Cloud Computing & its Applications

Course Code: SWE4004

Dr Sunil Kumar Singh

Assistant Professor

School - SCOPE

VIT-AP University

sunil.singh@vitap.ac.in

Cabin - AB2 (124D)

Fundamental Cloud Security & Mechanisms

Outline

Security mechanisms that can be used to counter and prevent the threats including the following:

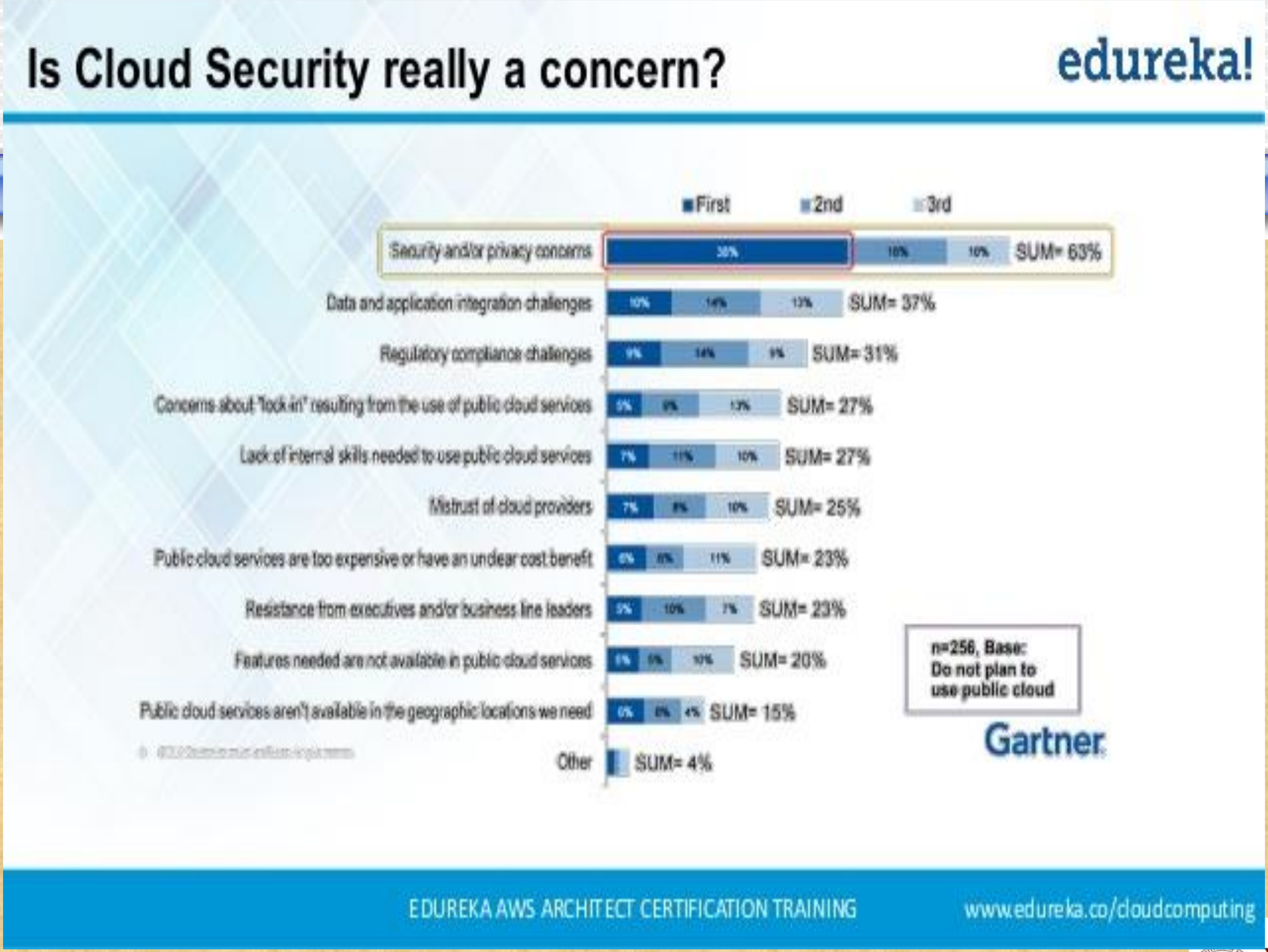
- **Basic terms and concepts**
- **Threat agents and Cloud security threats**
- **Encryption, Hashing and Digital Signature**
- **Public Key Infrastructure (PKI)**
- **Identity and Access Management (IAM)**
- **Single Sign-On (SSO)**
- **Cloud Based Security Groups**
- **Handed Virtual Server Machines**

Cloud Security

- Cloud security is a set of control-based safeguards and technology protection designed to protect resources stored online from leakage, theft, or data loss.

- Whether operating in public, private, or hybrid cloud environments, cloud security creates and maintains preventative strategies and actions to combat any threat to networked systems and applications.

- When adopting cloud technology, security is one of the most critical issues.
- Many Organizations still fear that their data is not secure in the cloud environment.



Is Cloud Security really a concern?

edureka!

n=256, Base:
Do not plan to
use public cloud

Gartner

EDUREKA AWS ARCHITECT CERTIFICATION TRAINING

www.edureka.co/cloudcomputing

Basic terms and concepts

Topics that fall under the umbrella of security in the cloud include:

- Data center security
- Access control
- Threat prevention
- Threat detection
- Threat mitigation
- Redundancy
- Legal compliance
- Cloud security policy

Risks and threats

The following are some common cloud security threats:

- Data breaches
- Malware injections
- Regulatory compliance
- Distributed Denial of Service (DDoS)
- Malicious insiders
- Advanced persistent threats (APTs)
- Insecure APIs

Security Frameworks

The NIST (National Institute of Standards and Technology) designed a policy framework that many companies follow when establishing their own cloud security infrastructures.

This framework has five critical pillars:

- Identify: Understand organizational requirements and complete security risk assessments.
- Protect: Implement safeguards to ensure your infrastructure can self-sustain during an attack.
- Detect: Deploy solutions to monitor networks and identify security-related events.
- Respond: Launch countermeasures to combat potential or active threats to business security.
- Recover: Develop and activate necessary procedures to restore system capabilities and network services in the event of a disruption.

Basic Terms and Concepts

The fundamental security terms relevant to cloud computing and describe associated concepts are:

- Confidentiality
- Integrity
- Authenticity
- Availability
- Threat
- Vulnerability
- Risk
- Security Controls
- Security Mechanisms
- Security Policies

Security Concepts

- 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.

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.

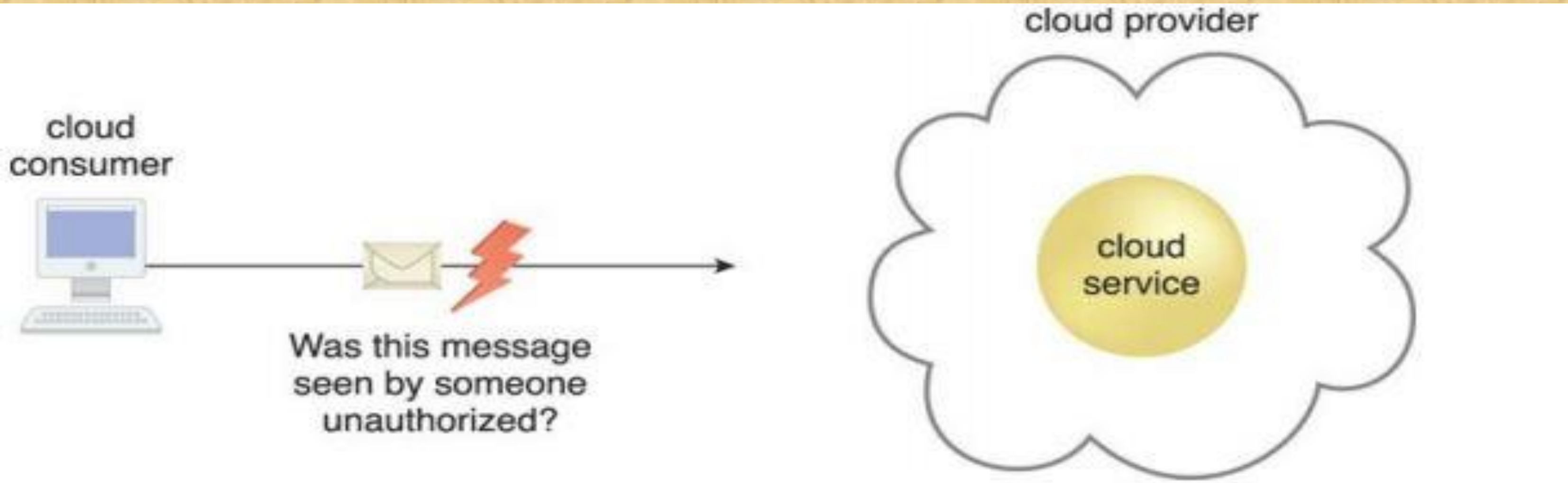


Figure 6.1. The message issued by the cloud consumer to the cloud service is considered confidential only if it is not accessed or read by an unauthorized party.

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.

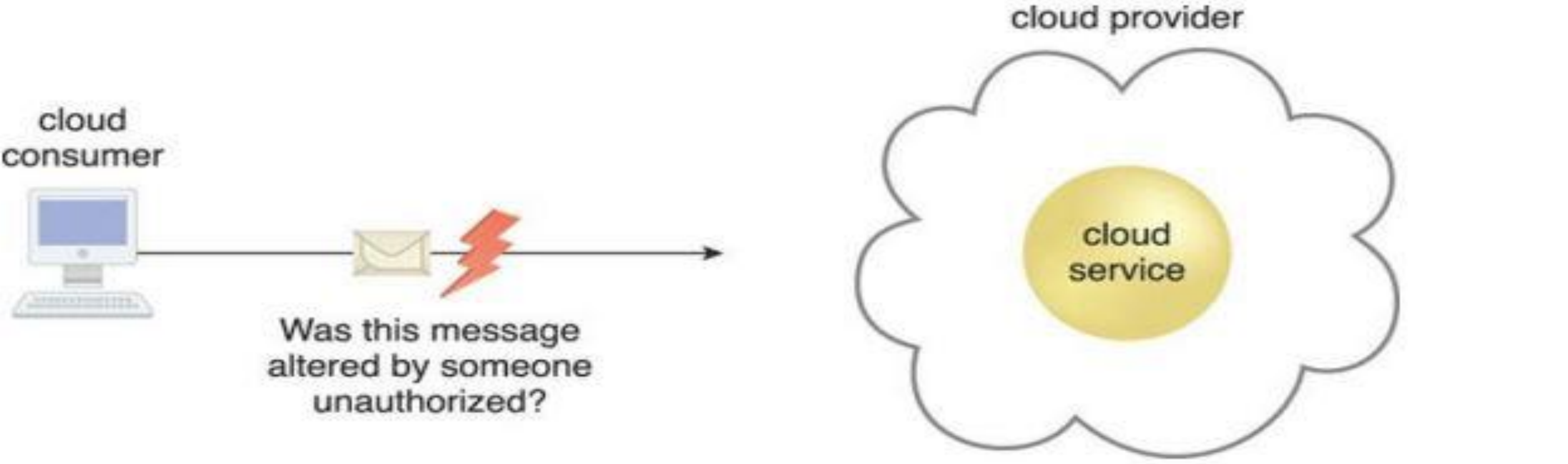


Figure 6.2. The message issued by the cloud consumer to the cloud service is considered to have integrity if it has not been altered.

Authenticity and Availability

- **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.

- **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.

Threat, Vulnerability and Risk

- **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.

- **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** 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

Security Controls, Security Mechanisms and Security Policies

- **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.

- **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.

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.

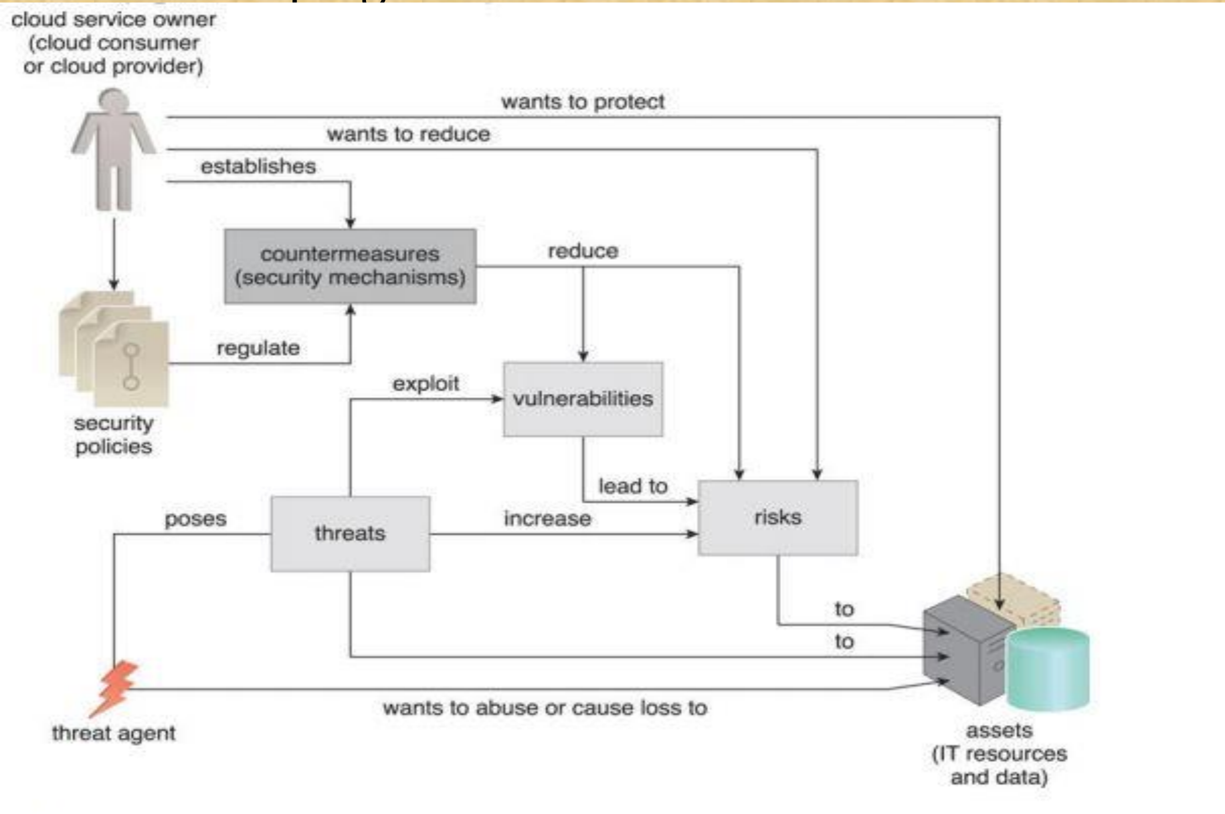


Figure 6.3. How security policies and security mechanisms are used to counter threats, vulnerabilities, and risks caused by threat agents.

Threat Agents

Anonymous Attacker

- An anonymous attacker is a non-trusted cloud service consumer without permissions in the cloud.

Figure 6.4. The notation used for an anonymous attacker.

Malicious Service Agent

- A malicious service agent is able to intercept and forward the network traffic that flows within a cloud

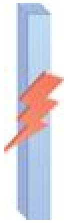


Figure 6.5. The notation used for a malicious service agent.

Threat Agents

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.

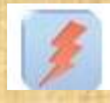


Figure 6.6. The notation that is used for a trusted attacker.

Malicious Insider

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

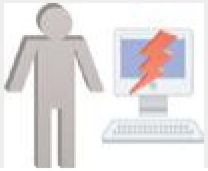


Figure 6.7. The notation used for an attack originating from a workstation. The human symbol is optional.

Cloud Security Threats

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

Traffic Eavesdropping

- It 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.

Traffic Eavesdropping

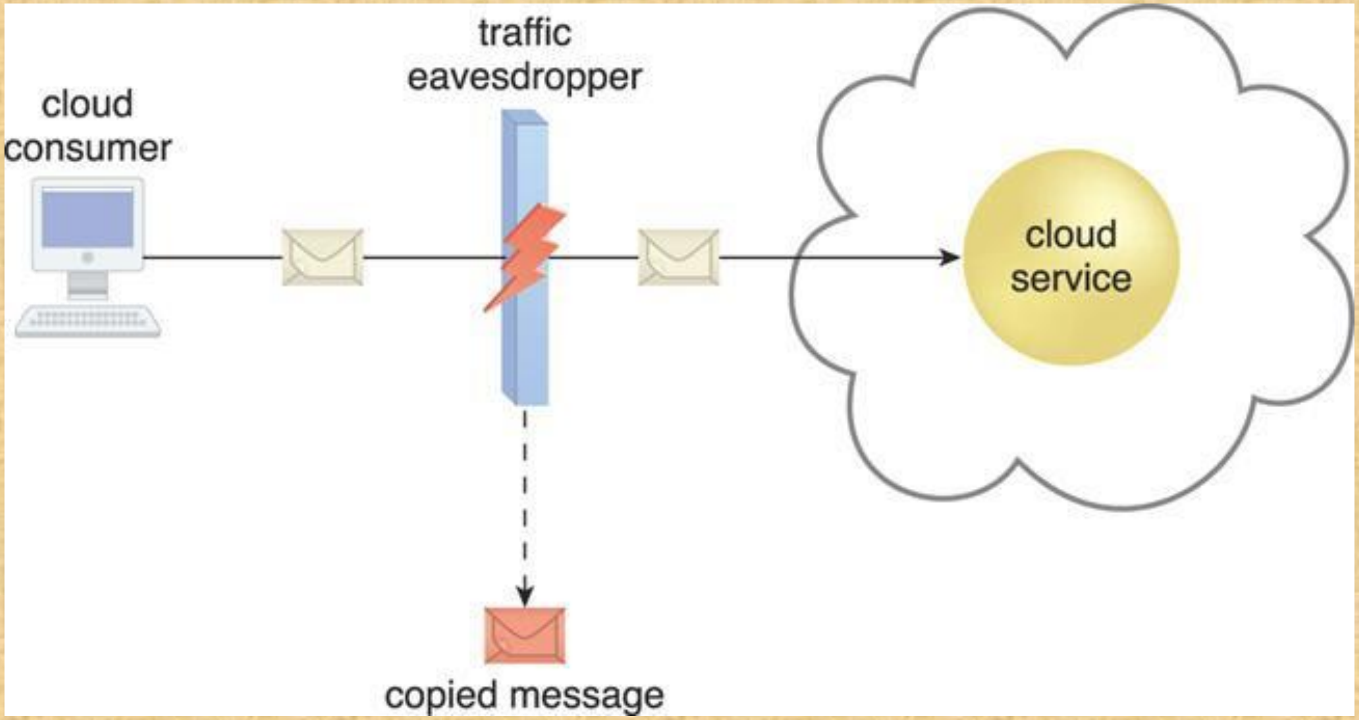


Figure 6.8 An externally positioned malicious service agent carries out a traffic eavesdropping attack by intercepting a message sent by the cloud service consumer to the cloud service. The service agent makes an unauthorized copy of the message before it is sent along its original path to the cloud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

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

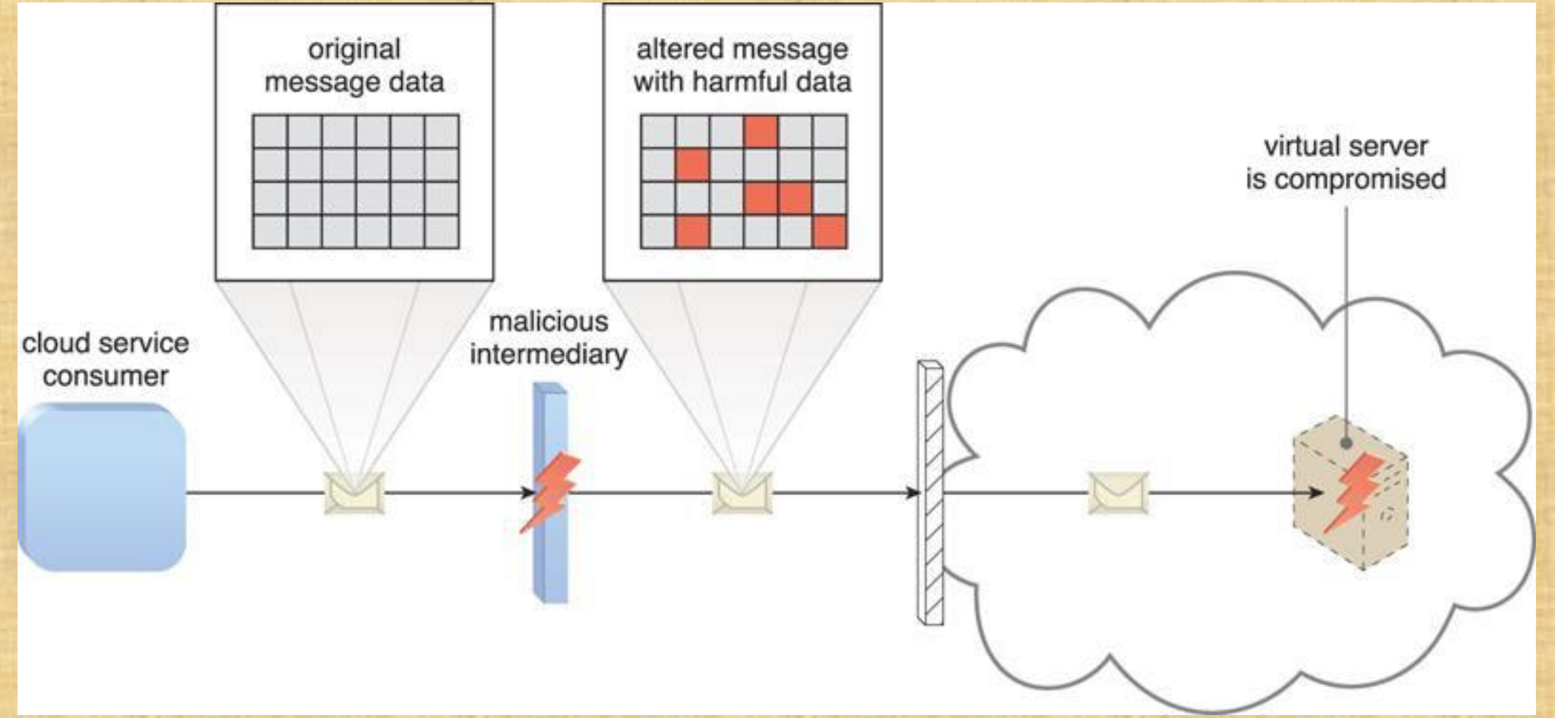


Figure 6.9 The malicious service agent intercepts and modifies a message sent by a cloud service consumer to a cloud service (not shown) being hosted on a virtual server. Because harmful data is packaged into the message, the virtual server is compromised.

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.

Denial of Service

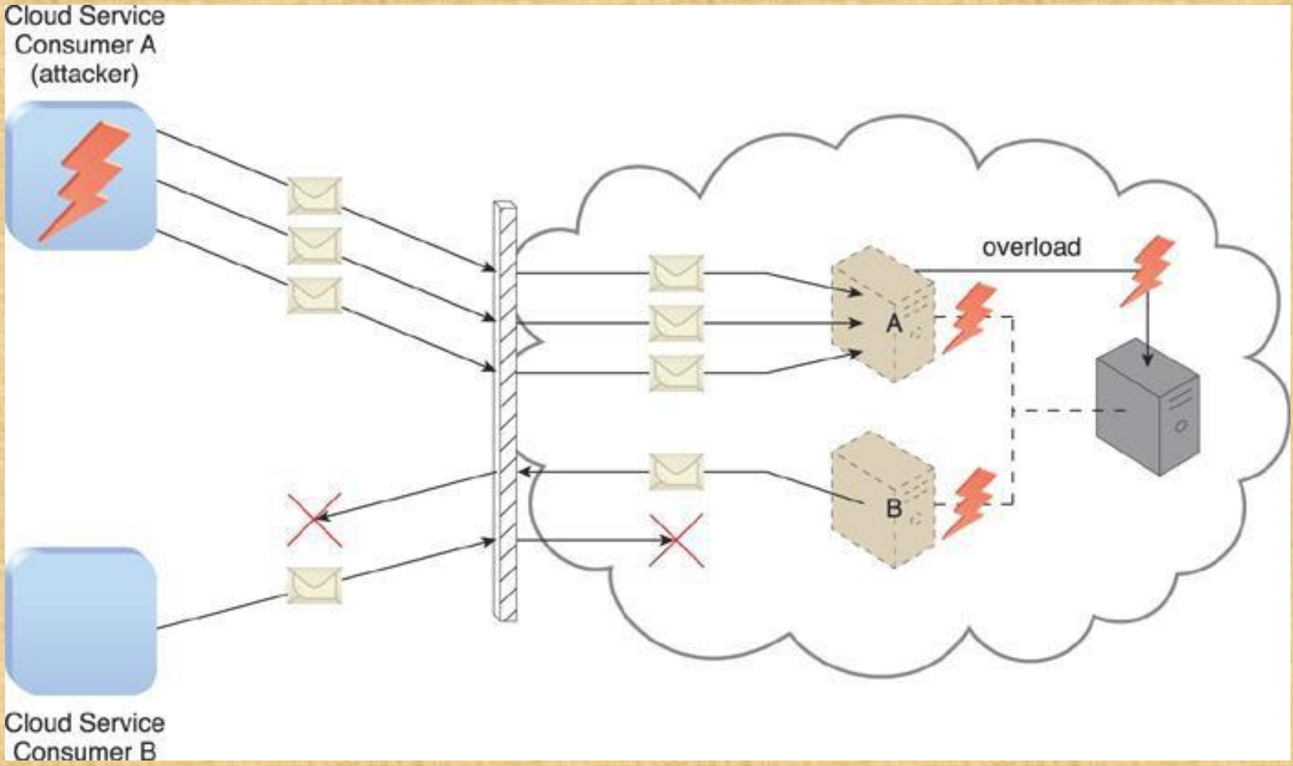


Figure 6.10 Cloud Service Consumer A sends multiple messages to a cloud service (not shown) hosted on Virtual Server A. This overloads the capacity of the underlying physical server, which causes outages with Virtual Servers A and B. As a result, legitimate cloud service consumers, such as Cloud Service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

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

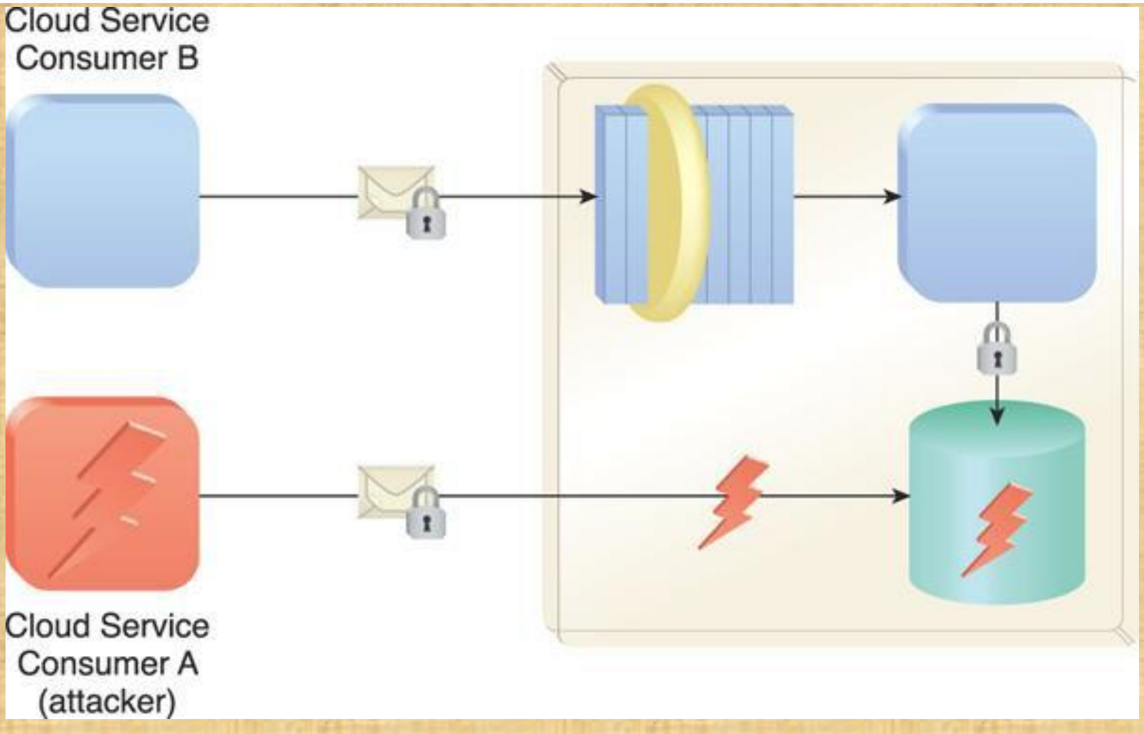


Figure 6.11 Cloud Service Consumer A gains access to a database that was implemented under the assumption that it would only be accessed through a Web service with a published service contract (as per Cloud Service Consumer B).

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 those IT resources the attacker gains .

Insufficient Authorization Attack

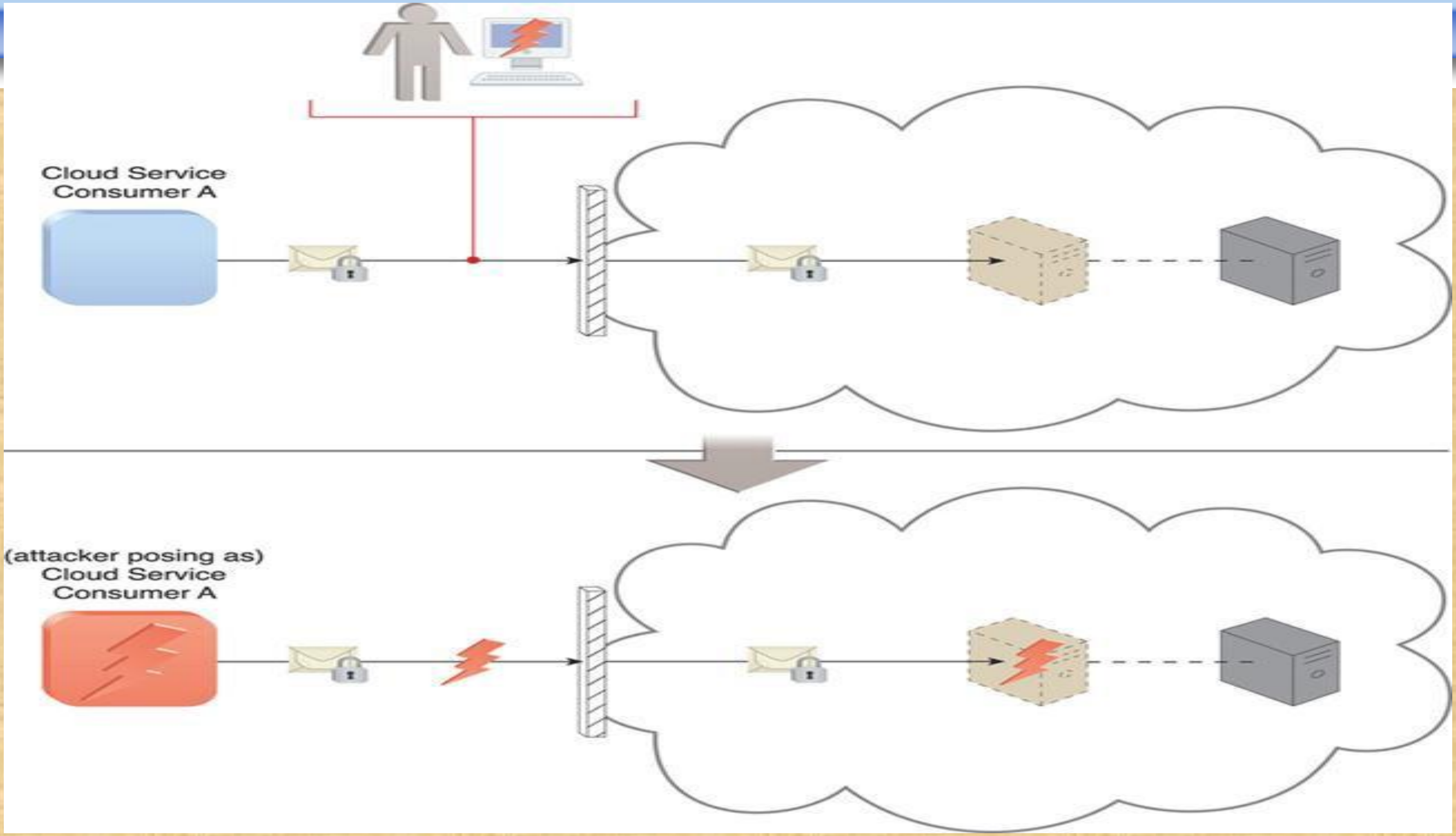


Figure 6.12 An attacker has cracked a weak password used by Cloud Service Consumer A. As a result, a malicious cloud service consumer (owned by the attacker) is designed to pose as Cloud Service Consumer A in order to gain access to the cloud-based virtual server.

Virtualization Attack

- It exploits vulnerabilities in the virtualization platform to 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

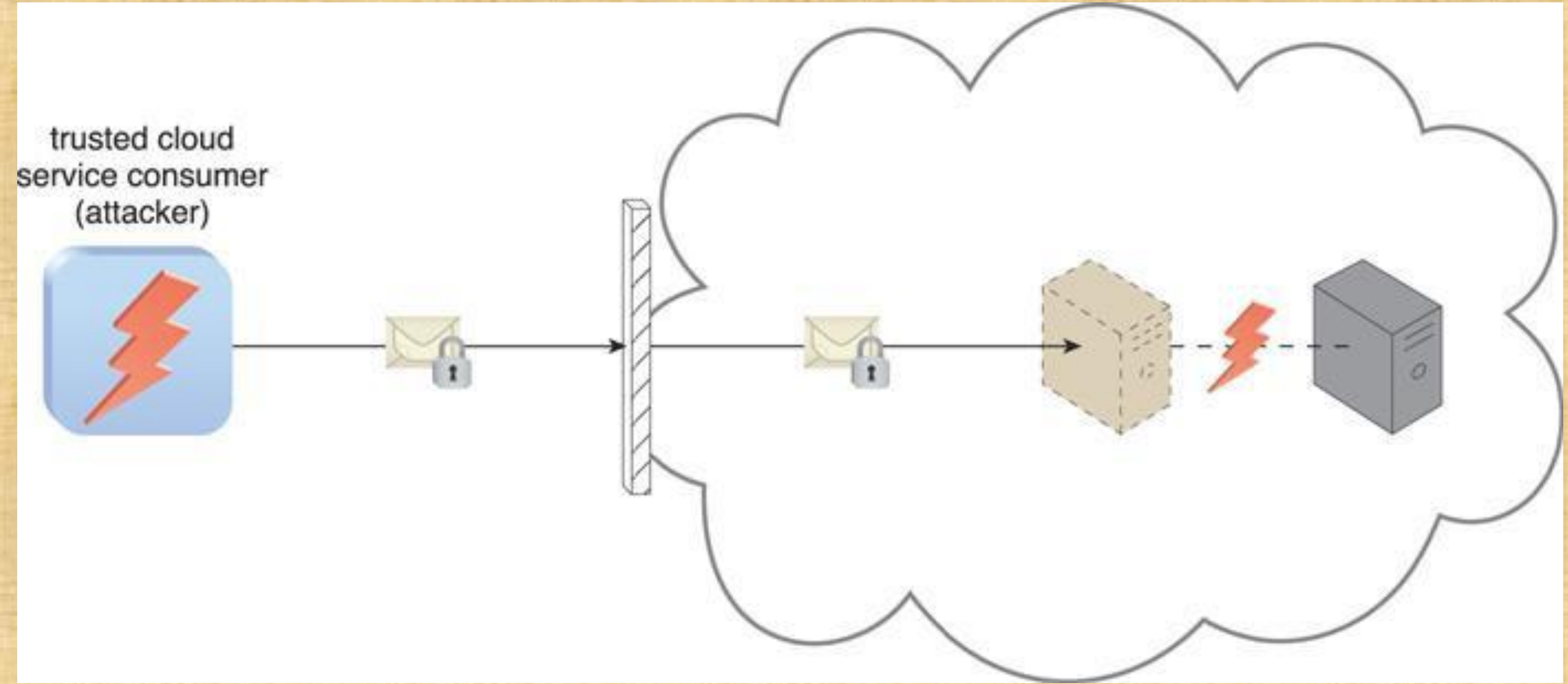


Figure 6.13 An authorized cloud service consumer carries out a virtualization attack by abusing its administrative access to a virtual server to exploit the underlying hardware.

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

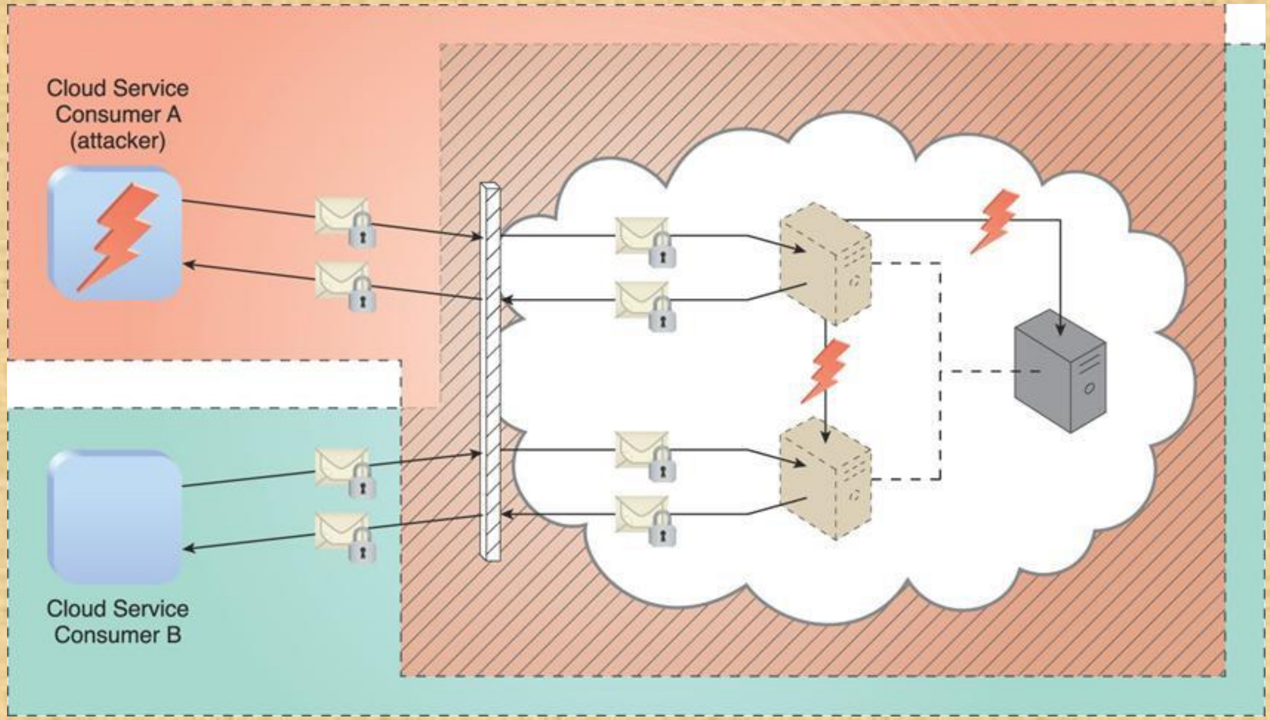
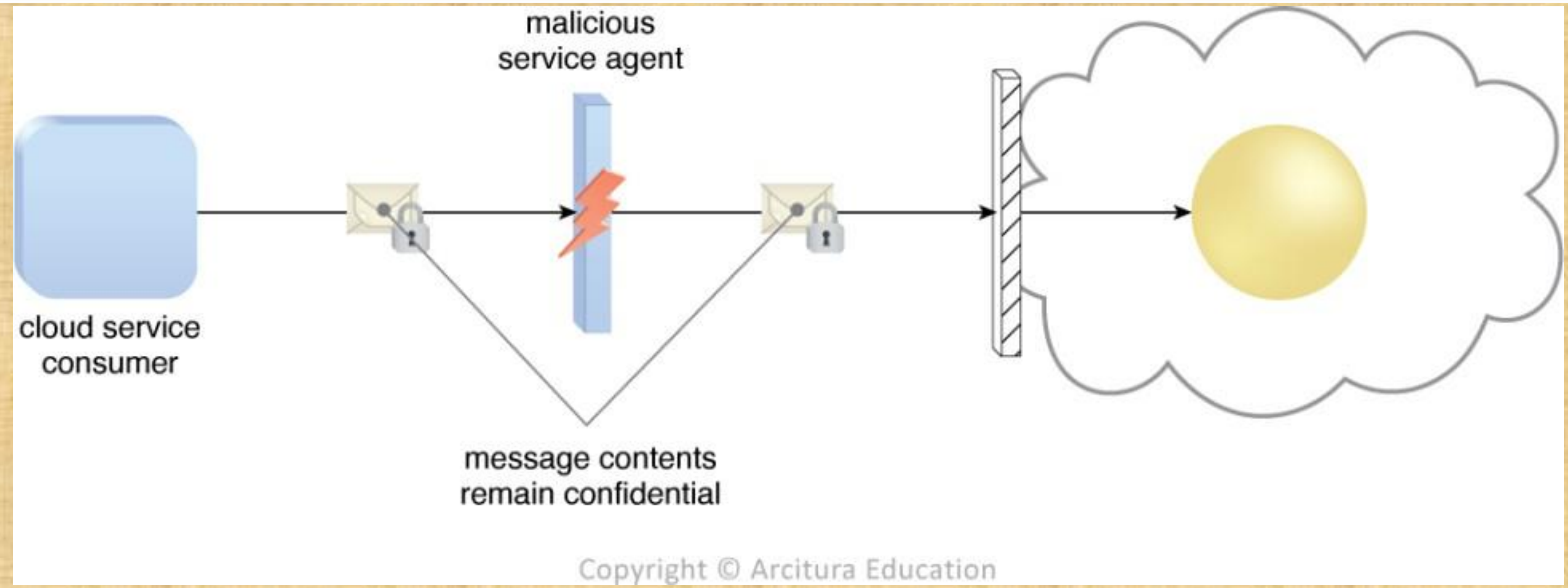


Figure 6.14 Cloud Service Consumer A is trusted by the cloud and therefore gains access to a virtual server, which it then attacks with the intention of attacking the underlying physical server and the virtual server used by Cloud Service Consumer B.

Encryption

- The encryption mechanism is a digital coding system dedicated to preserving the confidentiality and integrity of data.
- Encryption technology commonly relies on a standardized algorithm called a cipher to transform original plaintext data into encrypted data, referred to as ciphertext.
- The encryption mechanism can help counter the traffic eavesdropping, malicious intermediary, insufficient authorization, and overlapping trust boundaries security threats.

Encryption



- *Figure 10.1 - A malicious intermediary is unable to retrieve data from an encrypted message. The retrieval attempt may furthermore be revealed to the cloud service consumer. (Note the use of the lock symbol to indicate that a security mechanism has been applied to the message contents.)*

Encryption

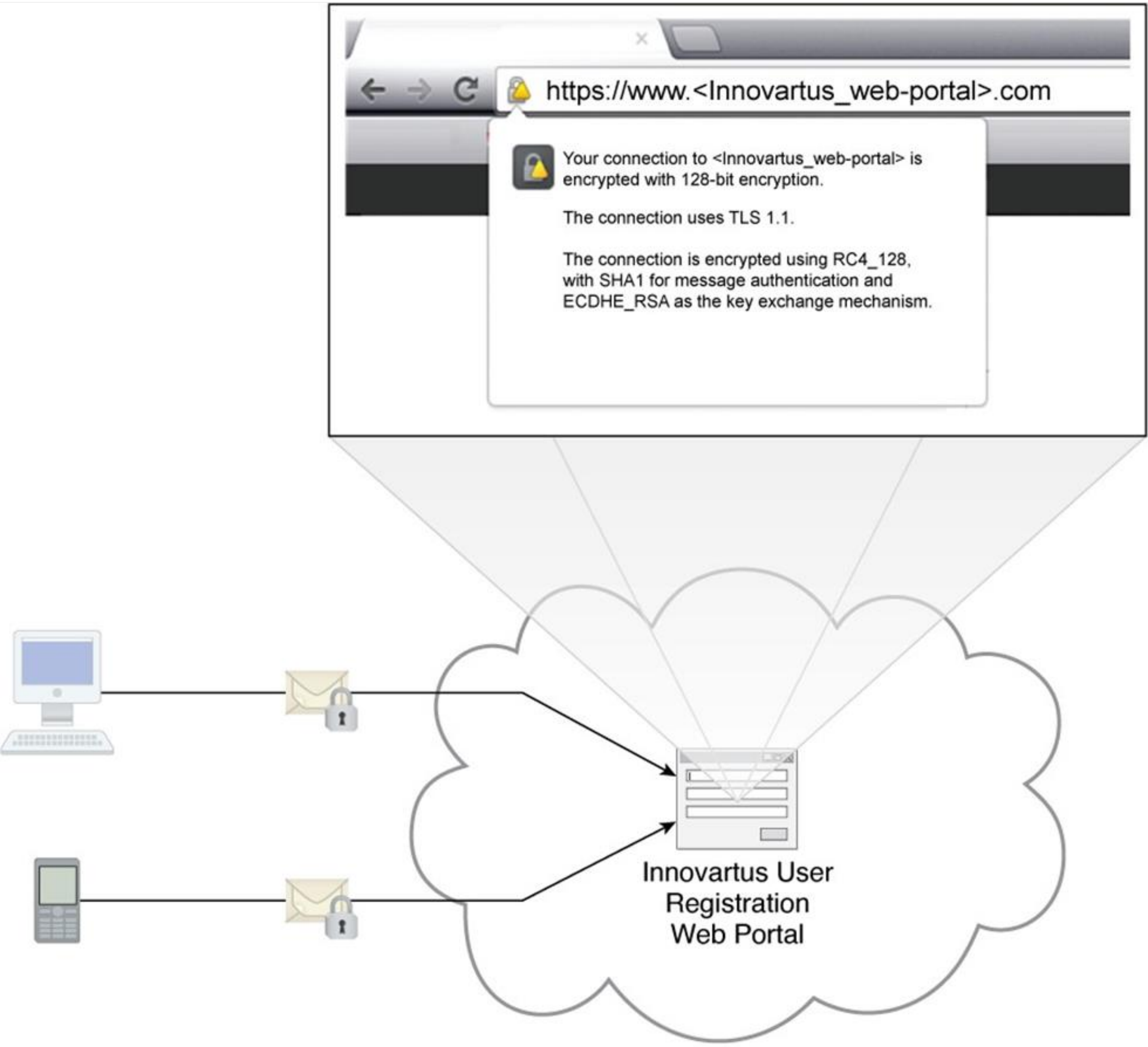
- Two common forms of encryption known as symmetric encryption and asymmetric encryption:
  - Symmetric encryption
- Symmetric encryption uses the same key for both encryption and decryption, both of which are performed by authorized parties that one shared key.
  - It provides data confidentiality but no non-repudiation (in a party of more than 2 people).
  - Asymmetric encryption
- Asymmetric encryption relies on the use of two different keys, namely a private key and a public key.

Encryption

- Message that were encrypted with a private key can be correctly decrypted by any party with the corresponding public key.
  - This method of encryption does not offer any confidentiality protection.
  - Private key encryption therefore offers integrity protection in addition to authenticity and non-repudiation.
- A message that was encrypted with a public key can only be decrypted by the rightful private key owner, which provides confidentiality protection.
  - Any party that has the public key can generate the ciphertext, meaning this method provides neither message integrity nor authenticity protection due to the communal mature of the public key.

Encryption

- *The encryption mechanism is added to the communication channel between outside users and Innovartus‘ User Registration Portal. This safeguards message confidentiality via the use of HTTPS (using SSL/TLS).*
- *TLS is a successor to SSL.*



https://www.<Innovartus_web-portal>.com

Your connection to <Innovartus_web-portal> is encrypted with 128-bit encryption.

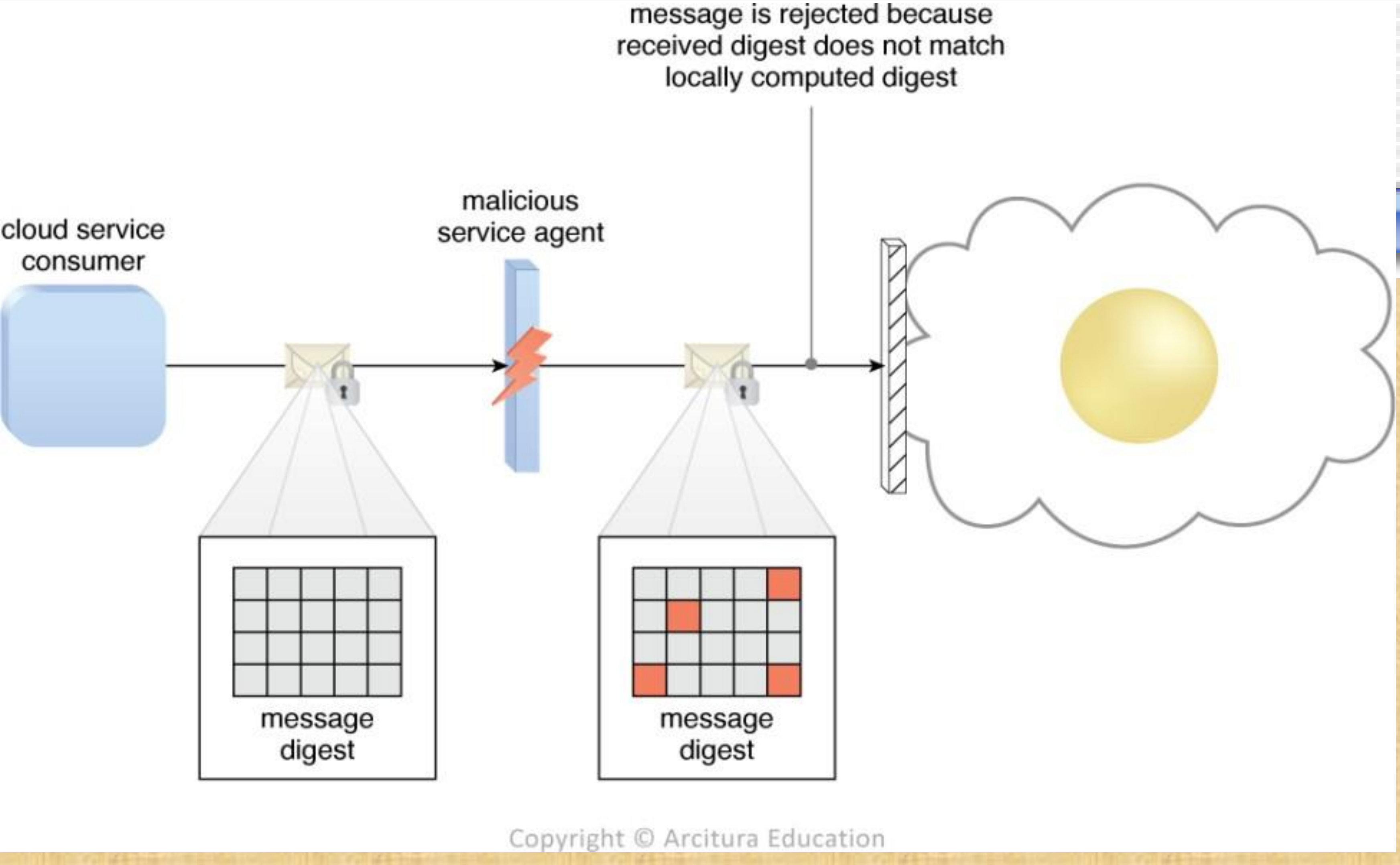
The connection uses TLS 1.1.

The connection is encrypted using RC4_128, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.

Copyright © Arcitura Education

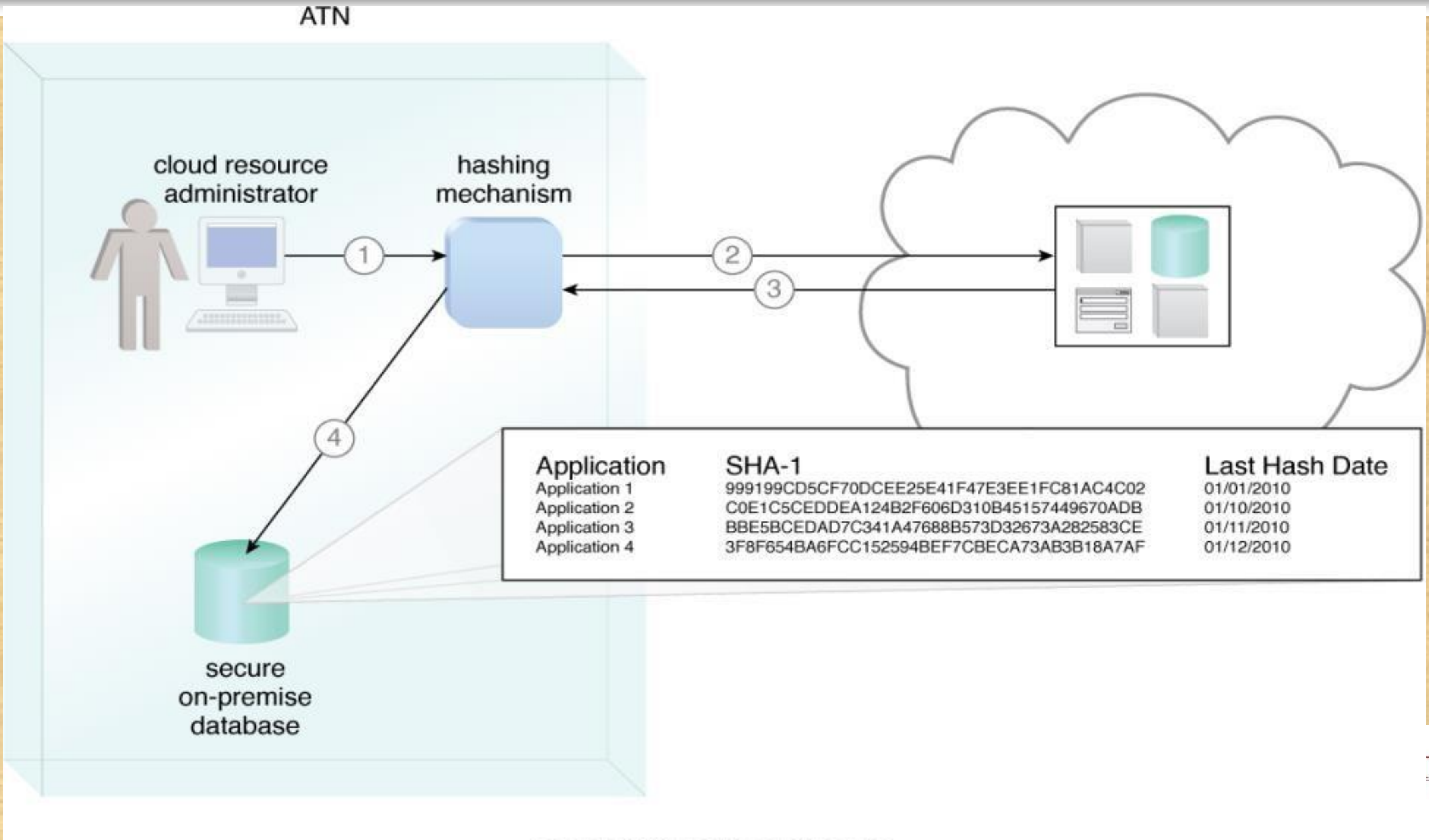
Hashing

- The hashing mechanism is used when a one-way, non-reversible form of data protection is required.
- 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.
- A common application of hashing is the storage of passwords.
- In addition to protect stored data, the cloud threats that can be mitigated by hashing including malicious intermediary and insufficient authorization.


message is rejected because received digest does not match locally computed digest
malicious service agent
cloud service consumer
message digest
message digest
Copyright © Arcitura Education

- *Figure 10.3 - 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.*

ATN’s Example



Application	SHA-1	Last Hash Date
Application 1	999199CD5CF70DCEE25E41F47E3EE1FC81AC4C02	01/01/2010
Application 2	C0E1C5CEDDEA124B2F606D310B45157449670ADB	01/10/2010
Application 3	BBE5BCEDAD7C341A47688B573D32673A282583CE	01/11/2010
Application 4	3F8F654BA6FCC152594BEF7CBECA73AB3B18A7AF	01/12/2010

Copyright © Arcitura Education

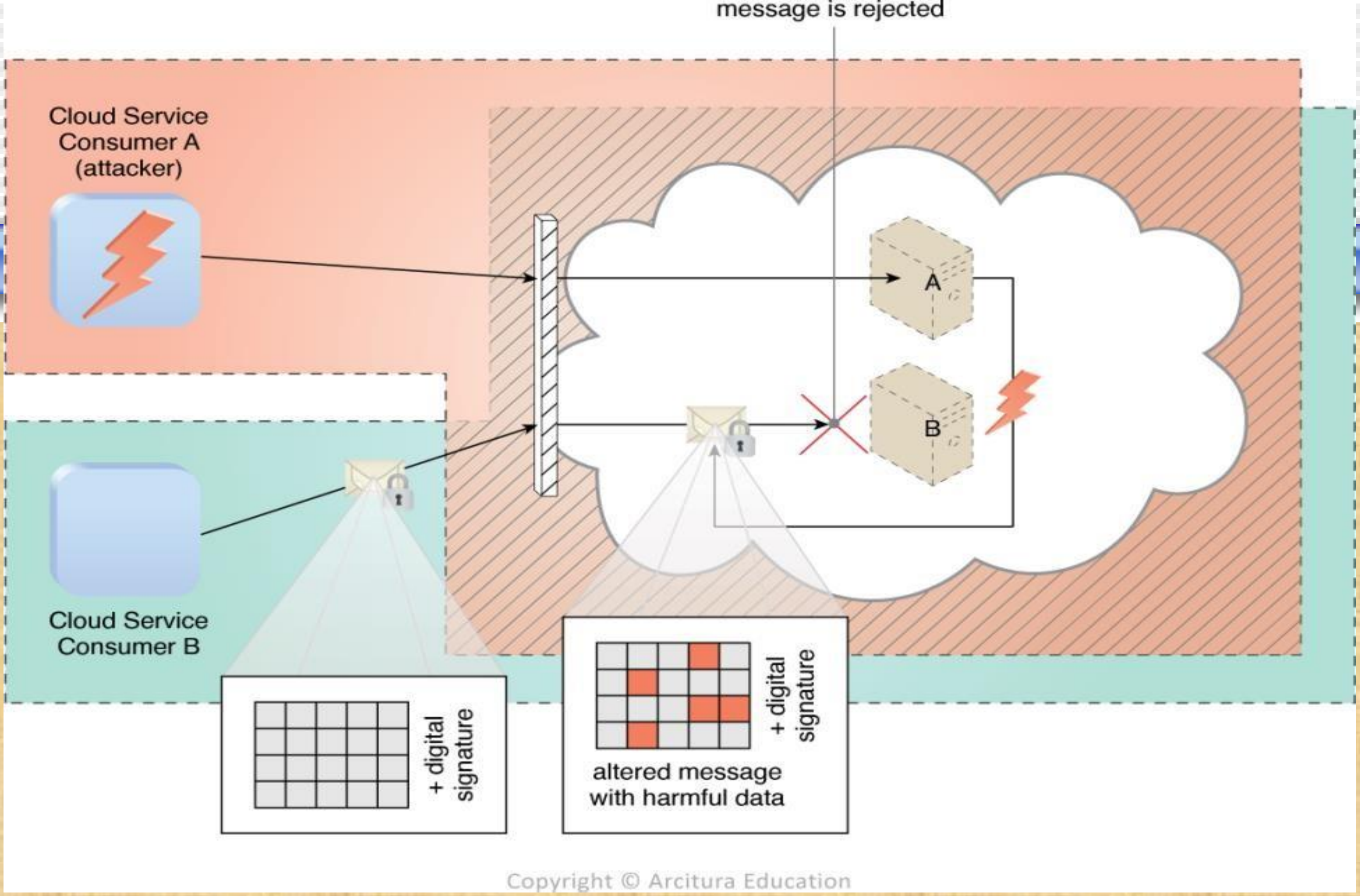
ATN’s Example

- A hashing procedure is invocated when the PaaS environment is accessed (1).
- The applications that were ported to this environment are checked (2) and their message digests are calculated (3).
- The message digests are stored in a secure on- premise database (4), and a notification is issued if any of their values are not identical to the ones in storage.

Digital Signature

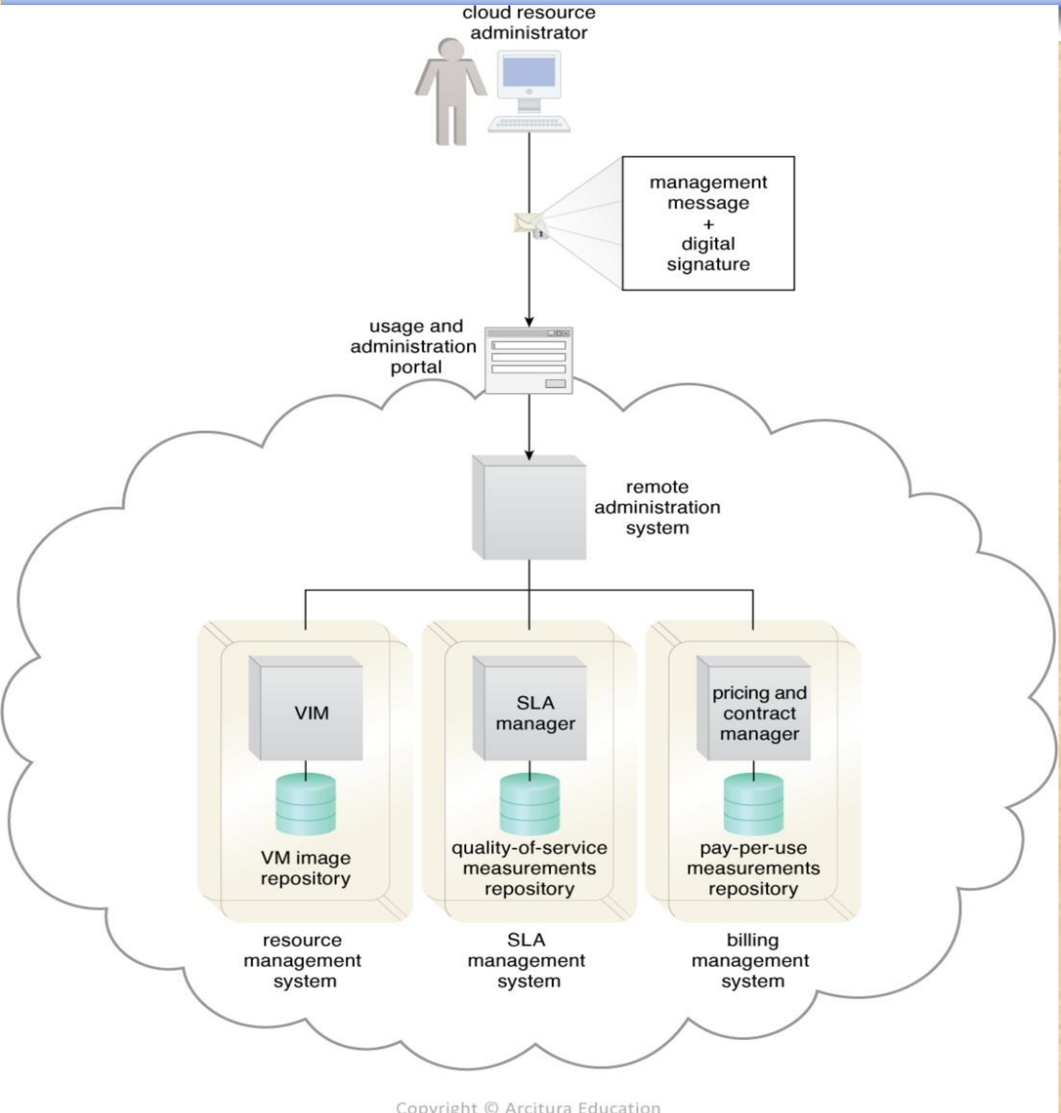
- The digital signature mechanism is a means of providing data authenticity and integrity through authentication and non-repudiation.

- 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.


message is rejected
Cloud Service Consumer A (attacker)
Cloud Service Consumer B
A
B
+ digital signature
+ digital signature
altered message with harmful data
Copyright © Arcitura Education

- *Figure 10.5 - 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.*

DTGOV's Example


cloud resource administrator
management message + digital signature
usage and administration portal
remote administration system
VIM
VM image repository
SLA manager
quality-of-service measurements repository
pricing and contract manager
pay-per-use measurements repository
resource management system
SLA management system
billing management system

Copyright © Arcitura Education

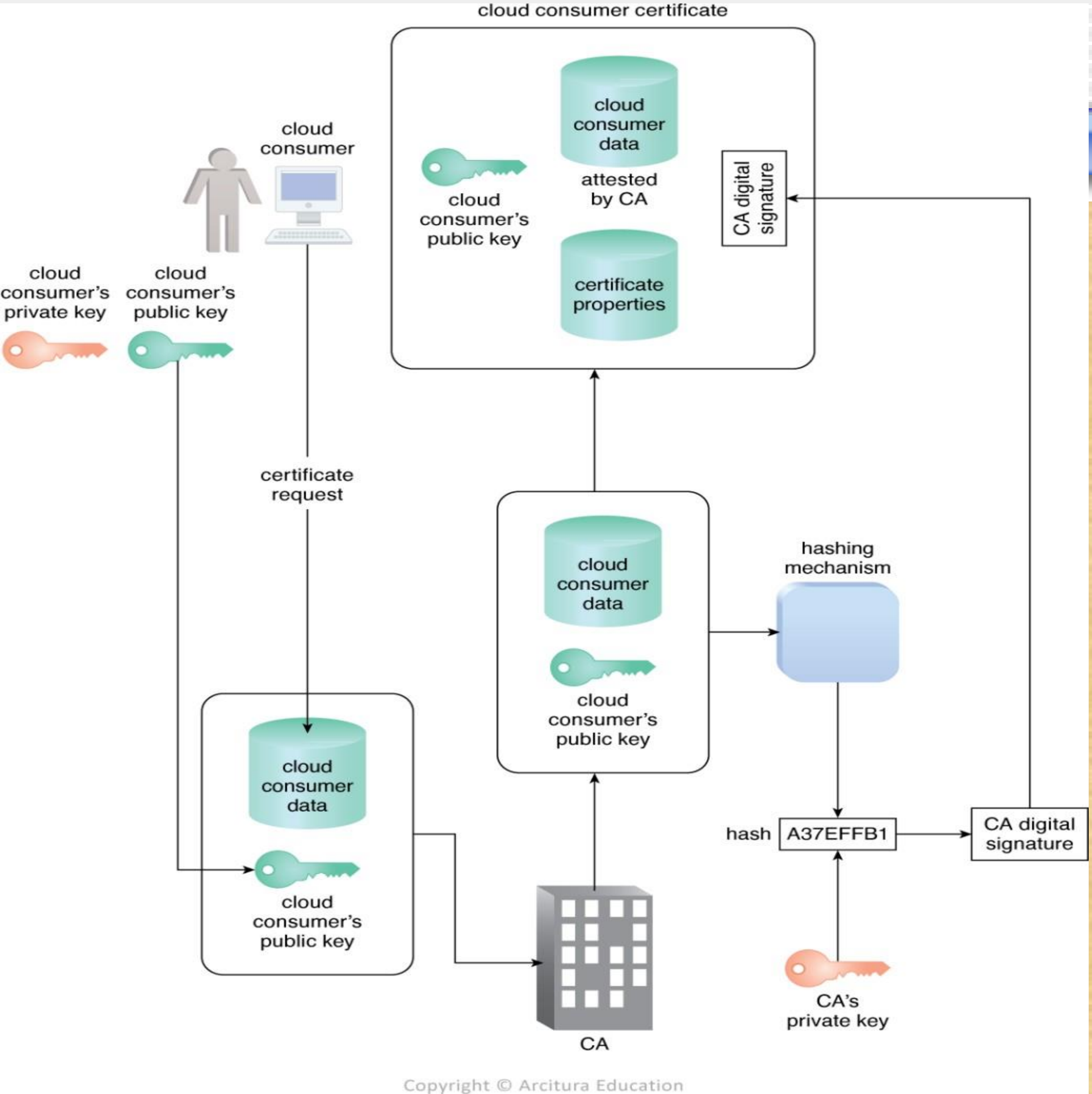
- Figure 10.6 - Whenever a cloud consumer performs a management action that is related to IT resources provisioned by DTGOV, the cloud service consumer program must include a digital signature in the message request to prove the legitimacy of its user.

Public Key Infrastructure (PKI) (1/2)

- The public key infrastructure (PKI) mechanism, which exists as a system of protocols, data formats, rules, and practices that enables large-scale systems to securely use public key cryptography.

- PKIs rely on the use of digital certificates, which are digitally signed data structures that bind public keys to certificate owner identities.

- Digital certificates are usually digitally signed by a third-party certificate authority (CA), such as VeriSign and Comodo.



- *Figure 10.7 - The common steps involved during the generation of certificates by a certificate authority (CA).*

Public Key Infrastructure (PKI) (2/2)

- The PKI is a dependable method for implementing asymmetric encryption, managing cloud consumer and cloud provider identity information.

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

Identity and Access Management (IAM 1/2)

- 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.
- IAM mechanisms exist as systems comprised of four main components:
  - Authentication
  - Authorization
  - User Management
  - Credential Management

Identity and Access Management (IAM 2/2)

- As opposed to PKI, 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, PKI is primarily used to counter the inefficient authorization threat.

Single Sign-On (SSO) (1/2)

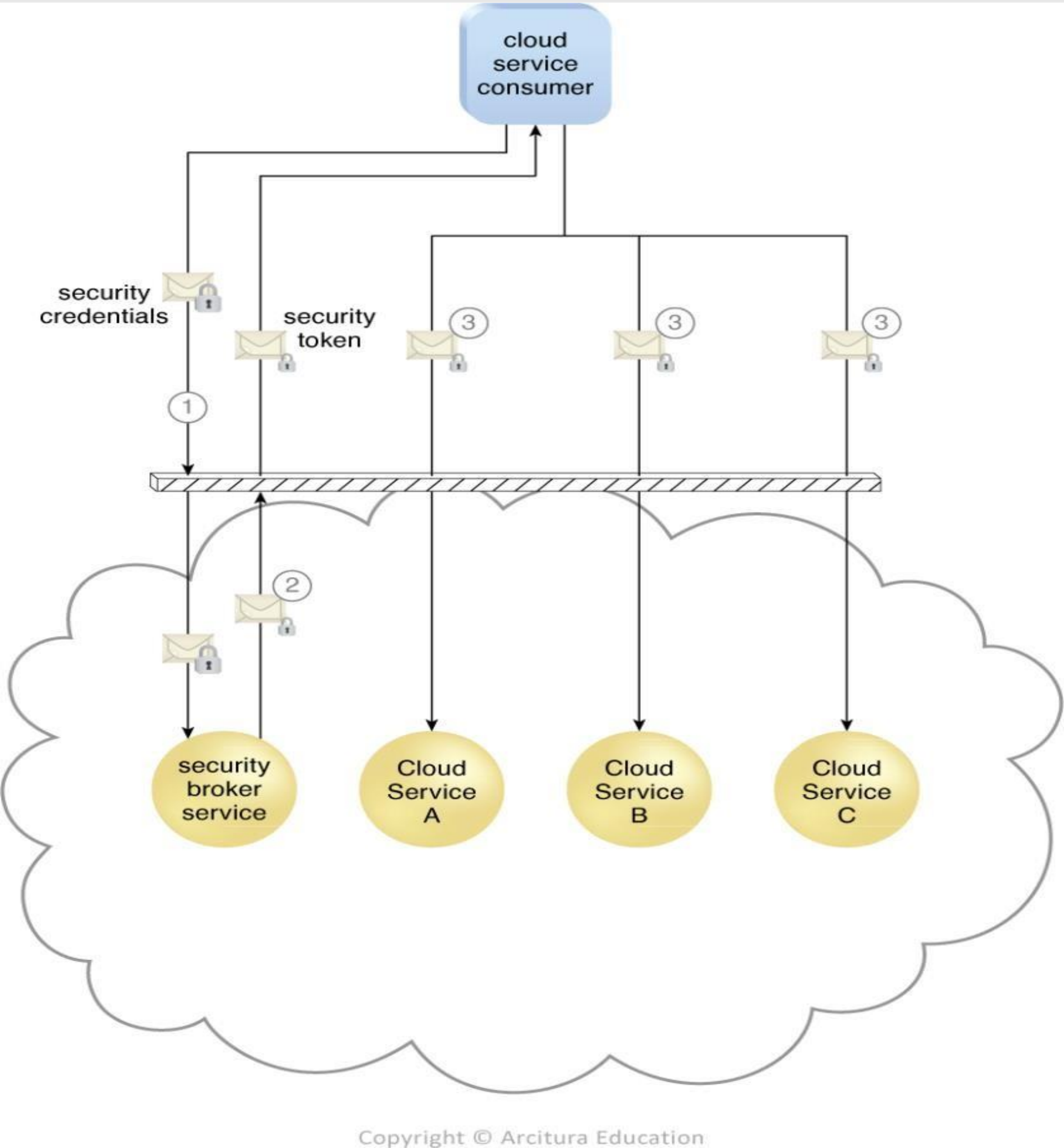
- Propagating the authentication and authorization for a cloud service consumer across multiple cloud services is inevitable and challenging.

- 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 resources, so that the cloud service consumer need not to re-authenticate itself with every subsequent request.

Single Sign-On (SSO) (2/2)

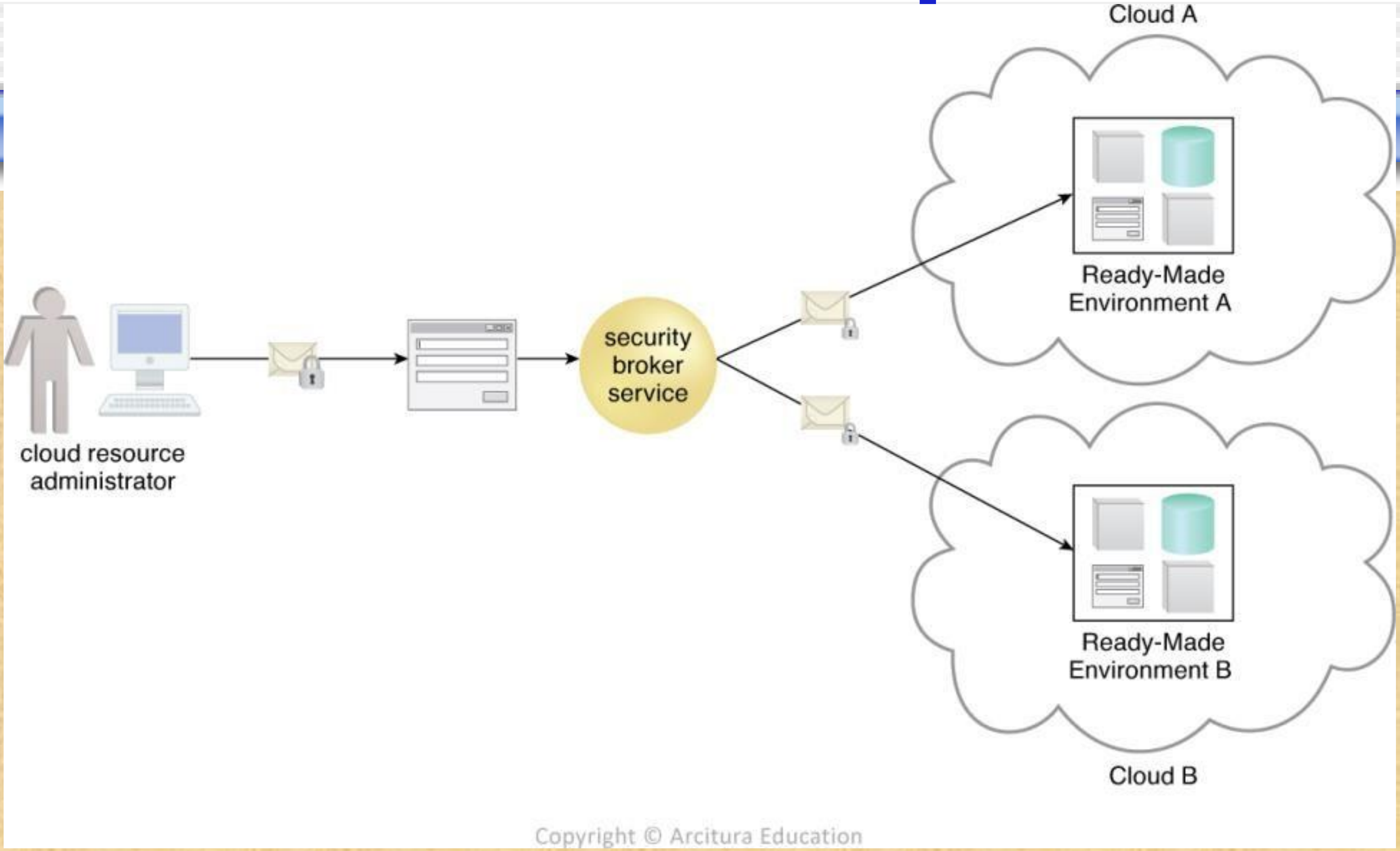
- The SSO mechanism essentially enables mutually independent cloud services and IT resources to generate and circulate runtime authentication and authorization credentials.

- SSO does not direct counter any of the cloud security threats. It primarily enhances the usability of cloud- based environments for access and management of resources and solutions.



- *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 for Cloud Services A, B, and C (3).*

ATN's Example



Copyright © Arcitura Education

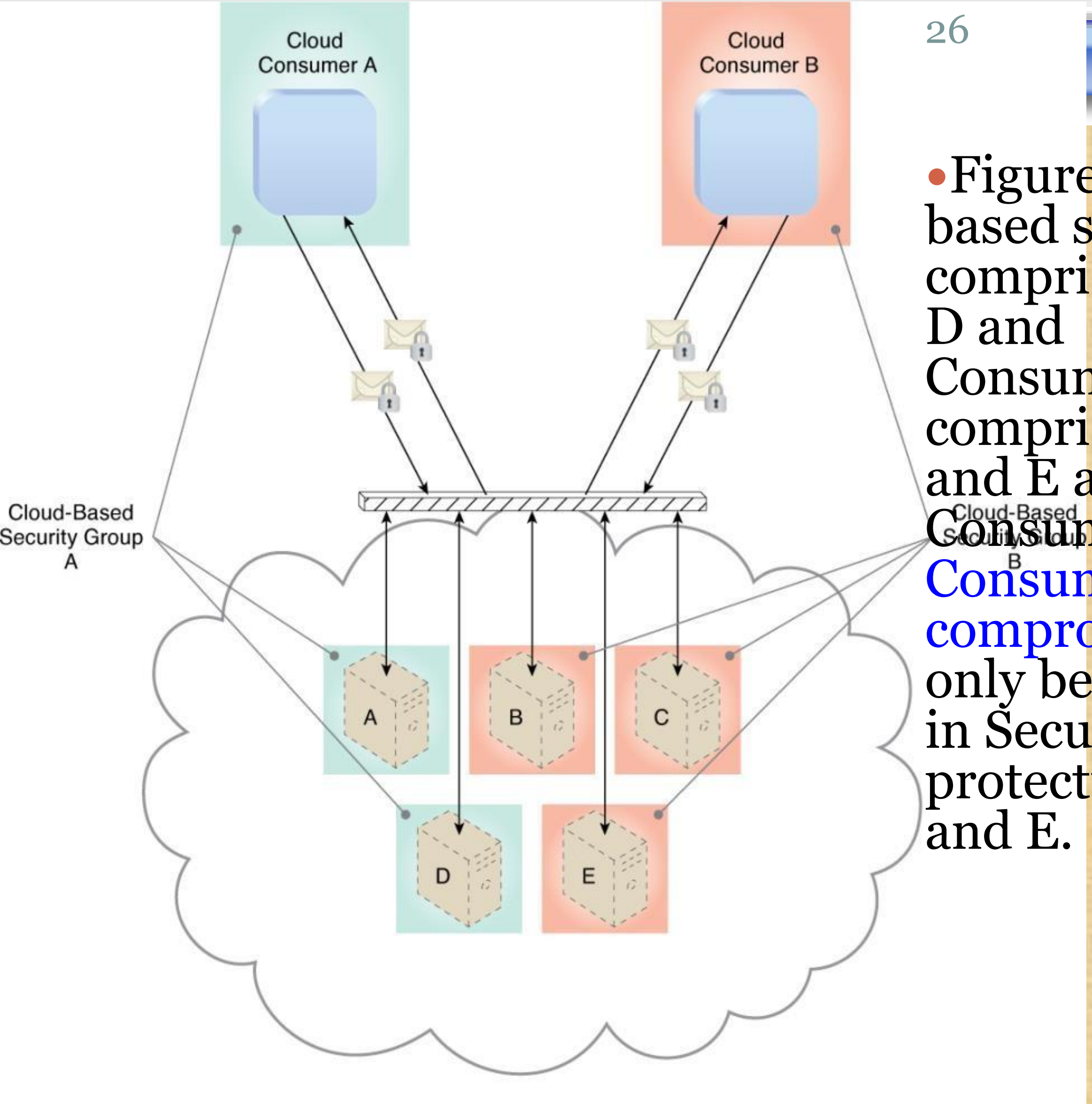
- *Figure 10.10 - The credentials received by the security broker are propagated to ready-made environments across two different clouds. The security broker is responsible for selecting the appropriate security procedure with which to contact each cloud.*

Cloud-Based Security Group (1/2)

- Cloud resource segmentation is a process by which separate physical and virtual IT environments are created for different users and groups.
- Resource segmentation is used to enable virtualization by allocating a variety of physical IT resource to virtual machines.
- 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.

Cloud-Based Security Group (2/2)

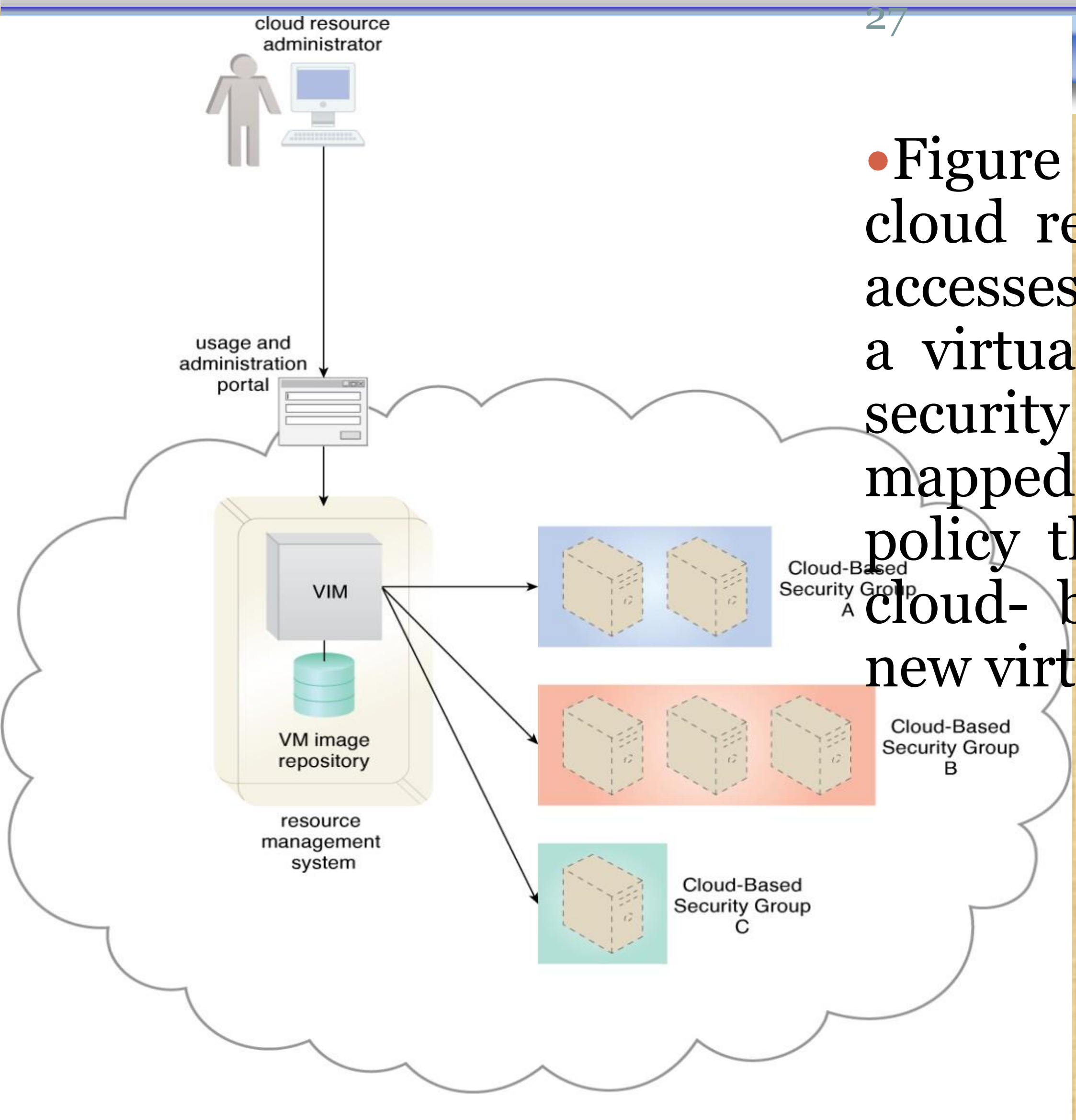
- Multiple virtual servers running on the same physical server can become members of different logical cloud-based security groups.
- Properly implemented cloud-based security groups help limit unauthorized access to IT resources in the event of a security breach.
- This mechanism can be used to help counter the denial of service, insufficient authorization, and overlapping trust boundaries threats, and is closely related to the logical network perimeter mechanism.



Copyright © Arcitura Education

- Figure 10.11 - A logical cloud-based security group, Group A, is comprised of Virtual Servers A and D and assigned to Cloud Consumer A, while Group B is comprised of Virtual Servers B, C, and E and assigned to Cloud Consumer B. If Cloud Service Consumer A's user account is compromised, the attacker would only be able to damage the servers in Security Group A, thereby protecting Virtual Servers B, C, and E.

DTGOV's Example


cloud resource administrator
usage and administration portal
VIM
VM image repository
resource management system
Cloud-Based Security Group A
Cloud-Based Security Group B
Cloud-Based Security Group C

- Figure 10.12 - When an external cloud resource administrator accesses the Web portal to allocate a virtual server, the requested security controls are assessed and mapped to an internal security policy that assigns a corresponding cloud- based security group to the new virtual server.

Hardened Virtual Server Images (1/2)

- A virtual server is created from a template configuration called a virtual server image (VM image).

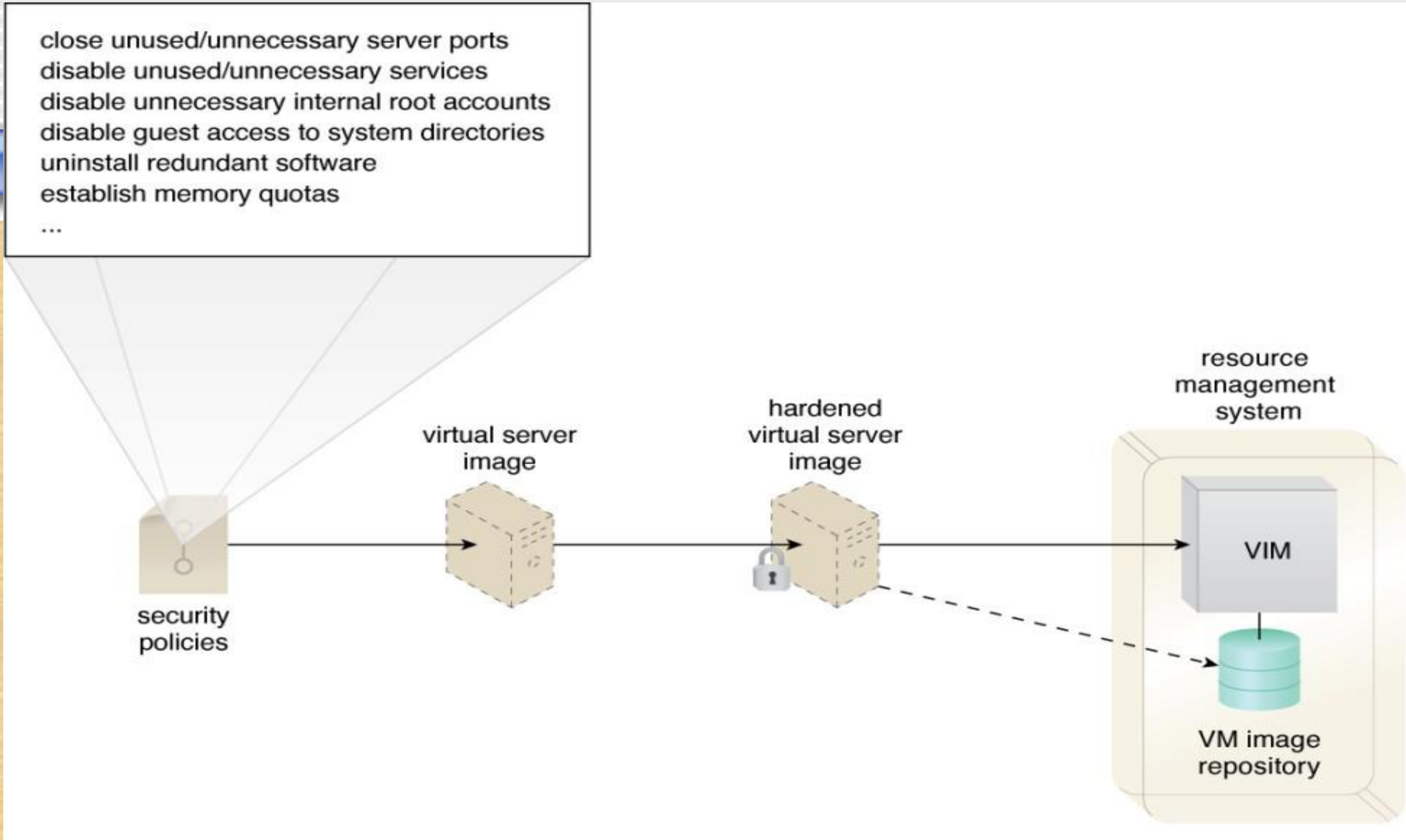
- Hardening is the process of stripping unnecessary software from a system to limit potential vulnerabilities that can be exploited by attackers.

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

Hardened Virtual Server Images (2/2)

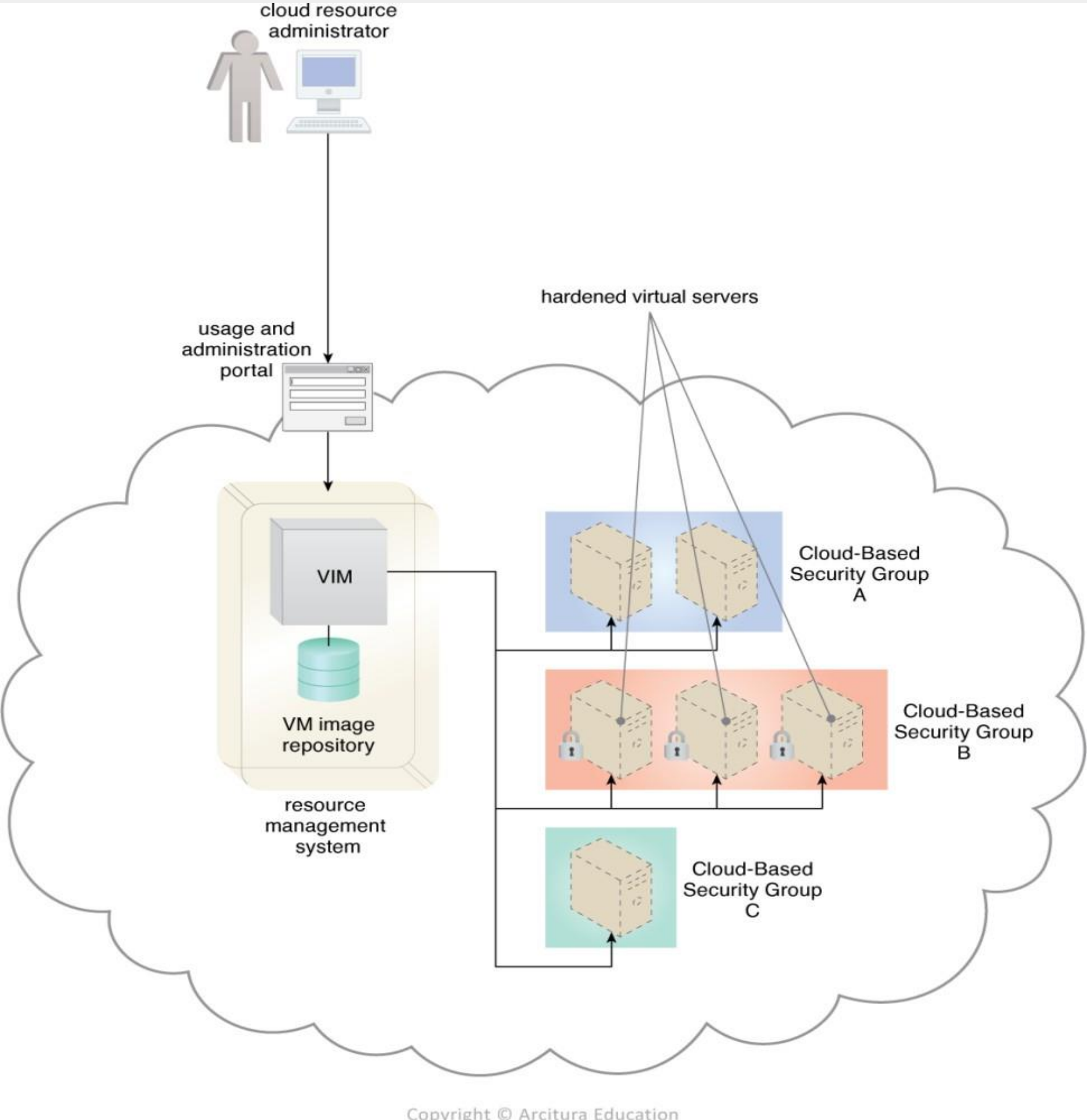
- A hardened virtual server image is a template for virtual service instance creation that has been subjected to a hardening process. It generally results in a virtual server template to be more secure than the original standard image.

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


close unused/unnecessary server ports
disable unused/unnecessary services
disable unnecessary internal root accounts
disable guest access to system directories
uninstall redundant software
establish memory quotas
...
security policies
virtual server image
hardened virtual server image
resource management system
VIM
VM image repository

- *Figure 10.13 - 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.*

(DTGOV's Example)



cloud resource administrator
usage and administration portal
hardened virtual servers
VIM
VM image repository
resource management system
Cloud-Based Security Group A
Cloud-Based Security Group B
Cloud-Based Security Group C
Copyright © Arcitura Education

- Figure 10.14 - The cloud resource administrator chooses the hardened virtual server image option for the virtual servers provisioned for Cloud-Based Security Group B.

Reference

- https://timesofcloud.com/cloud-tutorial/cloud-providers/

Conclusion

- Building and Launching your SaaS App

Exam: Shopify App store