Cloud Security

Cloud computing which is one of the most demanding technology of the current time, starting from small to large organizations have started using cloud computing services. Where there are different types of cloud deployment models are available and cloud services are provided as per requirement like that internally and externally security is maintained to keep the cloud system safe. Cloud computing security or cloud security is an important concern which refers to the act of protecting cloud environments, data, information and applications against unauthorized access, DDOS attacks, malwares, hackers and other similar attacks.

Community Cloud : These allow to a limited set of organizations or employees to access a shared cloud computing service environment.

Planning of security in Cloud Computing:

As security is a major concern in cloud implementation, so an organization have to plan for security based on some factors like below represents the three main factors on which planning of cloud security depends.

- Resources that can be moved to the cloud and test its sensitivity risk are picked.
- The type of cloud is to be considered.
- The risk in the deployment of the cloud depends on the types of cloud and service models.

Types of Cloud Computing Security Controls :

There are 4 types of cloud computing security controls i.e.

1. **Deterrent Controls** : Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.
2. **Preventive Controls** : Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.
3. **Detective Controls** : It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.
4. **Corrective Controls** : In the event of a security attack these controls are activated. They limit the damage caused by the attack.