Cloud security

It is set of control-based security measures and technology protection, designed to protect online stored resources from leakage, theft and data loss. Security applications use a software the same as SaaS (Software as a Service)

How to manage security in cloud

1. Firewall :- It protects traffic between various apps stored in cloud.

2. Access control :- It protects data by allowing user to set access lists for various resources.

e.g You can allow a specific employees while restricting other.

∴ Essential documents can be kept with strict ~~access~~ access control.

③ Data protection methods include VPN, encryption or masking it. It allows remote employees to connect the network. VPN accommodates the tablets and smartphone for remote access. Data masking maintains the data integrity by keeping identifiable information private

Benefits :-

① Protecting business from dangers
② Prevent data loss
③ Protect against internal threats

Data storage

Data stored in cloud (storage as a service) we refer to IaaS and data associated with an application running in the cloud on PaaS or SaaS.
~~The same thae~~ Amazon S3

security concerns

① confidentiality
② Integrity
③ Availability

Confidentiality :- Data should be confidentia. when stored in public cloud.

Two potential concerns

① Existing access control to protect data
It consists of both authentication and authorization.

a) Authentication (username + password)
b) Authorization (access control available to users)

Protection of data stored in cloud involves the use of encryption.

Which algorithm will [illegible] S3 do

(a) symmetric encryption
(Speed and computational effciency,
to handle

(b) Asymmetric encryption

Another confidentiality consideration for encryption is key management.
Proper key management is required

Integrity :- You need to worry the integrity of your data. Confidentiality does not imply integrity. Data can be encrypted for confidentiality purposes. For ~~veryf~~ verifying integrity of data, we can use message authentication code. (MAC)

digital signature

Availability :- If customer's data has maintained its confidentiality and integrity, you are also concerned about availability of data.

89 (c) Network-based attack

(1) Sniffing :- Reading, monitoring, or capturing packets of data from client and server. (account credentia's, bank details, personally identifiable information)

same (target one to one

(2) Eavesdropping

(3) Spoofing: Malicious ~~attacker is~~ user is pretending to be a legitimate entity or someone she is not

Cloud Security

If public cloud services, changing security requirements will require changes to network topology. We should address how the existing network interacts with cloud provider's network. There are four significant risk factors.

① Ensuring the confidentiality and integrity of organization's data to and from your cloud provider

② Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider.

③ Ensuring availability of resources in a public cloud that are being used by organization, or assigned to your organization by cloud provider.

④ Replacing the established model of network zone and tier with domains

<u>Denial-of-Service attack</u> :- It blocks or disrupt an organization or business's ability to use its own resources such as network bandwidth, system resources (CPU, memory, an application resources (web server, DNS server) It generally floods the target network with authentication requests or pings that have invalid return addresses

DDos is more advanced from of Dos attack where the target network is flooded by requests not from single server or machine but from multiple attack points