Cloud Security Challenges:

- Visibility into cloud data, in many cases, cloud service are accessed outside of the corporate network and from devices not managed by IT. This means that the IT team needs the ability to see into the cloud service itself to have full visibility over data, as opposed to traditional means of monitoring network traffic.
- In a third-party cloud service provider's environment, IT team have less access to data than when they controlled server and application on their own premises.
- Cloud customers are given limited control by default, and access to underlying physical infrastructure is unavailable.
- Users may access cloud application and data over the internet, making access controls based on the traditional data centre network perimeter no longer effective.
- Users access can be from location or device, including bring-your-own-device technology.
- Cloud provider infrastructure, as well as interfaces between in-house systems and the cloud are also included in compliance and risk management processes.

Cloud Security Solutions:

- Data classification classify data on multiple levels, such- as sensitive, regulated, or public, as it is created in the cloud. Once classified, data can be stopped from entering or leaving the cloud service.
- Data loss prevention implement a cloud DLP solution to protect data from unauthorized access and automatically disable access and transport of data when suspicious activity is detected.
- Manage controls within the cloud services, such as downgrading file and folder permission for specified users to editor or viewer, removing permission, and revoke shared links.
- Cloud data encryption can be used to prevent unauthorized access to data, event if that data is exfiltrated or stolen.
- User access control implement system and application access controls that ensure only authorized users access cloud data and applications.
- Device access control block access when a personal, unauthorized device tries to access cloud data.
- Identity all possible forms of access that privileged accounts may have to your data and application, and put in place controls to mitigate exposure.