Cloud Computing - Quick Notes:

- Cloud refers to the 'servers' that are accessed over the internet, present at remote location.

- Cloud computing is the on-demand availability of computer system resource without direct active management by the user.
  In short, storing, managing and process data on remote servers.
- Service Providers: (i) Google Cloud (ii) AWS (iii) MS Azure (iv) IBM Cloud.
- Types: 1) Public : Accessible for all
  2) Private : Services accessible within an org.
  3) Hybrid : public + private cloud features.
  4) Community : Services accessible by a group of orgs.

- Characteristics:
  1. On-demand self service : consumer can request and receive access to a service without third-party's (admin/staff) approval or need to accept request.
  2. Broad network Access : Access anywhere and anytime.
  3. Resoure Pooling : Multiple customers, same physical resources.
  4. Measured Services : Pay according to services used.
  5. Rapid Elasticity and Scalibility : Ability to quickly provision resources in the cloud as the org. need them.
  6. Easy or Zero Maintenance : Customer need not worry about resource failures.
  7. Security : Minimal data loss / failure as copy is stored on multiple servers and not just one. hence, data safe.

- Advantages:
  1. Resource accessible anywhere, anytime.
  2. On-demand self service.
  3. Reduced IT cost (Newer Hardware Purchase not required)
  4. Scalability.
  5. Collaboration over different region.
  6. Security / No data loss / failure.
  7. Location and device independence.
  8. We need not update software.
  9. Customer's maintenance not required hence, saves our time.

- Disadvantages
  1. Network Connection Dependency
  2. Lack of support if any resource is not working, hence trustworthy service provider is a must.
  3. May not get all features / Limited accessibility / Customers don't have say / not in control (Provider-chosen features)
  4. Vendor-lock-in problem.

* Vendor lock-in problem:

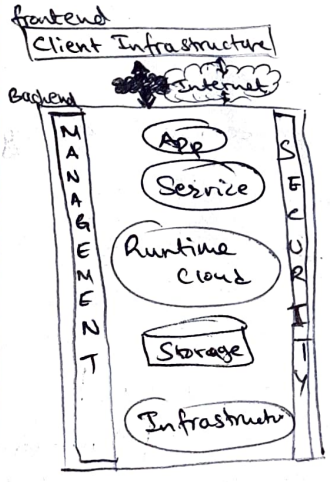
Situation where customers are dependent (i.e., locked in) on a single cloud provider technology, implementation and cannot easily move on in the future to a different vendor/service provider without substantial cost, legal constraint or technical incompatibilities i.e., org. can/may face problem when transferring their services from one vendor to another.

- Types of vendor lock-in Risks:

1. Data Transfer Risk : format of data extracted, cryptography or security mechanism used to encrypt data.
2. Application Transfer Risk: Compatibility, service provider's partnership cost, reconfiguration of app non-natively is expensive and difficult, lack of standard.
3. Human Resource Knowledge Risk: Employee's knowledge of the new platform may not be as good as the old platform. Relearning time.

* Cloud Computing Architecture: (2 parts: frontend & backend).

- front-end: • used by client
  • contains all client side interfaces and apps. required to access the cloud platform.
- back-end: • used by service provider
  • manages all resources required to provide C.C. services
  • includes huge amt. of data storage, security mechanisms, virtual machines, deployment models etc



7. Management.
8. Security
9. Internet

* Components of C.C. Architecture:

1. Client Infrastructure: front end/GUI
2. Application : Maybe software or platform.
3. Service: Model: SaaS (Software), PaaS (Platform), IaaS (Infrastructure) as a Service
4. Runtime Cloud: Execution & Runtime Env. to VM.
5. Storage.
6. Infrastructure: HW & S/W components, Server

* SaaS (Software as a Service):

- Way of delivering services and apps. over the internet.
- Maintenance of S/W & H/W done by vendor.
- Removes cost of h/w and S/W maintenance.
- Used as a finished product by the end users, can't make changes by themselves. E.g.: [redacted], Gmail, G-slide, MS Team, Dropbox etc.

- Characteristics:
  - S/W available over internet
  - S/W maintained by vendor
  - Cost effective
  - Available on-demand.
  - Scaled up/down as per need.
  - Worked on Shared Model, i.e, one S/f → multiple clients. Using registration/ accounts.
  - S/W automatically upgraded.

- Benefits:
  - Platform independent
  - Multi-tenant Solutions
  - Scale up/ Scale down.
  - Accessible anytime, anywhere.
  - Reduced time (accessible directly from browser).
  - Cost effective (pay as per use)

* PaaS (Platform as a Service):

- developers use it
- provides platform & env. (i.e., runtime env) to build apps. & services
- offers development and deployment tools.
- Hosted in cloud & accessed by user via web browsers.
- No control over the infrastructure. Only interact with the UI and OS provided by the vendor. No control over it.

Advantages:
- pay as per use, cost Effective
- No need to purchase expensive servers, S/W or storage.
- Scale up/down anytime.
- S/W management (updates) done by provides.
- Easy deployment of web applications.

* IaaS (Infrastructure as a Service)

- Provides infracture.
- Used by system admin/ or network architects (full control)
- Provides underlying O.S., security, networking and servers.
- Provides access to fundamental resources such as physical machine, virtual machine, storage etc.

*Advantages:
- Scale up/down as required.
- Cost effective (pay as use)
- full control over resources.

- Offers:
  - Virtual machine disk storage
  - IP address
  - Virtual LAN (VLAN)
  - Load balances.

Example: AWS, IBM Cloud, Azure.

IaaS	PaaS	SaaS	
Application Data Runtime Middleware OS	Application Data	Nothing	end-user manages or service user manages
Virtualisation Servers Storage Networking	Runtime Middleware OS Virtualisation Servers Storage Networking	Application Data Runtime Middleware OS Virtualisation Servers Storage Networking	Service Provider manages.

* Applications of C.C.

1) Business Application : E.g.: Salesforce, Paypal etc.
2) Data Storage & Backup Apps : E.g.: Google Drive, Onedrive, etc.
3) Educational Application : E.g.: Google Docs, Chromebook for edu. etc.
4) Entertainment App : E.g.: Online games, video conferencing, etc.
5) Art/Media App : E.g.: Photopea, Travid.live, etc.
6) Social Applications : E.g.: Twitter, FB, IG, etc.

* Types of Cloud:

1) Public :
- Pay as per use (for services)
- managed by third parties (provider)
- fundamental characteristics : MULTITENANCY (Shared resource)
- Advantages - maintenance, on-demand, anywhere, anytime, scalable
- Disadvantages - 1. less secure b/c resources publically shared
  2. less customisable as compared to private cloud.

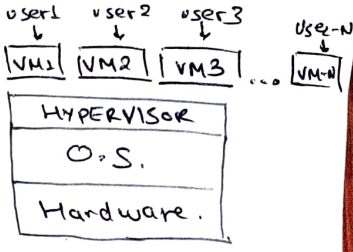
2) Private :
- Service accessible within an org.
- called internal/corporate cloud
- managed by either Org. or 3rd Party.
- Advantages - high security, more customisable, improved reliability
- Disadvantages - Limited operations, high cost, limited scalability

3) Hybrid :
- Critical activities performed/handled by private cloud.
- Non-critical activities performed/handled by public cloud.
- Advantages - scalability, security, Low cost, flexibility
- Disadvantages - Maintenance, Management, Dependency on infrastructure

4) Community :
- Services accessible by group of orgs. to share info b/w orgs.
- owned/Managed by 1 or more orgs. in community or by 3rd Party
- Advantages - cost effective, Shared Resource, Secure
- Disadvantages - Data Safety as shared resource, Maintenance, Increased cost

* Virtualisation in Cloud Computing:

- Technique that allows to share single physical instance of an app or resource among multiple org. or customers.
- Software called 'Hypervisor' deals with/manages virtualisation.
- All virtual resources will work independently



- Host Machine: Machine where virtual machine is actually built (on provider's side)
- Guest Machine: Virtual machine (on user's side).

- Hypervisor (Virtual Machine Monitor, VMM)
  - E.g.: VMware, Hyper-V
  - SW that creates and runs Virtual Machines.
  - Types: – Type 1 hypervisor (bare metal or native hypervisor)
    – Type 2 hypervisor (hosted or embedded hypervisor)
- Advantages:
  i) better resource utilisation
  ii) lowers the cost of IT infrastructure
  iii) Remote Access
  iv) Pay per use of IT infrastructure on demand.
  v) Enables running multiple O.S.
  vi) if one virtual machine is not working or having problem, others will not be affected.

* Serverless Computing:

- Cloud computing execution model in which cloud service provide allocates resources on demand, taking care of the servers on behalf of their customers.
  - no infrastructure management
  - autoscaling; based on incoming requests

  } managed by cloud provider

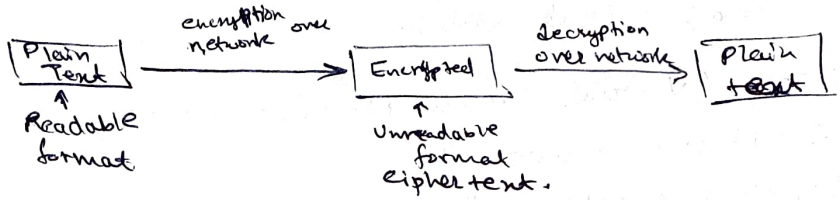
- Serverless Architecture is a way to build and run applications and services without having to manage infrastructure.
- Basically, SaaS and PaaS are serverless computing services
- Reduces cost/cost effective (no charge for idle time).

IMP→
- When invoked, Runs for a short duration only; i.e., when the app is not in use, there are no computing resources allocated to that app
- Application: E.g.: Weather update component in application.
  i.e, Gets invoked only when clicked, other time, idle or does not update automatically.

✱ Cloud Security Mechanisms:

- Encryption
- PKI (Public Key Infrastructure)
- SSO (Single Sign On): This mechanism enables one cloud service consumer to be authenticated by a security broker (3rd Party) to stay logged on, otherwise consumer would need to re-authenticate after every subsequent request.
- IaM (Identity and Access Management).

✱ Encryption:



- Types of Encryption: 1) Symmetric
  2) Asymmetric

} Read by crypto notes github.com/ghimiresubhgit

✱ Public Key Infrastructure (Asymmetric Encryption), PKI

- Three different formats of messages can be used in public key crypto system:
  - Encrypted message.
  - Signed message
  - Signed and Encrypted message.
- PKI Entities
  - CA (certification Authority)
  - RA (Registration Authority)
  - Subscriber
  - Relying Party
  - Repository.

✱ Identity and Access Management (IAM):

- It encompasses the components and policies necessary to control and track user identities and user privileges for IT resources, environments and systems.
- 4 components:
  1) Authentication : - Login Username & Password, biometric, digital signature/certificate etc.
  2) Authorisation : oversees relationship between identities, access control right & IT Resource availability
  3) User Management : Admin capabilities like create new user identity & access group, reset password, define policies etc.
  4) Credential Management. : Establishes identity access control rules for defined user accounts.
- IAM primarily used to counter:
  1. insufficient authorisation
  2. denial of service
  3. Overlapping boundary threats.