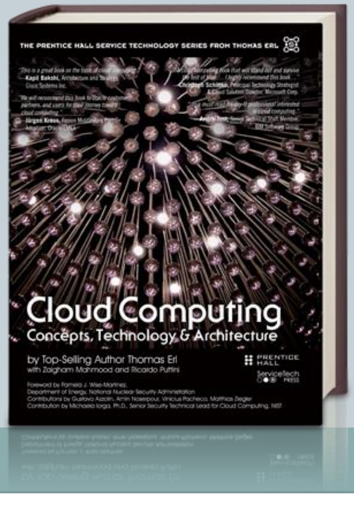
Cloud Computing

Concept, Technology & Architecture

Chapter 10

Cloud Security Mechanics

Taken from textbook "Cloud Computing Concepts, Technology and Architecture"



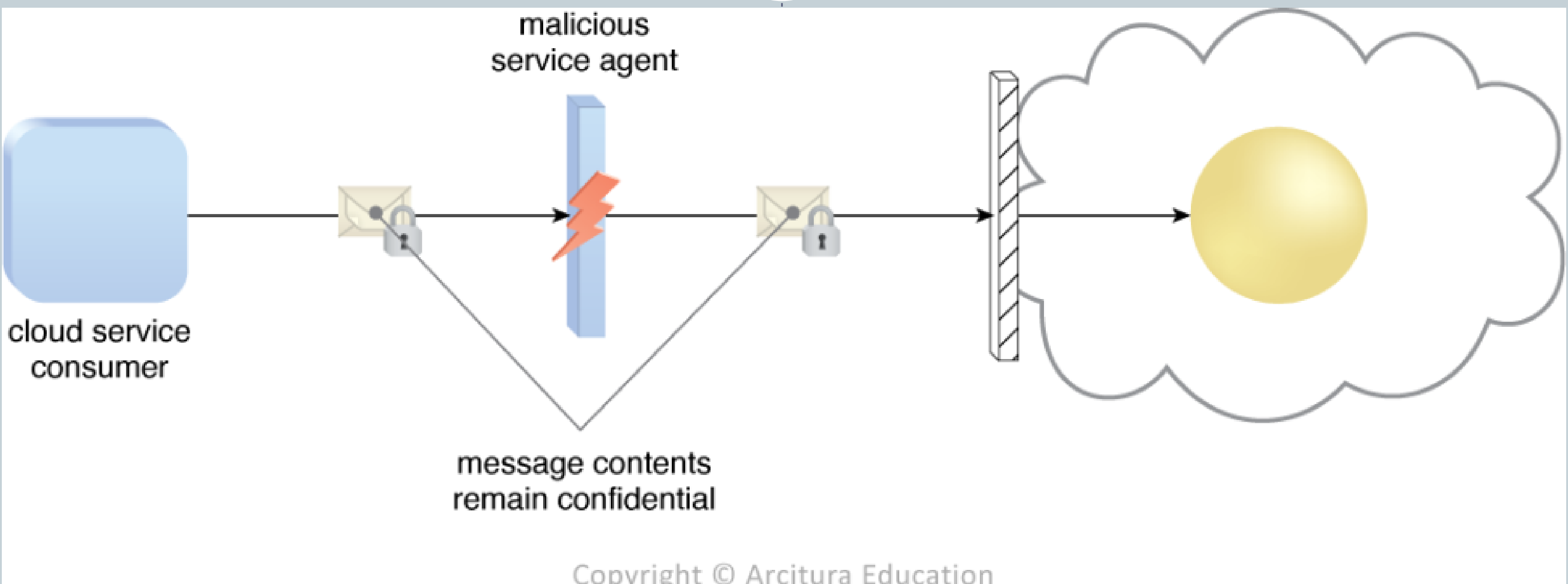
Contents

- Security mechanisms that can be used to counter and prevent the threats including the following:
  - 10.1 Encryption
  - 10.2 Hashing
  - 10.3 Digital Signature
  - 10.4 Public Key Infrastructure (PKI)
  - 10.5 Identity and Access Management (IAM)
  - 10.6 Single Sign-On (SSO)
  - 10.7 Cloud-Based Security Groups
  - 10.8 Hardened Virtual Server Images

10.1 Encryption (1/3)

- 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.

Figure 10.1



- *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.)*

10.1 Encryption (2/3)

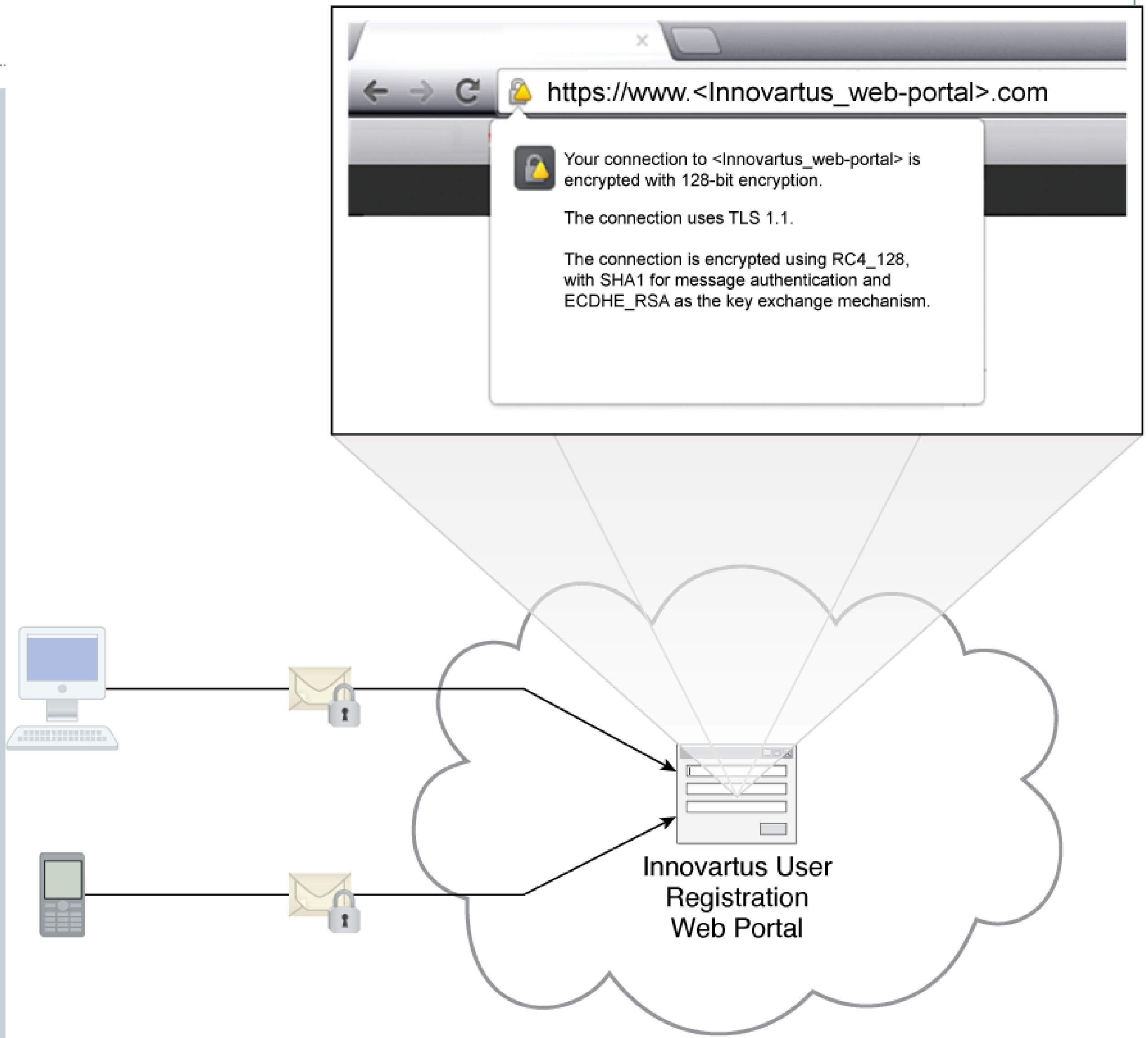
- Two common forms of encryption known as symmetric encryption and asymmetric encryption:
  - Symmetric encryption
    - Symmetric encryption uses the same key for both encryption and decryption, both of which are performed by authorized parties that one shared key.
    - It provides data confidentiality 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.

10.1 **Encryption** (3/3)

- Message that were encrypted with a private key can be correctly decrypted by any party with the corresponding public key. (以自己的私密加密送給對方，對方以公密解開)
  - 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.

Figure 10.2

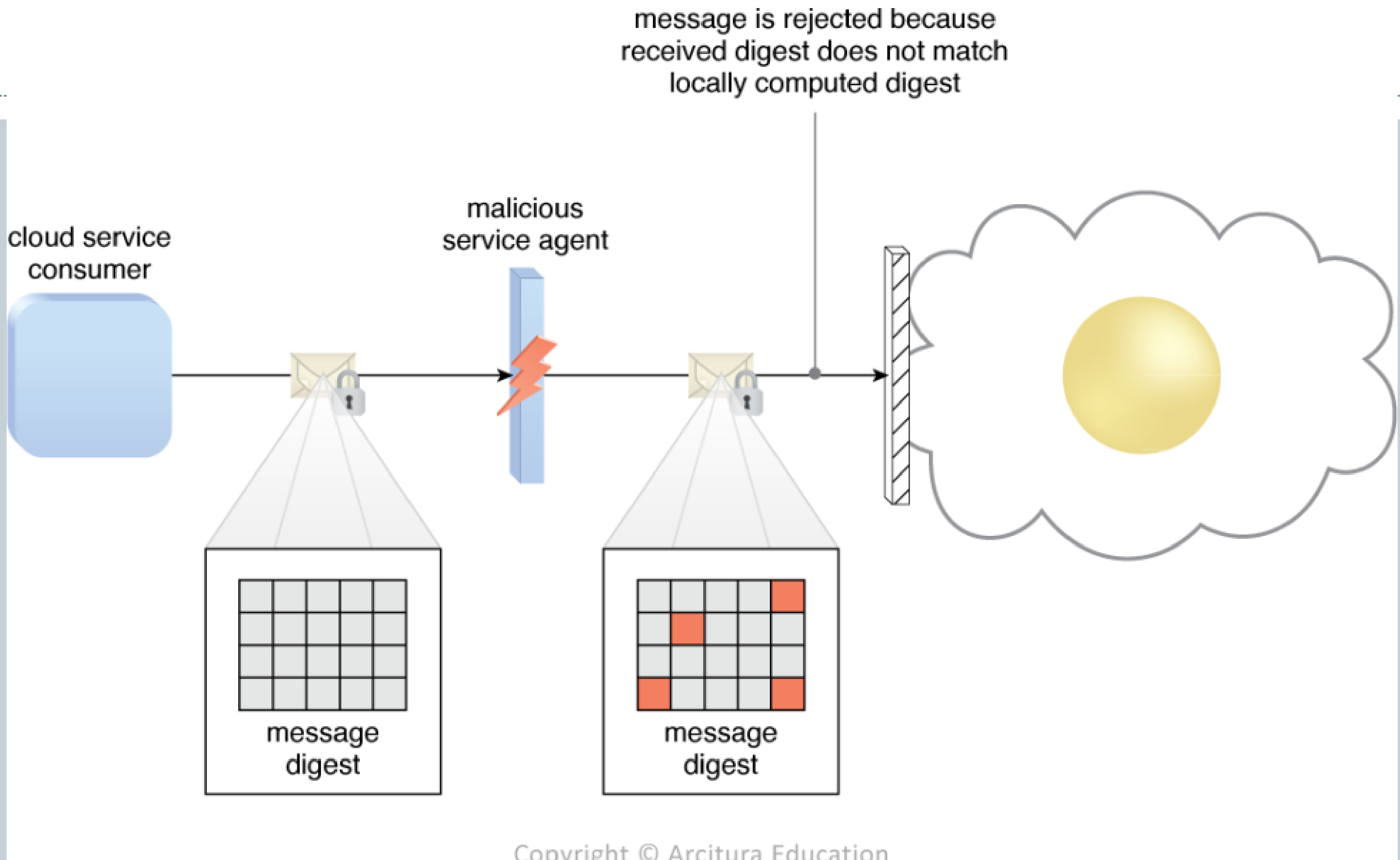
- *The encryption mechanism is added to the communication channel between outside users and Innovartus' User Registration Portal. This safeguards message confidentiality via the use of HTTPS (using SSL/TLS).*
- *TLS is a successor to SSL.*



10.2 Hashing

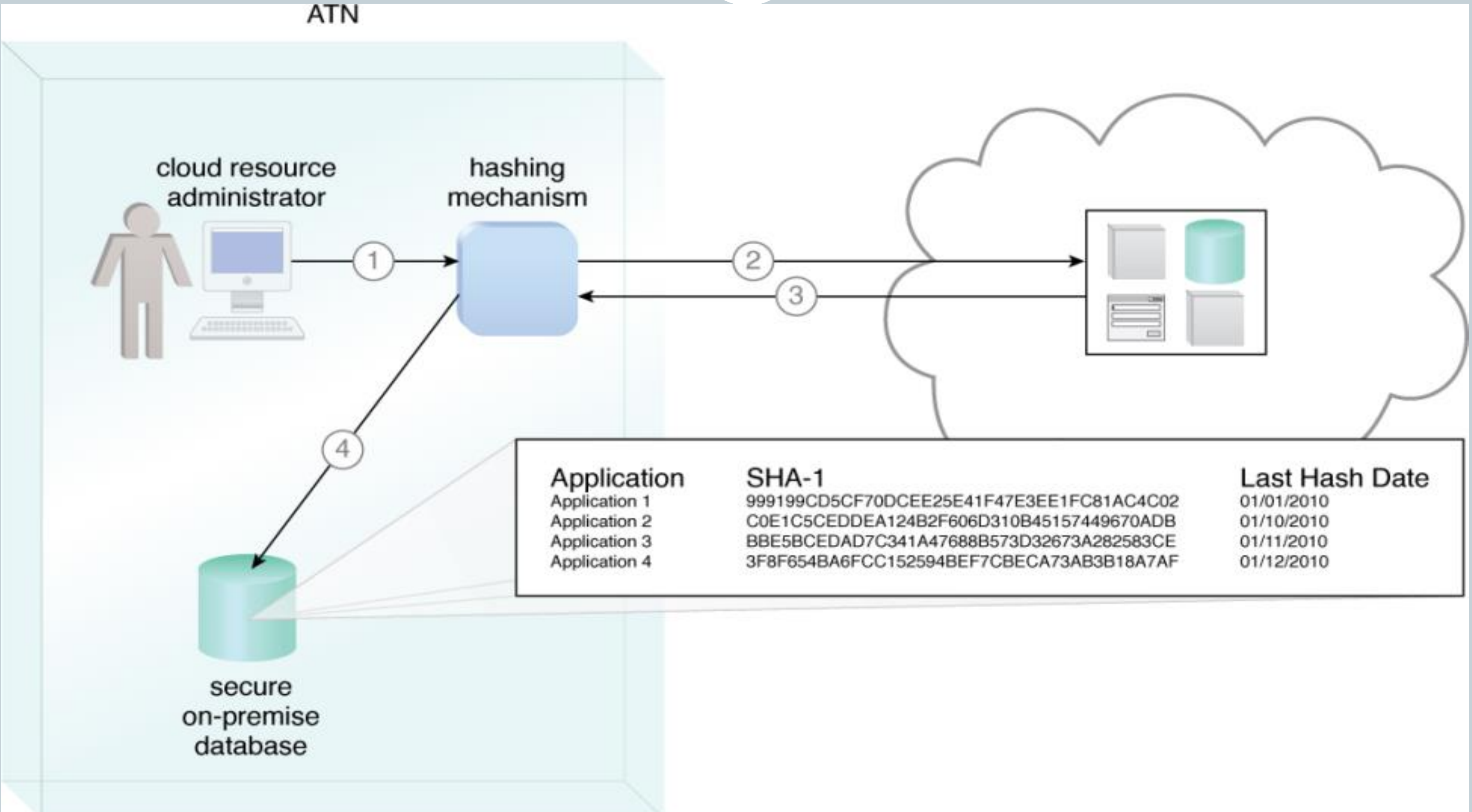
- The hashing mechanism is used when a one-way, non-reversible form of data protection is required.
- Hashing technology can be used to derive a hashing code or message digest from a message, which is often of a fixed length and smaller than the original message.
- A common application of hashing is 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.

Figure 10.3



- *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.*

Figure 10.4 (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

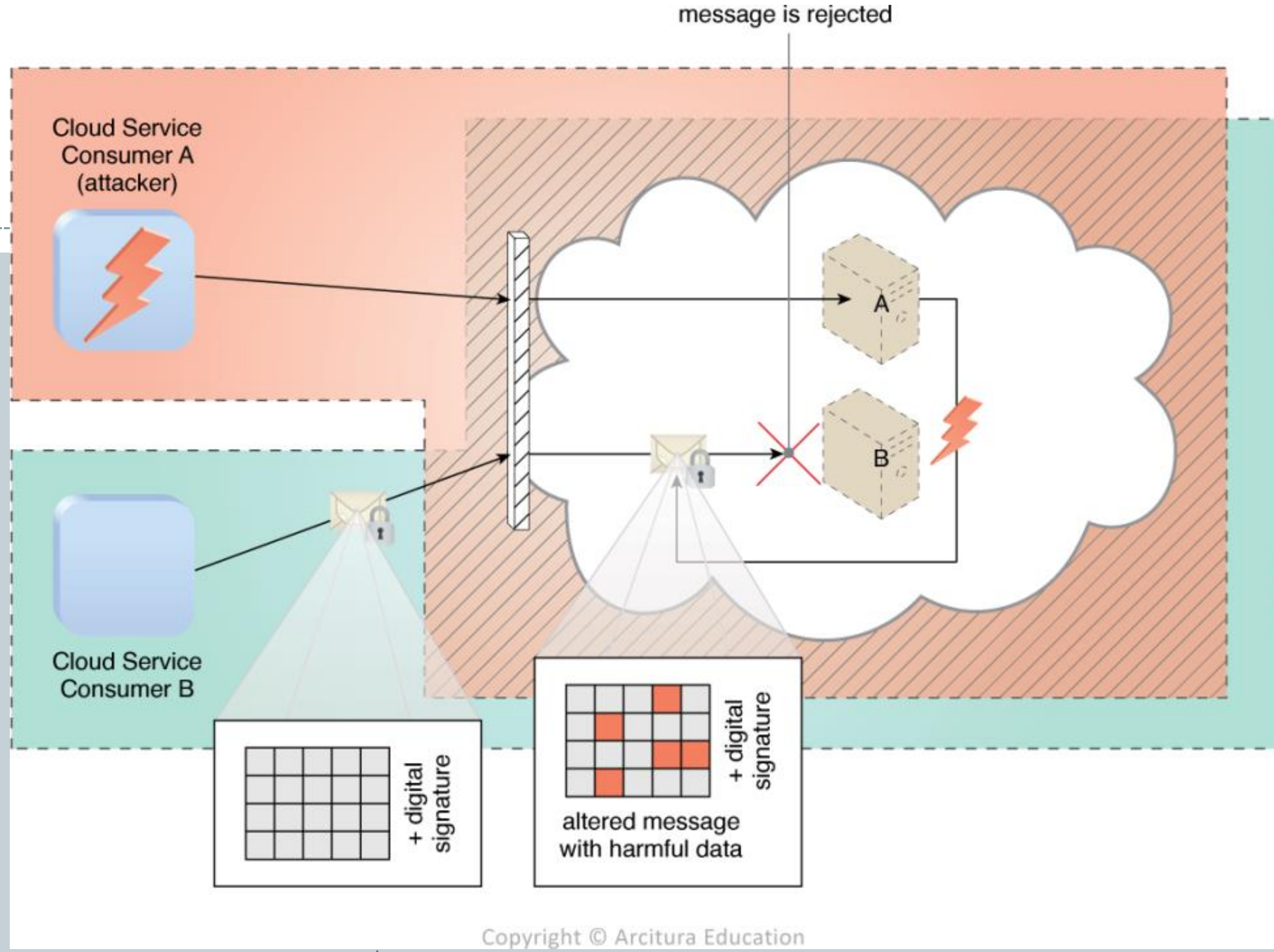
Figure 10.4 (ATN's Example)

- 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.

10.3 Digital Signature

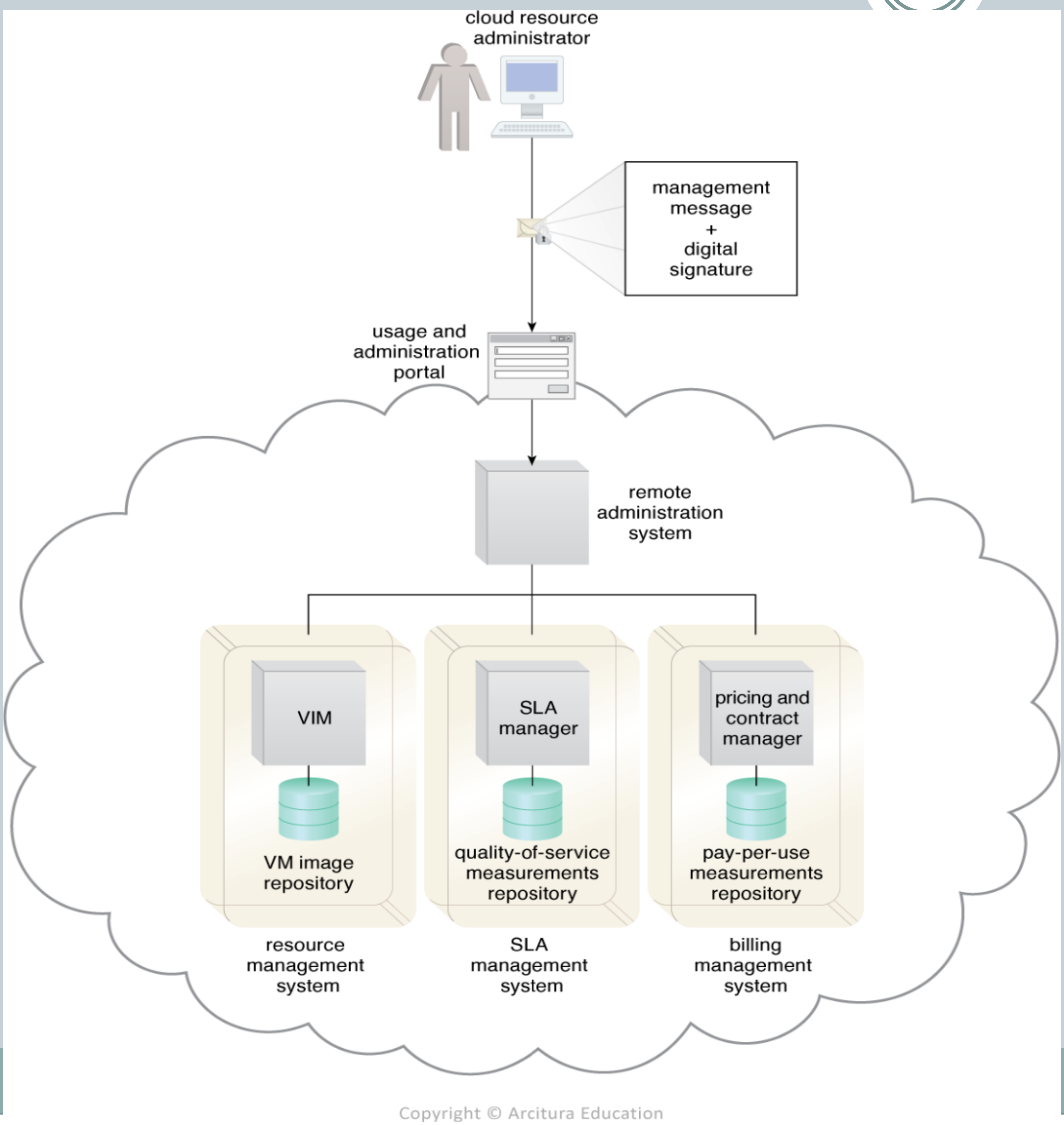
- The digital signature mechanism is a means of providing data authenticity and integrity through authentication and non-repudiation.
- Both hashing and asymmetrical encryption are involved in the creation of a digital signature, which essentially exists as a message digest that was encrypted by a private key and appended to the original message.

Figure 10.5



- *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.*

Figure 10.6 (DTGOV's Example)

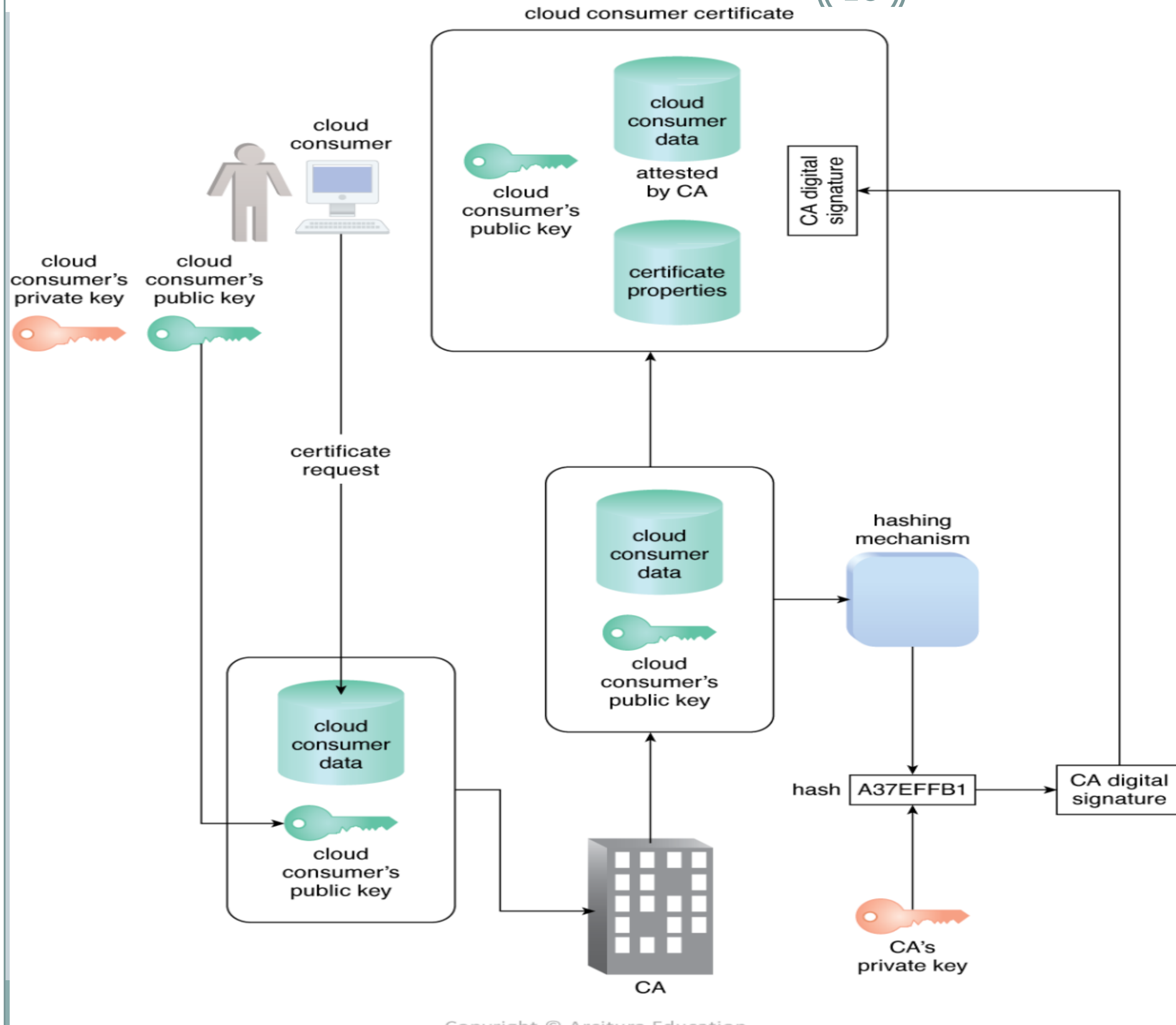


- Figure 10.6 - Whenever a cloud consumer performs a management action that is related to IT resources provisioned by DTGOV, the cloud service consumer program must include a digital signature in the message request to prove the legitimacy of its user.

10.4 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



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

10.4 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.

10.5 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

10.5 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.

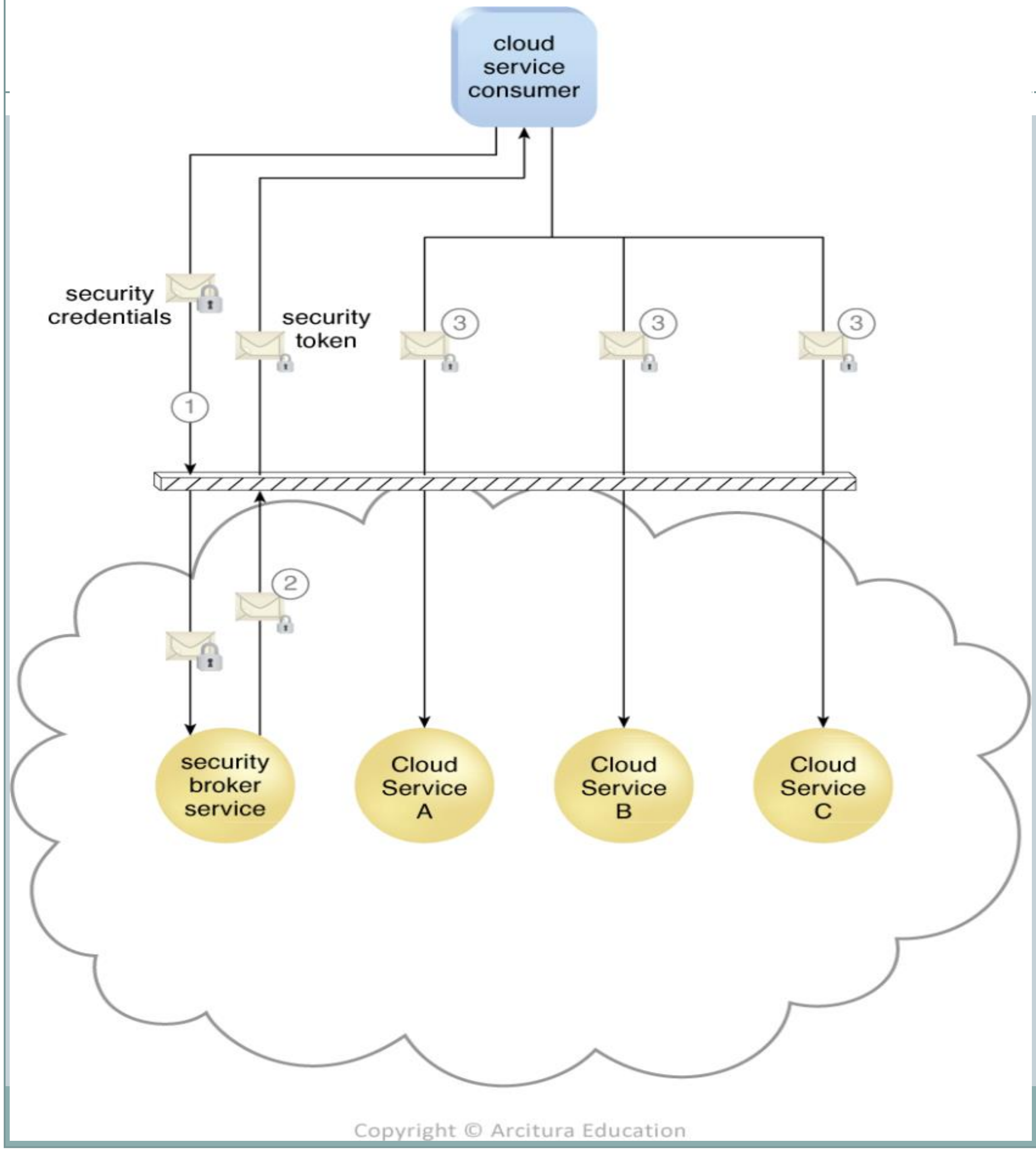
10.6 **Single Sign-On (SSO) (1/2)**

- 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.

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

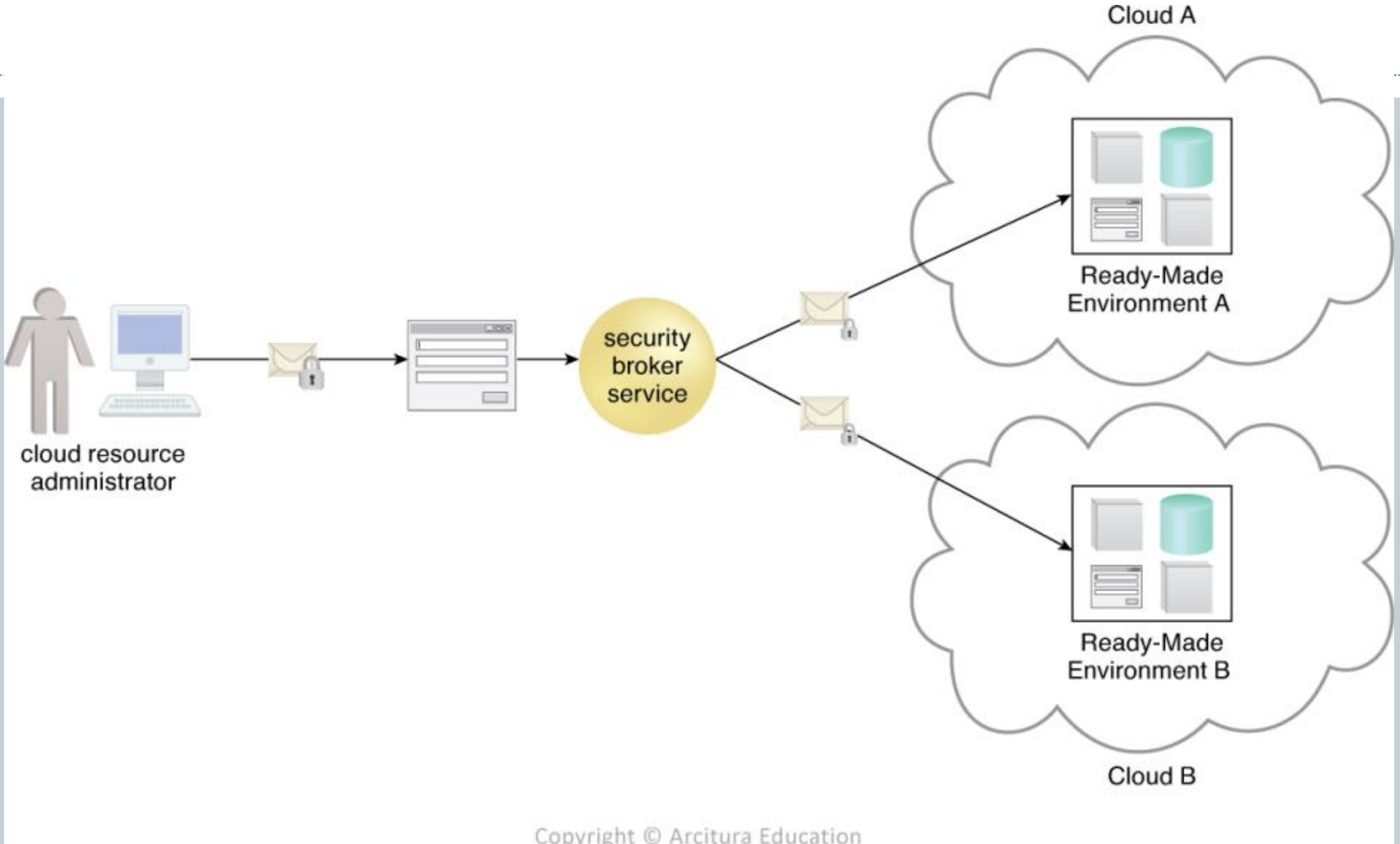
- The SSO mechanism essentially enables mutually independent cloud services and IT resources to generate and circulate runtime authentication and authorization credentials.
- SSO does not direct counter any of the cloud security threats. It primarily enhances the usability of cloud-based environments for access and management of resources and solutions.

Figure 10.9



- *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).*

Figure 10.10 (ATN's Example)



- *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.*

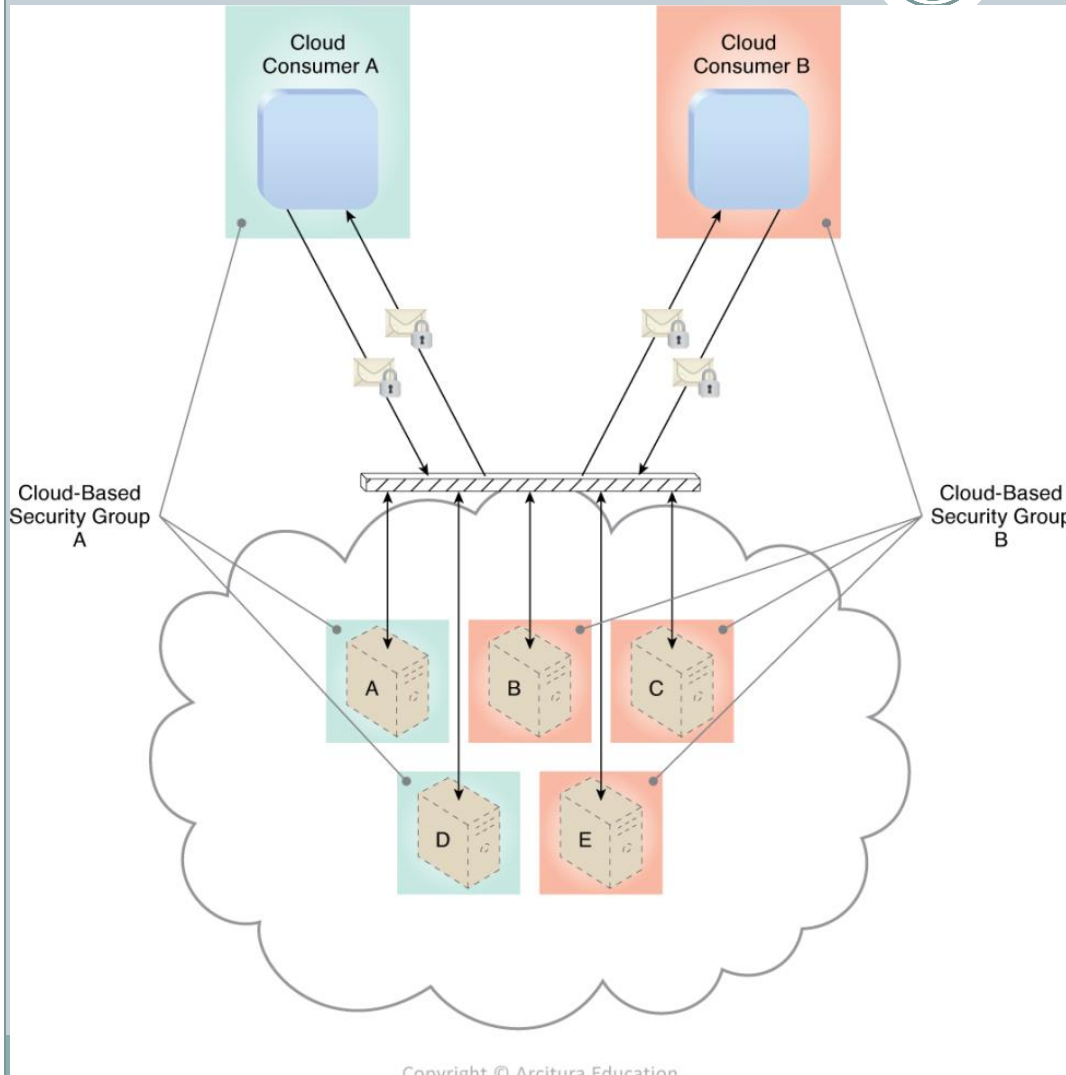
10.7 Cloud-Based Security Group (1/2)

- 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.

10.7 Cloud-Based Security Group (2/2)

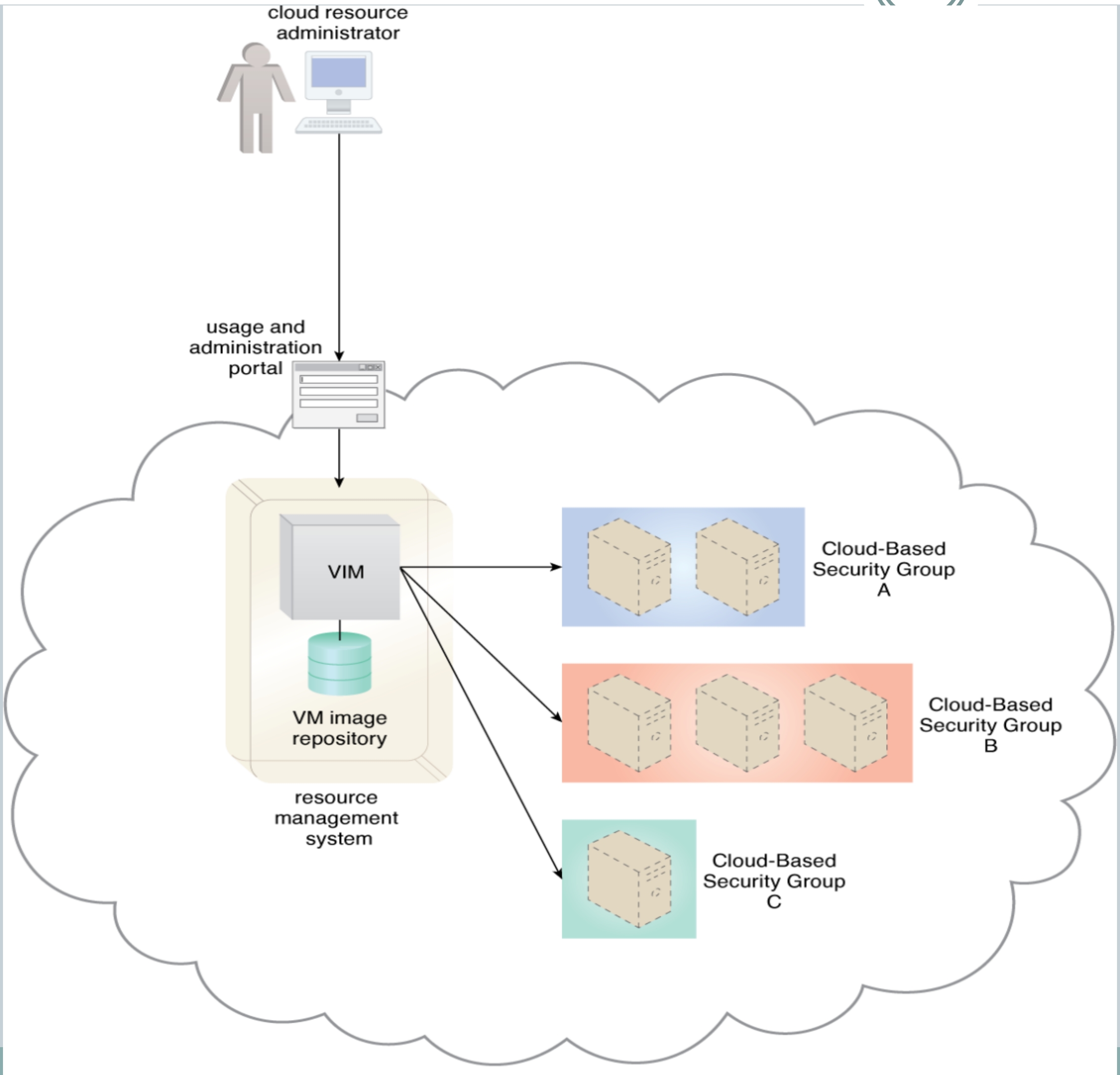
- Multiple virtual servers running on the same physical server can become members of different logical cloud-based security groups.
- Properly implemented cloud-based security groups help limit unauthorized access to IT resources in the event of a security breach.
- This mechanism can be used to help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

Figure 10.11



- 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.

Figure 10.12 (DTGOV's Example)



- 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.

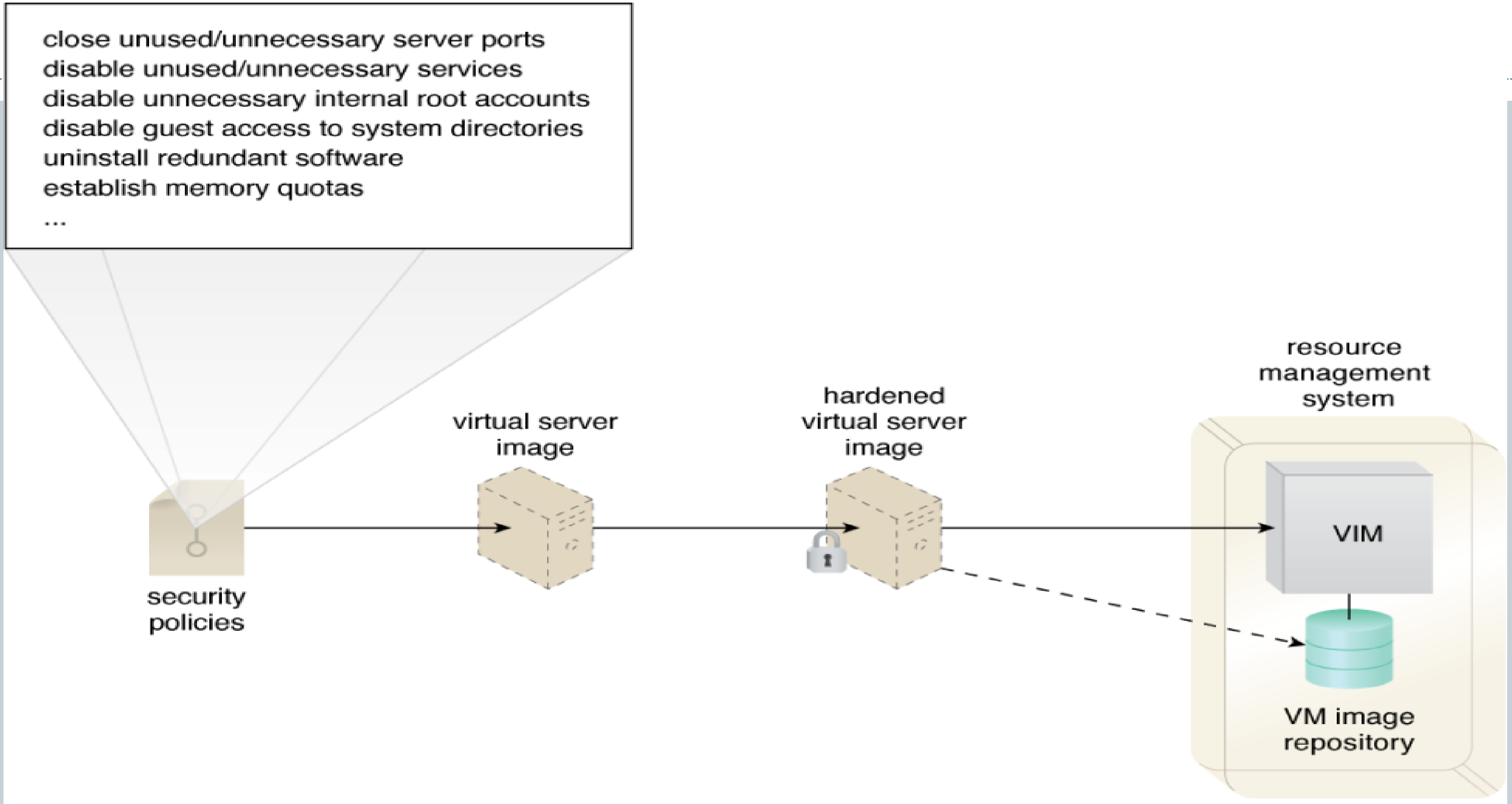
10.8 Hardened Virtual Server Images (1/2)

- 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.

10.8 Hardened Virtual Server Images (2/2)

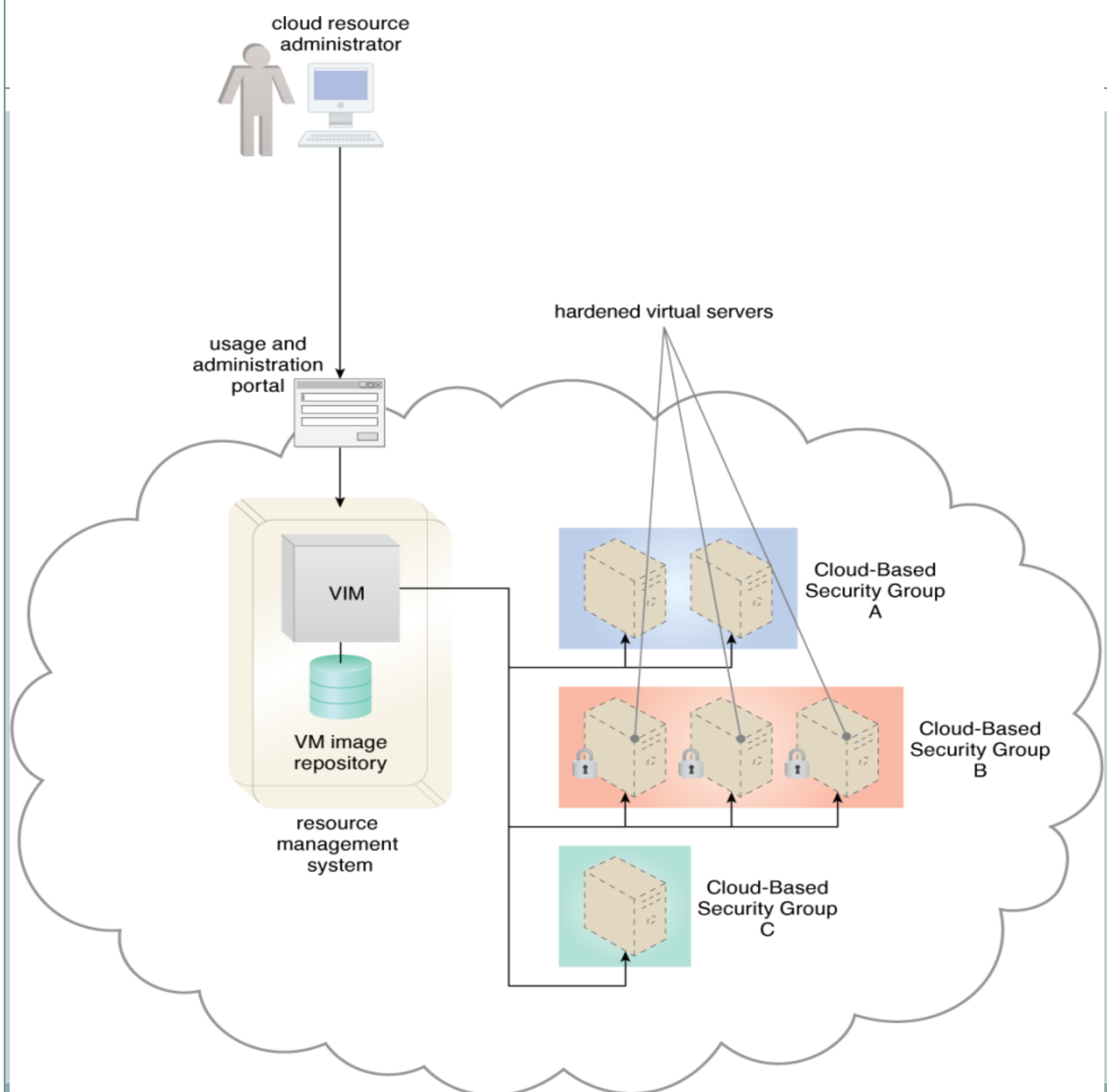
- A hardened virtual server image is a template for virtual service instance creation that has been subjected to a hardening process. It generally results in a virtual server template to be more secure than the original standard image.
- Hardened virtual server images help counter the denial of service, insufficient authorization, and overlapping trust boundaries threats.

Figure 10.13



- *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.*

Figure 10.14 (DTGOV's Example)



- 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.