures to resolve these issues because of all the data - related problems ..

Challenges with Cloud Data

- In this section , we will discuss data - related challenges in the cloud and how to implement effective mitigation measures.

Challenges with Data Redundancy

- Concurrent data access by multiple customers at all times and due to a mix of hardware types , complicate setting up data protection in any cloud.
- In any case , the copies of data must be stored at various locations and replicated in synchronous (for data sets that are geographically closer) or asynchronous modes (for data sets located across the country or in different continents).
- When replicating across datacenters , the system must be aware of the data location , latency , user workload , and activity such as backup , report generation , application testing , etc.

Challenges with Data Redundancy

- To check data redundancy the following requirements must be met :
- Different strategies must be setup to improve replication and data access .
- Load balancing of incoming data requests must be configured , so that users have ready access to data sets that are geographically closest .
- Data consistency must be maintained implicitly over a wide distribution of replicated data sources.
- Each data set must have internal redundancy , which enables the system to rebuild the entire data set even if some components are temporarily damaged , unavailable , powered off , or inaccessible due to connectivity problems .

Challenges with Disaster Recovery

- Disaster Recovery (DR) in cloud computing is one of the most vital selection criteria when evaluating cloud providers .
- On one hand , DR with cloud computing has several benefits such as cost effectiveness , ease of implementation , scalability , and quick provisioning ; on the other hand , there are numerous issues with cloud - based DR , which are as follows:

Challenges with Disaster Recovery

- Initial Data Copy for Existing Data - For large sets (TBs or many GBs) , it is not possible to make the first data copy over the Wide Area Network (WAN) by the cloud consumer to the cloud provider . Hence , a manual process , such as copying data to tape or hard disk and shipping the device to the cloud provider datacenter , takes time .
- Limited or No Support for Some Operating Systems - Most public cloud DR providers support common operating environments such as MS windows or Linux . There is no support for older , non - Web - based , or less common operating systems such as SolarisTM , HPUX , or AIX.

Challenges with Disaster Recovery

- Insufficient Bandwidth - Most DR providers prefer to create backup with incremental updates instead of taking a full copy .
- Financial Considerations - It makes financial sense for small and mid - sized organizations that have less data to use cloud for DR . However , for organizations that have vast amounts of data , a captive or owned DR site is more cost effective .
- Supplier Issues - Some cloud providers do not take the effort and time to understand the customer - specific needs . They , therefore , cannot justifiably meet all the DR requirements of the customer .

Challenges with Data Backup

- There are several problems related to backing up of cloud data . Following are some of them:
- If you download cloud data to your in - house hard disk or tape , you need to pay for the bandwidth.
- You need a safe place to store the data and frequently check the media integrity of the backup device.

Challenges with Data Backup

- If you keep the backup data in the cloud , you need to harden the security around it to protect it from hackers and malware attacks.
- Data recovery to a cloud - based service site is tough , slow , and prone to transfer interruptions . This is more pronounced if you need to upload a large amount of data to the cloud over a WAN connection.

Challenges with Data Replication

- Data replication is the process of creating copies of user data and application to use in case the data at the primary service site is corrupted , deleted , or unavailable . The problem with replication is that the location of the data copies is dynamic.
- There are two types of replication , each having its own issue when resident in the cloud:

Synchronous Replication

- In this type of replication , replicated copies are always in - sync with the primary site .
- This is used to replicate within distances of 100 kms , where latency is not expected to impact performance .
- This type of replication is not preferred in the cloud , because data is copied over the WAN , and its performance can impact many customers .

Asynchronous Replication

- In this type of replication , the replicated data lags behind the primary data by a time period of 10 minutes to a few hours .
- This is common in the cloud , but impacts performance .
- It is inconvenient and difficult to freeze a database , even momentarily , to get a snapshot .

Challenges with Data Residency or Location

- In the cloud , the location of data can pose a compliance or legal problem .
- For your data , you need to know which legal requirements you must comply with . Certain governments restrict the access of data according to the local or country laws .
- For certain data types , you must keep the data within the region or the country .

Challenges with Data Reliability

- Service reliability in the cloud is a concern because of several reasons . Some of them are the following:
- Heterogeneous hardware and software components
- Connectivity over multi - vendor WAN
- Massive user base sharing the same resource pool.
- Ease of access for users

Challenges with Data Fragmentation

- With numerous users simultaneously working on different datasets in the cloud , the user data is split or fragmented into many pieces and stored in various storage locations .
- The spread of data and overhead of keeping tracks of where different parts of a file are located , leads to inefficiency and degrades read - write performance .
- The provider must adopt comprehensive data - management techniques to reduce user - data fragmentation .

Challenges with Data Integration

- Various factors lead to challenges in cloud data integration , such as the following :
- Content Distribution - Contents of a file reside in different datacenters and various storage subsystems in the same datacenter .
- Exchange of Data - The cloud data interacts with applications residing on other public or private clouds . This exchange of data between cloud applications presents the challenge of having a compatible data format and application interfaces .

Challenges with Data Integration

- Speed of Change - There are innumerable changes per second and keeping track of the data poses a tough challenge for integration.
- Distributed Control - The control over data is shared between the cloud provider and the consumer . This increases the integration challenges .
- Connectivity - Cloud data can be accessed only when the user and the services are online . The integration and work done require bandwidth , which in turn depends on the amount of transaction and work - at - hand.

Challenges with Data Transformation

- In the cloud , various applications may need to use the same data .
- The data format needs to be converted to a format that can be used by other cloud applications .
- This is data transformation an allows use of data by several cloud applications .
- This creates challenges such as the following :

Challenges with Data Transformation

- Run - time Issues - There are several run - time environments in the cloud , and the new transformed data may not be compatible with many environments .
- Redundancy Issues - Data transformation creates multiple copies . Keeping track of location and changes of data in the various sets are a challenge .
- Implementation Issues – Data transformation can be expensive. To make it affordable and convenient, the transformation and tracking of various sets must be automated.

Challenges with Data Migration

- After you decide to rollout a cloud service within your organization , you need to migrate some use login , profile details , user data , and corporate information to the cloud .
- Cloud providers must have templates and procedures to conveniently migrate in - house data to public clouds .
- However , you must be aware of inherent challenges during and after migration , which are as follows:

Liability Concerns

- Cloud providers have a maximum data value for damage claims in the SLA .
- This value may be much lesser than the data value efforts needed to fix data loss or integrity problems .

Compliance Concerns

- The cloud provider must comply with various regulatory and legal requirements , such as the Federal Information Security Management Act (FISMA) , the Health Insurance Portability and Accountability Act (HIPAA) , and the International Organization for Standardization (ISO) , mandated by your business vertical for data protection and privacy .

Connectivity Concerns

- There can be several faults in the WAN links between the consumer and the provider .
- It is supported by various connectivity providers and is outside the control of the consumer or the provider .

Challenges with Data Security

A. Security Risks

- Due to inherent multi - tenancy and ease of access within a cloud , the data subjected to various security risks , which continues to be a serious concern.
- The major problems are as follows:

A. Security Risks

Snooping - The access each tenant should be limited to his / her own data . A tenant in the cloud should not gain access to another tenant's data . Any mechanism to connect to another tenant's data , such as mounts , shares , and symbolic links , should be limited to their own data set .

Unauthorized Discovery - Data should be invisible to all tenants except the owner.

Spoofing - Authentication mechanisms must be implemented to make sure that no cloud tenant can assume the identity of another tenant .

A. Security Risks

- Accidental or Malicious Deletion - No user (except the data owner) should be able to delete the data belonging to another tenant .
- Denial - of - service Attacks - Other cloud users should not be able to launch denial of service attacks on the shared storage volumes of another customer's data . Normal or abnormal application errors of one user should not cause an I / O storm on the shared volume of another customer's storage .

B. Quality of Service

- The second concern , after security , is quality of service . Apprehensions about performance , long response time , and WAN - induced latency , inhibit many potential customers from readily accepting cloud services .
- The cloud provider must be able to ensure that response time and performance do not pose any impediment to cloud adoption

C. Data Availability

- The third concern , after security and quality of service , is data availability .
- After a customer starts using cloud services and data , there are chances of unexpected downtime .
- There have been several outages at cloud providers despite their redundancy and replication .
- The most important lesson learnt from the history of outages at the world's leading datacenters is that there is no single - server datacenter or Business Continuity Planning (BCP) process that guarantees a 100 % uptime .
- As a provider , if you expect to offer 100 % availability of your cloud services , you can have problems maintaining the SLA with your users

Data Confidentiality & Encryption

- Data confidentiality in the cloud is a way to protect data or messages from being understood or by unintended users or tenants of the cloud .
- A common way to achieve data confidentiality is to encrypt the data . Even if the unauthorized party accesses the data , he or she cannot use it .
- Clond data is encrypted with an algorithm and a key . The encrypted data is called ' ciphertext .
- There are two phases in the process , which are as follows :

Data Confidentiality & Encryption

- In the first phase , a mathematical function is used to convert the plain text to encrypted cipher .
- This is the simpler of the two phases , but the mathematical function must be complex and sound enough to give a high degree of protection .
- The encryption should protect against those who may access the cipher text and try to figure out a pattern and understand it .

Data Confidentiality & Encryption

- The second phase is to enable the authorized recipients to decipher the ciphertext with ease .
- There are two common ways to encrypt data . They are as follows :
- Asymmetric Encryption - In asymmetric encryption , different keys are used for encrypting and decrypting , such as a public and a private key.
- Symmetric Encryption - This is an old and tested technique , which can be used for at - rest and in - transit cloud data . It uses a shared secret key to encrypt as well as decrypt data.

Key Protection

- The shared secret key can be a string of random letters , numbers , or a simple word .
- It is applied to the text to encrypt the content in a particular way .
- For example , it can be used to shift each alphabet by a number of places in the alphabet sequence .
- As long as the sender and the recipient are both aware of the key , they can quickly encrypt and decrypt documents and messages exchanged between them .

Encryption Standards

- Many cloud providers use encryption standards , such as Advanced Encryption Standards (AES) and 3 - Data Encryption Standards (3DES) , to ensure that data protection is the highest priority in rendering cloud services .
- There are several algorithms that can be used for cloud data encryption such as the following

RSA Algorithm

- This was developed in 1977 by three mathematicians , namely Ron Rivest , Adi Shamir , and Len Adleman , and named after the three inventors .
- The algorithm selects two large prime numbers and uses their product to form the required keys to encrypt the data . It is widely used , especially for digital signatures .

DES / 3DES

- The Data Encryption Standard (DES) was developed by the US government in 1977.
- The new version 3DES encrypts the data three times , using a different , unique key at least in one of the three passes .

IDEA

- International Data Encryption Algorithm (IDEA) was developed in the early 1990s by Dr. X. Lai and Prof. J. Massey in Switzerland , initially to replace the DES algorithm .
- It uses the same secret key for encryption and decryption .
- It uses a 128 - bit key .
- It is fast and can be used for cloud data .
- It operates on 64 - bit blocks at a time .

Blowfish

- Blowfish is another symmetric block - cipher algorithm (like DES and IDEA wild developed by Bruce Schneier in 1993 as a free algorithm .
- It is designed to use keys of length from 32 to 448 bits .
- It is a strong and fast algorithm and therefore suitable for use in the cloud .

Key Length

- The keys are usually 128 bits , 196 bits , or 256 bits .
- The longer the key , the more complicated it is to derive the key by intercepting a series of encrypted data .
- You also need to ensure that the keys are rigorously protected and well - managed .

Example

- Let us review a simple example :
- If you lock all the doors of your home , a single key should not be able to open all the locks at all entrances . Ideally , you need a unique key for each door .
- Similarly , different parts of a cloud data must be encrypted using different keys .
- Just as you trust and give your house keys to a few people , you need to make sure only a small set of trusted users have your data encryption keys .

Backup Data

- Besides encrypting the cloud data , there are other things that the user needs to be concerned about The backup data (either on online disks or on tapes) must be protected and kept in a secure location.
- Furthermore , you need to make sure that the cloud provider encrypts the backup copies too .
- Another issue with encryption is latency . Encryption and decryption slow down applications However , there has been progress in technologies that enable users to work directly with encrypted data .
- In other words , after a user encrypts cloud data , he / she can process and use the encrypted version without having to decrypt it .

Application Architecture for Cloud

Cloud Application Requirements

- Without a documented design and plan , cloud developers will fail to capitalize on the advantages of cloud over traditional environments and on cloud practices and patterns .
- The new applications must be able to coexist with and use other cloud services such as a cloud - based authentication , security and replication .
- While working with cloud applications , requirements and architecture must be the first two documents to be written and reviewed .
- There are two types of requirements : functional and non functional .

Cloud Application Requirements

- Functional requirements list the purpose and objectives of the application .
- Non functional requirements include performance , response time , built - in security , replication , ease - of use , productivity , agility , backups , business continuity , scalability and modularity .
- These requirements are shown in the following Figure 1:

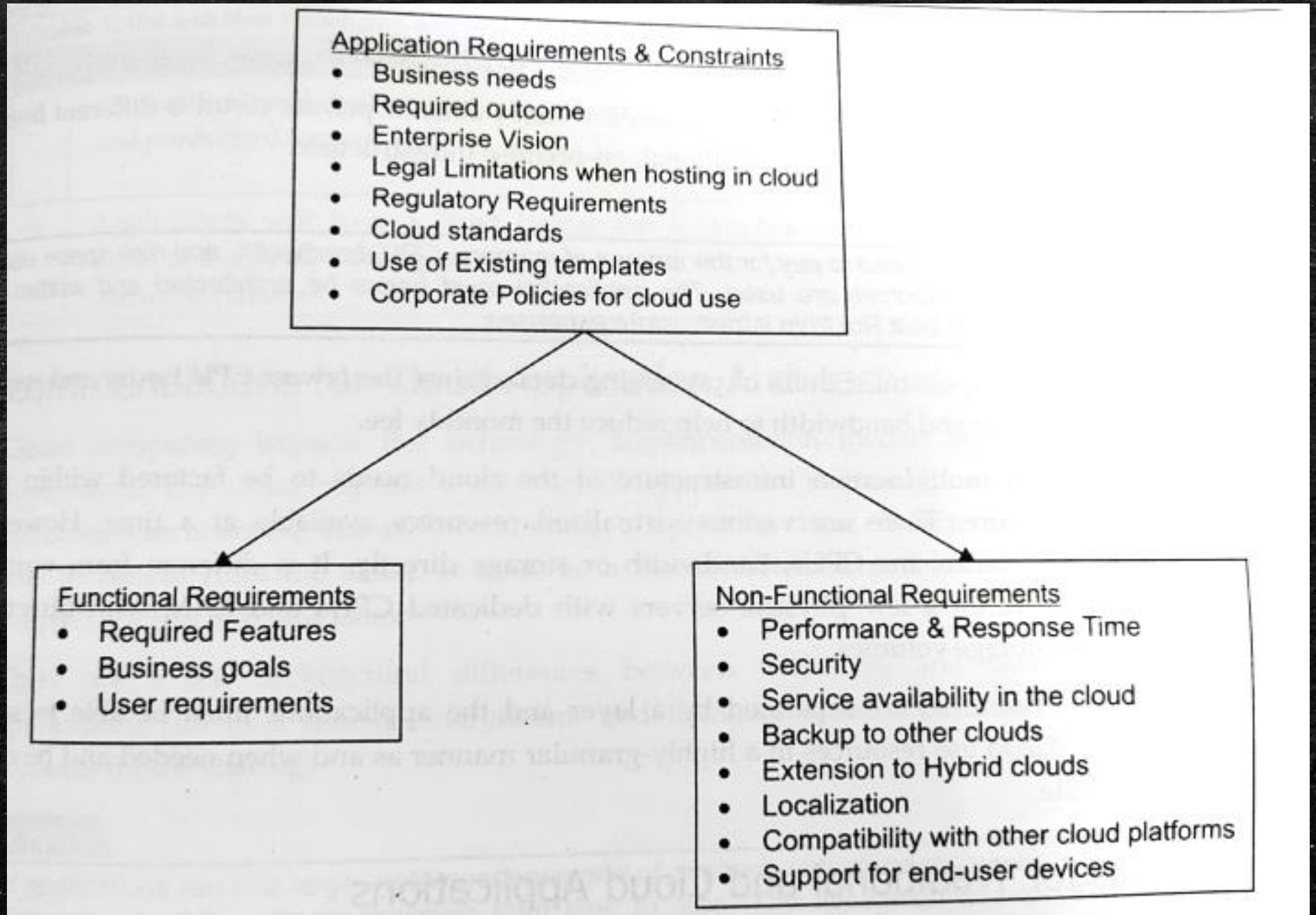


Figure 1: Cloud Application Requirements

Google Classroom code for "Cloud Computing"

- Join the Google Classroom by Using following Code:

2t6xpa5

Thank You!!!Any Query?

asktoshivsir@gmail.com

Shivkumar Chandey

(+91 9987389441)

Scan QR Code to connect on LinkedIn