UNIT-VI: Security in Cloud Computing(Part-I)

Chap-6 from Thomas Erl Book

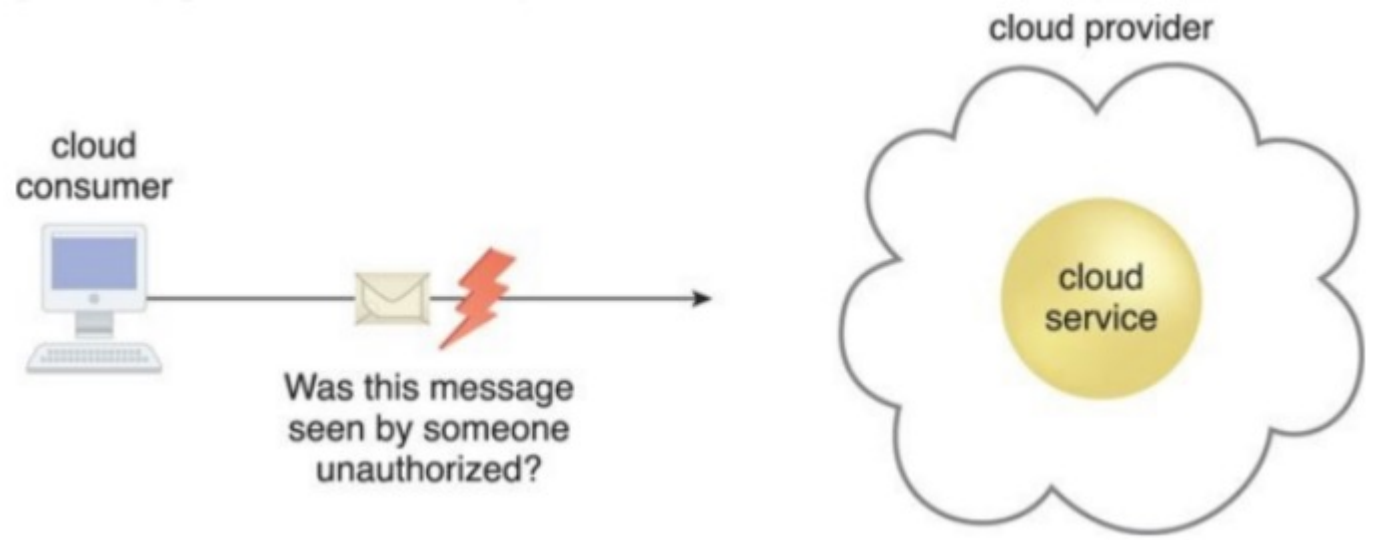
- This chapter introduces terms and concepts that address basic ***information security within clouds***, and then concludes by defining a set of threats and attacks common to ***public cloud environments***.

Basic Terms and Concepts

- Information security is a ***complex ensemble of techniques***, technologies, regulations, and behaviours that ***collaboratively protect the integrity of and access to computer systems and data.***
- IT security measures aim to defend against ***threats and interference that arise from both malicious intent and unintentional user error***.
- The upcoming sections define fundamental security terms relevant to cloud computing and describe associated concepts.

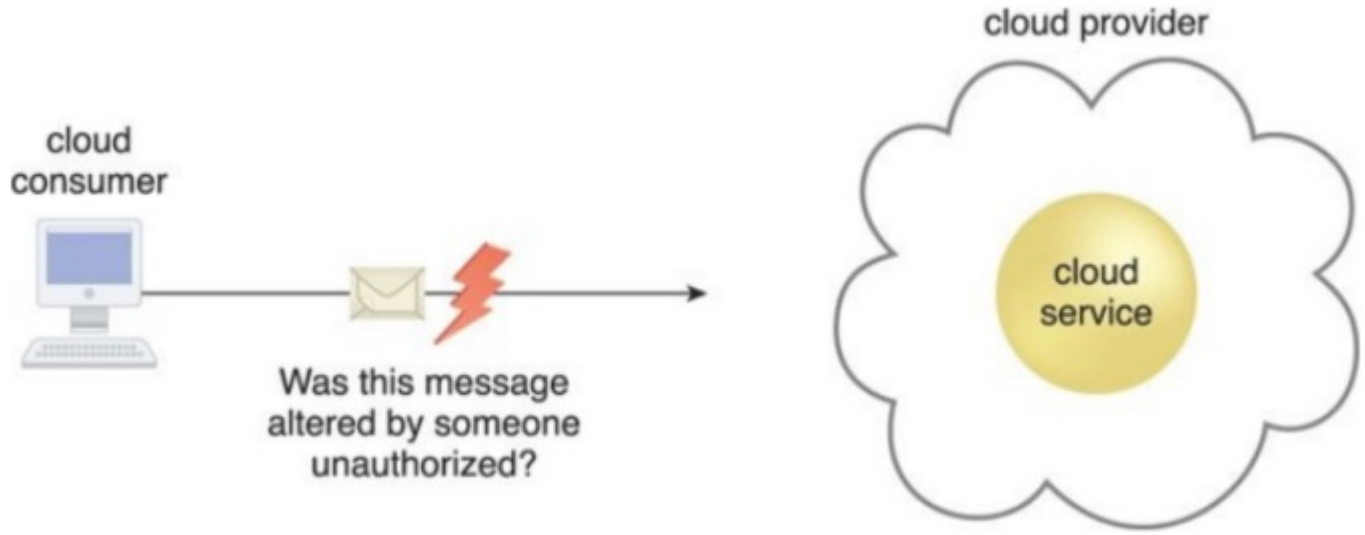
Confidentiality

Confidentiality is the characteristic of something being made accessible only to authorized parties.



Integrity

- Integrity is the characteristic of not having been altered by an unauthorized party.
- 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.



Authenticity

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

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.

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.

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.

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.

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.

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.

For example, the positioning and usage of security controls and mechanisms can be determined by security policies.

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.

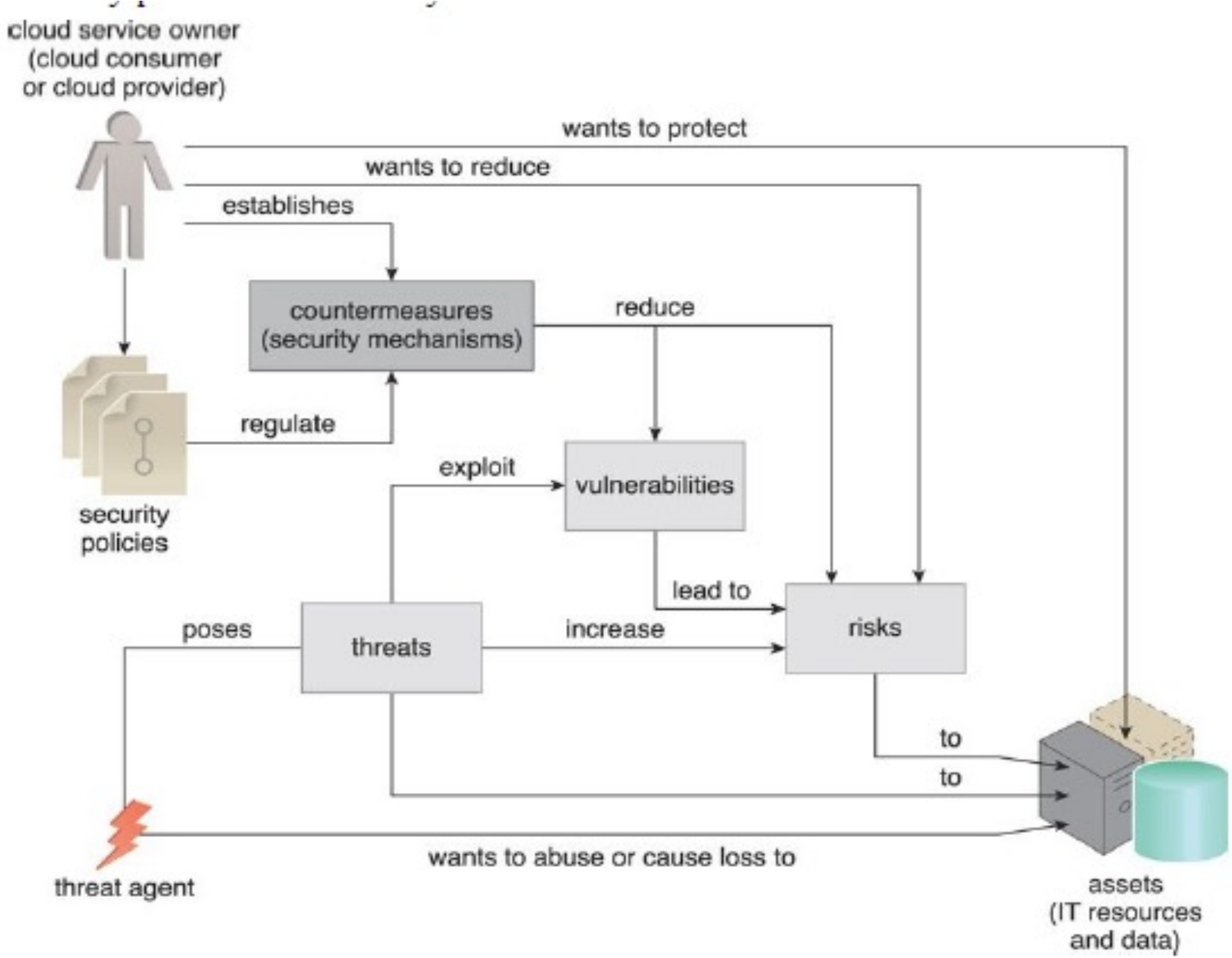
→Security controls, mechanisms, and policies are associated with establishing countermeasures and safeguards in support of improving security.

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.

Figure (in next slide) illustrates the role a threat agent assumes in relation to vulnerabilities, threats, and risks, and the safeguards established by security policies and security mechanisms.



How security policies and security mechanisms are used to counter

threats, vulnerabilities, and risks caused by threat agents.

Anonymous Attacker

An anonymous attacker is 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.***

When anonymous attackers ***have limited information on security policies and defenses***, it can inhibit their ability to formulate effective attacks.

Therefore, ***anonymous attackers often resort to committing acts like bypassing user accounts or stealing user credentials***, while using methods that either ensure anonymity or require substantial resources for prosecution.

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

A 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.

Unlike anonymous attackers (which are non-trusted), trusted attackers usually launch their attacks from within a cloud's trust boundaries by abusing *legitimate credentials or via the appropriation of sensitive and confidential information.*

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*. They are typically *current or former employees or third parties with access to* the cloud provider's premises.
- This type of threat agent carries tremendous damage potential, as the malicious insider may have administrative privileges for accessing cloud consumer IT resources.

Key Points 160

→An anonymous attacker is a non-trusted threat agent that usually attempts attacks from outside of a cloud's boundary.

→A malicious service agent intercepts network communication in an attempt to maliciously use or augment the data.

→A trusted attacker exists as an authorized cloud service consumer with legitimate credentials that it uses to exploit access to cloud-based IT resources.

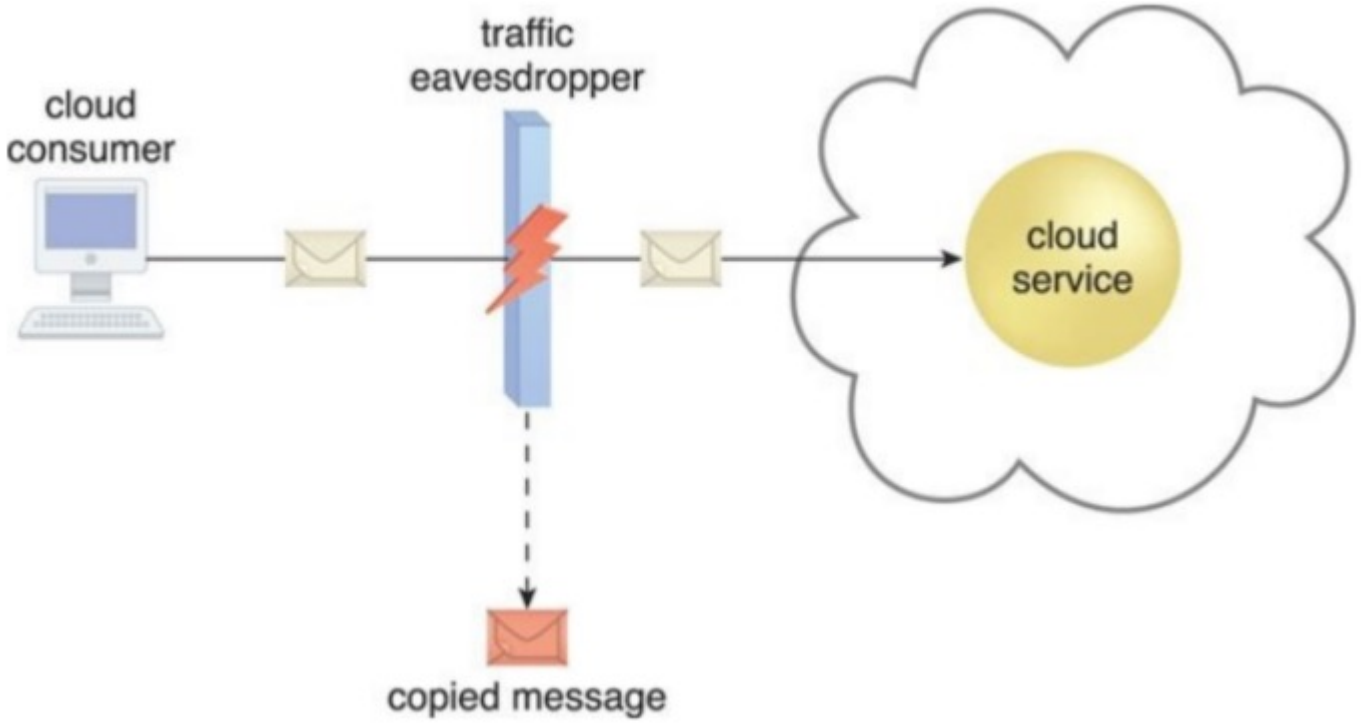
→A malicious insider is a human that attempts to abuse access privileges to cloud premises.

Cloud Security Threats

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

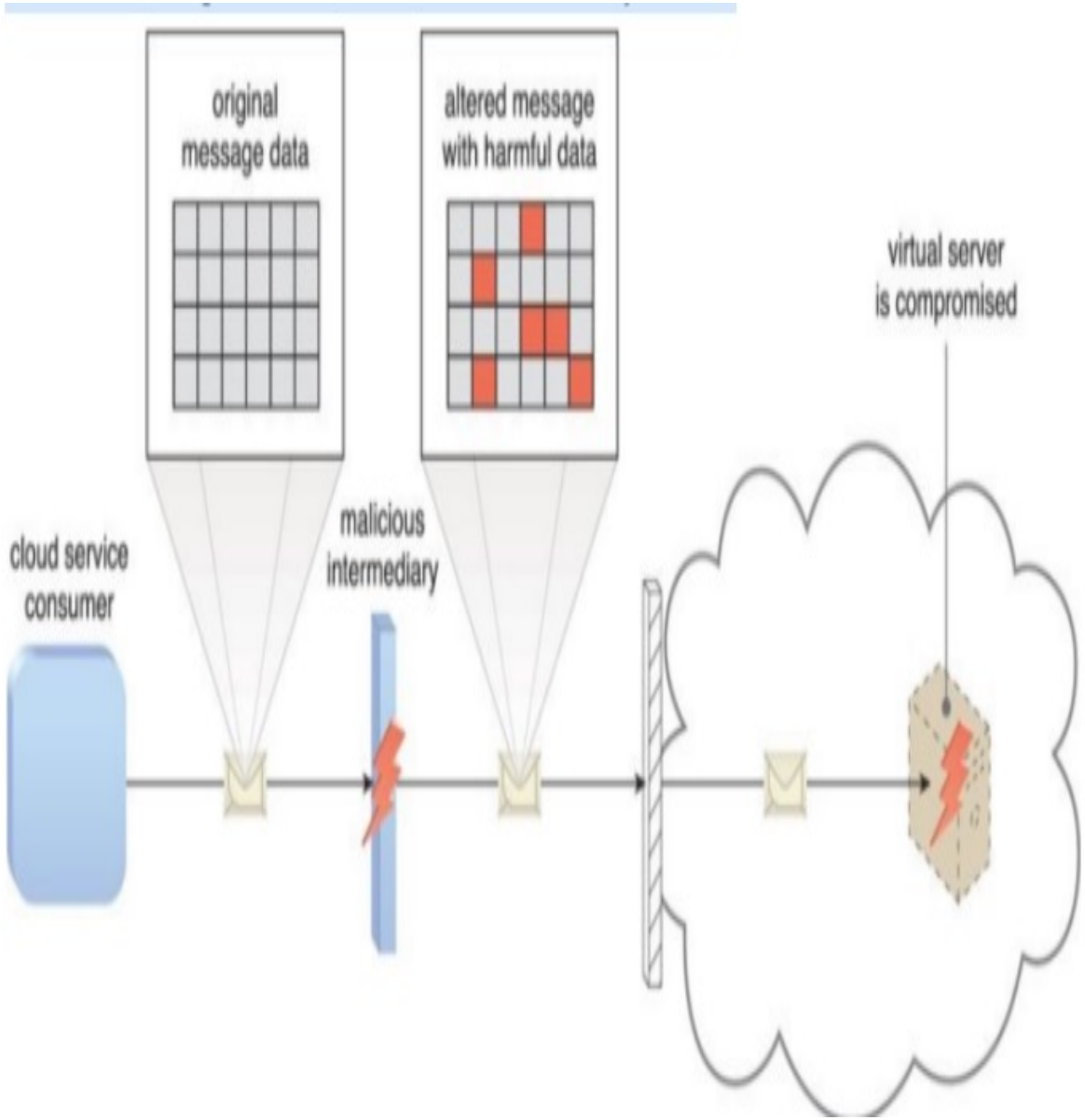
Traffic Eavesdropping

- 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.



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.

The ***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***. It may also insert harmful data into the message before forwarding it to its destination. Figure in the next slide illustrates a common example of the malicious intermediary attack.



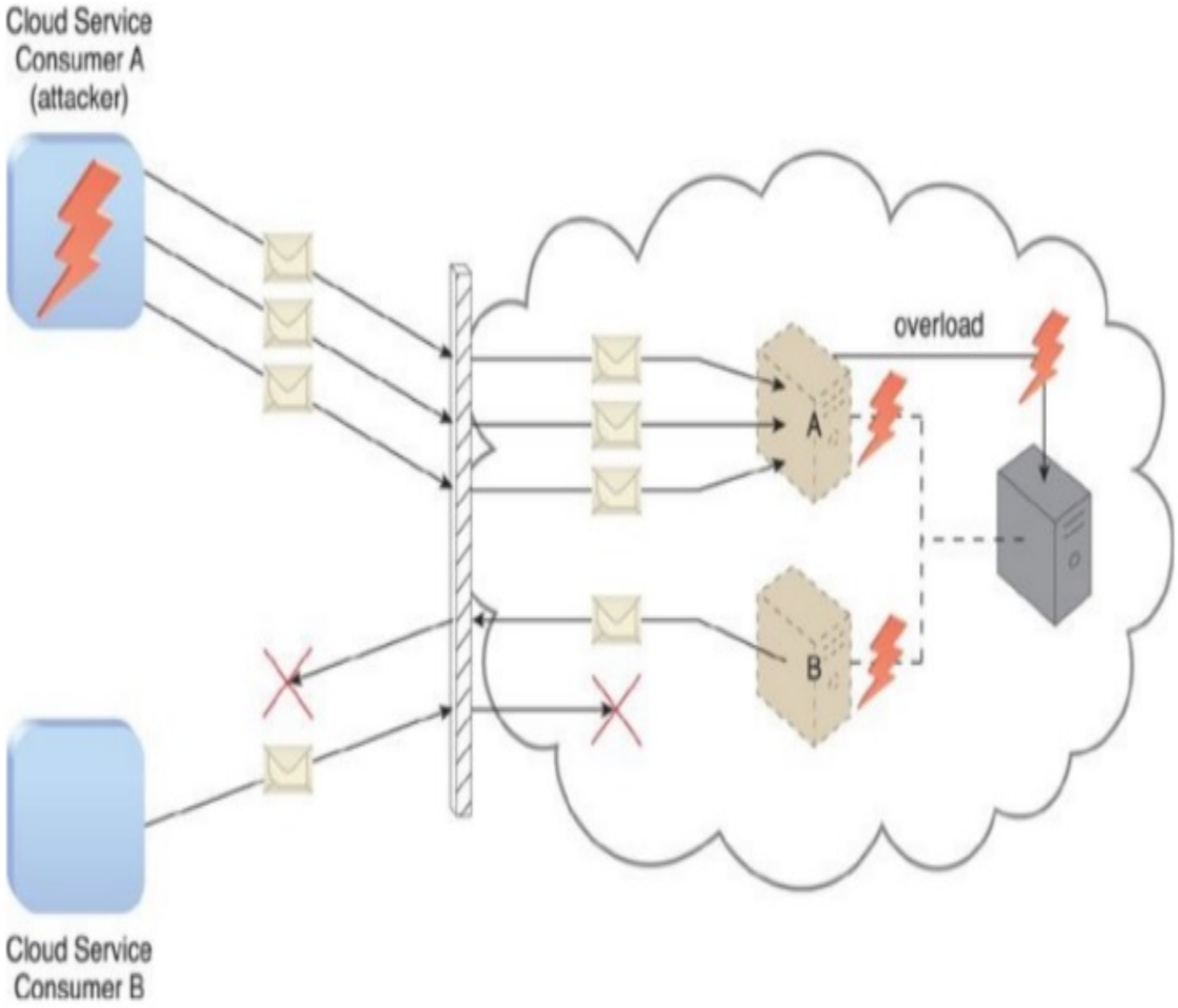
The *malicious service* agent intercepts and modifies a message sent by a cloud service consumer to a cloud service (not shown) being hosted on a virtual server. Because harmful data is packaged into the message, the virtual server is compromised.

Denial of Service

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.

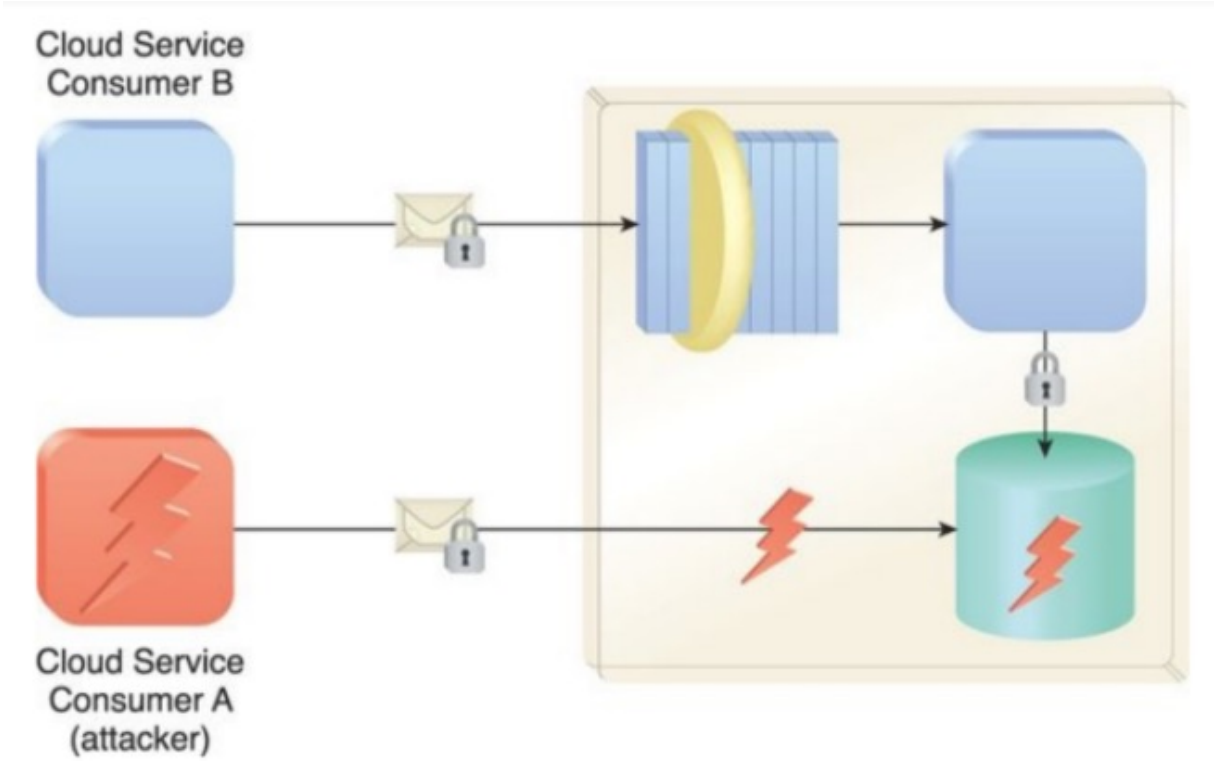
→Successful DoS attacks produce server degradation and/or failure, as illustrated in figure in next slide.



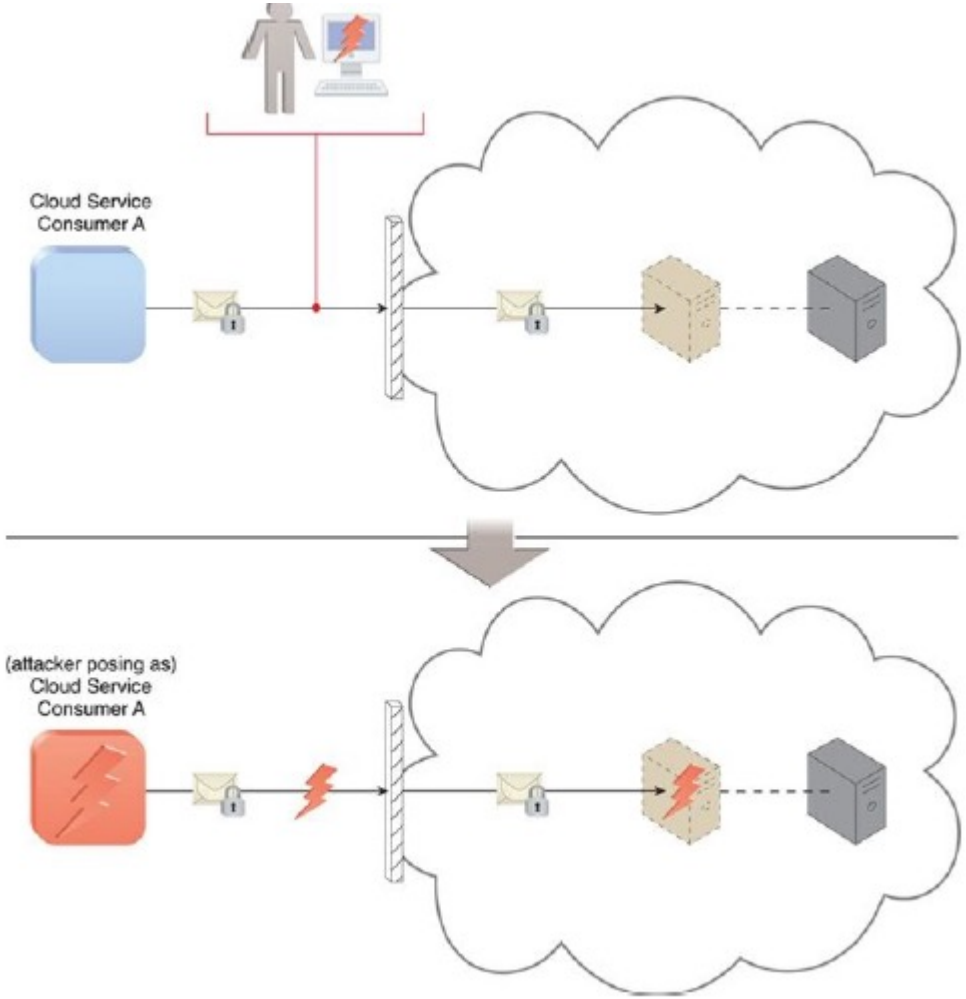
Cloud Service Consumer A sends multiple messages to a cloud service (not shown) hosted on Virtual Server A. This overloads the capacity of the underlying physical server, which causes outages with Virtual Servers A and B. *As a result, legitimate cloud service consumers, such as Cloud Service Consumer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

Insufficient Authorization

- The 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.



A variation of this attack***, known as weak authentication, 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 those IT resources the attacker gains.***



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.

Virtualization Attack

- Virtualization provides multiple cloud consumers with access to IT resources that share underlying hardware but are logically isolated from each other. *Because cloud providers grant cloud consumers administrative access to virtualized IT resources (such as virtual servers), there is an inherent risk that cloud consumers could abuse this access to attack the underlying physical H/W*
- A 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 bad effect.

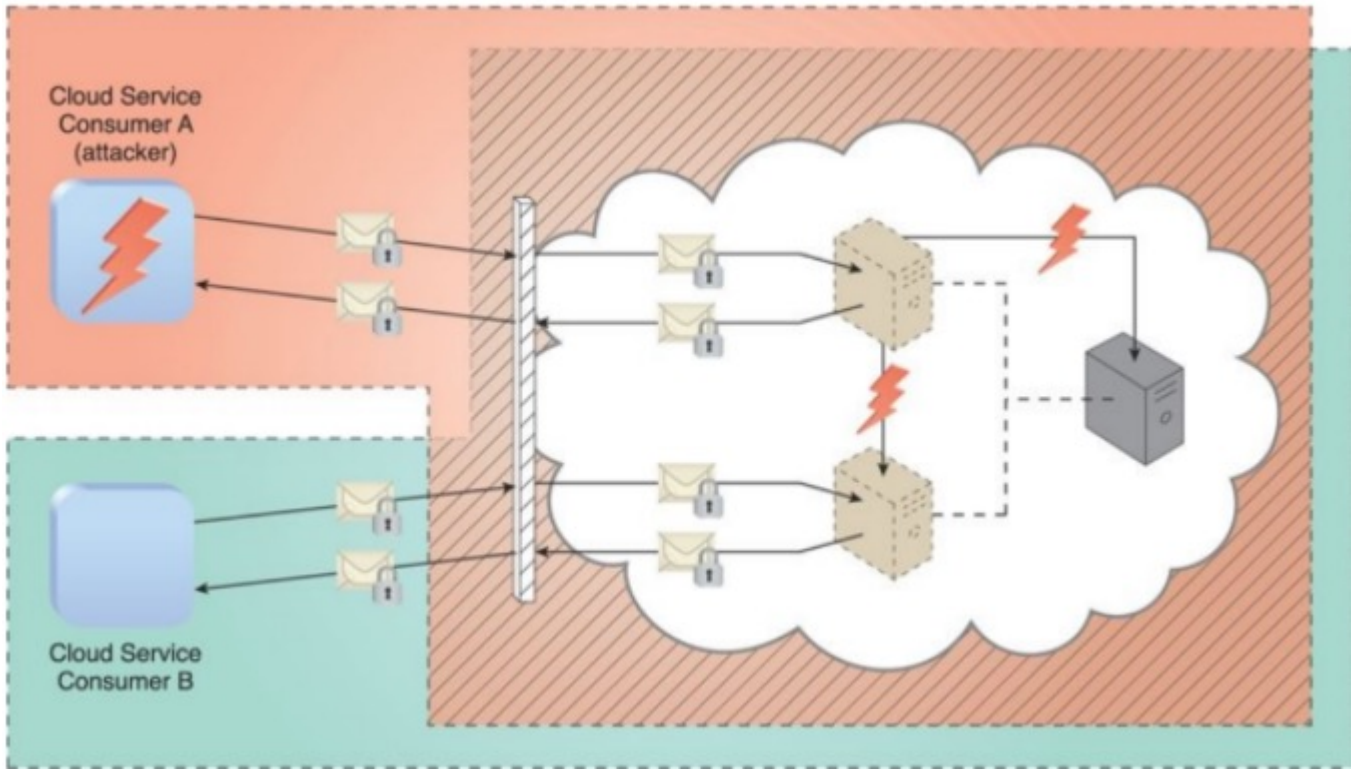
Overlapping Trust Boundaries

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.

The consequence is that some or all of the other cloud service consumers could be impacted by the attack and/or the attacker could use virtual IT resources against others that happen to also share the same trust boundary.

Figure in the next slide illustrates an example in which two cloud service consumers share virtual servers hosted by the same physical server and, resultantly, their respective trust boundaries overlap.



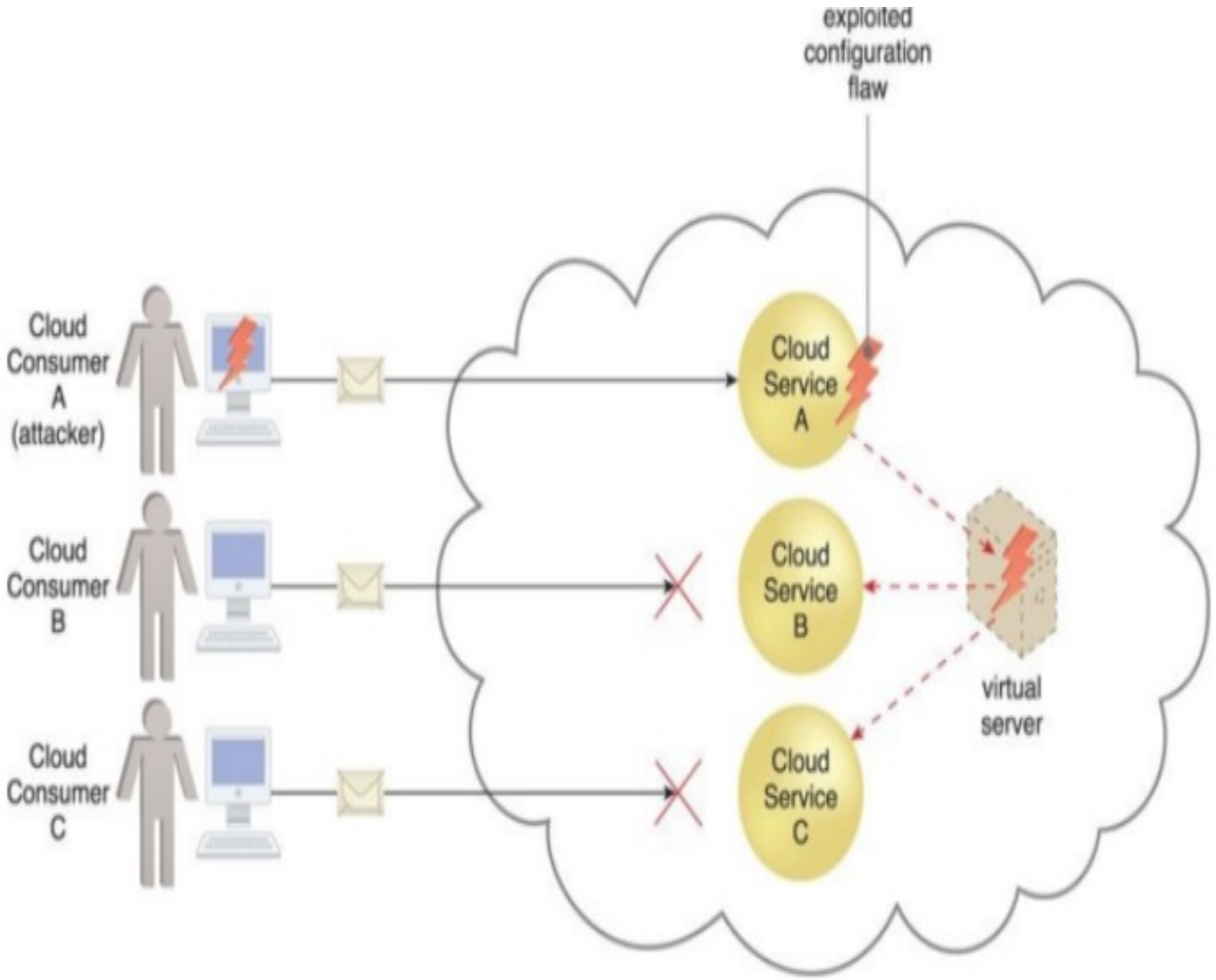
Cloud Service Consumer A is trusted by the cloud and therefore gains access to a virtual server, which it then attacks with the intention of attacking the underlying physical server and the virtual server used by Cloud Service Consumer B.

Additional Considerations

Flawed Implementations:-The substandard design, implementation, or configuration of cloud service deployments can have undesirable ***consequences, beyond runtime exceptions and failures***.

If the cloud provider's software and/or hardware have inherent security flaws or operational weaknesses, attackers can exploit these vulnerabilities to impair the ***integrity, confidentiality, and/or availability of*** cloud provider IT resources and cloud consumer IT resources hosted by the cloud provider.

- Figure in next slide depicts a poorly implemented cloud service that results in a server shutdown. Although in this scenario the ***flaw*** is exposed accidentally by a legitimate cloud service consumer, *it could have easily been discovered and exploited by an attacker.*



Cloud Service Consumer A's message triggers a configuration flaw in Cloud Service A, which in turn causes the virtual server that is also hosting Cloud Services B and C to crash.

Security Policy Disparity

- When a cloud consumer places IT resources with a public cloud provider, it may ***need to accept that its traditional information security approach*** may not be identical or even similar to that of the cloud provider.
- This incompatibility needs to be ***assessed to ensure that any data or other IT assets being relocated to a public cloud are adequately protected.***
- Even when leasing raw infrastructure-based IT resources, the cloud consumer ***may not be granted sufficient administrative control or influence over security policies that apply to the IT resources leased from the cloud provider.***
- This is primarily because those IT resources are still legally owned by the cloud provider and continue to fall under its responsibility.

With some public clouds, additional third parties, such as security brokers and certificate authorities, may ***introduce their own distinct set of security policies and practices, further complicating any attempts to standardize the protection of cloud consumer assets.***

Contracts (Who is responsible for the attack?)

- Cloud consumers need to carefully examine contracts and SLAs put forth by cloud providers ***to ensure that security policies, and other relevant guarantees, are satisfactory when it comes to asset security.***
- There needs *to be clear language that indicates the amount of liability assumed by the cloud provider* and/or the level of indemnity the cloud provider may ask for.
- ***The greater the assumed liability by the cloud provider, the lower the risk to the cloud consumer.***

Another aspect to contractual obligations is where the lines are drawn between cloud consumer and cloud provider assets.

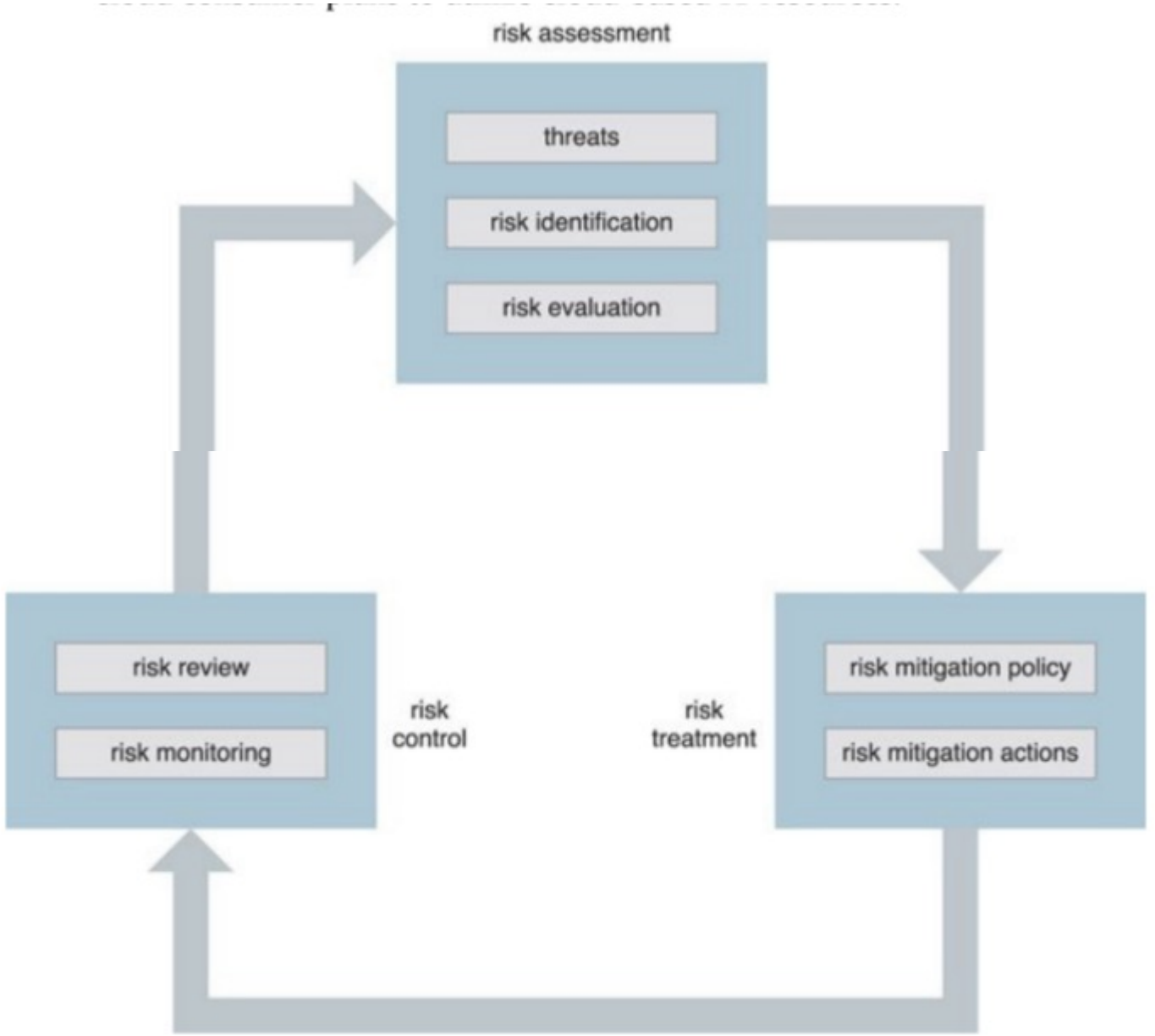
A cloud consumer that deploys its own solution upon infrastructure supplied by the cloud provider will produce a technology architecture comprised of artifacts owned by both the cloud consumer and cloud provider.

If a security breach (or other type of runtime failure) occurs, how is blame determined? Furthermore, if the cloud consumer can apply its own security policies to its solution, but the cloud provider insists that its supporting infrastructure be governed by different (and perhaps incompatible) security policies, how can the resulting disparity be overcome?

Sometimes the best solution is to look for a different cloud provider with more compatible contractual terms.

Risk Management

- When assessing the potential impacts and challenges pertaining to cloud adoption, cloud consumers are encouraged to perform a formal *risk assessment as part of a risk management strategy*.
- A cyclically executed process used to enhance strategic and tactical security, *risk management is comprised of a set of coordinated activities for overseeing and controlling risks.*
- The main activities are generally defined as risk assessment, risk treatment, and risk control.



The on-going risk management process, which can be initiated from any of the three stages.

Risk Assessment

- In the risk assessment stage, the cloud environment is *analyzed to identify potential vulnerabilities and shortcomings* that threats can exploit.
- The cloud provider can be asked to produce statistics and other information about past attacks (successful and unsuccessful) carried out in its cloud.
- The identified risks are quantified and qualified according to the probability of occurrence and the degree of impact in relation to how the cloud consumer plans to utilize cloud-based IT resources.

Risk Treatment

Mitigation policies and plans are designed during the risk treatment stage ***with the intent of successfully treating the risks that were discovered during risk assessment***.

Some risks can be ***eliminated, others can be mitigated***, while others can be dealt with via outsourcing or even incorporated into the insurance and/or operating loss budgets.

The cloud provider itself may agree to assume responsibility as part of its contractual obligations.

Risk Control

- The risk control stage is related to risk monitoring, a three-step process that is comprised of surveying related events, ***reviewing these events to determine the effectiveness of previous assessments and treatments, and identifying any policy adjustment needs.***
- Depending on the nature of the monitoring required, this stage may be carried out or shared by the cloud provider.

Summary of Key Points

- 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.
- 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.

Cloud Security Mechanisms

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.

There are two common forms of encryption known as symmetric encryption and asymmetric encryption.

Symmetric Encryption

Symmetric encryption uses the same key for both encryption and decryption, both of which are performed by authorized parties that use the one shared key. Also known as secret key cryptography, messages that are encrypted with a specific key can be decrypted by only that same key.

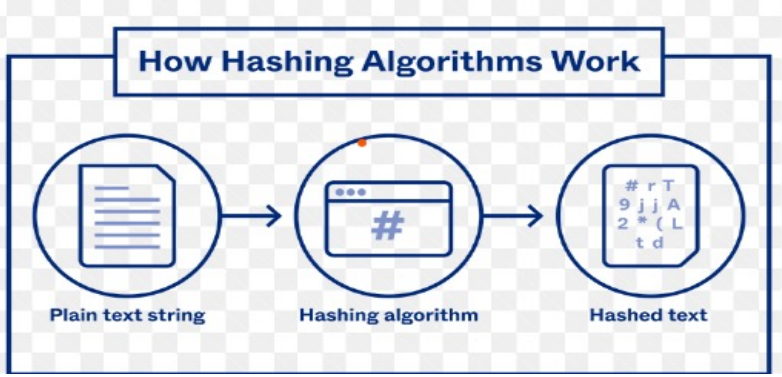
Parties that rightfully decrypt the data are provided with evidence that the original encryption was performed by parties that rightfully possess the key. A basic authentication check is always performed, because only authorized parties that own the key can create messages. This maintains and verifies data confidentiality.

Asymmetric Encryption

- Asymmetric encryption relies on the use of two different keys, namely a private key and a public key. With asymmetric encryption (which is also referred to as public key cryptography), the private key is known only to its owner while the public key is commonly available.

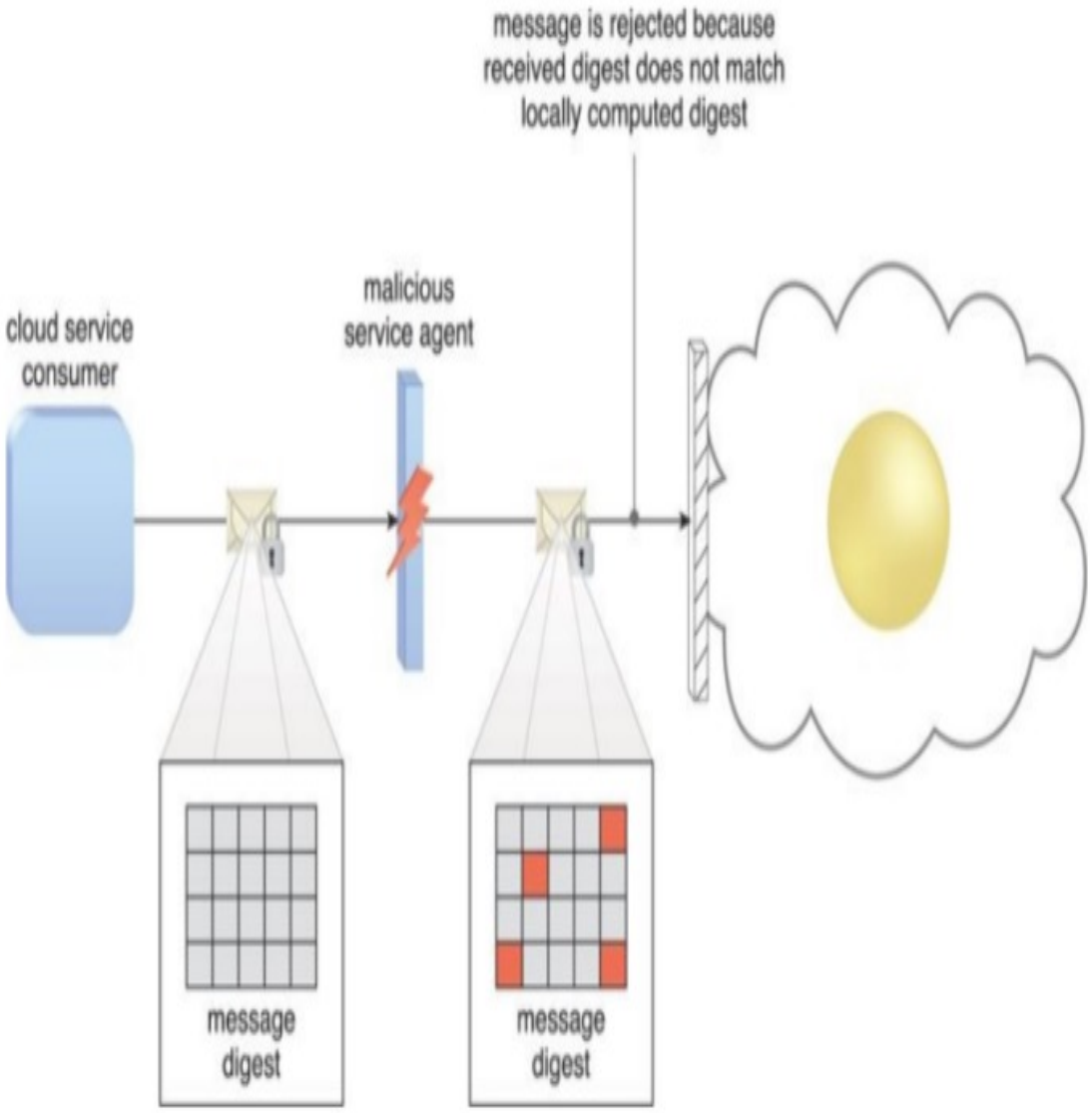
Hashing

A hash function is a mathematical function or algorithm that simply **takes a variable number of characters (called a "message") and converts it into a string with a fixed number of characters** (called a hash value or simply, a hash).



- 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.***
- A common application of this mechanism is the storage of passwords.
- 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.

- In addition to its utilization for protecting stored data, the cloud threats that can be mitigated by the hashing mechanism include malicious intermediary and insufficient authorization. An example of the latter is illustrated in Figure in the next slide.



→A hashing function is applied to protect the integrity of a message that is intercepted and altered by a malicious service agent, before it is forwarded.

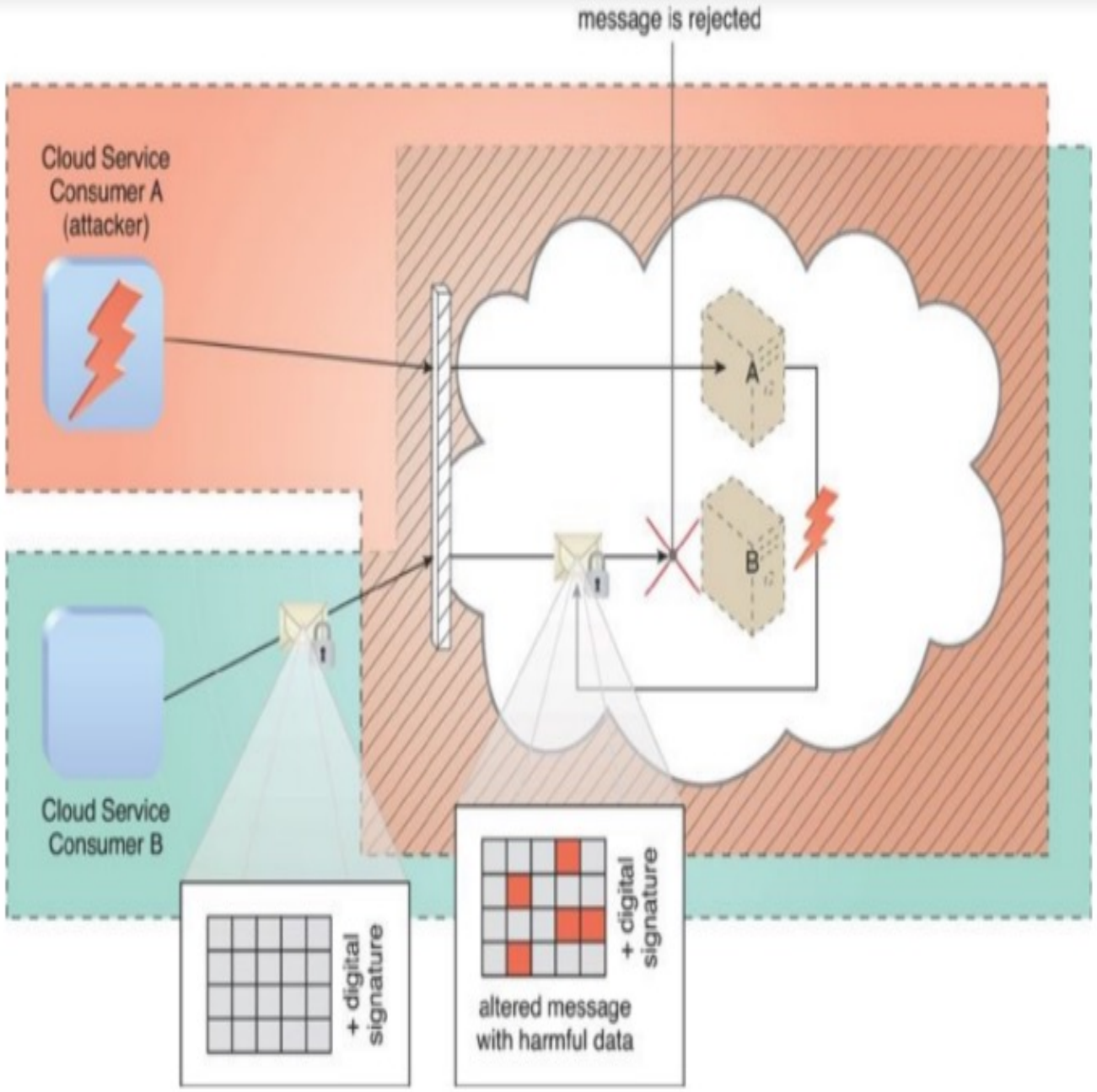
→The firewall can be configured to determine that the message has been altered, thereby enabling it to reject the message before it can proceed to the cloud service.

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.

[More specifically, it is the inability to refute responsibility. For **example**, if you take a pen and sign a (legal) contract your signature is a **nonrepudiation** device. You cannot later disagree to the terms of the contract or refute ever taking party to the agreement.]

- Both hashing and asymmetrical encryption are involved in the creation of a digital signature, which essentially exists as a message digest that was encrypted by a private key and appended to the original message.
- The recipient verifies the signature validity and uses the corresponding public key to decrypt the digital signature, which produces the message digest.
- The hashing mechanism can also be applied to the original message to produce this message digest.
- Identical results from the two different processes indicate that the message maintained its integrity.



Cloud Service Consumer B sends a message that was digitally signed but was altered by trusted attacker Cloud Service Consumer A. Virtual Server B is configured to verify digital signatures before processing incoming messages even if they are within its trust boundary. The message is revealed as illegitimate due to its invalid digital signature, and is therefore rejected by Virtual Server B.

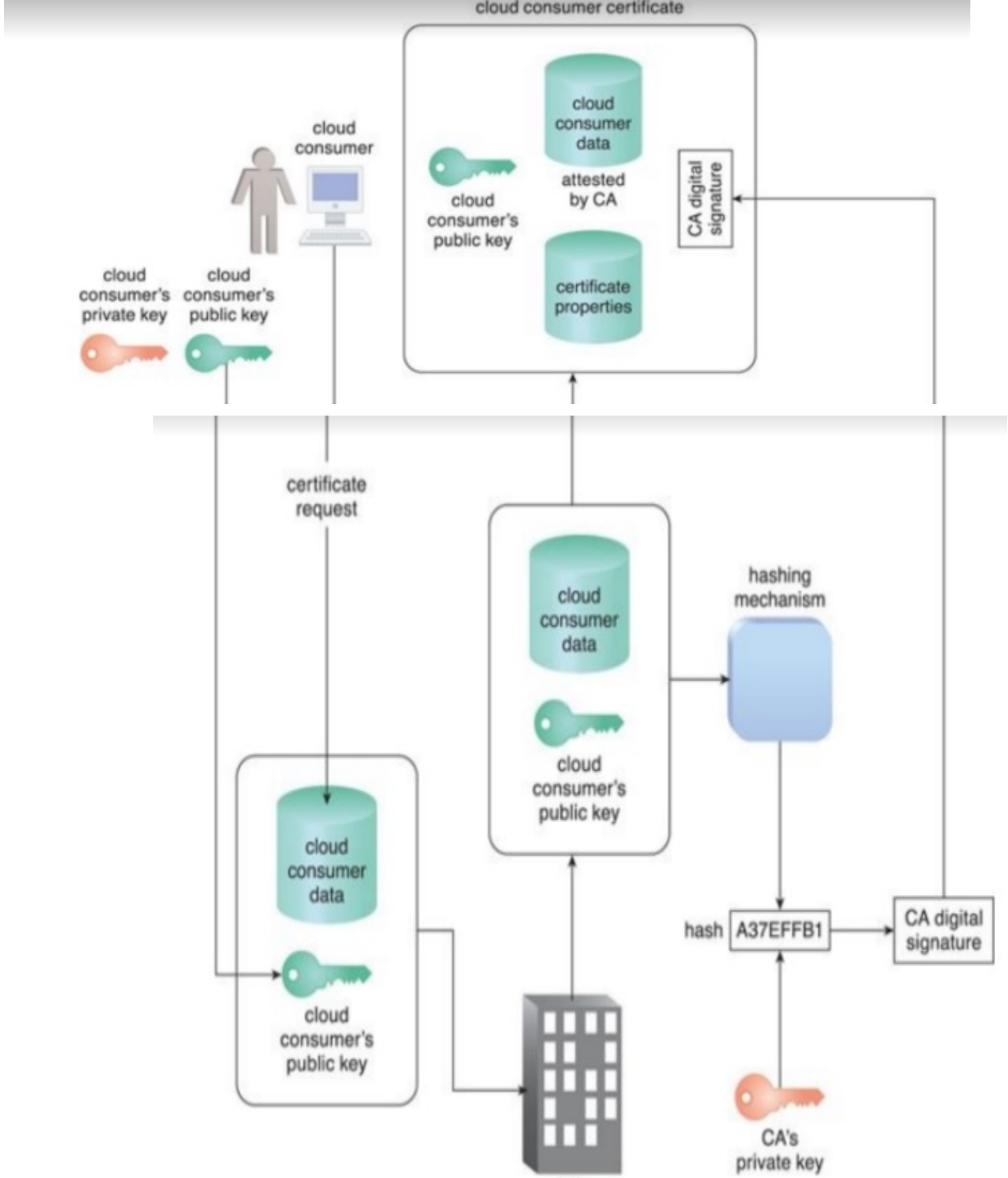
Public Key Infrastructure (PKI)

A common approach for managing the issuance of asymmetric keys is based on the public key infrastructure (PKI) mechanism, which exists as a system of protocols, data formats, rules, and practices that enable large-scale systems to securely use public key cryptography.

This system is used to associate public keys with their corresponding key owners (known as public key identification) while enabling the verification of key validity.

PKIs rely on the use of digital certificates, which are digitally signed data structures that bind public keys to certificate owner identities, as well as to related information, such as validity periods.

Digital certificates are usually digitally signed by a third-party certificate authority (CA), as illustrated in next slide.



The common steps involved during the generation of certificates by a certificate authority.

- Other methods of generating digital signatures can be employed, even though the majority of digital certificates are issued by only a handful of trusted CAs like VeriSign and Comodo.
- Larger organizations, such as Microsoft, can act as their own CA and issue certificates to their clients and the public, since even individual users can generate certificates as long as they have the appropriate software tools.

Building up an acceptable level of trust for a CA is time-intensive but necessary.

Rigorous security measures, substantial infrastructure investments, and stringent operational processes all contribute to establishing the credibility of a CA. ***The higher its level of trust and reliability, the more esteemed and reputable its certificates***.

The PKI is a dependable method for ***implementing asymmetric encryption, managing cloud consumer and cloud provider identity information, and helping to defend against the malicious intermediary and insufficient authorization threats.***

The PKI mechanism is primarily used to counter the insufficient authorization threat.

Identity and Access Management (IAM)

The 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. Specifically, IAM mechanisms exist as systems comprised of four main components:

- ***Authentication*** – Username and password combinations remain the most common forms of user authentication credentials managed by the IAM system, which also can support digital signatures, digital certificates, biometric hardware (fingerprint readers), specialized software (such as voice analysis programs), and locking user accounts to registered IP or MAC addresses.
- ***Authorization*** – The authorization component defines the correct granularity for access controls and oversees the relationships between identities, access control rights, and IT resource availability.
- ***User Management*** – Related to the administrative capabilities of the system, the user management program is responsible for creating new user identities and access groups, resetting passwords, defining password policies, and managing privileges.
- ***Credential Management*** – The credential management system establishes identities and access control rules for defined user accounts, which mitigates the threat of insufficient authorization.

Although its objectives are similar to those of the PKI mechanism, the IAM mechanism's scope of implementation is distinct because its structure encompasses access controls and policies in addition to assigning specific levels of user privileges.

The IAM mechanism is primarily used to counter the insufficient authorization, denial of service, and overlapping trust boundaries threats.

Single Sign-On (SSO)

Propagating the authentication and authorization information for a cloud service consumer ***across multiple cloud services can be a challenge, especially if numerous cloud services or cloud-based IT resources need to be invoked as part of the same overall runtime activity.***

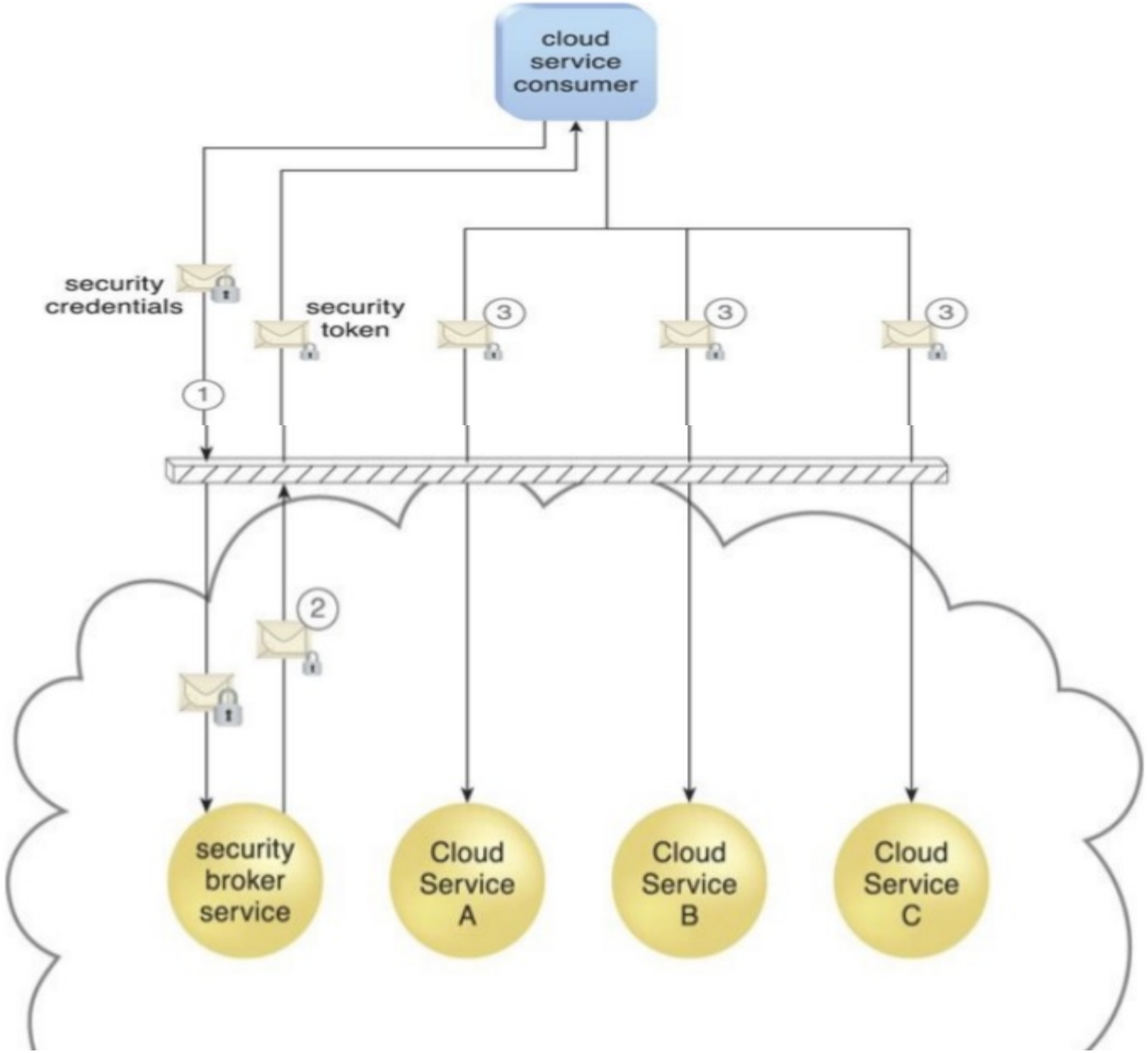
The single sign-on (SSO) mechanism enables one cloud service ***consumer to be authenticated by a security broker, which establishes a security context that is persisted while the cloud service consumer accesses other cloud services or cloud-based IT resources.***

Otherwise, the cloud service consumer would need to re-authenticate itself with every subsequent request.

Note: Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

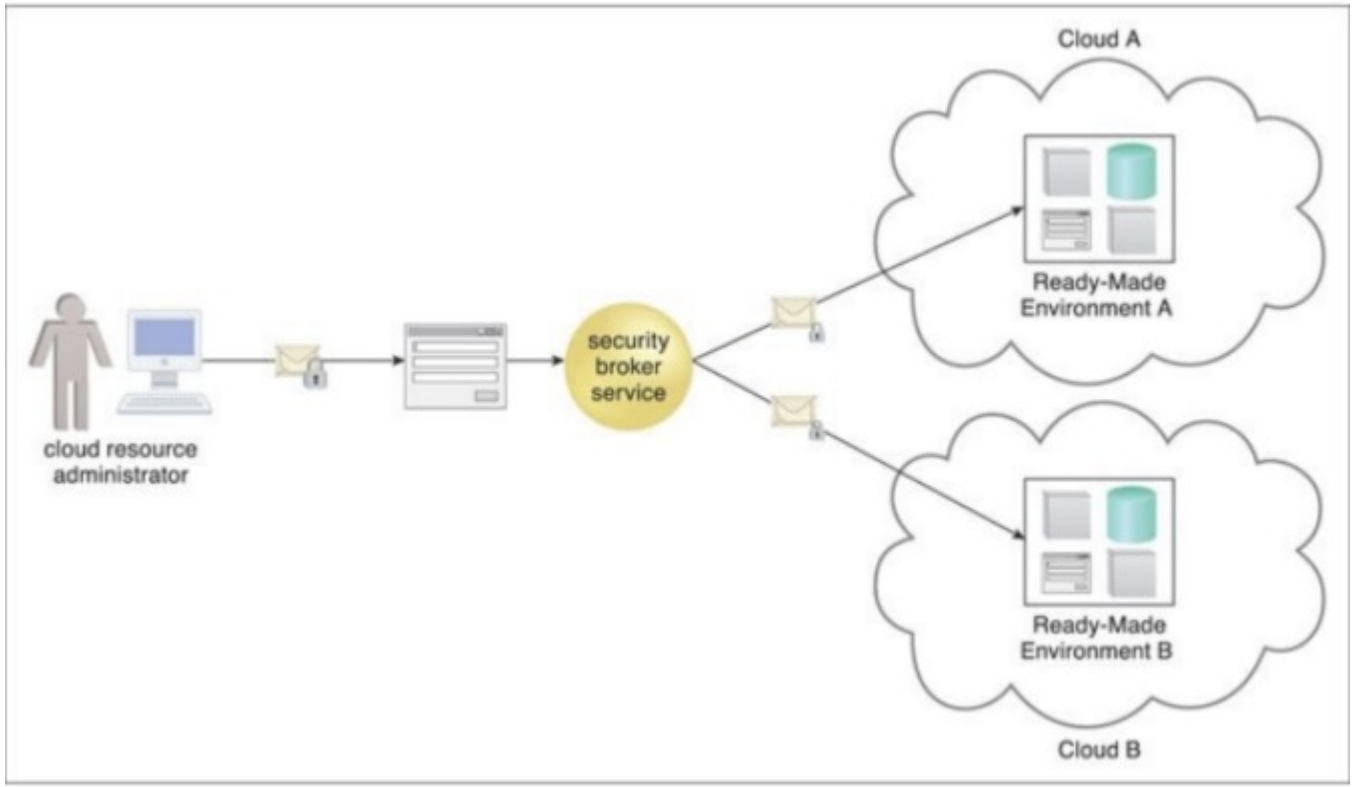
The SSO mechanism essentially *enables mutually independent cloud services and IT resources to generate and circulate runtime authentication and authorization credentials.*

The credentials initially provided by the cloud service consumer remain valid for the duration of a session, while its security context information is shared (diagram in the next slide)



A cloud service consumer provides the security broker with login credentials (1). The security broker responds with an authentication token (message with small lock symbol) upon successful authentication, which contains cloud service consumer identity information (2) that is used to automatically authenticate the cloud service consumer across Cloud Services A, B, and C (3).

- The SSO mechanism's security broker is especially useful when a cloud service consumer needs to access cloud services residing on different clouds.



The credentials received by the security broker are propagated to ready-made environments across two different clouds. The security broker is responsible for selecting the appropriate security procedure with which to contact each cloud.

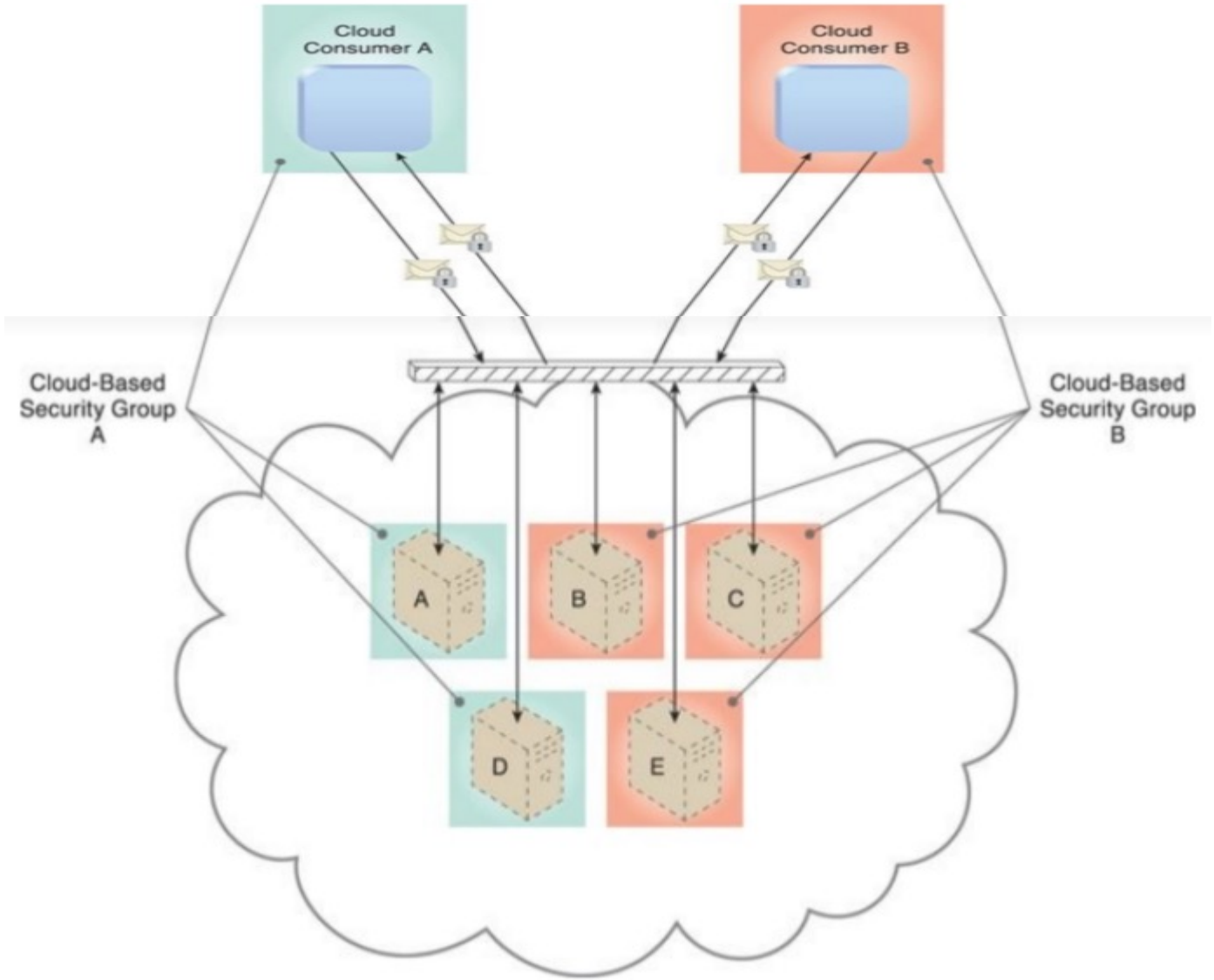
Cloud-Based Security Groups

- Cloud resource segmentation is a process by which separate physical and virtual IT environments are created for different users and groups. ***For example, an organization's WAN can be partitioned according to individual network security requirements.***
- One network can be established with a resilient firewall for external Internet access, while a second is deployed without a firewall because its users are internal and unable to access the Internet.

- Resource segmentation is used to enable virtualization by allocating a variety of physical IT resources to virtual machines.
- It needs to be optimized for public cloud environments, since organizational trust boundaries from different cloud consumers overlap when sharing the same underlying physical IT resources.
- The cloud-based resource segmentation process creates cloud-based security group mechanisms that are determined through security policies.
- Networks are segmented into logical cloud-based security groups that form logical network perimeters.
- Each cloud-based IT resource is assigned to at least one logical cloud-based security group.
- Each logical cloud-based security group is assigned specific rules that govern the communication between the security groups.

Multiple virtual servers running on the same physical server can become members of different logical cloud-based security groups (Figure in the next slide).

Virtual servers can further be separated into public-private groups, development- production groups, or any other designation configured by the cloud resource administrator.



Cloud-Based Security Group A encompasses Virtual Servers A and D and is assigned to Cloud Consumer A. Cloud-Based Security Group B is comprised of Virtual Servers B, C, and E and is assigned to Cloud Consumer B.

If Cloud Service Consumer A's credentials are compromised, the attacker would only be able to access and damage the virtual servers in Cloud-Based Security Group A, thereby protecting Virtual Servers B, C, and E.

Cloud-based security groups delineate areas where different security measures can be applied.

Properly implemented cloud-based security groups help limit unauthorized access to IT resources in the event of a security breach.

This mechanism can be used to help counter the denial of service, insufficient authorization, and overlapping trust boundaries threats, and is closely related to the logical network perimeter mechanism.

Hardened Virtual Server Images

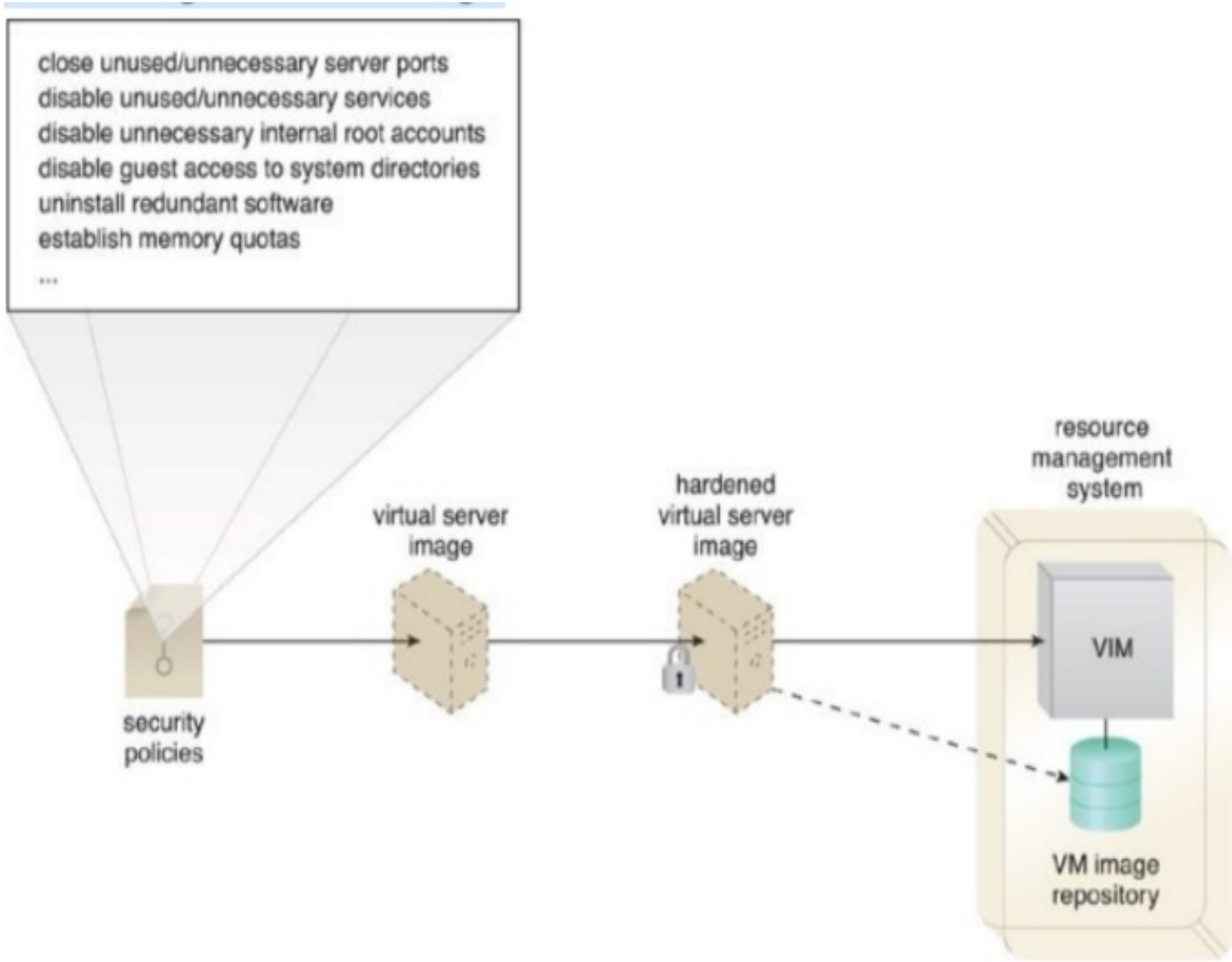
A virtual server is created from a template configuration called a virtual server image (or virtual machine image).

Hardening is the process of stripping unnecessary software from a system to limit potential vulnerabilities that can be exploited by attackers.

Removing redundant programs, closing unnecessary server ports, and disabling unused services, internal root accounts, and guest access are all examples of hardening.

A hardened virtual server image is a template for virtual service instance creation that has been subjected to a hardening process (Figure in the next slide).

This generally results in a virtual server template that is significantly more secure than the original standard image.



About the figure: A cloud provider applies its security policies to harden its standard virtual server images. The hardened image template is saved in the VM images repository as part of a resource management system.

Hardened virtual server images help counter the denial of service, insufficient authorization, and overlapping trust boundaries threats.

- UNIT ends here