

Cloud security

Chapter 7

Outline

- 1 [Cloud security](#)
- 2 [Cloud Security Threats](#)
- 3 [Cloud Security Mechanisms](#)
- 4 [Self Study](#)

Cloud security

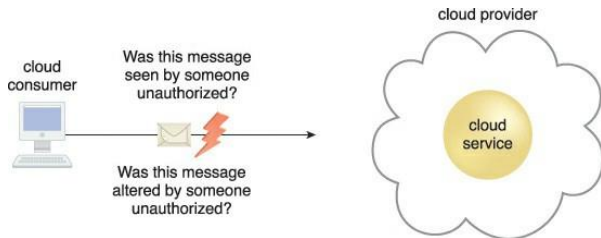
- The use of cloud systems is increasing day by day, and the challenges for ensuring cloud security are also increasing
 - Security in the cloud is similar to security in on-premises data centres
 - Cloud doesn't have any physical servers or storage devices,
 - Software-based security tools to monitor and protect the flow of information into and out of cloud resources
 - Cloud service providers enable proper and effective security measures to ensure the security of the cloud environment
 - Cloud security actually refers to the policies and the mechanism that is employed by the cloud providers to provide a bug and virus-free environment where the users can safely store, manage, and access their data and infrastructures
 - The major risks that can hamper cloud security are as follows:
 - Risk of leakage or exposure of information to others.
 - Risk of internal data of an organization being accessed by any unauthorized user or person who is not an employee of that particular organization.
- Any type of malattack that damages tcious cloud infrastructurbe

Cloud security

- Cloud service providers enable proper and effective security measures to ensure the security of the cloud environment
- Cloud security actually refers to the policies and the mechanism that is employed by the cloud providers to provide a bug and virus-free environment where the users can safely store, manage, and access their data and infrastructures
- The major risks that can hamper cloud security are as follows:
 - Risk of leakage or exposure of information to others.
 - Risk of internal data of an organization being accessed by any unauthorized user or person who is not an employee of that particular organization.
 - Any type of malicious attack that damages the cloud infrastructure results in data insecurity.
 - Intrusion of a virus in the cloud storage.

Fundamental security terms relevant to cloud computing

- Confidentiality: The message issued by the cloud consumer to the cloud service is considered confidential only if it is not accessed or read by an unauthorized party
- Integrity: The message issued by the cloud consumer to the cloud service is considered to have integrity if it has not been altered by an unauthorized party



Fundamental security terms relevant to cloud computing

- Threat: A threat is a potential security violation that can challenge defenses in an attempt to breach privacy and/or cause harm
- Vulnerability: A vulnerability is a weakness that can be exploited either because it is protected by insufficient security controls, or because existing security controls are overcome by an attack.
- Risk: Risk is the possibility of loss or harm arising from performing an activity. Risk is typically measured according to its threat level and the number of possible or known vulnerabilities. Two metrics that can be used to determine risk for an IT resource are:
 - the probability of a threat occurring to exploit vulnerabilities in the IT resource
 - the expectation of loss upon the IT resource being compromised

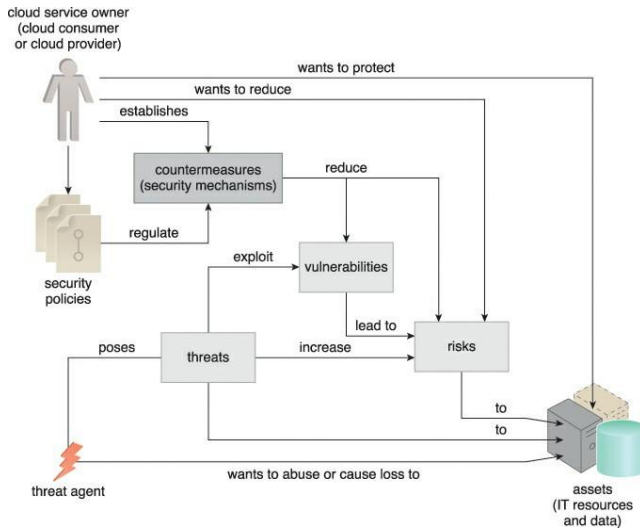
Security Controls

- Security controls are countermeasures used to prevent or respond to security threats and to reduce or avoid risk
- Details on how to use security countermeasures are typically outlined in the security policy, which contains a set of rules and practices specifying how to implement a system, service, or security plan for maximum protection of sensitive and critical IT resources.

Threat Agents

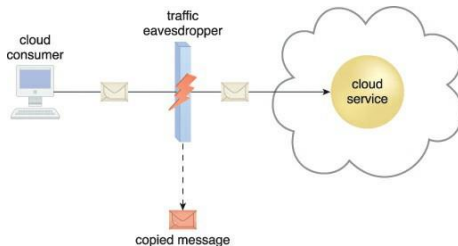
an entity that poses a threat because it is capable of carrying out an attack

Threat Agents



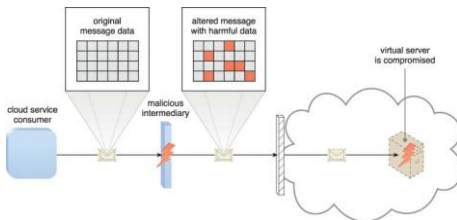
Cloud Security Threats: Traffic Eavesdropping

- occurs when data being transferred to or within a cloud (usually from the cloud consumer to the cloud provider) is passively intercepted by a malicious service agent for illegitimate information-gathering purposes
- The aim of this attack is to directly compromise the confidentiality of the data and, possibly, the confidentiality of the relationship between the cloud consumer and cloud provider
- Because of the passive nature of the attack, it can more easily go undetected for extended periods of time



Cloud Security Threats: Malicious Intermediary

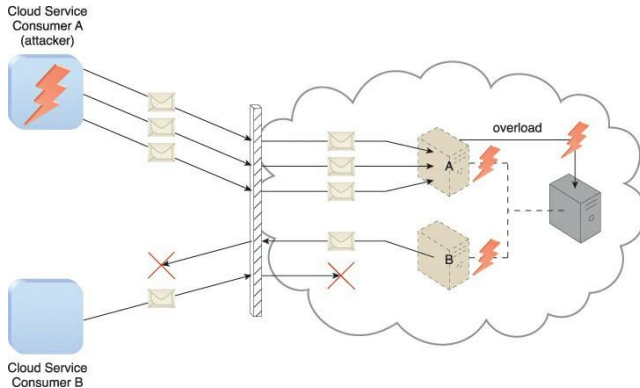
- threat arises when messages are intercepted and altered by a malicious service agent, thereby potentially compromising the message's confidentiality and/or integrity
- also inserts harmful data into the message before forwarding it to its destination



Cloud Security Threats: Denial of Service

- Attack is to overload IT resources to the point where they cannot function properly.
- This form of attack is commonly launched in one of the following ways:
 - The workload on cloud services is artificially increased with imitation messages or repeated communication requests
 - The network is overloaded with traffic to reduce its responsiveness and cripple its performance
 - Multiple cloud service requests are sent, each of which is designed to consume excessive memory and processing resources
- Successful DoS attacks produce server degradation and/or failure

Denial of Service



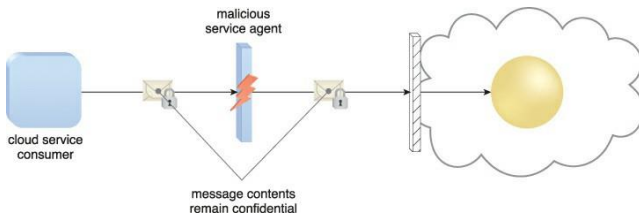
Cloud Security Mechanisms

- Encryption
- Hashing
- Digital Signature
- Identity and Access Management (IAM)
- Single Sign-On (SSO)


Encryption

- Data, by default, is coded in a readable format known as plaintext
- When transmitted over a network, plaintext is vulnerable to unauthorized and potentially malicious access
- The encryption mechanism is a digital coding system dedicated to preserving the confidentiality and integrity of data
- It is used for encoding plaintext data into a protected and unreadable format
- Encryption technology commonly relies on a standardized algorithm called a *cipher* to transform original plaintext data into encrypted data, referred to as *ciphertext*
- Access to ciphertext does not divulge the original plaintext data, apart from some forms of metadata, such as message length and creation date
- Encryption mechanism can help counter the traffic eavesdropping, malicious intermediary

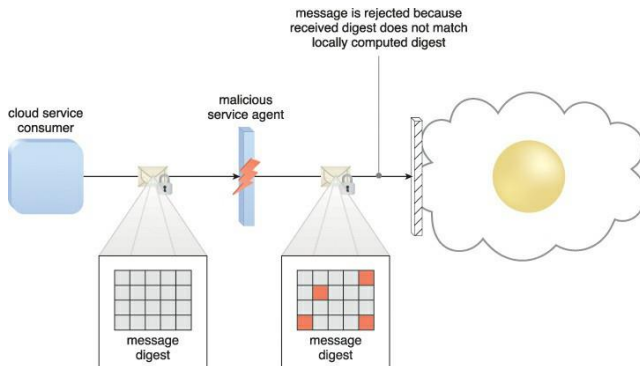
Encryption



Hashing

- The hashing mechanism is used when a one-way, non-reversible form of data protection is required.
- Once hashing has been applied to a message, it is locked and no key is provided for the message to be unlocked.
- Hashing technology can be used to derive a hashing code or message digest from a message, which is often of a fixed length and smaller than the original message.
 - The message sender can then utilize the hashing mechanism to attach the message digest to the message.
 - The recipient applies the same hash function to the message to verify that the produced message digest is identical to the one that accompanied the message.
- Any alteration to the original data results in an entirely different message digest and clearly indicates that tampering has occurred.
- Identical results from the two different processes indicate that the message maintained its integrity.
- A common application of this mechanism is the [storage of passwords](#). 

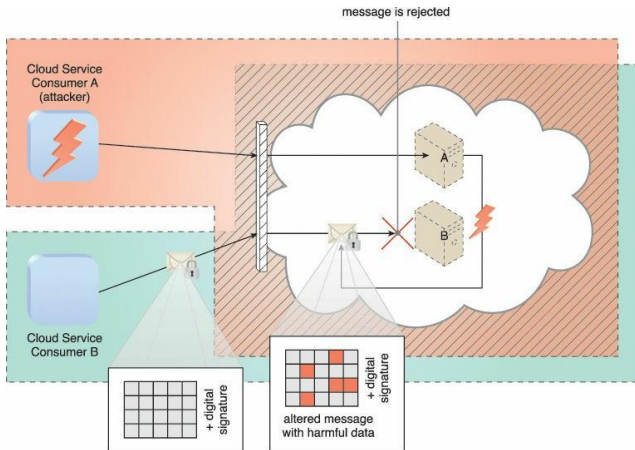
Hashing



Digital Signature

- The digital signature mechanism is a means of providing data authenticity and integrity through authentication and non-repudiation
- A message is assigned a digital signature prior to transmission, which is then rendered invalid if the message experiences any subsequent, unauthorized modifications
- A digital signature provides evidence that the message received is the same as the one created by its rightful sender

Digital Signature



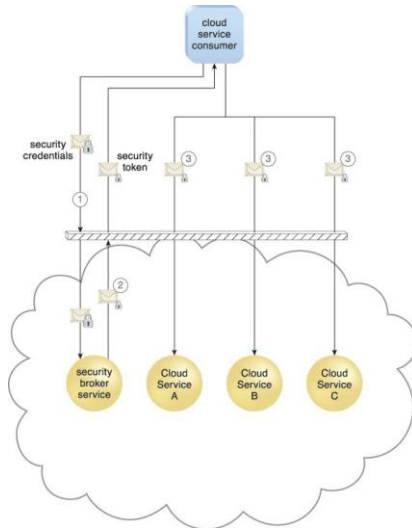
Identity and Access Management (IAM)

- mechanism encompasses the components and policies necessary to control and track user identities and access privileges for IT resources, environments, and systems
- Four main components
 - **Authentication:** Username and password combinations remain the most common forms of user authentication credentials managed by the IAM system
 - **Authorization:** defines the correct granularity for access controls and oversees the relationships between identities, access control rights, and IT resource availability
 - **User Management:** responsible for creating new user identities and access groups, resetting passwords, defining password policies, and managing privileges
 - **Credential Management:** establishes identities and access control rules for defined user accounts, which mitigates the threat of insufficient authorization

Single Sign-On (SSO)

- mechanism enables one cloud service consumer to be authenticated by a security broker
 - which establishes a security context that is persisted while the cloud service consumer accesses other cloud services or cloud-based IT resources
- Otherwise, the cloud service consumer would need to re-authenticate itself with every subsequent request.
- The SSO mechanism essentially enables mutually independent cloud services and IT resources to generate and circulate runtime authentication and authorization credentials
- The credentials initially provided by the cloud service consumer remain valid for the duration of a session, while its security context information is shared

SSO



Self Study

- 1 Map reduce
- 2 Cloud Cube Model