

ONE PAGE SUMMARY

IT & Software > Cyber Security > Cloud Security

Introduction to Cloud Security

Secure your cloud: Protecting data in the digital sky.

DEFINITION

Cloud security involves protecting data, applications, and services hosted in the cloud. It ensures that sensitive information is safe from unauthorized access and cyber threats.

KEY CONCEPTS

Data Encryption

Transforming data into a secure format that can only be read with a key.

Access Control

Regulating who can view or use resources in the cloud to prevent unauthorized access.

Compliance Standards

Guidelines and regulations that cloud services must follow to ensure data protection.

Threat Detection

Identifying and responding to potential security breaches or vulnerabilities in the cloud.

Backup and Recovery

Creating copies of data and having plans to restore it after a loss or breach.

EXAMPLES

- Using encryption to secure sensitive customer data stored in the cloud.
- Implementing multi-factor authentication for accessing cloud services.
- Regularly updating software to protect against known vulnerabilities.

MEMORY TIPS

- ★ Remember 'DAC' for Data, Access, Compliance.
- ★ Think of 'EAT' for Encryption, Access control, Threat detection.
- ★ Visualize a cloud with a lock to recall cloud security.

COMMON MISTAKES

- ✗ Neglecting to encrypt sensitive data before uploading to the cloud.
- ✗ Failing to regularly update security settings and software.
- ✗ Overlooking compliance requirements for data protection.

QUICK RECAP

Cloud security is essential for protecting data in online environments. Key aspects include encryption, access control, and compliance with regulations. Always remember to back up data and stay vigilant against threats.