Cloud

PAGE NO.
DATE: / /

Unit - 4 → Cloud Security

→ It refers to a broad set of policies technologies, applications, & controls utilized to protect virtualized IP, data applications services & the associated infrastructure of cloud computing.

Data Security → It is a process of protecting files, databases & accounts on a n/w or cloud by adopting a set of controls, applications techniques & policies.

Aspects of Data Security:

→ The main aspects of data security are:

- **Confidentiality** → ensures that data is accessed only by authorized individuals.
- **Integrity** → It ensures information is reliable & accurate.
- **Availability** → It ensures that data is both available & accessable by all users

Data Security Mitigation:

⇒ It refers policies & processes put in place by companies to help prevent security incidents & data breaches as well as limit the extent of damage when security attacks happen.

→ Threat mitigation in data security can be broken down into 3 components or layers of mitigations.

- Threat Prevention ⇒ Best practices & policies to protect data.
- Threat Identification ⇒ Security tools & management to identify security threat
- Threat Remedy ⇒ Strategies & tools to reduce the impact of active security threats.

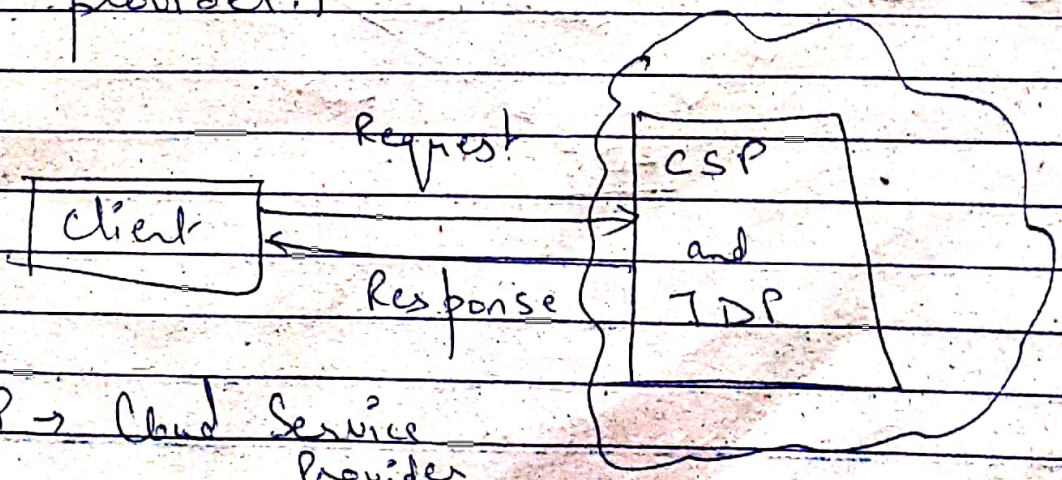
Identity & Access Management

→ It is a framework of policies & technologies for ensuring that the ppl. in an enterprise have the appropriate access to technology resources.

→ It not only identifies, authenticate & authorize an individual (who will utilize IT resources), but also the h/w & application employees need to access.

⇒ 4 Types of Identity Management system :-

i) Isolated IDMs → In this system, there is only 1 server which works as a cloud service provider as well as identity provider.



CSP → Cloud Service Provider

IDP → Identity Provider.

Its drawback:

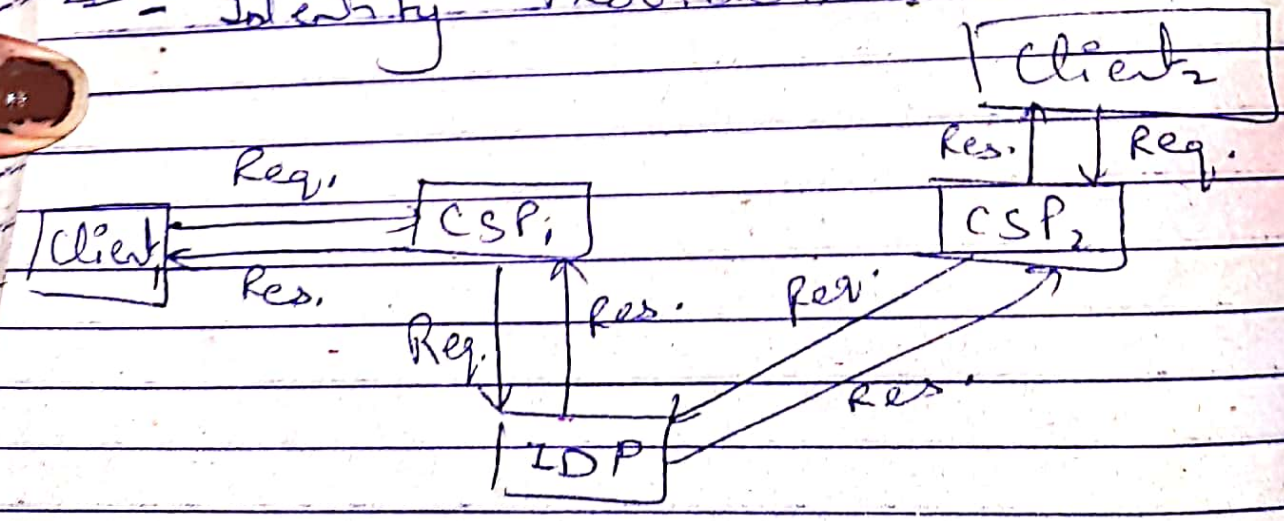
→ If no. of users get increased then server gets overloaded.

→ Single pt. failure → If server fails then whole sys. will collapse.

2) Centralized IDM → It is slightly improved then isolated IDM i.e. server is divided into 2 parts.

1st Part
- Cloud service Provider

2nd Part
- Identity Providers.



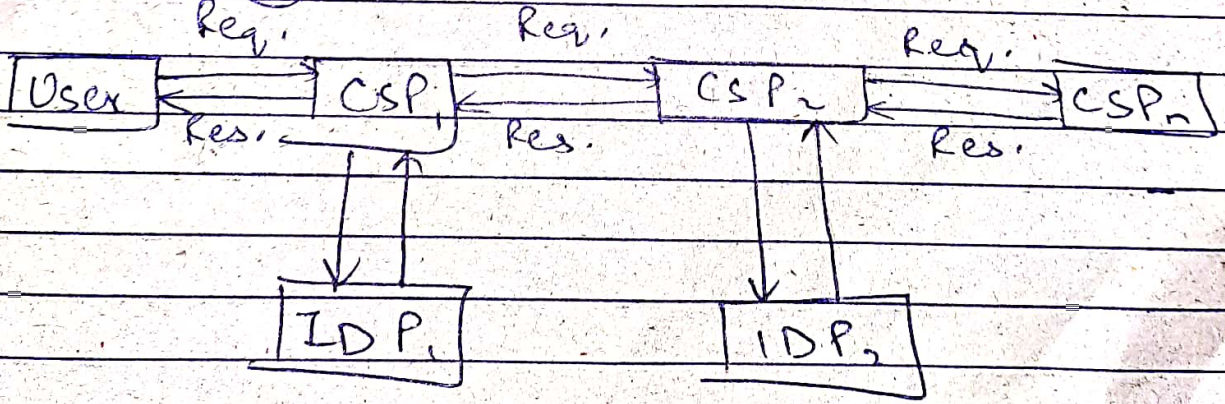
Client's request is accepted by Cloud Servers Providers & forwarded to IDP server that authenticates it.

and provides the response to CSP & it forwards it to Client.

Here, IDP server acts as a centralized server.

⇒ The overloading problem is solved slightly but single pt. failure problem is still in IDP server.

3. Federated IDM → This is the most popular system on the cloud in which the system uses single identity to access multiple cloud service providers belong to single trusted group.



PAGE NO.
DATE: / /

This system stores identity information at multiple places & can be accessed from anywhere & anytime by any cloud service provider.

4.) Anonymous IDM → It is a special type of IDM which is used for specific purpose generally by the defence organisation or research organisation.

In this the main identity is hidden with a particular message or image.

→ The system is based on basic 3 IDMs (isolated, centralized & ~~Anonymous~~ federated).

→ The communication will be done according to these 3 only.

IDM standards & Protocols in Practice :

→ They are designed specially for the transfer of authentication information & consist of a series of messages in a preset sequence designed to protect data while travelling on n/w b/w servers.

Protocols -

1) LDAP - Lightweight Directory Access Protocol.

→ It is an open-source protocol not associated with any specific vendor. It runs above TCP/IP & is most often used in modern organisat° to handle authentication inside premises.

2) SAML - Security Assertion Markup language.

→ It is often used in systems employing the single Sign-On (SSO) method of access control.

PAGE NO.
DATE: / /

3.) Open ID → It is used for web applications. It can be seen in practice when interacting with products from Google & Yahoo!
Implementation of this protocol is less complicated than implementation of SAML.

4.) RADIUS → It works by encrypting authentication credentials within a packet.
→ It is suited for application requiring general authentication.

5.) SCIM → System for Cross-Domain Identity Management.
→ It has ability to support dynamic shifts in access requirements.