Chapter 6: Fundamental Cloud Security

This Module introduces terms and concepts that address basic information security within clouds, and then concludes by defining a set of threats and attacks common to public cloud environments.

Module 6 :

- Basic terms and concepts
- Threat agents,
- Cloud security threats,
- Encryption, Hashing,
- Digital Signature, Public Key Infrastructure(PKI),
- Identity and Access Management(IAM), Single Sign-On(SSO),
- Cloud Based Security Groups,
- Handed Virtual Server Machines

Outline

- Basic terms and concepts
- Threat Agents
- Cloud Security Threats
- Additional Considerations

6.1. Basic Terms and Concepts

- **Confidentiality**

Confidentiality is the characteristic of something being made accessible only to authorized parties (Figure 6.1). Within cloud environments, confidentiality primarily pertains to restricting access to data in transit and storage.

1. Confidentiality

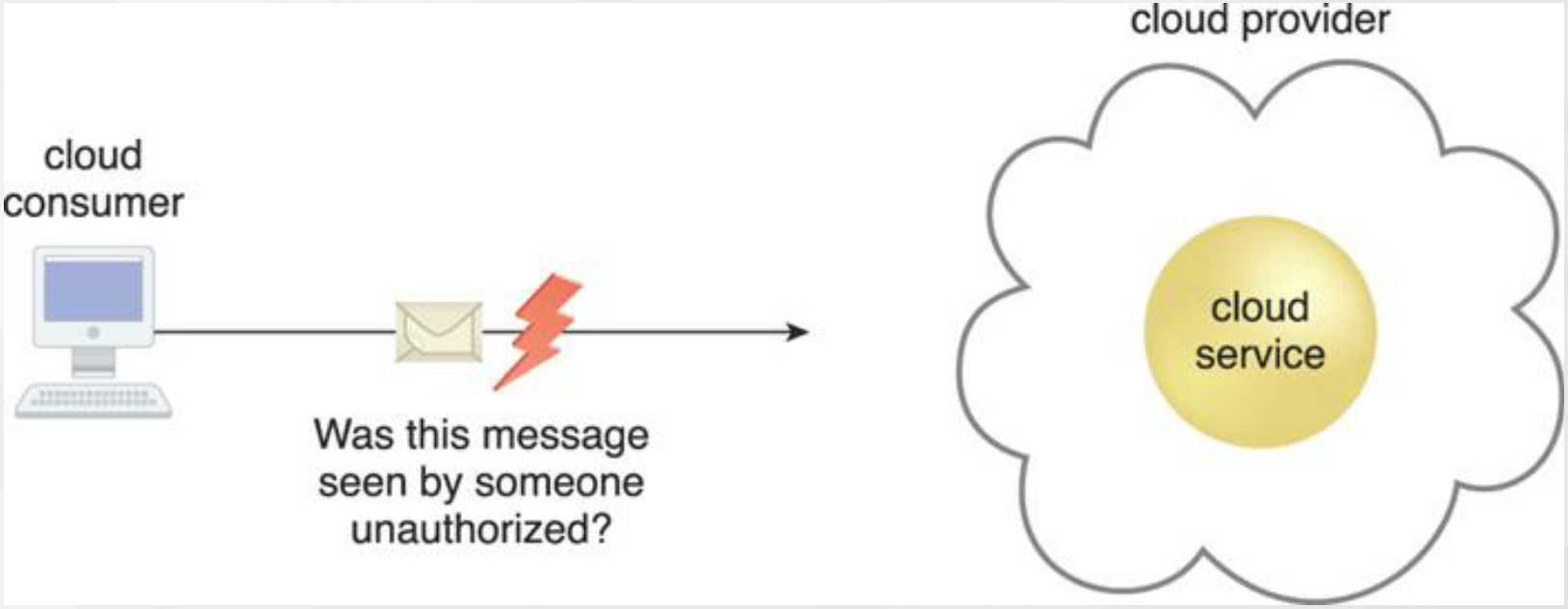


Figure 6.1 The message issued by the cloud consumer to the cloud service is considered confidential only if it is not accessed or read by an unauthorized party.

2. Integrity

Integrity is the characteristic of not having been altered by an unauthorized party (Figure 6.2).

An important issue that concerns data integrity in the cloud is whether a cloud consumer can be guaranteed that the data it transmits to a cloud service matches the data received by that cloud service.

Integrity can extend to how data is stored, processed, and retrieved by cloud services and cloud-based IT resources.

Integrity

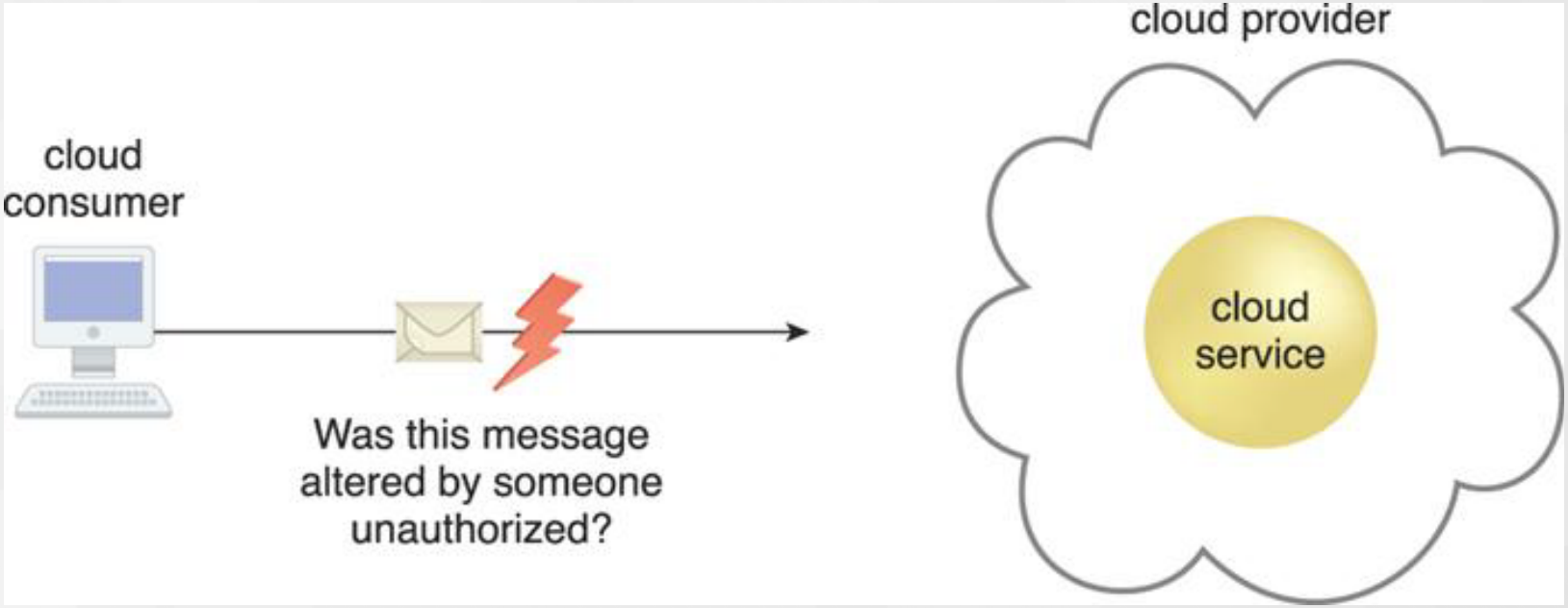


Figure 6.2 The message issued by the cloud consumer to the cloud service is considered to have integrity if it has not been altered.

3. Authenticity

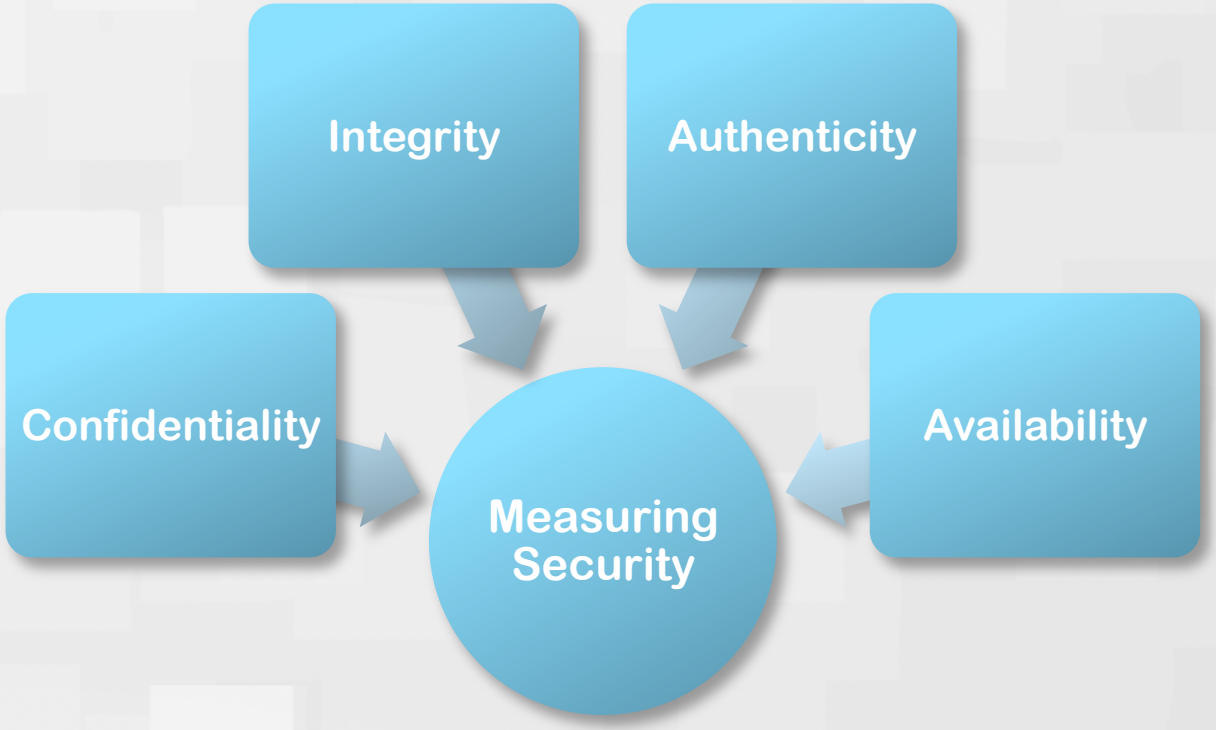
Authenticity is the characteristic of something having been provided by an **authorized source.**

This concept encompasses non-repudiation, which is the inability of a party to deny or challenge the authentication of an interaction.

Authentication in non-repudiable interactions provides proof that these interactions are uniquely linked to an authorized source. For example, a user may not be able to access a non-repudiable file after its receipt without also generating a record of this access.

4. Availability

- Availability is the characteristic of being accessible and usable during a specified time period.
- In typical cloud environments, the availability of cloud services can be a responsibility that is shared by the cloud provider and the cloud carrier.
- The availability of a cloud-based solution that extends to cloud service consumers is further shared by the cloud consumer.


Integrity
Authenticity
Confidentiality
Availability
Measuring Security

5. Threat

- A threat is a potential security violation that can challenge defenses in an attempt to breach privacy and/or cause harm.
- Both manually and automatically instigated threats are designed to exploit known weaknesses, also referred to as vulnerabilities.
- A threat that is carried out results in an attack.

6. 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.

- IT resource vulnerabilities can have a range of causes, including configuration deficiencies, security policy weaknesses, user errors, hardware or firmware flaws, software bugs, and poor security architecture.

7. 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


Vulnerability
Threats
Risks
Measure the lack of security

8. Security Controls

- Security controls are countermeasures used to prevent or respond to security threats and to reduce or avoid risk.

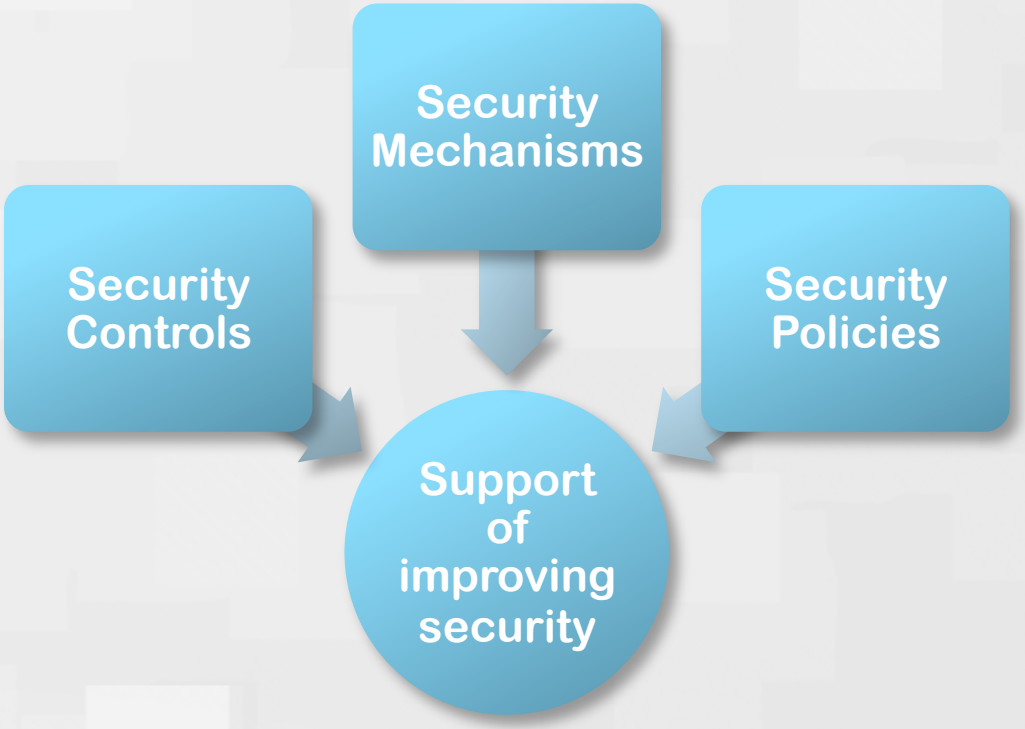
- Details on how to use security countermeasures are typically outlined in the security policy, which contains a set of rules and practices specifying how to implement a system, service, or security plan for maximum protection of sensitive and critical IT resources.

9. Security Mechanisms

- Countermeasures are typically described in terms of security mechanisms, which are components comprising a defensive framework that protects IT resources, information, and services.

10. Security Policies

- A security policy establishes a set of security rules and regulations. Often, security policies will further define how these rules and regulations are implemented and enforced.


Security Mechanisms
Security Controls
Security Policies
Support of improving security

Summary of Key Points

- Confidentiality, integrity, authenticity, and availability are characteristics that can be associated with measuring security.

- Threats, vulnerabilities, and risks are associated with measuring and assessing insecurity, or the lack of security.

- Security controls, mechanisms, and policies are associated with establishing countermeasures and safeguards in support of improving security.

6.2. Threat Agents

- A *threat agent* is an entity that poses a threat because it is capable of carrying out an attack.
- Cloud security threats can originate either internally or externally, from humans or software programs.

Threat agents

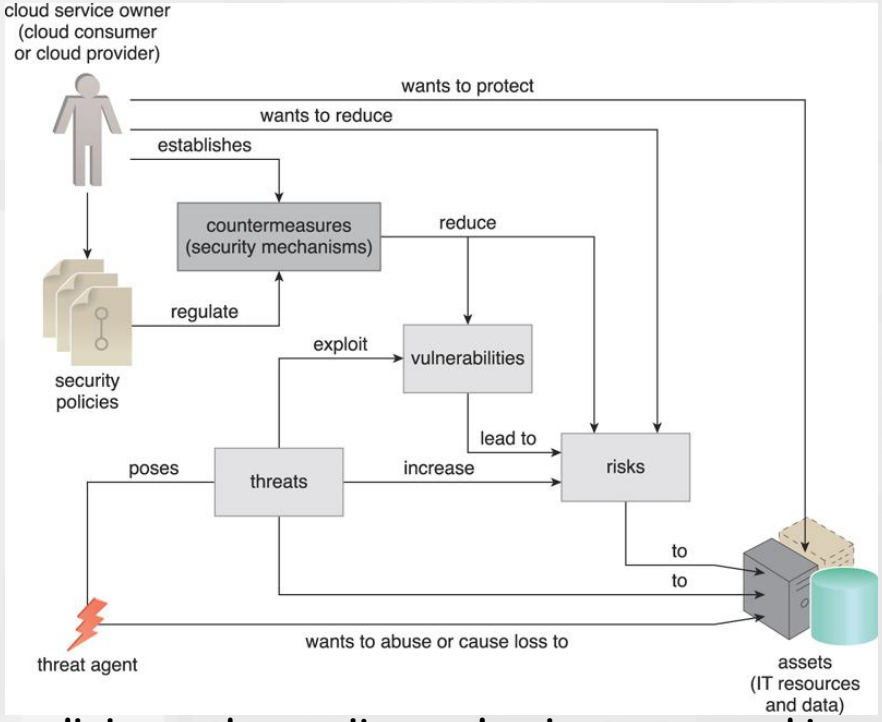


Figure 6.3 How security policies and security mechanisms are used to counter threats, vulnerabilities and risks caused by threat agents.

Anonymous Attacker

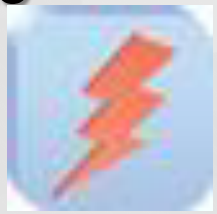
- a non-trusted cloud service consumer without permissions in the cloud .
- It typically exists as an external software program that launches network-level attacks through public networks.

Malicious Service Agent

- A *malicious service agent* is able to intercept and forward the network traffic that flows within a cloud.
- It typically exists as a service agent (or a program pretending to be a service agent) with compromised or malicious logic.
- It may also exist as an external program able to remotely intercept and potentially corrupt message contents.

Trusted Attacker

- shares IT resources in the same cloud environment as the cloud consumer and attempts to exploit legitimate credentials to target cloud providers and the cloud tenants with whom they share IT resources.
- Trusted attackers (also known as *malicious tenants*) can use cloud-based IT resources for a wide range of exploitations, including the hacking of weak authentication processes, the breaking of encryption, the spamming of e-mail accounts, or to launch common attacks, such as denial of service campaigns.



Malicious Insider

- *Malicious insiders* are human threat agents acting on behalf of or in relation to the cloud provider.

Figure 6.7 The notation used for an attack originating from a workstation. The human symbol is optional.

6.3. Cloud Security Threats

- This section introduces several common threats and vulnerabilities in cloud-based environments and describes the roles of the aforementioned threat agents.

1. Traffic Eavesdropping

To be successful, an eavesdropping attack requires a weakened connection between a client and a server that the attacker can exploit to reroute network traffic.

The attacker installs network monitoring software, the "sniffer," on a computer or a server to intercept data as it is transmitted.

Traffic Eavesdropping

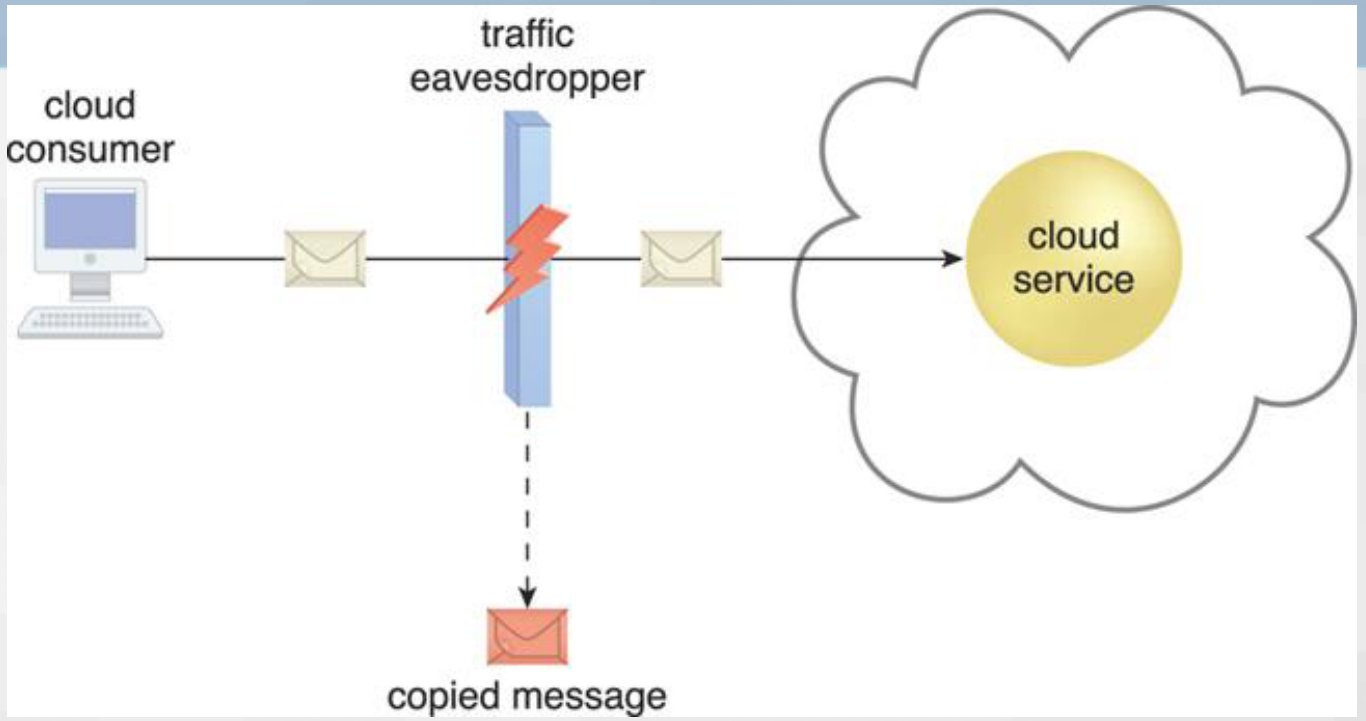


Figure 6.8 An externally positioned malicious service agent carries out a traffic eavesdropping attack by intercepting a message sent by the cloud service consumer to the cloud service. The service agent makes an unauthorized copy of the message before it is sent along its original path to the cloud service.

2. Malicious Intermediary

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

Malicious Intermediary

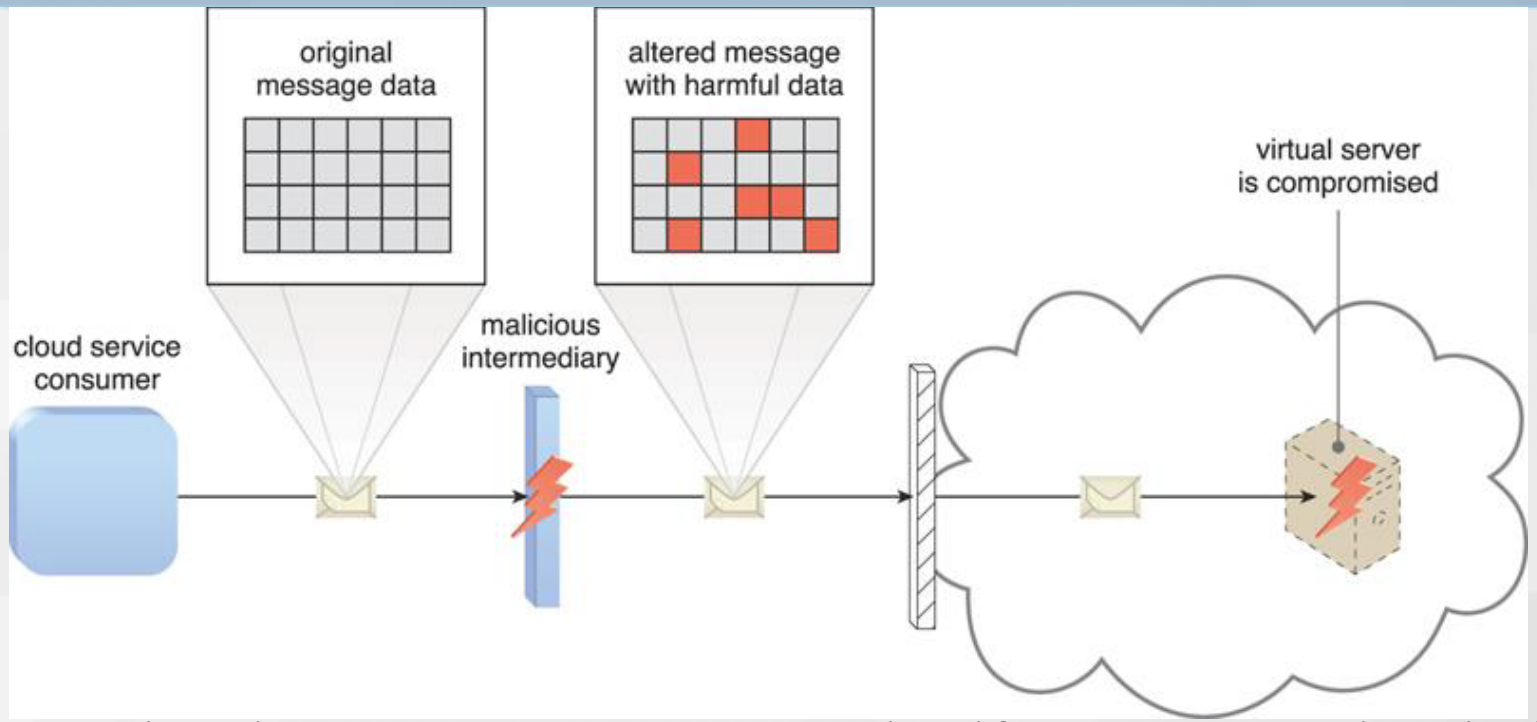


Figure 6.9 The malicious service agent intercepts and modifies a message sent by a cloud service consumer to a cloud service (not shown) being hosted on a virtual server. Because harmful data is packaged into the message, the virtual server is compromised.

3. Denial of Service(thru.flooding)

- The objective of the denial of service (DoS) 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:

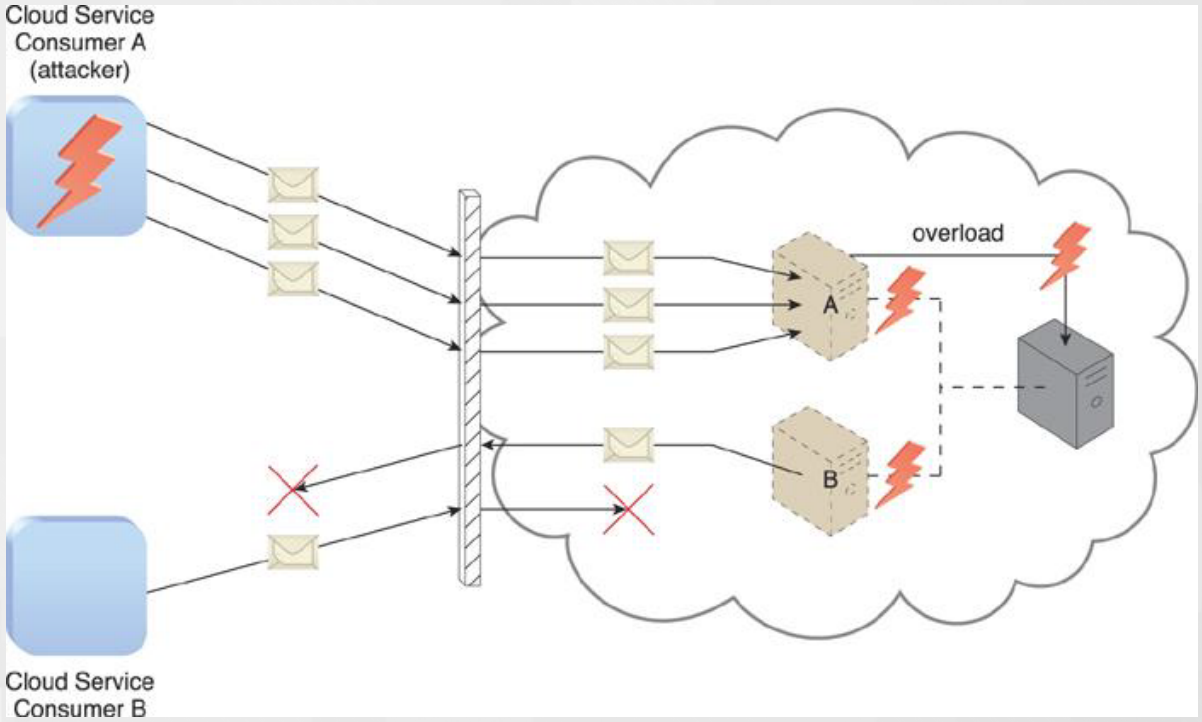
• The workload on cloud services is artificially increased with imitation messages or repeated communication requests.

• 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.

Denial of Service

Figure 6.10 Cloud Service Consumer A sends multiple messages to a cloud service (not shown) hosted on Virtual Server A. This overloads the capacity of the underlying physical server, which causes outages with Virtual Servers A and B. As a result, legitimate cloud service consumers, such as Cloud Service Consumer B, become unable to communicate with any cloud services hosted on Virtual Servers A and B.



4. Insufficient Authorization Attack

- occurs when access is granted to an attacker erroneously or too broadly, resulting in the attacker getting access to IT resources that are normally protected.
- This is often a result of the attacker gaining direct access to IT resources that were implemented under the assumption that they would only be accessed by trusted consumer programs.

Insufficient Authorization Attack

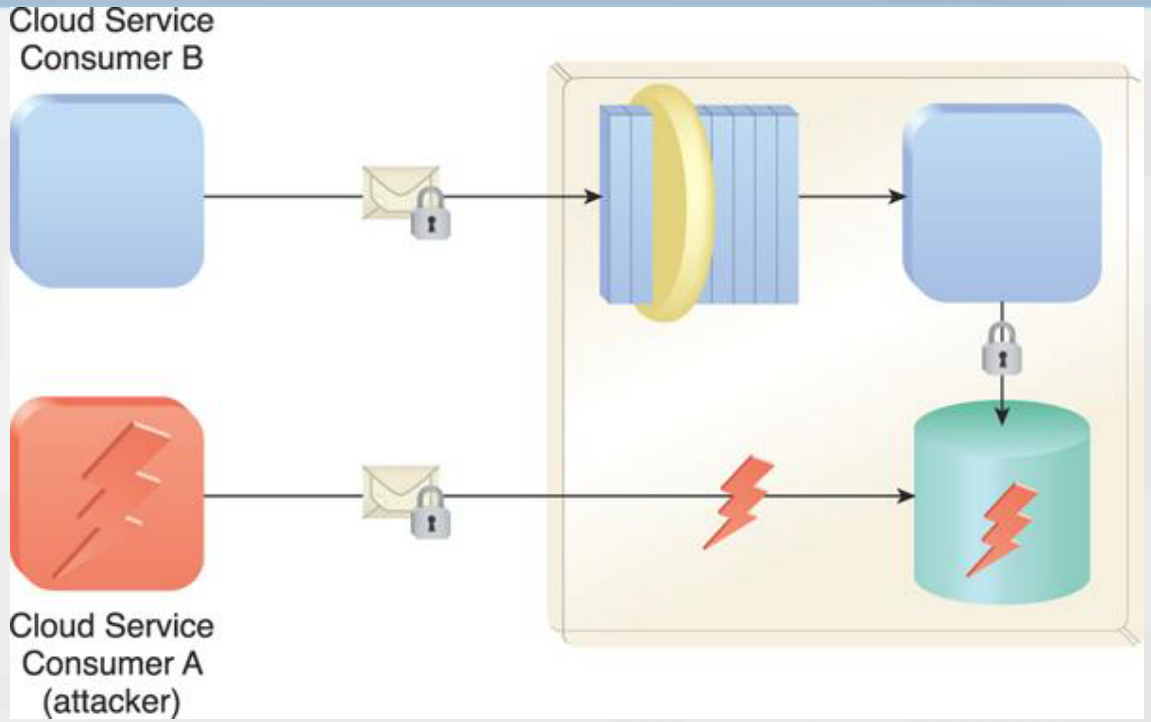


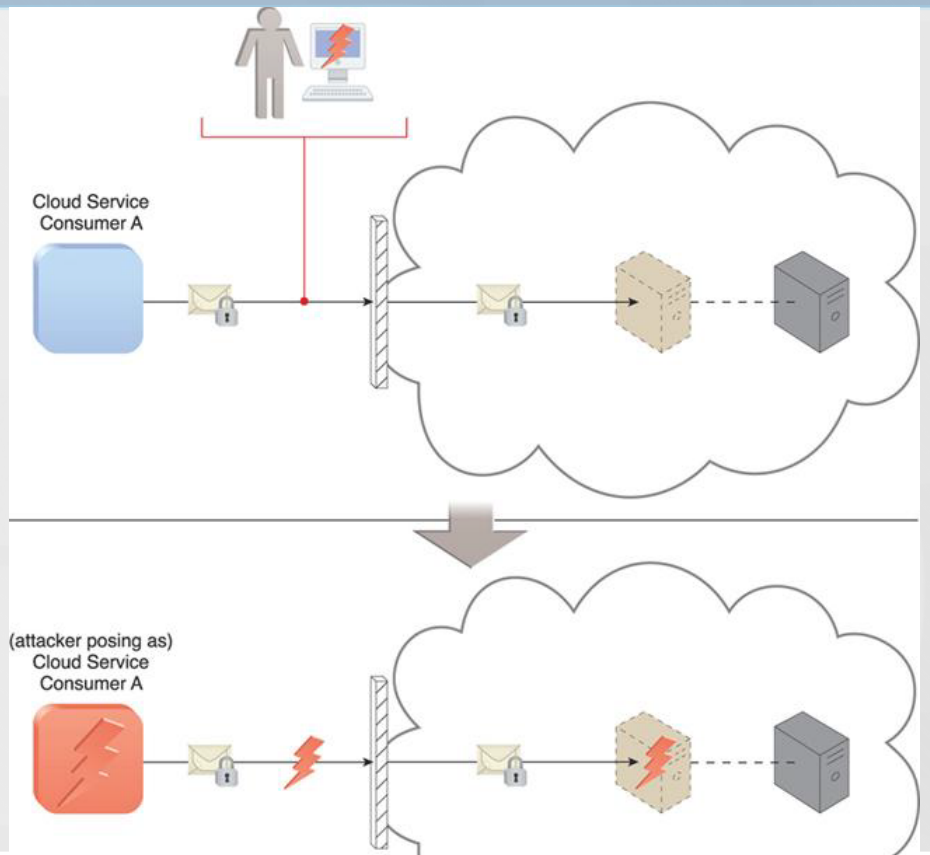
Figure 6.11 Cloud Service Consumer A gains access to a database that was implemented under the assumption that it would only be accessed through a Web service with a published service contract (as per Cloud Service Consumer B).

Insufficient Authorization Attack

- *weak authentication attack:* can result when weak passwords or shared accounts are used to protect IT resources.
- Within cloud environments, these types of attacks can lead to significant impacts depending on the range of IT resources and the range of access to thoseIT resources the attacker gains .

Insufficient Authorization Attack

Figure 6.12 An attacker has cracked a weak password used by Cloud Service Consumer A. As a result, a malicious cloud service consumer (owned by the attacker) is designed to pose as Cloud Service Consumer A in order to gain access to the cloud-based virtual server.



5. Virtualization Attack

- exploits vulnerabilities in the virtualization platform to jeopardize its confidentiality, integrity, and/or availability.
- With public clouds, where a single physical IT resource may be providing virtualized IT resources to multiple cloud consumers, such an attack can have significant repercussions.

Virtualization Attack

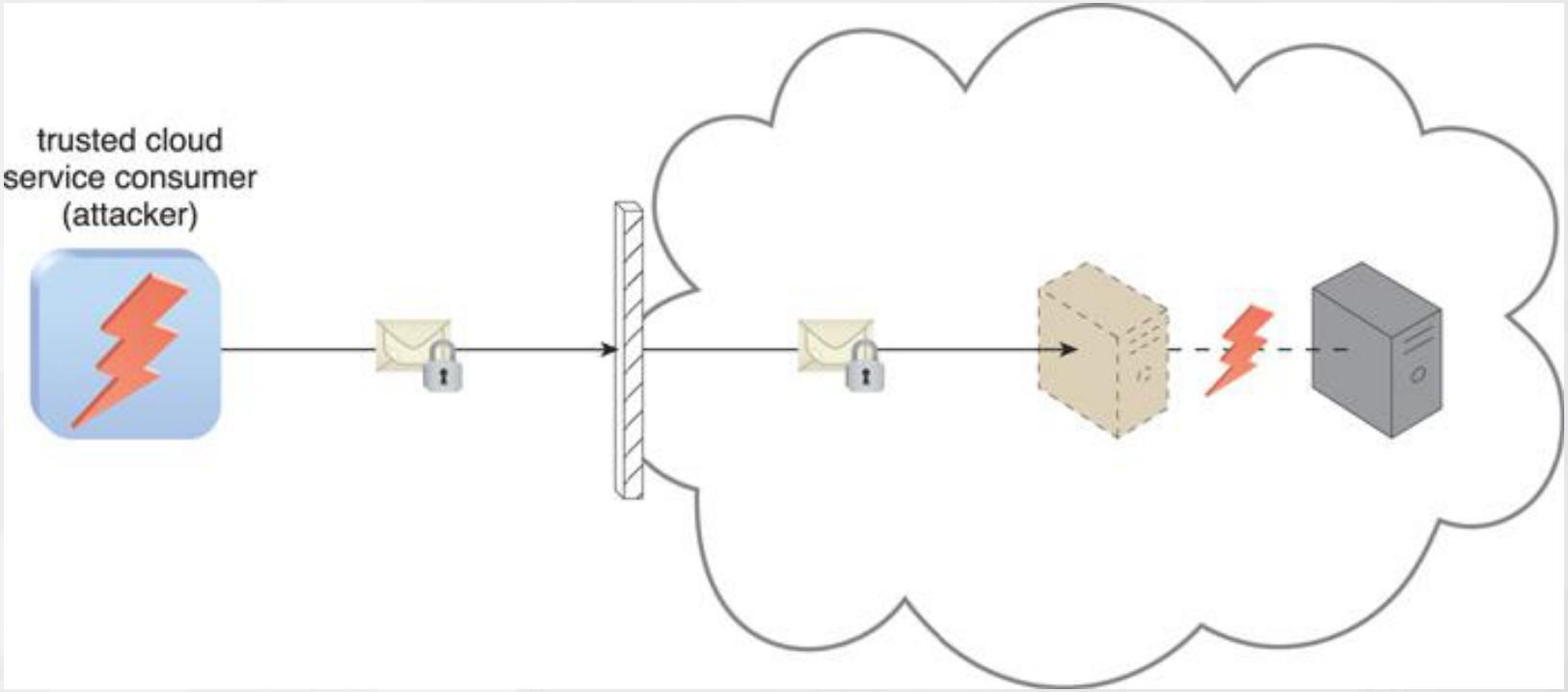


Figure 6.13 An authorized cloud service consumer carries out a virtualization attack by abusing its administrative access to a virtual server to exploit the underlying hardware.

6.Overlapping Trust Boundaries

- If physical IT resources within a cloud are shared by different cloud service consumers, these cloud service consumers have overlapping trust boundaries.
- Malicious cloud service consumers can target shared IT resources with the intention of compromising cloud consumers or other IT resources that share the same trust boundary.

Overlapping Trust Boundaries

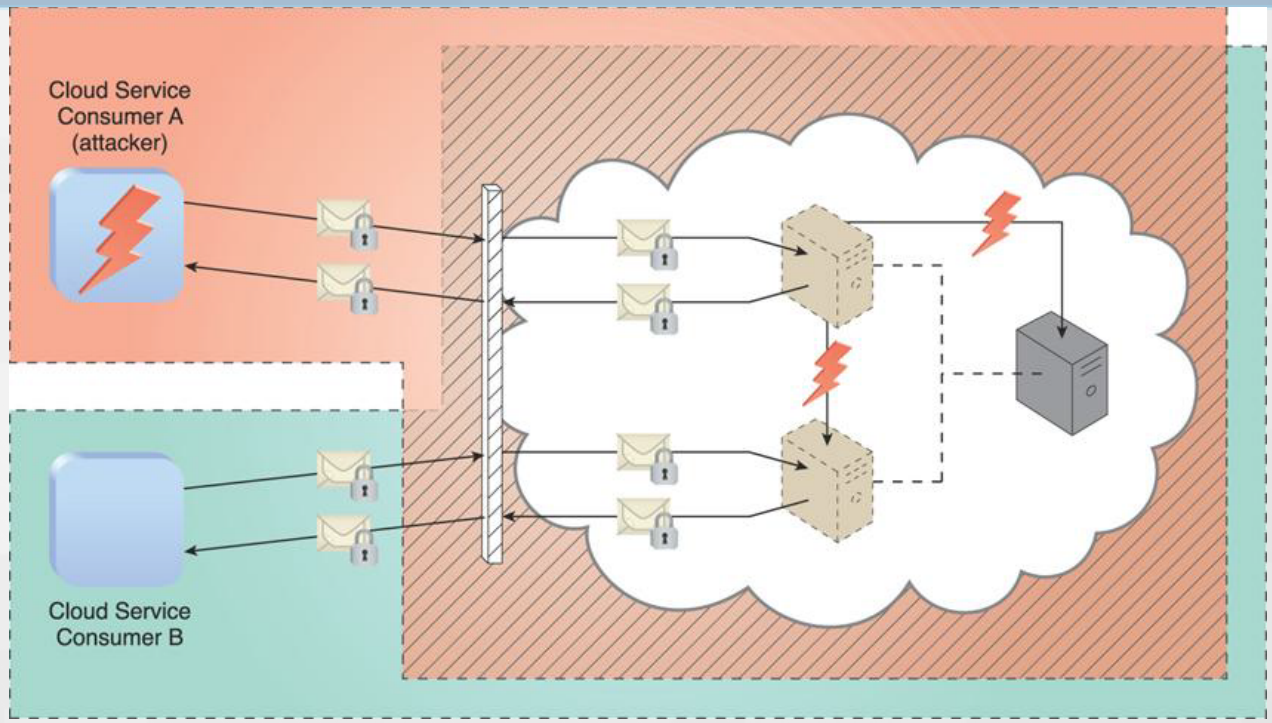


Figure 6.14 Cloud Service Consumer A is trusted by the cloud and therefore gains access to a virtual server, which it then attacks with the intention of attacking the underlying physical server and the virtual server used by Cloud Service Consumer B.

Summary

1. **Traffic Eavesdropping** - Intercept the msg sent by CC
2. **Malicious Intermediary**- altering the original msg and add extra info
3. **DOS** - Sending bulk req .to the point to stop proper functioning.
4. **Insufficient Authorization Attack**-granted access to attackers erroneously
5. **Virtualization Attack**- attack to virt.server in virtulzn. environment
6. **Overlapping trusted boundaries**-sharing of physical IT resource to CC(attacker)

6.4. Additional Considerations

- Cloud consumers need to be aware that they may be introducing security risks by deploying flawed cloud-based solutions.
- An understanding of how a cloud provider defines and imposes proprietary, and possibly incompatible, cloud security policies is a critical part of forming assessment criteria when choosing a cloud provider vendor.

6.4. Additional Considerations

- Liability, indemnity, and blame for potential security breaches need to be clearly defined and mutually understood in the legal agreements signed by cloud consumers and cloud providers.
- It is important for cloud consumers, subsequent to gaining an understanding of the potential security-related issues specific to a given cloud environment, to perform a corresponding assessment of the identified risks.