* Compute Services :-

Compute services provide dynamically scalable compute capacity in cloud.

Compute resources can be provisioned on-demand in form of virtual machines. Virtual machines can be created from standard images provided by cloud service provider or custom images created by users. Compute services can be accessed from web consoles of these services that provide graphical user interface for provisioning, managing & monitoring these services.

It provides API's for various programming languages that allow developers to access & manage these services programmatically.

⇒ Amazon EC2

Amazon Elastic Compute cloud (EC2) is compute service provided by Amazon.

⇒ Google Compute Enginee is a compute service provided by Google.

⇒ Windows Azure Virtual Machines is compute service from Microsoft.

* Storage Services :-

Cloud storage services allow storage & retrival of any amount of data, at any time from anywhere on web. Most cloud storage services organize data into buckets or containers.

Scalability → cloud storage services provide high capacity & scalability. Objects upto several terabytes in size can be uploaded & multiple buckets/containers can be created on cloud storages.

Replication → when an object is uploaded, it is replicated at multiple facilities ~~[illegible]~~ and/or on multiple devices within each facility.

Access Policies → cloud storage services provide several security features such as Access Control List (ACL), bucket container level policies, etc.

ACL can be used to selectively grant access permissions

on individual objects. Bucket/container level policies can also defined to allow or deny permission across some or all objects within a single bucket/container.

⇒ Encryption → Cloud storage services provide server side encryption (SSE) options to encrypt all data stored in cloud storage.

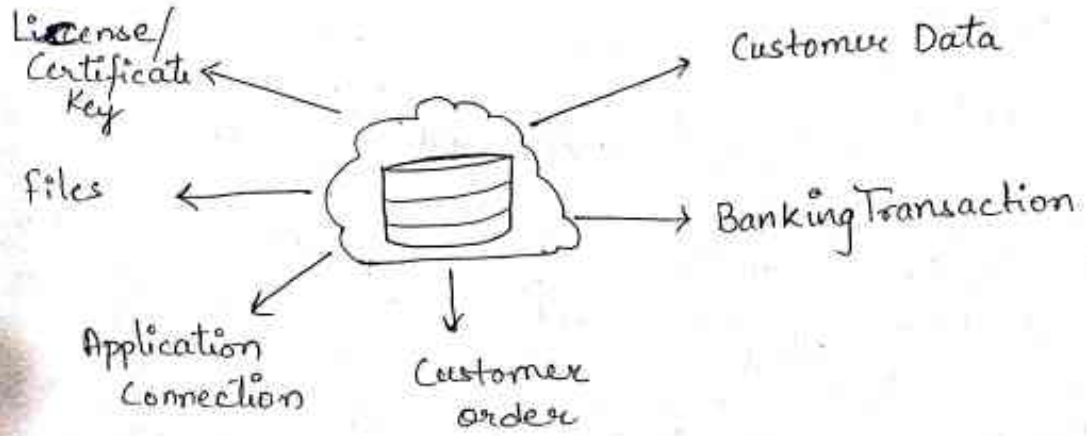
⇒ Consistency → Strong data consistency is provided for all upload & delete operations. Therefore, any object that is uploaded can be immediately downloaded after the upload is complete.

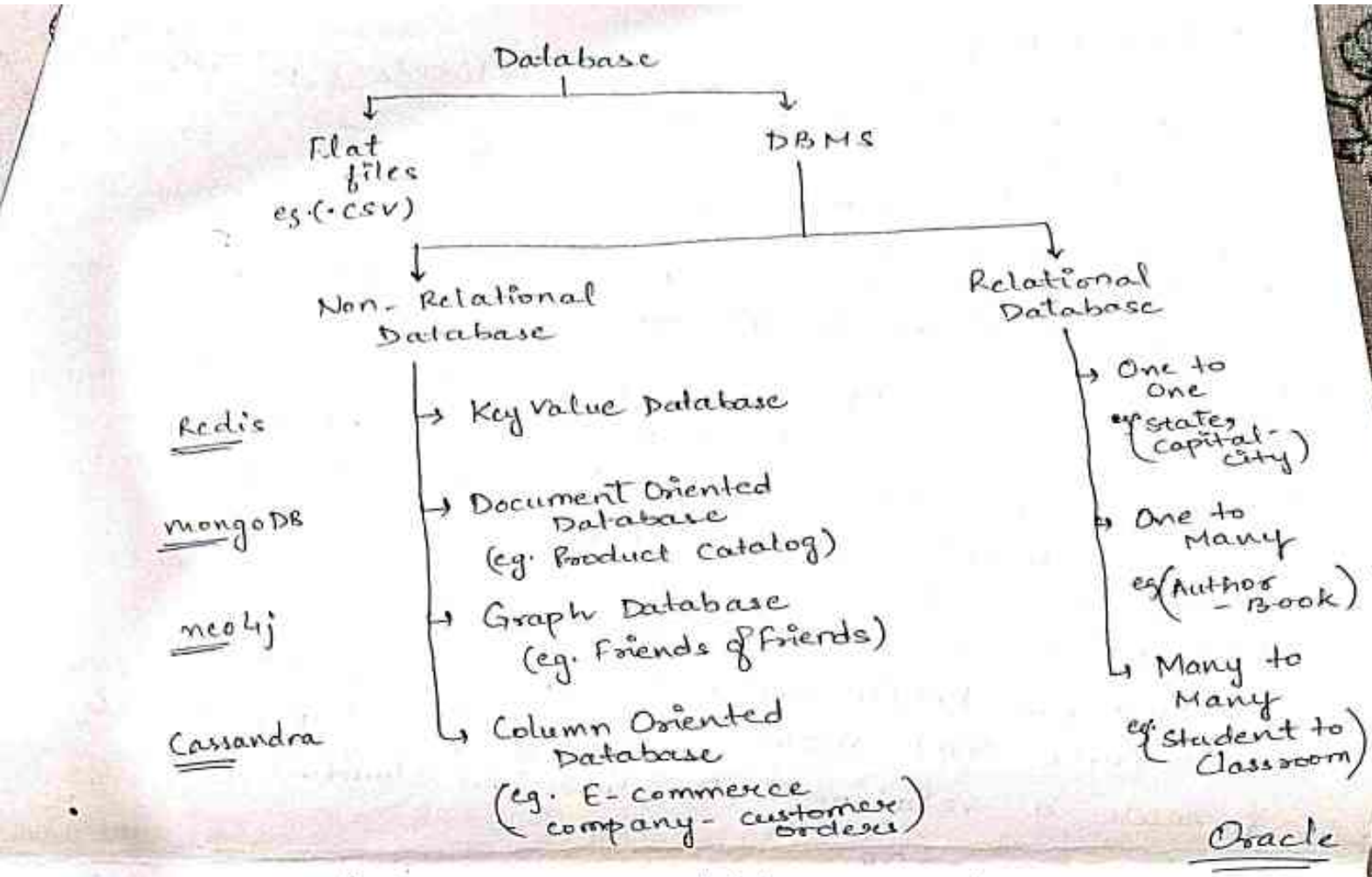
⇒ Amazon S3 (Amazon Simple Storage Service) is online cloud based data storage infrastructure for storing any amount of data.
S3 provides highly scalable, fast, fully redundant & affordable storage infrastructure.

⇒ Google Cloud Storage (GCS) is cloud storage service from google.

⇒ Windows Azure Storage is cloud storage service from microsoft. It provides various storage services such as a blob, table & queue storage service.
The blob storage service allows storing unstructured binary data or binary large objects (blobs).

* Database Services :-





For oracle, Redis, mongoDB, neo4j & cassandra you need to purchase their licenses & have to install the whole setup.
So we require an easy database service.

→ Cloud database services allows you to set up & operate Relational & Non-relational Database in Cloud.

Relation Databases provided by various cloud service providers may include MySQL, Oracle, SQL server, etc.

The Non-Relation Databases are like Redis, mongo DB, neo4j, etc.

→ Benefits of Database Services in Cloud:-

i) Scalability Cloud Database services allow provisioning as much compute & storage resources as required to meet the application workloads levels. Provisioned capacity can be scaled up or down. For read heavy workloads, read replicas can be created.

ii) Reliability
Cloud DB services are reliable & provide automated backup & snapshot options.

iii) Performance
Cloud DB services provides guaranteed performance with options such as guaranteed input / output operations per second (IOPS) which can be provisioned upfront.

iv) Security Cloud DB services provides several security features to restrict the access to database instances & stored data, such as n/w firewalls & authentication mechanisms.

v) Easy to setup
Database Services - • Amazon RDS
Amazon Relational Database Service (RDS) is a web service that makes it easy to setup, operate & scale a relational Database in cloud.

Amazon Dynamo DB
Amazon Dynamo DB is non relational (No-SQL) database services from Amazon.

- Neptune
AWS provides Neptune DB service for Graphical Database

- Windows Azure SQL DB
Windows Azure SQL Database is relational Database service from Microsoft.
- Windows Azure Table service
It is a Non-Relational (No-SQL) database service from Microsoft.
- Oracle Database - It is Relational Database service provide by Oracle.
- Oracle No SQL Cloud Service - It is non relational Database service provided by Oracle.
- Google Cloud SQL - Relational DB service by google.
- Google Cloud Datastore - It is fully managed non-relational database from google.

Application Services :-

Cloud based application runtime & frameworks allow developers to develop & host application in cloud.

- Support for various programming languages.
  Application runtimes provide support for programming languages.
- Resource Allocation
  Application runtime automatically allocate resources for application & handle the application scaling, without the need to run & maintain servers.

⇒ Google App Engine → Google App Engine is platform as a service (PaaS) from Google, which includes both an application runtime & web frameworks.

- Runtimes
  App Engine provides runtime environment for Java, Python, PHP and Go programming language.

→ Google App Engine (GAE) is one of many components of the Google cloud Platform (GCP) suite.

→ Google App Engine is a fully managed, easy to use, and extremely scalable Platform as a service offering that allows for efficient development of custom applications.

- Web Frameworks
  App Engine provides a ~~simpl~~ simple Python web application framework called webapp2. App Engine also supports any framework written in pure python that speaks WSGI, including Django, CherryPy, Pylons, web.py & web2py.
- Datastore
  App engine provides a noSQL data storage service.
- Authentication
  App engine applications can be integrated with google accounts for user authentication.
- Offers automatic scaling for web apps.

Why to use Google App Engine

i) It's language Java, Python are easy to understand.
ii) It's platform is absolutely free, you can purchase additional resources if needed.

iii) It provides Marketing facility to our apps.

Cost of Google App Engine

i) It provides limited resource usage as free of cost.
ii) After resource usage limit users can pay per day or per minute basis.

⇒ Windows Azure Web Services →

Windows Azure web services is a Platform as a service from Microsoft.
Azure websites allows you to host web applications in Azure cloud.

* Queuing Services :-

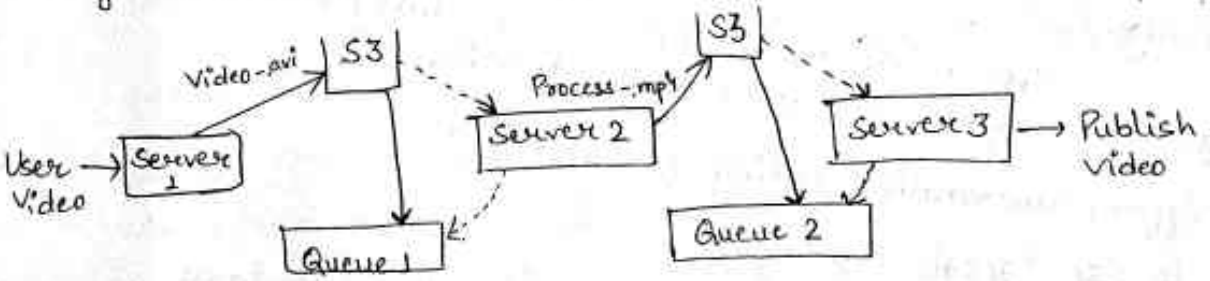
Amazon Simple Queue Service (SQS) is a queuing service from Amazon.
It is fully managed message queuing service that enable you to decouple & scale microservices, distributed systems, serverless applications.
It is a type of middleware solution that allows applications & services to communicate within a cloud computing environment.

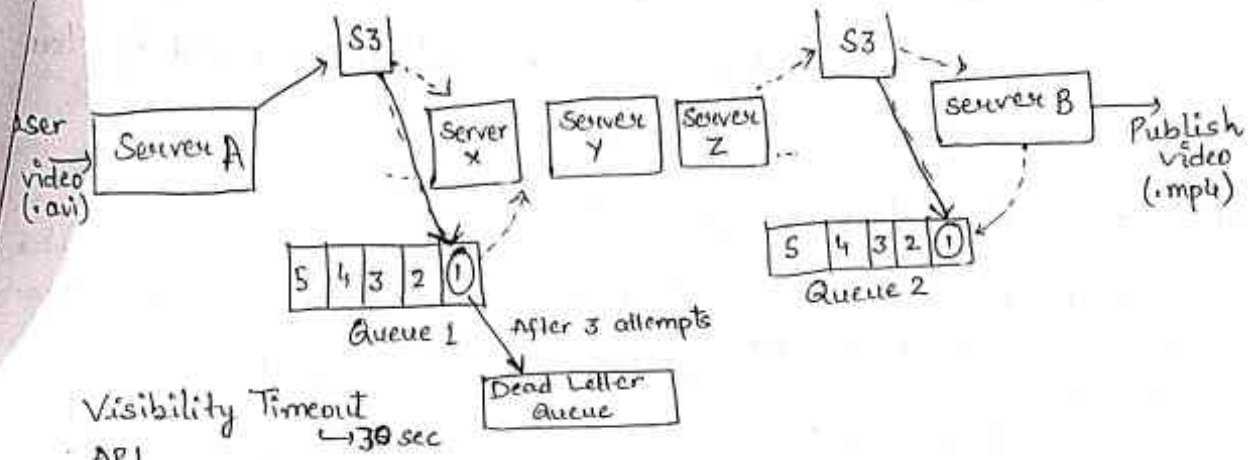
- Short Message SQS is a distributed queue that supports message of up to 256 KB in size.
- Multiple Writers / Readers

SQS supports multiple writers & readers & locks message while they being processed.

- High Availability

To ensure high availability for delivering messages, SQS service trade-offs on the first out capability & doesnot guarantee that messages will be delivered in FIFO order





Visibility Timeout → 30 sec

API

To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period of time during which Amazon SQS prevents other consumers from receiving & processing the message. It is the time period or duration you specify for queue item which when is fetched & processed by Consumer is made hidden from queue & other Consumers. The main purpose is to avoid multiple Consumers consuming same item repetitively.

API (Applicat^n Programming Interface) is a software intermediary that allows 2 applications to talk to each other.

→ Google Task Queue Service

It is a queuing service from google & is part of Google App Engine Platform.

Task queues allows to execute tasks in background. Push queue is default queue that processes tasks based on processing rate configured in queue definit^n. Pull Queue allow task consumers to lease a specific duration. The tasks are processed & deleted before the lease ends.

→ Windows Azure Queue Service

It is a queuing service from Microsoft.

* E-mail Services :-

Cloud based email services allow applications hosted in cl... to send emails.

⇒ Amazon Simple Email Service (SES) →

Amazon Simple Email Servic... is bulk and transactional email-sending service from Amazo... SES is a cost-effective email service built on the reliable & scalable infrastructure that Amazon.com developed to serve its own customer base. With Amazon SES, you can send & receive email with no requirement minimum commitments you pay as you go, and you only pay for what you use. This service is preferably use for sending emails. SES service can be accessed & used from SES console, the Simple Mail Transfer Protocol (SMTP) interface, or the SESAPI.

Some of purposes where you can use SES are as below:-

a) Marketing Email → Use Amazon SES to promote your products and services to your large customer base. You can send advertisements, special offers, or any other type of high quality content that your existing customers value.

b) Transactional Email → Amazon SES is low cost solution for sending automated emails such as order confirmatio... shipping orders notices, order status updates, policy changes, password resets, and other messages that keep your customers informed.

c) Notifications → Use amazon SES to send out system health reports, application error alerts, workflow status updates, and any other event that requires reporting.

Benefits of SES

i) Inexpensive
ii) Reliable
iii) Scalable

* Note:- To send an email in SES you need 3 things :- servername, username & password.

Google Email Service →

Google email service is part of the google App engine platform that allows App Engine applications to send email messages on behalf of app's administrators, and on behalf of users with Google accounts.
App Engine apps can also receive emails. Apps send messages using the Mail service messages in the form of HTTP requests initiated by App Engine & posted to app.

Notification Services :-

Cloud based notification services or push messaging services allow applications to push messages to internet connected smart devices such as smartphones, tablets, etc.
Push messaging services are based on publish-subscribe model in which consumers subscribe to various channels provided by a producer/publisher. whenever new content is available on one of those channels, the notification service pushes that information out to consumer.
Push Notifications are used for such smart devices as they help in displaying the latest information while remaining energy efficient.
Consumer applications on such devices can increase their consumer engagement with help of push notifications.

⇒ Amazon Simple Notification Service

SNS is fully managed, fast & flexible push notification service.
It is a web service that coordinates & manages the delivery or sending of messages to subscribing endpoints or clients.
It allows for sending individual messages or fan-out messages to large number of recipients or to other distributed AWS services.
Messages published to an SNS Topics will be delivered to the subscriber immediately.
SNS has two types of clients:-

a) Publishers : → Publishers communicate asynchronously with subscribers by producing & sending messages to topics. A topic is a logical access point & a communication channel.

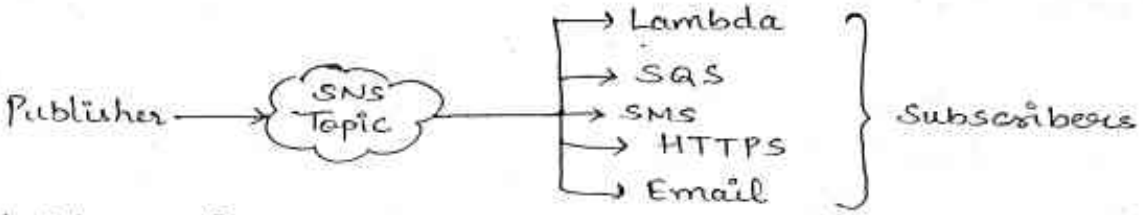
b) Subscribers:→

Subscribers are the consumers who subscribe to topics to receive notifications.

Benefits of SNS →

i) Inexpensive, pay as you go model with no upfront cost.

ii) Reliable, Atleast 3 copies of the data are store across multiple regions.



⇒ Google Cloud Messaging →

Google cloud Messaging for android provides Push messaging for android devices.

GCM allows applications to send data from the application severers to their users Android devices, and also to receive messages from devices on same connection.

GCM is useful for notifying applications on android devices that there is new data to be fetched from the application servers.

GCM supports messages with payload data upto 4KB.

GCM provides a 'send to sync' message capability that can be used to inform an application to sync data from server.

GCM for chrome is another notification service from google that allows messages to be delivered from cloud to apps & extensions running in chrome.

⇒ Windows Azure Notification Hubs →

Windows Azure Notification Hubs is a push notification service from Microsoft.

It provides common interface to send notifications to all major mobile platforms including Windows store, iOS, and Android.

Media Services :-

Cloud service providers provide various types of media services that can be used by applications for manipulating, transforming or transcoding media such as images, videos, etc.

- Amazon Elastic Transcoder is a cloud-based video transcoding service from Amazon.
- Google Images Manipulat^n Service is a part of Google App Engine platform. It provides capability to resize, crop, rotate, flip & enhance images.
- Windows Azure Media Services is a cloud based media service by Microsoft.

Content - Delivery Services :-

Cloud based Content Delivery Service include Content Delivery Networks (CDN's).

CDN is a distributed system of servers located across multiple geographic locations to serve content to end users with high availability & high performance. CDNs have a number of edge locations deployed in multiple locations, often over multiple backbones.

- Amazon CloudFront is a Content Delivery service from Amazon
- Windows Azure Content Delivery Network is Content delivery service from Microsoft.

* Analytics Services :-

Cloud based analytics service allows analyzing massive data sets stored in cloud either in cloud storages or in cloud databases using programming models such as MapReduce.

- Amazon Elastic MapReduce It is the mapreduce analytics service from Amazon.
- Google MapReduce Service is provided by Google.
- Windows Azure HDInsight is an analytics service from Microsoft.

* Deployment & Management Services :-

Cloud based Deployment & Management services allow you to easily deploy & manage applications in the cloud. These services automatically handle deployment tasks such as capacity provisioning, load balancing, auto-scaling & application health monitoring.

• Amazon Elastic Beanstalk

Amazon provides deployment service called Elastic Beanstalk that allows you to quickly deploy & manage applications in AWS cloud.

It supports Java, PHP, .NET, Node.js, Python, Ruby applications. With elastic Beanstalk you just need to upload the applications & specify configuration settings in simple wizard & the service automatically handles instances provisioning, server configuration, load balancing & monitoring.

• Amazon Cloudformation

It is a deployment service from Amazon. With Cloudfront you can create deployments from a collection of AWS resources such as Amazon Elastic Compute Cloud, Amazon Elastic Block Store, Amazon SNS, Elastic load Balancing & Auto-scaling.

A collection of AWS resources that you want to manage together are organized into a stack.

* Identity & Access Management Services :-

IDAM services allows managing the authenticat^n & authorizat^n of users to provide secure access to cloud resources.

Using IDAM services you can manage user identifiers, user permissions, security credentials & access keys.

• Amazon Identity & Access Management by Amazon.
• Windows Azure Active Directory by Microsoft.

Security Issues in Cloud Computing :-

Security Issues in cloud Computing are:-

i) Cyber Attacks → Cybercrime is a business, and cybercriminals select their targets based upon the expected profitability of their attacks. Cloud based Infrastructure is directly accessible from public internet, is often improperly secured and contains a great deal of sensitive and valuable data. Additionally, the cloud is used by many different companies, meaning that a successful attack can likely be repeated many times with a high probability of success. As a result, organizations cloud deployments are a common target of cyberattacks.

ii) Malicious Insiders → Insider threats are major security issue for any organization's network and some of the sensitive resources that it contains. Attempts to gain this level of access are what reveals most attackers to their target, making it hard for an unprepared organization to detect a malicious insider.

iii) Insecure Interfaces & API → Software user interfaces and API's are usually responsible for provision, monitoring and management of cloud services. If a customer has not properly secured the interfaces for their cloud-based infrastructure. The documentation designed for customer can also be used by a cybercriminal to identify & exploit potential methods for accessing & exfiltrating sensitive data from an organizations cloud environment.

iv) Data Loss → when you migrate large amount of data to cloud, there will be always a chance of data loss.

v) Compromised user accounts → Weak password protocols are leading cause of compromised user accounts. Many users who work with cloud services do not have strong password protection, as they either use weak passwords reuse older passwords, or don't change their passwords regularly.

vi) Third Party handling data.

⇒ Security Threats :- i) DOS :- In a Denial-of-service (DOS) attack, a hacker floods a system with more web traffic than it can handle at its peak. This results in operations stalling entirely, with internal users and customers unable to access the system, making it unable to operate the business. Tries to bring server Down.

ii) Man in the Middle Attack :→ It is a type of cyberattack where the attacker performs its functions by staying b/w the two parties. The type of function it can do is to alter the communicat" b/w two parties and make both of the parties feel that they are communicating in a secured network.

iii) Sniffing Attacks → Sniffing attacks refers to data thefts caused by capturing network traffic through packet sniffers that can unlawfully access & read the data which is not encrypted. The data packets are captured when they flow through a computer network.

iv) Port Scan → A port scan is a common technique hacker use to discover open doors or weak points in a network. It helps cyber criminals find open ports & figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organizations.

i) Data Breaches :→ Data Breaches occur when unauthorized individuals access cloud systems & interfere with data stored in them. whether the attackers view, copy or transmit data, an organization's safety is not guaranteed once such individuals gain access.

ii) Misconfiguration :→ It is one of the leading threats business face in their cloud based systems. It often results from need to make cloud data accessible & shareable.

⇒ Data Security in Cloud Computing :→

Cloud data security is combination of technology solutions, policies and procedures that you implement to protect cloud-based applications & systems, along with the associated data users access.

The core principles of information security & Data governance - data confidentiality, integrity & availability also applied to cloud :

- Confidentiality → Protecting the data from unauthorized access & disclosure.
- Integrity → Safeguard the data from unauthorized modification so it can be trusted.
- Availability → Ensuring the data is fully available & accessible when it's needed.

You need to consider data security during all stages of cloud computing & the data lifecycle from development, deployment or migration of applications and systems, to the management of cloud environment.

⇒ Information Security :→ Security related to information exchanged b/w different hosts or b/w hosts and users. This issues pertaining to secure communication, authentication & issues concerning single sign on & delegation. Secure communication issues includes

those security concerns that arise during the communicat' b/w two entities.

These include confidentiality & integrity issues. Confidentiality indicates that all data sent by users should be accessible to only 'legitimate' receivers & integrity indicates that all data received should only be sent by 'legitimate' senders.