14.1.4 Cloud Threats Facts

Many companies have adopted cloud services to simplify administration. However, the cloud is also susceptible to many threats constantly being exploited by hackers.

The table below describes some of the most prominent threats against the cloud.

Threat	Definition	Defense
Data breach or loss	Data breach or loss can happen in a few different ways. Data can be erased, changed, or decoupled. Encryption keys can be stolen or lost. Data could also be accessed illegally because of weak authentication, authorization, and access controls.	Cloud data encryption; strong key generation, storage, and management; design and runtime protection for data.
Account and service traffic hijacking	Account and service traffic hijacking happens when the hacker exploits application weaknesses to take control of an account. A hacker may then launch a number of attacks, including phishing, sniffing, and man-in-the-middle.	Strong passwords and encryption; finding and fixing software flaws continuously.
Unsecure interfaces and APIs	Some of the risks associated with unsecure interfaces and APIs are credential information leaks, facility breach, inadequate validation for input data, user defined policies being bypassed, passwords and tokens being reused, and having unknown API dependencies.	Cloud provider interface's security model analysis; secure authentication and access controls; transit data encryption; API dependency chain analysis.
Denial of service	Denial of service attacks are less likely to happen in a cloud environment, but they still occur and can cause a lot of damage.	Implement security best practices; monitor environment for unauthorized activity; secure authentication and access control.
Malicious insiders	Malicious insiders are usually resentful people who have some kind of connection with a company or cloud service. These people are usually current or former employees, contractors, or business partners. They usually have authorized access to cloud resources and perform malicious acts.	Strict supply chain management; comprehensive supplier assessment; HR resource requirements; transparent information security and management; compliance reporting; security breach notification process.
Poor security or lack of due diligence	Knowledge and understanding of content security policies in a cloud environment are essential. Lacking them creates several risks for operational responsibilities like security, encryption, and incident response among others.	Research risks; CSP due diligence; capable resources.
Multi-tenancy	Since resources are shared between clients in a multi-tenant environment, this kind of situation can lead to data leak or breach. Sometimes it's accidental, but it is often intentional.	End-to-end protection.
Natural disasters	Data centers can be affected by floods, lightening, earthquakes, and other natural disasters that could lead to service and data loss.	Data center located in safe geographical area; have backups at different locations; mitigation measures; disaster recovery plan.
Hardware failure	When hardware components such as servers or switches fail, cloud data cannot be accessed.	Physical security program; pre-installed standby hardware devices.