Chapter 1

Date 14/03/2023
Page

Cloud Computing:

Cloud Computing is a on-demand delivery of IT resources over the internet with pay-as-you-go pricing. Instead of buying, owning & maintaining physical data centers & servers, we can access technology services such as computing power, storage & databases on an as-needed basis from a cloud provider like AWS.

Cloud Computing is a model of computing that enables access to shared pool of computing resources such as servers, storage, applications, & services over the internet.

What is Cloud Computing? Explain 3 deployment models with Example?

The Cloud deployment model identifies the specific type of cloud environment based on the ownership, scale & access as well as the cloud's nature & purposes.

The location of the servers we are utilizing & who controls them are defined by a cloud deployment m

Deployment Models are:

1. Public cloud
2. Private cloud
3. Hybrid cloud
4. Community cloud.
5. Multi-cloud

1 Public cloud:

This is a deployment model where the cloud infrastructure is owned & operated by a 3rd party service provider who offers their services to the public over the internet.

The resources of a public cloud are shared among multiple users & the customers only pay for what they use. and includes 6 advantages of Cloud Computing

Example:

AWS, Microsoft Azure, & Google Cloud platform

2. Private Cloud:

In this deployment model the cloud infrastructure is owned and operated by a single organization. The organization has full control over the resources & can customize the cloud environment to meet their specific needs & is not exposed to the public.

Private Clouds are typically used by large organizations that require a high level of security & compliance.

Example:
IBM cloud private & VMware cloud.

3. Hybrid Cloud:
This is a deployment model that combines both public and private cloud.
In Hybrid Cloud, the organization can use both public and private clouds to meet their specific needs. For example an organization can use a public cloud for their non-sensitive data & a private cloud for their sensitive data.
Example:
IBM and Microsoft Azure.

4. Community Cloud:
In this deployment model the cloud infrastructure is shared among a specific community or industry.
Community Clouds are typically used by Government agencies or Research organizations.
Example:
National Institute of Standards & Technology (NIST) & the European Union Community Cloud.

2. Give 6 Characteristics of Cloud Computing?

1 On-demand Self Service
2 Broad Network Access
3 Multy tenancy & Resource pooling
4 Rapid elasticity & Scalability
5 Measured Service
6 Security & Availability.

1. On-demand self-service:

Cloud Computing enables users to providing computing resources such as servers, storage & network on demand without requiring human interaction with each service provider.

2. Broad Network Access:

Cloud Computing resources are accesible over the internet or a private network, by allowing users to access the resources from anywhere in the world using a variety of devices such as laptop, phone etc.

3 Multi-tenancy & Resource Pooling:

Cloud Computing provides multiple customers using the same physical & virtual resources with security & privacy.

Multiple customers are serviced from the same physical resources.

4. Rapid Elasticity & Scalability:

Cloud computing resources can be quickly scaled up or down to meet changing user demand, often in real-time, without disrupting ongoing bussiness opeations.

5. Measured Service :

Cloud Computing providers measure the usage of their resources, allowing users to pay only for what they use. This can result in significant cost savings for users, as they do not need to invest in expensive hardware & software upfront.

6 Security & Availability :

Cloud Computing providers implement strict security measures to protect their user's data & ensure compliance with regulatory requirements.

Cloud Computing resources are highly available,

CAPEX

OPEX

3. Give 6 Advantages of Cloud Computing:

1 Cost Saving: Trade Capital expense for operational expense.
Cloud computing eliminates the need for organizations to invest in expensive hardware, software & infrastructure upfront. Instead, organizations pay for the resources they use on a pay-as-you-go basis, which can result in significant cost savings over time.

2. Benefit from massive economies of scale:
Prices are reduced as AWS is more efficient due to large scale.

3. Scalability: Stop guessing Capacity.
Cloud Computing resources can be scaled up or down quickly & easily, and scale based on actual measured usage

4. Increased Speed and Flexibility or Agility:
Cloud Computing enables the organizations to experiment with new applications & technologies quickly & easily,

5. Disaster Recovery:
Cloud Computing provides typically offer backup & recovery services, which can help organizations to recover quickly in the event of a disaster or outage.

6 Go Global in minutes: Leverage or control the AWS global infrastructure.

7 Economies of Scale:
Stop spending money on running & maintaining data centers.

4. Explain the problems faced by the traditional IT approach, and how the cloud managed to solve those problems.

Traditional Computing, as a name suggests, is a process of using physical data centers for storing digital assets & running complete networking system for daily operations.

The Traditional It approach is often characterized by the use of on-premises hardware & software, which requires significant upfront capital investment & ongoing maintainance cost. This approach can lead to number of problems, including.

1 Limited Scalability:

Traditional IT systems are often designed to handle a specific amount of traffic or workload, & adding more capacity can be difficult & costly.

2 Costly infrastructure:

Purchasing & maintaining hardware & software can be expensive, especially for small and medium-sized bussinesses that may not have the resources to invest in enterprise-grade equipment.

3 Maintainance & Updates:

Traditional IT systems require regular maintainance & updates to keep them secure & functioning properly.

4 Limited Access:

Traditional IT systems are often tied to a specific location or network, which can limit access for remote workers or employees who need to access data from outside the office.

5 Backup:

Problem solved by the Cloud:

1 Flexibility: Change resource types when needed

2. Cost-Effectiveness: Pay as you go for what you use

3 Scalability: Accomodate larger loads by making hardware stronger or adding additional nodes.

4. High Availability & Fault Tolerance: build across data centers

5 Elasticity:
Ability to scale out & scale in when needed

6 Agility:
Rapidly develop, test & launch software applications

Explain the Types of Cloud Computing with an Example?

There are 3 primary types of Cloud Computing:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

1 Infrastructure as a Service (IaaS):

It provides users with access to virtualized computing resources over the internet, such as Virtual Machines (VMs), storage, networks & OS.

IaaS allows users to create and manage their own IT infrastructure in the cloud, giving them complete control over their computing resources.

IaaS acts as a building blocks for cloud IT with Highest level of flexibility & easy parallel with traditional on-primises IT.

Example:

* Amazon EC2 & Simple Storage Service (S3) on AWS.
* GCP, Azure, Digital Ocean, Linode, Rackspace.

2 Platform as a Service (PaaS):

It provides users with a complete development & deployment environment in the cloud, where they can build, test & deploy applications without worrying about the underlying infrastructure.

PaaS is designed for developers who want to focus on building applications rather than managing the underlying infrastructure.

Example:

* Elastic Beanstalk on AWS.
* Heroku, Google App Engine (GCP), Windows Azure (Mi

3. Software as a Suvice (SaaS):

It provides users with access to software applications over the internet, which are hosted & managed by a third-party provider.

SaaS eliminates the need for users to install, maintain & upgrade software applications on their own devices as the software is accessed over the internet.

Example:

* Many AWS Services Ex: Rekognition for ML.
* Google Apps (Gmail), Dropbox, Zoom
* Salesforce.

6 Explain the Terms 1) AWS Region
2) AWS Availability Zones
3) AWS Data Centers
4) AWS Edge Locations or Points of Presence
in AWS Global infrastructure?

→

1. AWS Region:

Amazon Cloud Computing resources are hosted in multiple locations world-wide. These locations are composed of AWS Regions, Availability Zones & Local Zones.

AWS Regions are separate geographic areas that AWS uses to house its infrastructure. These are distributed around the world so that the customers can choose the region closest to them in order to host their cloud infrastructure there.

The closer our region is to the better, so that we can reduce network latency as much as possible for our end users. AWS currently has over 25 regions globally.

2. AWS Availability Zones:

Availability Zones (AZs) are distinct locations or physically separate data centers within an AWS Region that are designed to be Fault-tolerant.

Each availability zone is isolated from other Availability Zones within the same region, with its own power, cooling & networking infrastructure.

Each region has many Availability Zones usually 3, min is 2 max is 6.

Availability Zones are separated from each other, so that they are isolated from disaster and but they are connected with high bandwidth, ultra-low latency networking.

3 AWS Data Center:

A Data Center is a physical location that stores computing machines & their related hardware equipments. It contains the Computing infrastructure that IT systems require, such as severs, data storage drives, & network equipment.

It is the physical facility that stores any company's digital data, So each data center is designed to be highly secure, reliable & scalable.

4. AWS Edge Locations or Points of Presence:

Edge Locations or Points of Presence (PoPs) are AWS data centers designed to deliver services with low latency and high data transfer rates to end-users by caching the content closure to them.

AWS currently has over 250 Edge Locations globally in 84 cities across 42 countries.

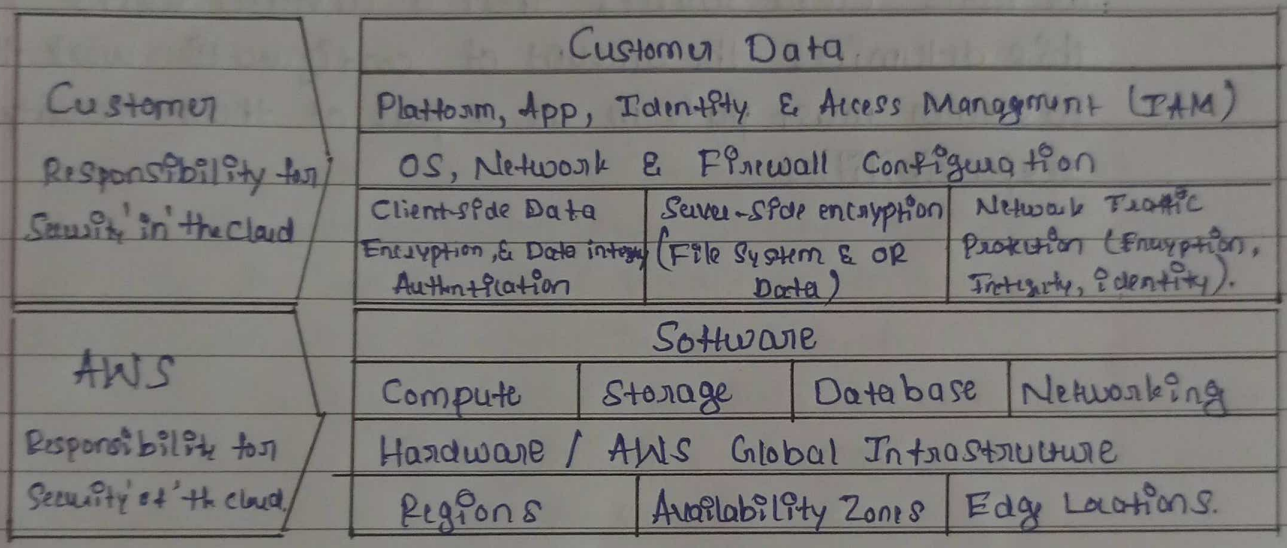
with a Diagram.

Explain the Shared Responsibility Model of Customer & AWS

The AWS shared Responsibility Model is a concept of dividing responsibilities blw AWS & Customers for securing & protecting the IT infrastructure & data that is hosted on AWS Cloud.

AWS's responsibilities are the Security of the Cloud
Customer responsibilities are Security in the Cloud

Following Diagram illustrates the Shared Responsibility Model blw Customer & AWS.



1 AWS Responsibility:

The bottom layer of the model represents AWS's responsibility for securing the cloud infrastructure. This includes securing the physical data centers, networks & hardware as well as providing foundational security suviles such as identity & access management, compliance & patch management.

2. Customer Responsibility:

The Top layer of the model represents the customer's responsibility for securing their data & applications running on AWS.

This includes securing their OS, applications, data & network configurations as well as implementing appropriate security controls to meet their compliance & regulatory requirements.

Customer Responsibilites ~~are~~ will be determined by the AWS cloud Sevices that a customer selects. this determines the amount of configuration work the customer must perform as a part of their security responsibilities.

Chapter 2.

IAM:

AWS Identity and Access Management (IAM) is a global service provided by AWS that enables us to manage access to our AWS resources securely.

IAM allows us to create & manage users, groups & permissions to control who can access our AWS resources and how they can access them.

Moreover; IAM is a Web Service that helps us securely control access to AWS resources. We use IAM to control who is authenticated & authorized to use resources.

1. Explain the IAM Users and Groups with a Diagram

When we create an AWS account, we begin with one sign-in identity that has complete access to all AWS services & resources in the Account.

This identity is called the AWS account root user & is accessed by signing in with the email address & password that we used to create the account.

The best practice is not to use root user for our everyday tasks.

IAM users & groups are fundamental components of the AWS Identity and Access Management (IAM) Service. Users are individual entities in IAM that have their own credentials & can be assigned permissions to access AWS resources, while groups are collection of users who share the same set of permissions.

1 Users:

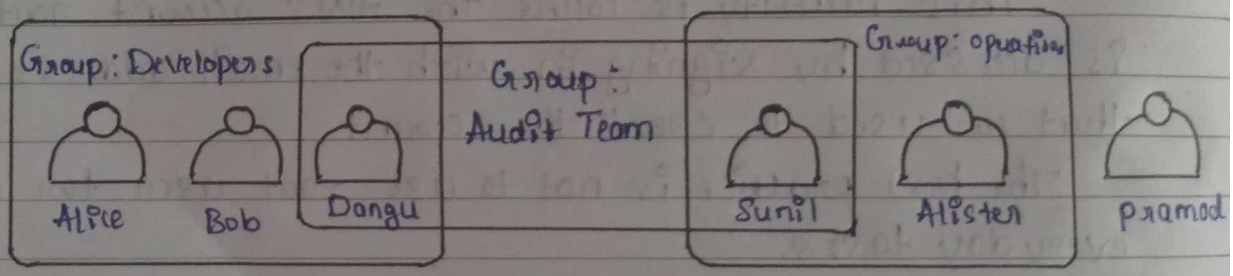
IAM users are created within our AWS account and can be assigned a unique username & password or access keys for programmetic access.

Users can be granted permissions through IAM policies that are attached to the user or the groups to which the user belongs.

2 Groups:

Groups are collection of IAM users that share the same set of permissions.

We can create groups and add users to them, & then assign permissions to the group using IAM policies. When a user is added to the group they inherit the permissions assigned to that group.



with JSON.

8. What are IAM policies, explain the IAM policie Structure

IAM policies are JSON documents that defines the permissions & resources that are allowed or denied for a user or group in AWS IAM.

IAM policies are used to control access to AWS resources & services, & they can be attached to IAM users, groups & roles.

IAM Policy Structure:

```
{
  "version" : "yyyy-mm-dd",
  "Id"      : "s3-Account-Permissions",

  "Statement" : [

    {
      "SId : "1",
      "Effect" : "Allow",

      "Principal" : {
         "AWS" : ["arn:aws:iam :123456789012 :root"]
      },

      "Action" : [
         "s3 : Getobject",
         "s3 : putobject"
       ],

      "Resource" : ["arn : aws : s3 : : : mybucket/*"]

    }
  ]
}
```

Consist of :

1 Version : this is required field that specifies the version of the policy language being used. The value must be in the format of "yyyy-mm-dd"

2. Id : An identifier for the policy → optional

3 Statement :

this is an array of one or more statements that define the permissions being granted or denied. Each statement consisting of the following elements.

a) Sid : An identifier for the statement (optional)

b) Effect : Whether the statement allows or denies the access.

c) Principal : Account / User / Role to which this policy applied to

d) Action : List of Actions this policy allows or denies.

e) Resource : List of Resources to which the actions applied t

f) Condition : Conditions for when this policy in effect (optional).

3. Give the IAM Guidelines & Best practice as an AWS Administrator

As an AWS Administrator, here are some IAM Guidelines & Best practice to help us manage access to AWS resources securely.

1. Use the principle of least privilege:

When creating IAM policies, only grant permissions that are necessary for the user, group or role to perform their intended actions.

2. Don't use the Root account except for AWS account setup
3. Assign users to groups and Assign permissions to groups.
4. Create a Strong password policy
5. Use and enforce the use of Multi Factor Authentication (MFA)
6. Create and use Roles for giving permissions to AWS services
7. Use Access keys for Programmetic Access (CLI/SDK).
8. Never share IAM users & Access keys.
9. Regularly review & update IAM policies.
10. Monitor IAM activity

4. Explain How to Secure AWS accounts & How can users access AWS ?

Securing AWS Accounts is essential to protect our data, applications & infrastructure from potential attacks or unauthorized access. Here are some best practice for securing AWS accounts:

1 Use Strong passwords:

Ensure that all users have strong, unique passwords that are not easy to guess.

2 Enable Multi-factor Authentication (MFA):

MFA adds an additional layer of security to the login process. Basically, any users have access to our account and can possibly change configurations or delete resources in our AWS account.

So MFA => Password we know + Security devile we own.

Main benefits of MFA is that if a password is stolen or hacked, then the account is not compromised.

3. Use IAM Roles & Policies:

AWS IAM allows us to create Role & policies that control access to our resources.

4 Allow all IAM users to change their own passwords.

5 Add password expiration

6 Prevent Password Reuse.

7 Use encryption.

How can Users access AWS:

To access AWS we have 3 options:

1. AWS Managment Console
2. AWS Command Line Interface (CLI)
3. AWS Software Development kits (SDKs)

7

1. AWS Management Console:

This is a web-based interface that allows users to manage AWS resources through a browser.

Access keys are generated through the AWS console & users manages their own access keys.

It provides a simple & easily understandable interface for managing AWS resources.

2. AWS CommandLine Interface: CLI

AWS CLI is a commandline tool that allows users to interact with AWS service using commands in a command prompt or terminal window.

This is a useful option for automating tasks or integrating with scripts.

3 AWS Software Development Kits: SDKs

AWS provides SDKs for various programming languages that enable developers to interact with AWS service programmetically.

This allows users to build custom applications that can integrate with AWS services.

5. Explain Shared responsibility model of the IAM service.

The shared Responsibility model for AWS IAM outlines the division of security responsibilities blw AWS & the Customer.

In general AWS is responsible for the security of the cloud infrastructure & services, while the customer is responsible for the security of their own content & applications running on the cloud infrastructure. Specifically, the shared responsibility of IAM says that

1. AWS is responsible for providing IAM as a service, including the infrastructure and IAM functionality such as creating & managing users, groups & permissions
2. The customer is responsible for using IAM to manage their own user accounts, groups & permissions & for ensuring that the IAM policies are properly configured to control access to their resources.
3. Customer is also responsible for implementing security best practices for IAM such as regularly reviewing & auditing their IAM policies, enabling multi-factor authentication (MFA) & using AWS trusted advisor to monitor IAM configurations for potential security risks.

List 6 AWS Acceptable Use policy:

Certainly AWS has an acceptable Use Policy (AUP) that outlines the rules & guidelines for using their services. The AUP is designed to ensure that AWS customers & users use the services in a responsible & lawful manner, & to protect the security & integrity of the AWS network & systems. Some of the key points covered by AUP includes:

1. No illegal, Harmful or offensive Use of Content.
2. Prohibited activities, such as Hacking, Spamming & distributing malware.
3. Use of AWS services for legal & ethical purposes only.
4. Obidience with all applicable laws & regulations.
5. Protection of Confidential & personal info.
6. No Security Violations
7. No Network misuse or abuse
8. No Email or other message misuse
9. Reporting of security incidents or violations to AWS.