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 IV Syllabus

Unit IV	Risks, Consequences, and Costs for Cloud Computing AAA Administration for Clouds Regulatory and Compliance Requirements for Clouds Security as A Service

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

Risks, Consequences, and Costs for Cloud Computing

Risks, Consequences, and Costs for Cloud Computing

- Introducing Risks in Cloud Computing
- Risk Assessment and Management
- Risk of Vendor Lock - in
- Risk of Loss of Control
- Risk of Not Meeting Regulatory Compliances
- Risk of Resource Scarcity or Poor Provisioning
- Risk in a Multi - Tenant Environment
- Risk of Failure
- Risk of Failure of Supply Chain
- Risk of Inadequate SLA

Risks, Consequences, and Costs for Cloud Computing

- Risks of Malware and Internet Attacks .
- Risk of Management of Cloud Resources
- Risk of Network Outages
- Risks in the Physical Infrastructure
- Legal Risk Due to Legislation
- Risks with Software and Application Licensing
- Security and Compliance Requirements in a Public
- Cloud Calculating Total Cost of Ownership (TCO) for Cloud Computing

Risks, Consequences, and Costs for Cloud Computing

- Direct and Indirect Cloud Costs
- Costs Allocations in a Cloud
- Chargeback Models for Allocation of Direct and Indirect Cost
- Chargeback Methodology
- Billable Items
- Maintaining Strategic Flexibility in a Cloud

Cloud Computing Risks & Issues by Gartner

- Cloud computing is fraught with security risks, according to analyst firm Gartner. Smart customers will ask tough questions, and consider getting a security assessment from a neutral third party before committing to a cloud vendor.
- Here are seven of the specific security issues Gartner says customers should raise with vendors before selecting a cloud vendor.

1. Privileged user access

- Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. "Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access," Gartner says.

2. Regulatory compliance

- Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions," according to Gartner.

3. Data location

- When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises.

4. Data segregation

- Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says.

5. Recovery

- Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

6. Investigative support

- Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible."

7. Long-term viability

- Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application," Gartner says.

Risk Assessment and Management

- The first thing that you must do with a public cloud provider is a thorough risk analysis .
- The objective is to identify the existing and potential vulnerabilities .

Risk management involves the following tasks

- Risk identification
- Risk analysis and evaluation .
- Selection of counter measures
- Deployment of suitable counter measures
- Continuous monitoring to assess effectiveness of the solution .

Risk of Vendor Lock-in

- The vendor lock-in problem in cloud computing is the situation where customers are dependent (i.e. locked-in) on a single cloud provider technology implementation and cannot easily move in the future to a different vendor without substantial costs, legal constraints, or technical incompatibilities

Risk of Loss of Control

- Loss of control occurs when clients lose their control over their own resources in the hand of service provider.
- As lack of authentication and access control placed by providers, loss of control contributes to greater security concern.

Risk of Not Meeting Regulatory Compliances

- Cloud providers must certify their platforms as to whether or not they meet compliance regulations .
- The audit certification would be an assurance to consumers , who must in - turn ask the provider for a copy of the certifications for their own corporate audits .
- You must make sure that the providers get the certifications for acceptable configurations .

Risk of Not Meeting Regulatory Compliances

- For example , if an open - source DR solution or virtualization is used , it may not have the availability and protection , required for compliance .
- If the data is located outside the country , it may fail compliance requirements for banks and financial institutions having retail account clients .

Risk of Resource Scarcity or Poor Provisioning

- There could be several problems related to infrastructure resources in a public cloud .
- When multiple users are competing for a fixed set of server , bandwidth and storage resources , it could lead to a situation where supply becomes inadequate.
- The available resource pool could also be improperly provisioned . The cloud provider may have deployed lesser amount of resources .

Risk of Resource Scarcity or Poor Provisioning

- The dynamic resource scheduling policies are supposed to be provided with resources to meet user lead requirements in real - time , but the algorithm may not function properly or may erroneously allocate the same logical resource to multiple users , which is meant for a single user .
- There could also be some hardware failure leading to non- availability of resources in the pool .

Risk in a Multi - Tenant Environment

- In multi - tenancy , multiple users access the same physical or logical resource .
- In this environment , a tenant can also access , copy , alter , or delete the data of a co - tenant .
- Such unsecure access to data could be disastrous for the targeted cloud consumer .
- It will also hurt the reputation of the cloud provider and create loss of confidence amongst other consumers .
- Any instance of un - authorized access will lead to perilous defamation for the cloud provider , which in - turn will impact all cloud users .

Risk of Failure

- A cloud provider may go out of business .
- This could be due to competitive technology , inability to keep up with technical innovations or cash - flow issues .
- This will lead to low quality of service from the provider before they give in or stop services .
- All this will impact the consumers , who in - turn will not be able to meet the demands of their user community .
- The vicious chain of inadequate services can adversely impact many businesses

Risk of Failure of Supply Chain

- Cloud providers use service partners for various aspects such as network bandwidth , service monitoring , physical security , etc.
- The provider will have to abide by the conditions of the third party vendors .
- Any failure on part of the vendors or partners will impact the provider , consumer and end - users .
- There could be a service outage , data loss , corruption or unacceptable performance .

Risk of Inadequate SLA

- Service Level Agreements (SLAS) dictate the expected service availability , performance and security .
- SLAS must be able to meet user and compliance requirements . The document helps to establish responsibility areas and settle disputes .
- An inadequate SLA may turn out to be inadequate for the user load management or irrelevant for compliances by business verticals .
- In some cases , service provider may be acquired by another provider .
- In such cases , inadequate SLAs may need to be replaced , leading to another discussion and risk of non - compliance .

Risks of Malware and Internet Attacks

- Anyone can open an account in a cloud as the level of screening is minimal .
- This means that malicious users can also create accounts and launch attacks .
- These attacks can be directed to disable the entire cloud service or disable a particular customer site within the cloud .
- Two common forms of Internet attacks are :

Distributed Denial of Service (DDoS) Attacks

- This is an attempt by hackers to disable certain services or a network for users .
- It is an effort by one or more hackers to temporarily or indefinitely interrupt services by server overload .
- One of the most commonly used processes is to saturate the target network or server with lots of external communication requests , such that it cannot respond to legitimate user traffic , or respond so slowly that it becomes practically useless

Economic Denial of Sustainability (EDoS) Attacks

- These are attacks that use up cloud resources , and hence drive up costs for other cloud users to levels that they cannot pay for the resources anymore .

Risk of Management of Cloud Resources

- There are many ways that the cloud resources can be abused or mismanaged , such as : The user authentication process may be flawed .
- It may allow unidentified users to access resources that belong to another cloud user .
- The network bandwidth can be choked or consumed by viruses .
- The server and storage resources may be locked by one user for no productive use .

Risk of Network Outages

- Network outage is one of the key cloud risks .
- During an outage , the latest data changes cannot be accessed from other sites , as the updates may not have been replicated .
- It results in hard sales losses for those who use the cloud for e - commerce or customer services .
- The BCP site will usually take time to start , may have problems initiating , or fail to come online .
- During an outage , there may not be enough coordination to redirect requests to another datacenter or work with other cloud providers .

Risks in the Physical Infrastructure

- There can be several security risks in the physical infrastructure of the datacenter and IT assets .
- Some of these physical risks are :

Risks in the Physical Infrastructure

- Theft of equipment that belongs to the customers and is located at the datacenter of the cloud or hosting provider .
- The physical scanning of visitors may be flawed and someone can enter the datacenter with items that can damage the IT hardware .
- Malicious employees and insiders , who have privileged access , can damage the equipment in the datacenter .

Risks in the Physical Infrastructure

- There could be power outages and problems in the power backup mechanisms (diesel generator , UPS , etc.)
- The Precision Air Conditioning (PAC) is critical and any failures will cause a rise in the surrounding temperature and impact the sensitive IT equipment in the datacenter

Legal Risk Due to Legislation

- Data for different business verticals (healthcare , financial , etc.) resides in a cloud provider's datacenter .
- The data is subject to several regulations , which relates to data privacy , access , location , backup and DR mechanism .
- The cloud provider must comply with the regulations in your vertical . If not , you will have to look for another provider .
- The compliance requirement must be clearly stated in the SLA document .
- You also need to get and keep certification copies that prove that the cloud provider complies with the requirements .

Risks with Software and Application Licensing

- A key problem in the cloud is to control the use of licenses for applications , development tools , middleware , database , OS , etc. Traditionally , there are three categories of licenses :

Licenses based on User Count

- User count licenses are based on the number of users allowed to access a service or application .
- For example , you may have a license for 25 concurrent users and 400 named users.
- This means a maximum of 400 user accounts can be created for the application ; however , only a maximum of 25 could be logged in at any time .

Licenses based on Devices

- In this case , the application is tied to resources in the server .
- For example , Oracle license could be for a server with 8 cores .
- The server could have a single 8 - core CPU or have two 4 - core CPUs or any combination thereof , as long as the number of cores is 8 or less .
- The server could be used by any number of users .

Enterprise - wide License

- In this case , there could be any number of users or devices .
- As long as the users and devices are owned or leased for use for the enterprise , it is licensed.

Security and Compliance Requirements in a Public Cloud

- There are several risks associated to data security and privacy in the cloud due to inherent multi tenancy and ease of accessing services .
- In this section , we provide a checklist to cross - examine your service provider on inherent hazards of keeping your data at a shared location and about risk mitigation measures:

Security and Compliance Requirements in a Public Cloud

- Privileged User Access
- Regulatory Compliance
- Investigative Support
- Data Locations
- Data Separation
- Service Recovery
- Long-term business sustaninability

Calculating Total Cost of Ownership (TCO) for Cloud Computing

- The TCO for a product or service refers to the cost calculation that adds the direct and indirect expenditure over an extended time frame of 1 to 10 years .
- It helps to arrive at a final cost estimate that includes all cloud - related expenses by an organization .
- The TCO is helpful in finding the incremental expenses and RoI , in case the consumer organization decides to increase its use of certain cloud services .
- There are certain guidelines for providing a useful insight for TCO analysis :

Identify all Cloud Cost Components

- These include bandwidth , reserved and on - demand server and storage resources, backup , use of storage at DR sites , permanent IP addresses for applications , etc.
- For example , if you have reserved permanent IP addresses but are not using those, there would be a charge for not using it .

Identify the Combination of Cloud Services

- Some applications process large amounts of data and use lots of storage space.
- Other applications may use more computing services.
- It is important to list the utilization category for each expense.

Identify the Variations in Utilization

- If the utilization levels change a lot , the cost bracket per unit resource will vary, which will affect TCO.
- You must understand the way resources are used and include that in the TCO calculation .

AAA Administration for Clouds

AAA (Authentication, Authorization, Accounting)

- AAA is a standard-based framework used to control who is permitted to use network resources (through authentication), what they are authorized to do (through authorization), and capture the actions performed while accessing the network (through accounting).

Authentication

- Validating a user's identity to permit or reject a login is called authentication .
- It is as if the system requires proof that the user is who he / she claims to be . This kind of access can be required for a system (a router , switch , storage system , server , etc.) , an application , or a database .
- Authentication requires an identifier and its corresponding credential . An identifier could be a login name or a login ID .

Authentication

- The credential could be a password , a digital certificate , a calling or called phone number , or a one - time token .
- The AAA server compares the entered details with a stored database .
- If the identifier and credentials match , the user is allowed access to the application or the system . If they do not match , the user is denied access

Authorization

- Authorization permits a user to do certain activities and denies other activities . After accessing a system or application , a user issues a command .
- The AAA server decides whether the user should be allowed or denied execution of the command .

Authorization

- Compared to authentication , authorization is much more complicated and with several steps .
- After successful authentication , the AAA or access server provides several user - related information , such as the following :
  - Data the user can view
  - Data the user can edit
  - Commands the user can run
  - Applications the user can start
  - Level of access within each application or system

Accounting of Cloud Resource Utilization

- Accounting does not allow or deny anything . It just keeps a log of resource consumption such as the following :
  - Identity of the user
  - Amount of resource used
  - Start and end time of use
  - Amount of data transferred
  - Length of connection
  - Purpose of using the resource
  - Nature of service delivered

Following are the two types of accounting reports

- Real Time Accounting Information:
  - This is delivered concurrently with resource consumption .
  - This is useful for cloud users to track usage and predict the bill , expected at the end of the payment cycle .
- Batch Accounting Information :
  - This information is saved and delivered at a later time .
  - Such data is useful for cloud service providers for billing at the end of each payment cycle .
  - The data is also used for studying utilization trends and capacity planning .

Single sign-on (SSO)

- Single sign-on (SSO) is an important cloud security technology that reduces all user application logins to one login for greater security and convenience.

Regulatory and Compliance Requirements for Clouds

Regulations for Clouds

- Several regulations , such as Health Insurance Portability and Accountability Act (HIPAA) , Sarbanes Oxley Act (SOX) , and Payment Card Industry - Data Security Standard (PCI - DSS) , are asking organizations to re - evaluate their data protection procedures and schemes .
- Moving to a public cloud and giving a large part of the control to the cloud service provider will add several unknown risks to their ability to comply with these regulations .
- In survey results published by IDG News Service in October 2010 , nearly half the enterprises using cloud providers admitted that their cloud data would not pass or would have great difficulty in passing a compliance audit .

What to ask?

- In order to proactively protect data , an organization must confidently answer the following questions :
- What data or information is stored on each system ?
- Where is the data and system physically located ?
- Which corporate or partner users have access to the information ?
- What is the degree of access for each user ?
- What is the business or technical need for access given to each user ?

GLBA Act

- The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

How to Evaluate Compliance within a Cloud

- Adoption of cloud computing gets a quick approval from business heads because of cost and convenience of use , but audit and compliance teams have been averse to proposing cloud .
- This could be due to a variety of reasons .
- They may question the effectiveness of security components , they may have concerns over inadequate levels of controls and privacy of data , and they may not be sure if the provider will go to lengths to comply with regulatory requirements .

How to Evaluate Compliance within a Cloud

- On the other hand , providers are abundantly aware that business houses , although convinced of the competitive advantages of the cloud , will stay away because of non - compliance .
- Hence , public cloud providers have taken great strides to meet compliance and put the compliance concerns to rest .
- As a cloud consumer , you need to audit the provider and ensure compliance for yourself .
- Here are five steps for consumer organizations to ensure their comfort with compliance in the cloud .

Understand Compliance Requirements and Work with Your Cloud Service Provider

- Compliance requirements are different for different business verticals , such as healthcare , insurance , banking , etc.
- You would expect the cloud provider to know and implement the compliance for all verticals , but consumer organizations have a far deeper understanding of their vertical requirements , the mandatory security controls , and technologies that can be used to meet the requirements

Select a Cloud Provider with a History of Transparency in Security and Policies

- The cloud provider must display flexibility to incorporate controls and security in the environment you use .
- Banking and finance verticals have strict guidelines for data continuity , data retention and classification , confidentiality , data integrity , backups , and service availability .
- Your provider must incorporate these policies . Different industries have different policies for :

Select a Cloud Provider with a History of Transparency in Security and Policies

- Backup Retention Periods
- Encryption for Data at Rest and In Transit
- Data Replication and Business Continuity Plans
- Data Classification Policies
- Data Integrity for Online and Offline Data
- User Identity and Access Management and Authentication Procedures

Separate Your and Your Cloud Provider's Responsibilities

- The responsibilities of both the parties differ depending on the cloud services you use .
- For example , for laas the cloud provider is accountable for hardware , facilities , hypervisor , hardware redundancy , etc.
- The consumer organization is responsible for applications , user access , data , and host software .

Understand Your Application and Data Requirements

- For example , if you are processing credit card data , many countries will want your environment to comply with PCI - DSS .
- You must work with the cloud provider to comply on this .
- You can also segment your data to separate out the financial data .
- The tight security controls can be limited to the financial information and the rest of the environment will not need such stringent controls .

Know About the Certifications and Compliance of Your Cloud Provider

- Most cloud providers have a compliance program to evaluate and implement controls and policies for meeting compliance .
- For example , cloud providers often adhere to SSAE 16 (formerly SAS70) program, which is usually audited by a third party .
- It provides the reassurance that the controls and policies that have been stated within the provider's compliance program are implemented and practiced .
- This provides a quick path toward completing compliance audits .

Security as a service

There are two kinds of cloud - based security providers

- Leading Security Product Vendors , who are now trying to establish new models and are looking to deliver their products as a service over the cloud . These are traditional anti - virus vendors .
- Emerging Small - Or - Medium Sized Security Vendors , who do not provide any security product , but only deliver security services over the internet for their customer's IT environment . They may use products from other ISVS or ones they have developed internally .

What Can Security - as - a - Service Offer ?

- There are several valuable services provided by vendors who focus on delivering security over the internet :

Cleansing Incoming Email

- This includes filtering spam and cleansing phishing and malware infected content so that they are cleanly delivered to the organization's email server .
- This is done by several security and anti - virus engines running in the cloud .
- The advantage is that the engines are agnostic to the end - point type , OS or processor .
- The client is not burdened with performance . running the anti - virus or cleansing the software and hence , does not suffer from degraded

Filtering Outbound Email

- Cleaning and filtering outgoing email is just as critical as it is for incoming email .
- Policies for content encryption can be implemented by the cloud provider at the email server - level so as to free the user from key management and encryption .
- The cloud based engine will detect and remove viruses from outbound emails .
- Sending spams or virus infected emails are an embarrassment to the sending organization and corrupts the recipient's data .

Web Content Filtering

- Web filtering started in the early 1990's as means to check for URL addresses on firewalls within the premises .
- However , with the proliferation of websites , it quickly became an ineffective technique .

Security as a service

- Security in cloud computing is a major concern.
- Data in cloud should be stored in encrypted form.
- To restrict client from accessing the shared data directly, proxy and brokerage services should be employed.

Security Planning

- Before deploying a particular resource to cloud, one should need to analyze several aspects of the resource such as:
  - Select resource that needs to move to the cloud and analyze its sensitivity to risk.
  - Consider cloud service models such as IaaS, PaaS, and SaaS. These models require customer to be responsible for security at different levels of service.
  - Consider the cloud type to be used such as public, private, community or hybrid.
  - Understand the cloud service provider's system about data storage and its transfer into and out of the cloud.
- The risk in cloud deployment mainly depends upon the service models and cloud types.

Understanding Security of Cloud

- Security Boundaries:
  - A particular service model defines the boundary between the responsibilities of service provider and customer. Cloud Security Alliance (CSA) stack model defines the boundaries between each service model and shows how different functional units relate to each other.

Key Points to CSA Model

- IaaS is the most basic level of service with PaaS and SaaS next two above levels of services.
- Moving upwards, each of the service inherits capabilities and security concerns of the model beneath.
- IaaS provides the infrastructure, PaaS provides platform development environment, and SaaS provides operating environment.
- IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.

Key Points to CSA Model

- This model describes the security boundaries at which cloud service provider's responsibilities end and the customer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system and should be maintained by the customer.
- Although each service model has security mechanism, the security needs also depend upon where these services are located, in private, public, hybrid or community cloud.

Understanding Data Security

- Since all the data is transferred using Internet, data security is of major concern in the cloud. Here are key mechanisms for protecting data.
  - Access Control
  - Auditing
  - Authentication
  - Authorization
- All of the service models should incorporate security mechanism operating in all above-mentioned areas.

Isolated Access to Data

- Since data stored in cloud can be accessed from anywhere, we must have a mechanism to isolate data and protect it from client's direct access.
- Brokered Cloud Storage Access is an approach for isolating storage in the cloud. In this approach, two services are created:
  - A broker with full access to storage but no access to client.
  - A proxy with no access to storage but access to both client and broker.

Encryption

- Encryption helps to protect data from being compromised.
- It protects data that is being transferred as well as data stored in the cloud.
- Although encryption helps to protect data from any unauthorized access, it does not prevent data loss.

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