॥ त्वं ज्ञानमयो विज्ञानमयोऽसि ॥

IIT Jodhpur

Excellence above all

SME

Technology • Innovation • Leadership

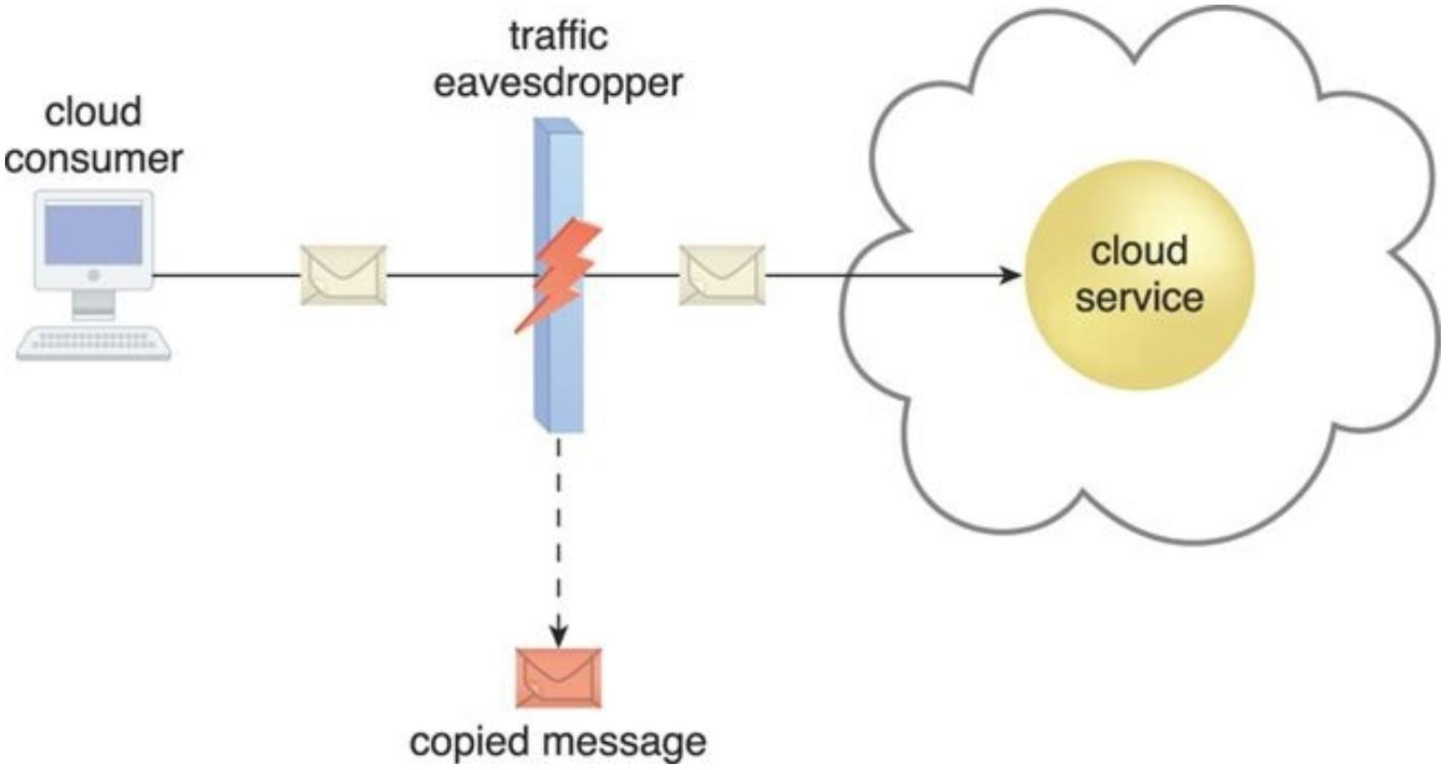
Cloud Security

Dr. Deepak Saxena, SME IIT Jodhpur

Cloud Security Threats

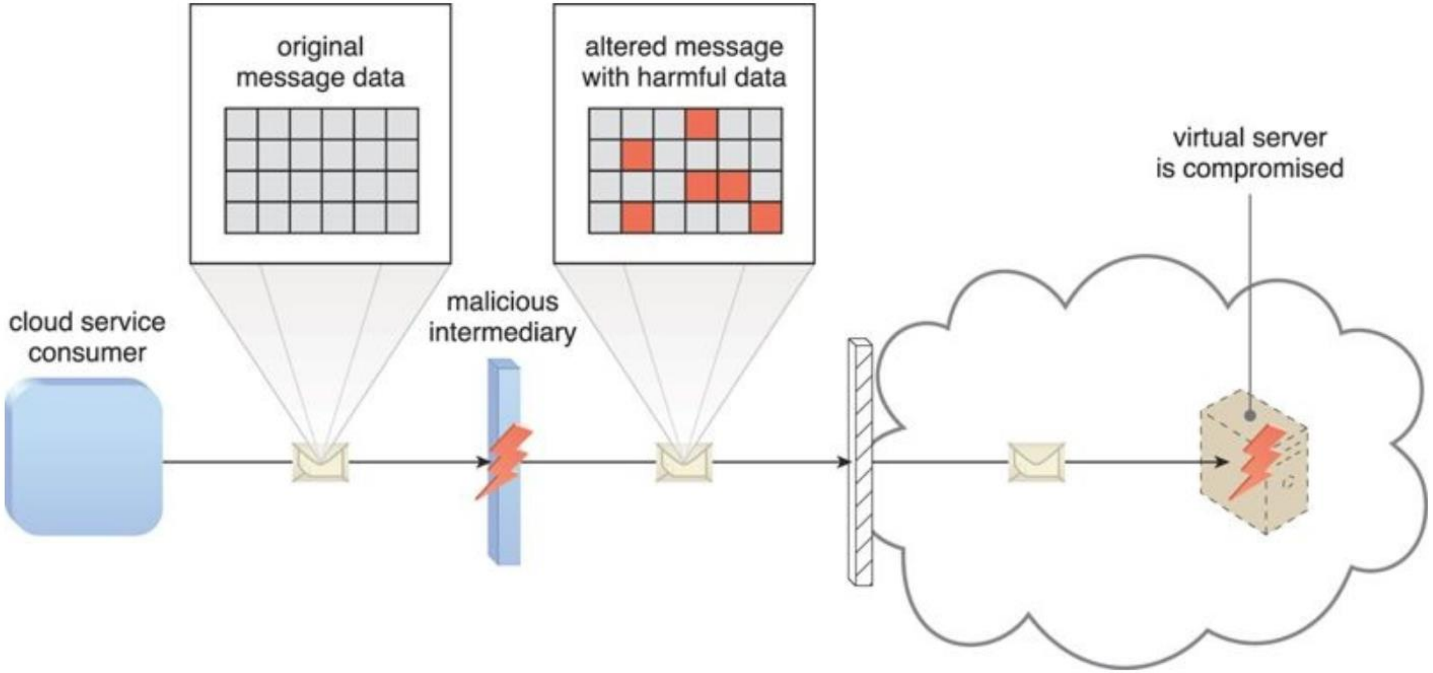
- Traffic Eavesdropping
- Malicious Intermediary
- Insufficient Authorization
- Denial of Service (DoS) Attack
- Virtualization Attack

Traffic Eavesdropping



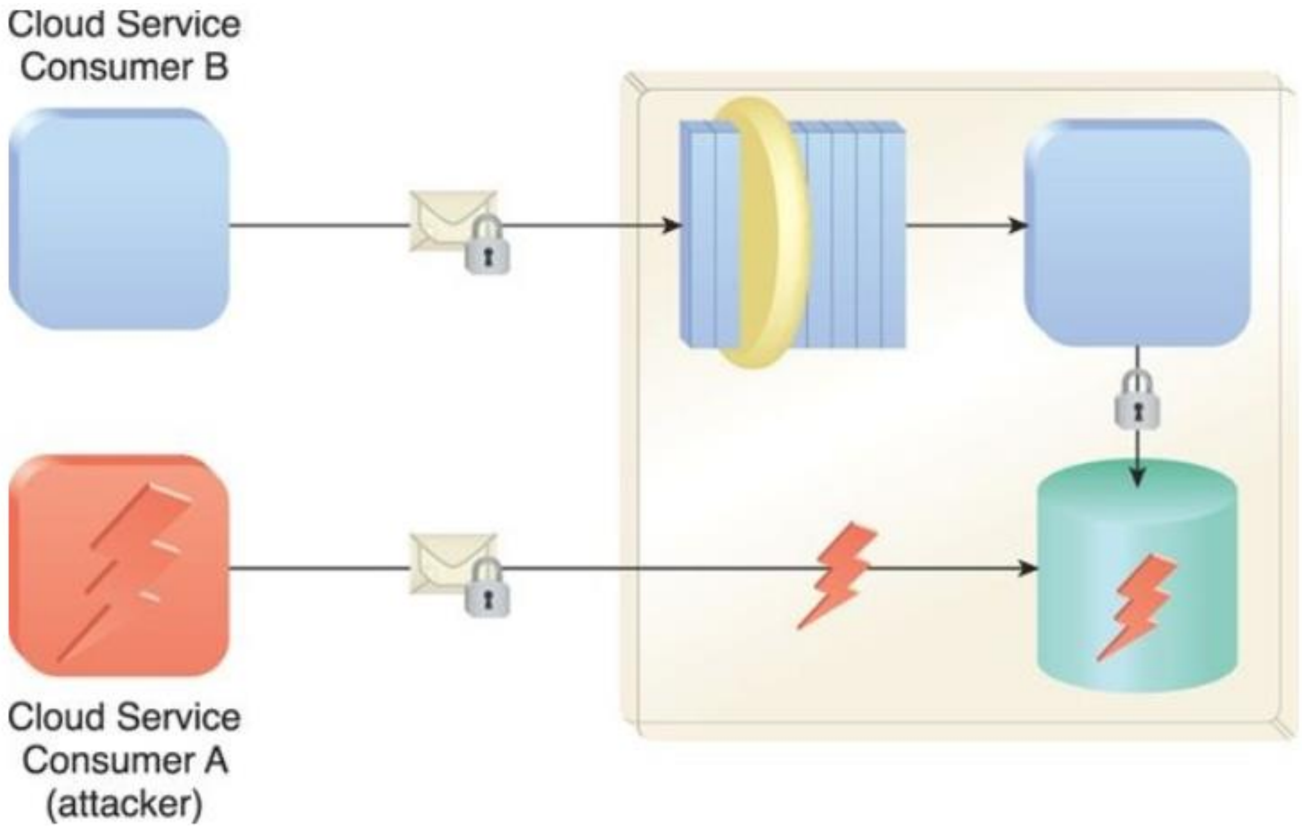
When data being transferred to or within a cloud (usually from the cloud consumer to the cloud provider) is passively intercepted by a malicious service agent for illegitimate information gathering purposes

Malicious Intermediary



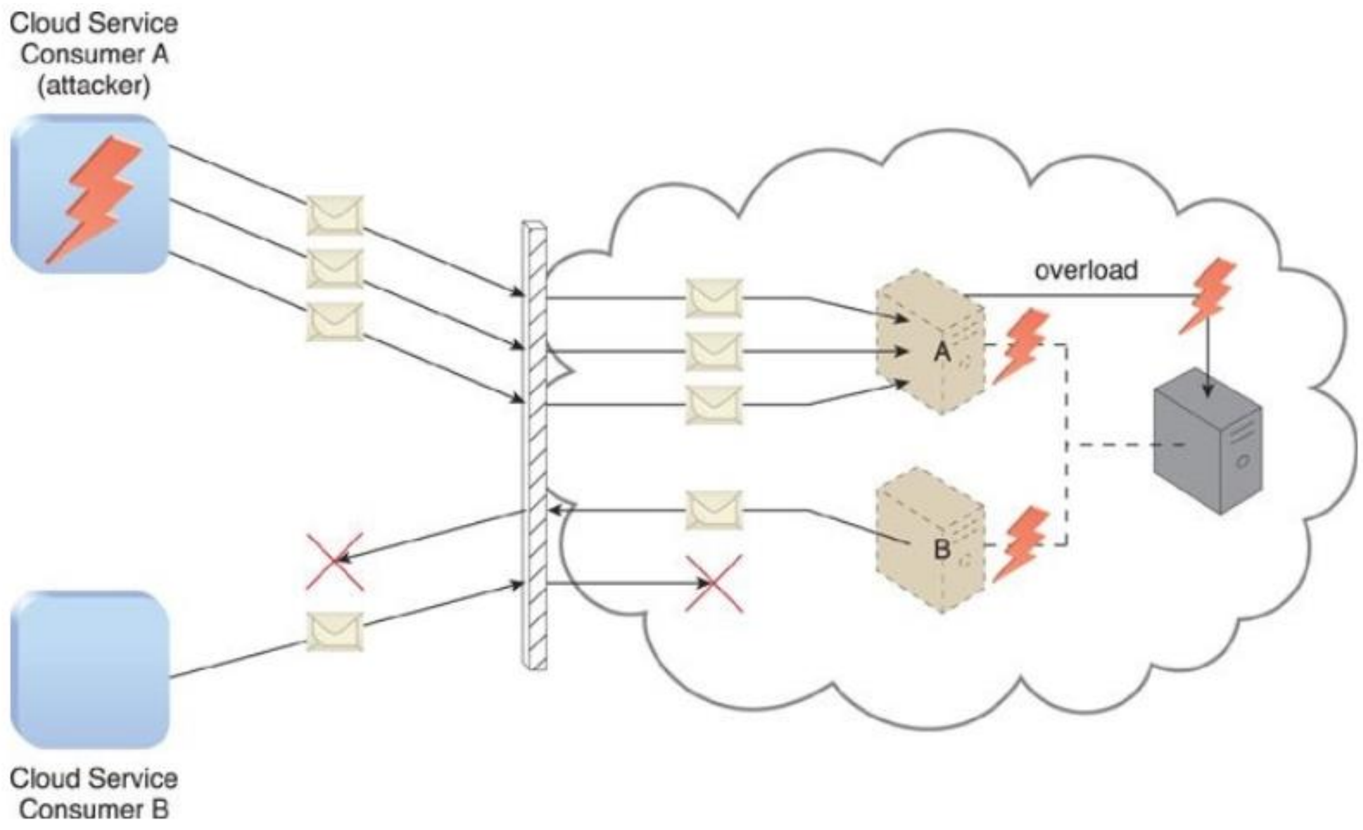
When messages are intercepted and altered by a malicious service agent, thereby potentially compromising the message's confidentiality and/or integrity.

Insufficient Authorization



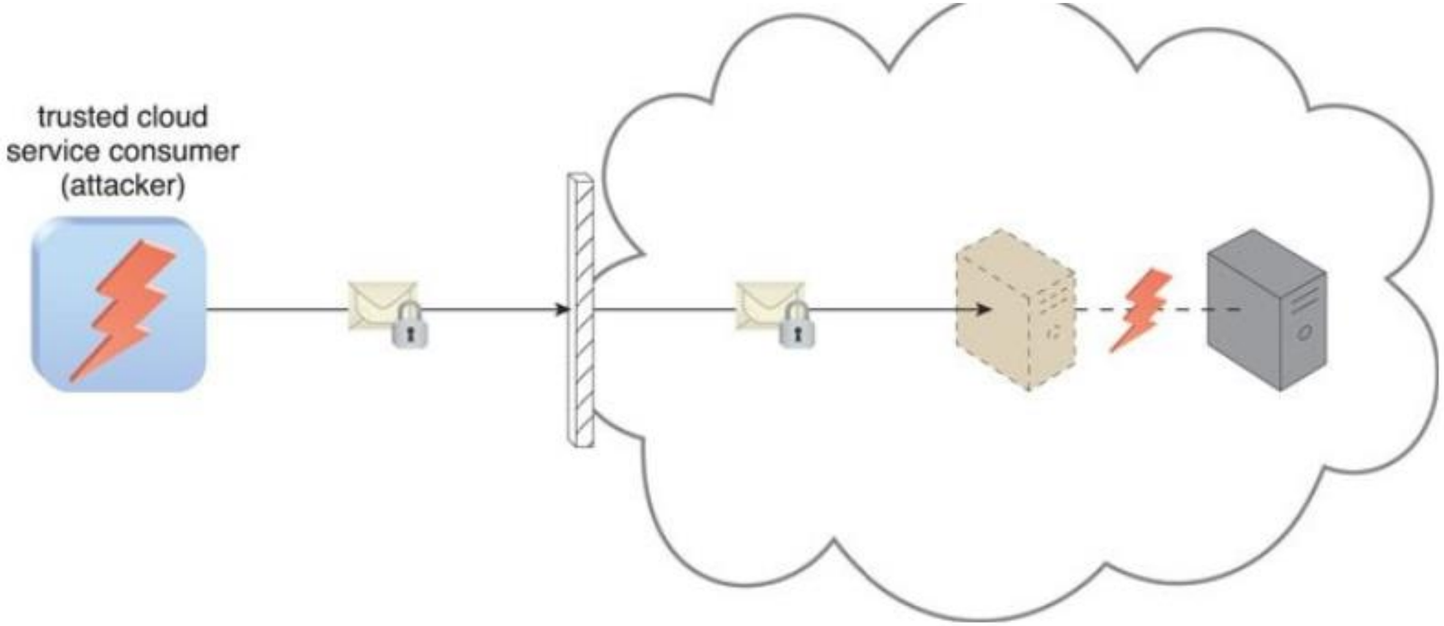
when access is granted to an attacker erroneously or too broadly, resulting in the attacker getting access to IT resources that are normally protected.

Denial of Service (DoS) Attack



Overloads IT resources to the point where they cannot function properly.

Virtualization Attack



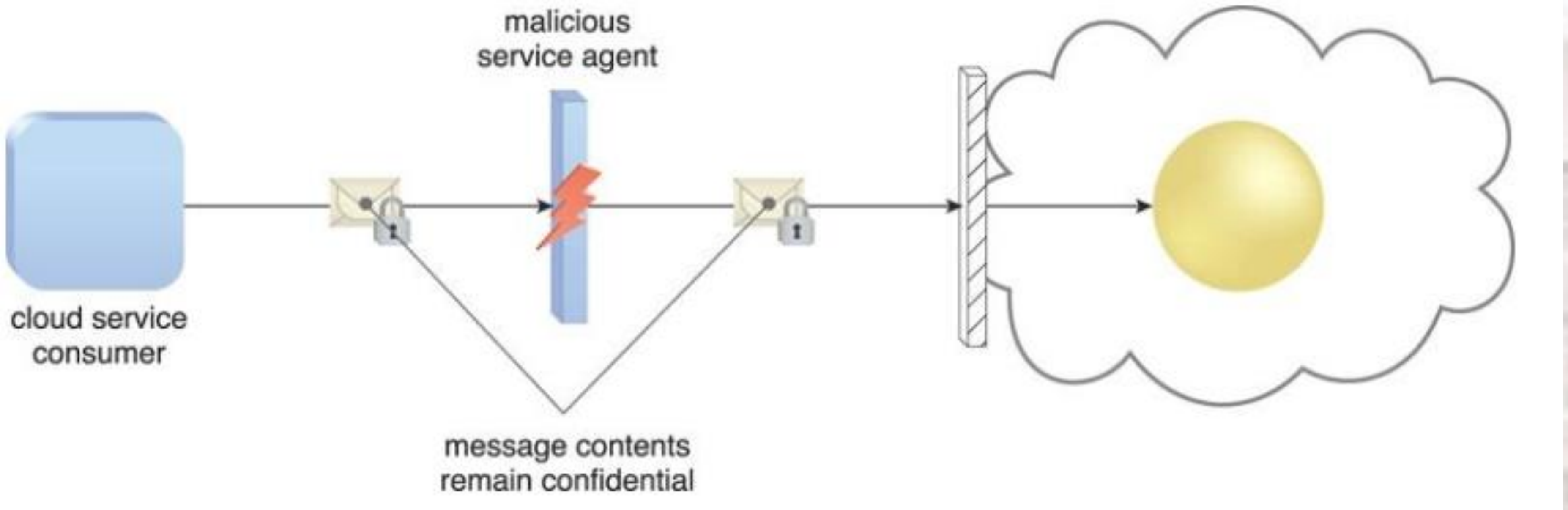
where a trusted attacker successfully accesses a virtual server to compromise its underlying physical server.

Cloud Security Mechanisms

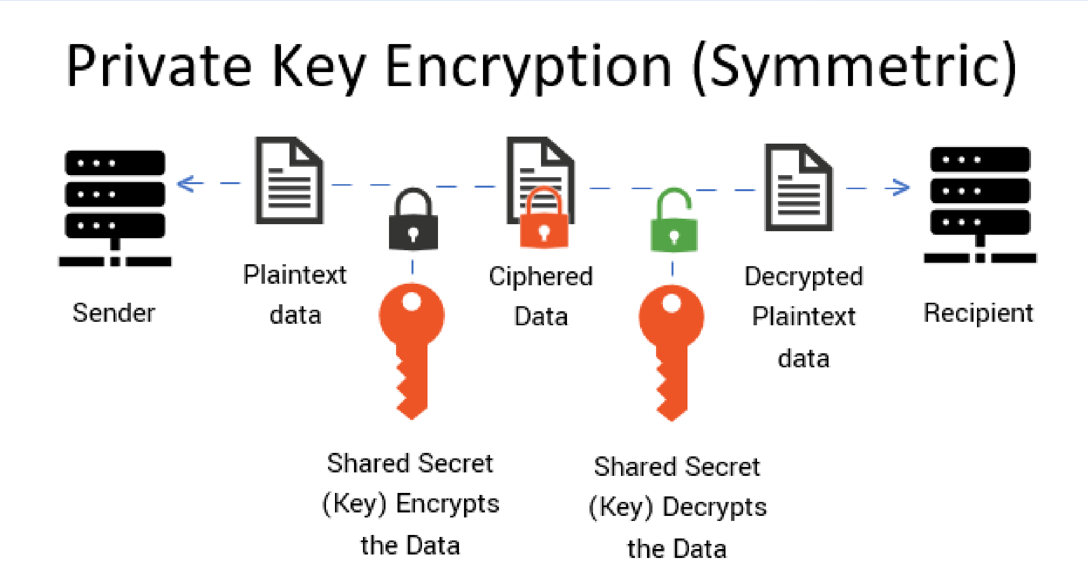
- (Public Key) Encryption
- Hashing
- Digital Signature
- Identity and Access Management (IAM)
- Single Sign-On (SSO)
- Cloud-Based Security Groups
- Hardened Virtual Server Images

Encryption

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.



Symmetric vs Asymmetric Encryption



Private Key Encryption (Symmetric)

Sender

Plaintext data

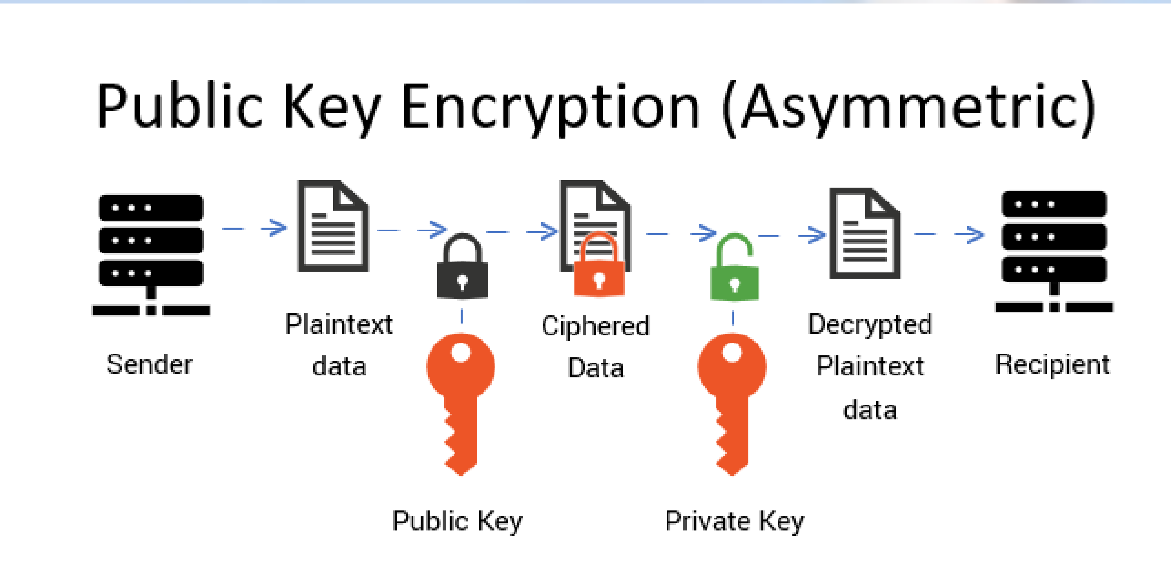
Ciphered Data

Decrypted Plaintext data

Recipient

Shared Secret (Key) Encrypts the Data

Shared Secret (Key) Decrypts the Data



Public Key Encryption (Asymmetric)

Sender

Plaintext data

Ciphered Data

Decrypted Plaintext data

Recipient

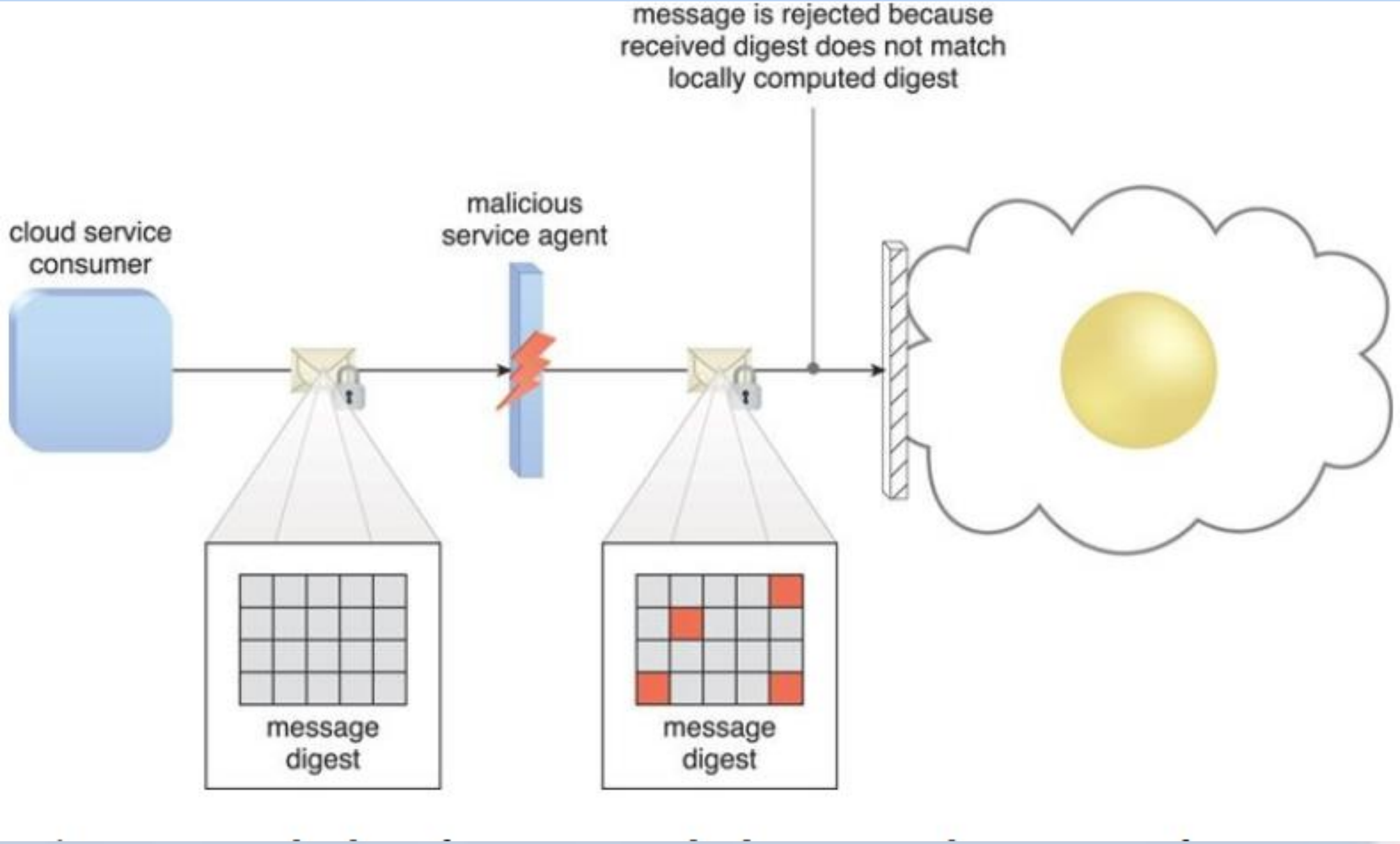
Public Key

Private Key

Hashing

- 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.

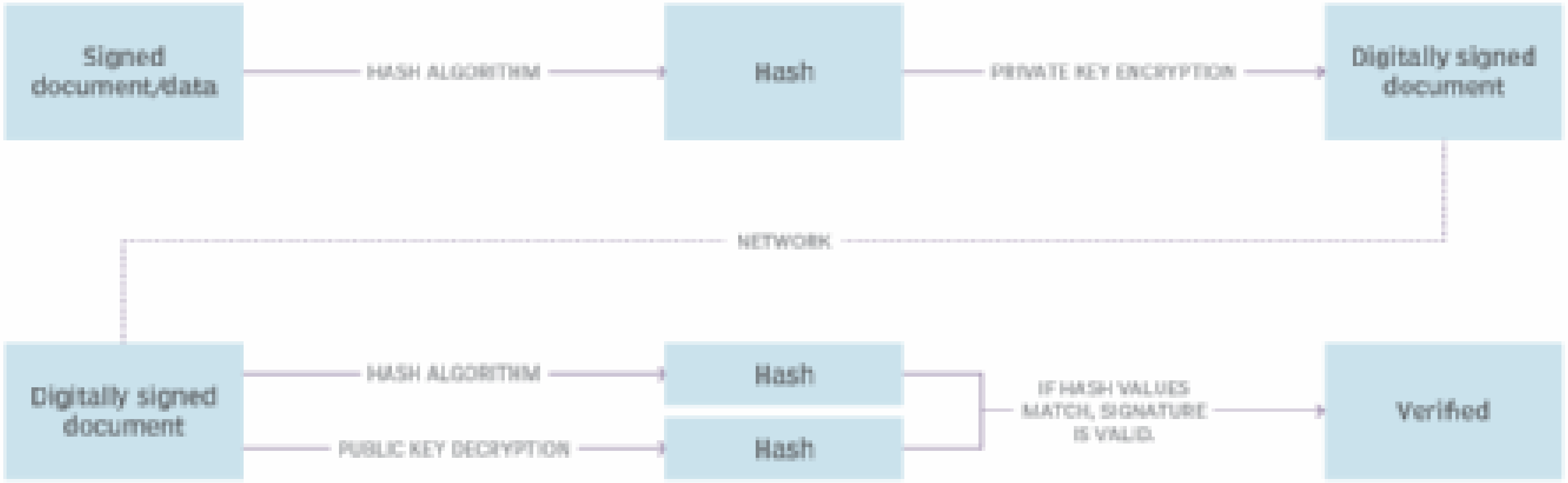
How hashing provides integrity?



Digital Signature

- A message is assigned a digital signature prior to transmission, which is then rendered invalid if the message experiences any subsequent, unauthorized modifications.
- 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.
- Hashes are used to verify the message integrity only, digital signatures are used to verify message authenticity and message integrity both.

The digital signature process



Signed document/data

HASH ALGORITHM

Hash

PRIVATE KEY ENCRYPTION

Digitally signed document

NETWORK

Digitally signed document

HASH ALGORITHM

Hash

PUBLIC KEY DECRYPTION

Hash

IF HASH VALUES MATCH, SIGNATURE IS VALID.

Verified

Identity and Access Management (IAM)

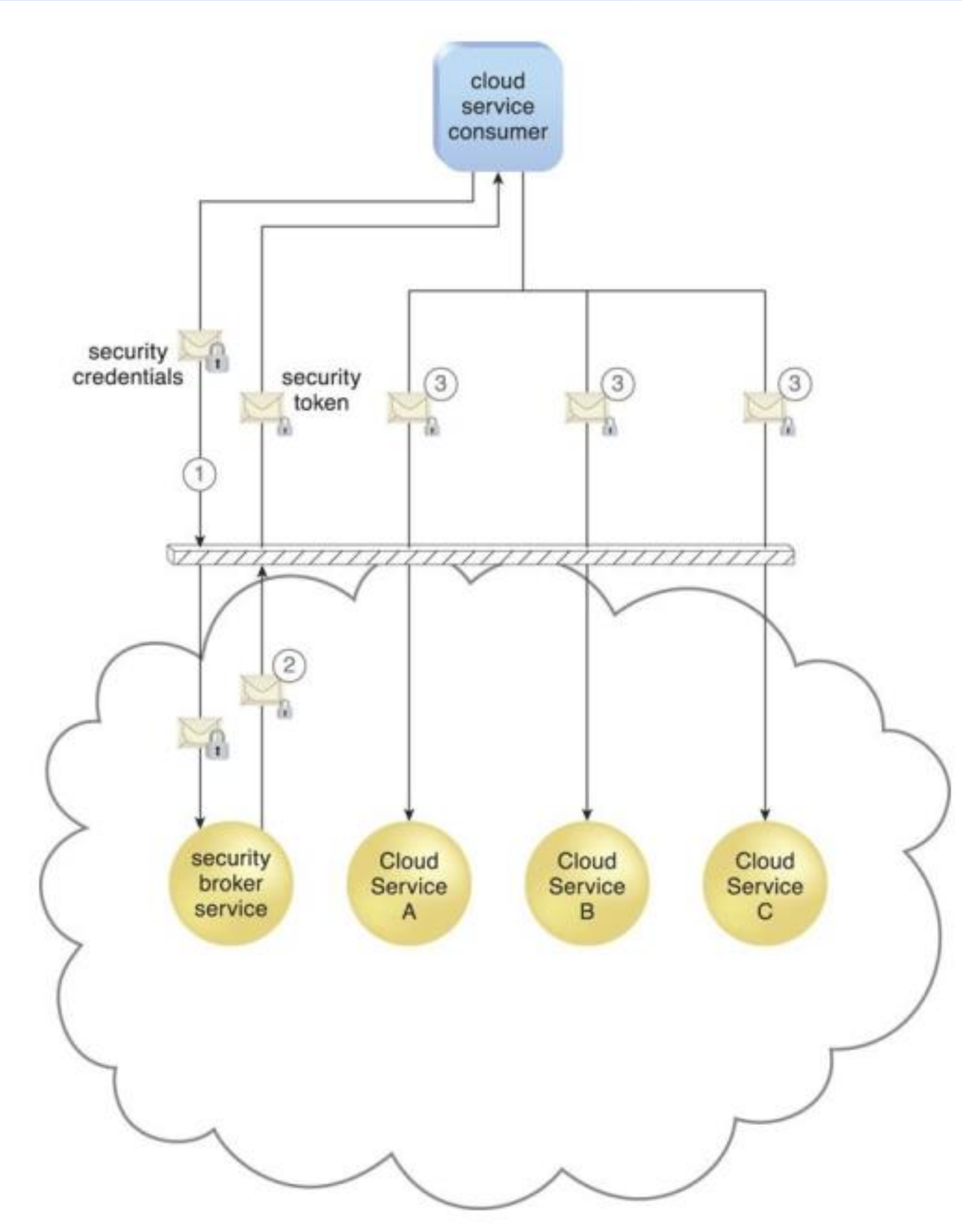
- Authentication (Who you are?)
- Authorization (What you can do?)
- User Management
- Credential Management

Single Sign-on (SSO)

- 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.
- Less about security per se, more about ease of security for the user.

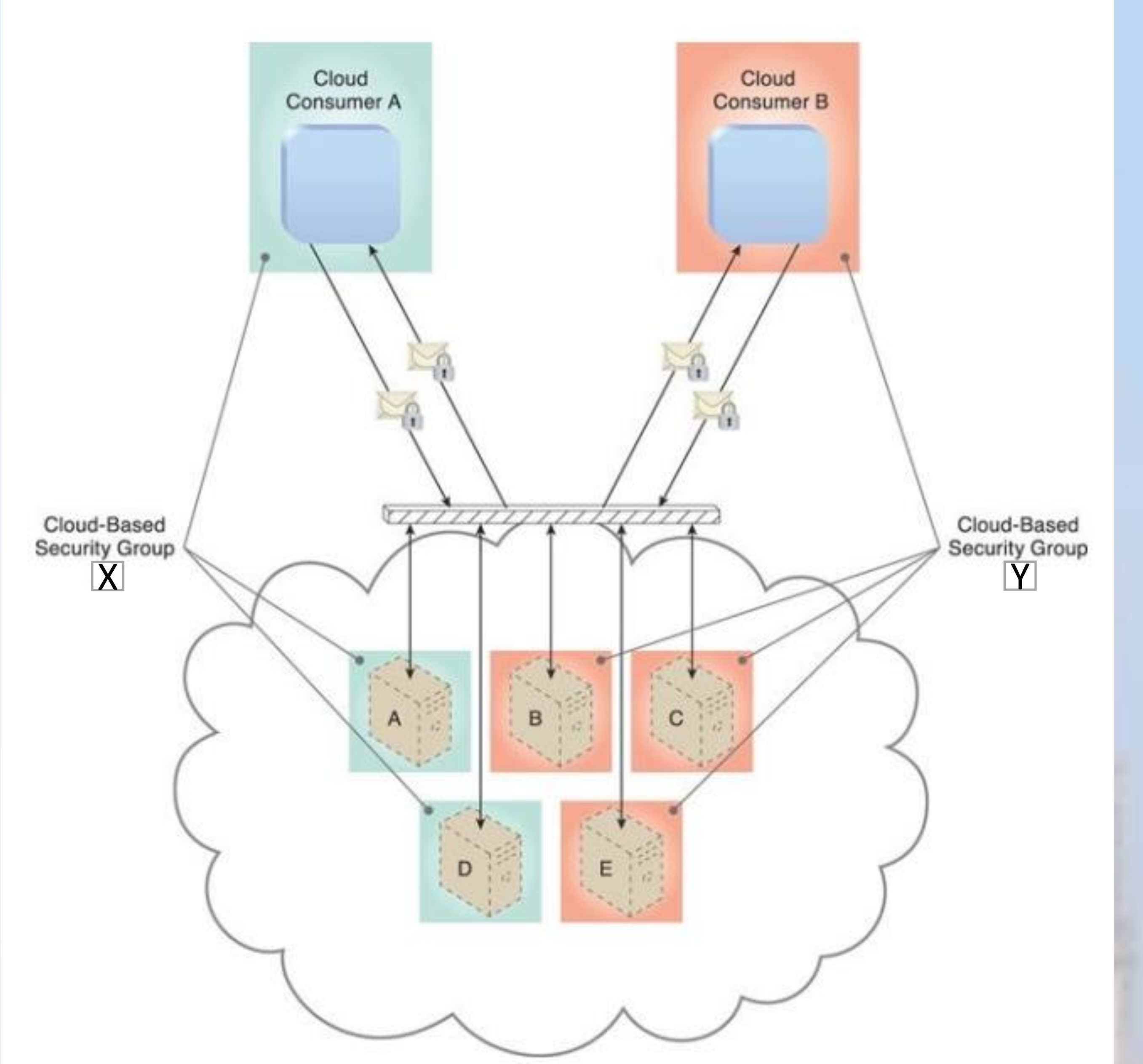
SSO Process

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



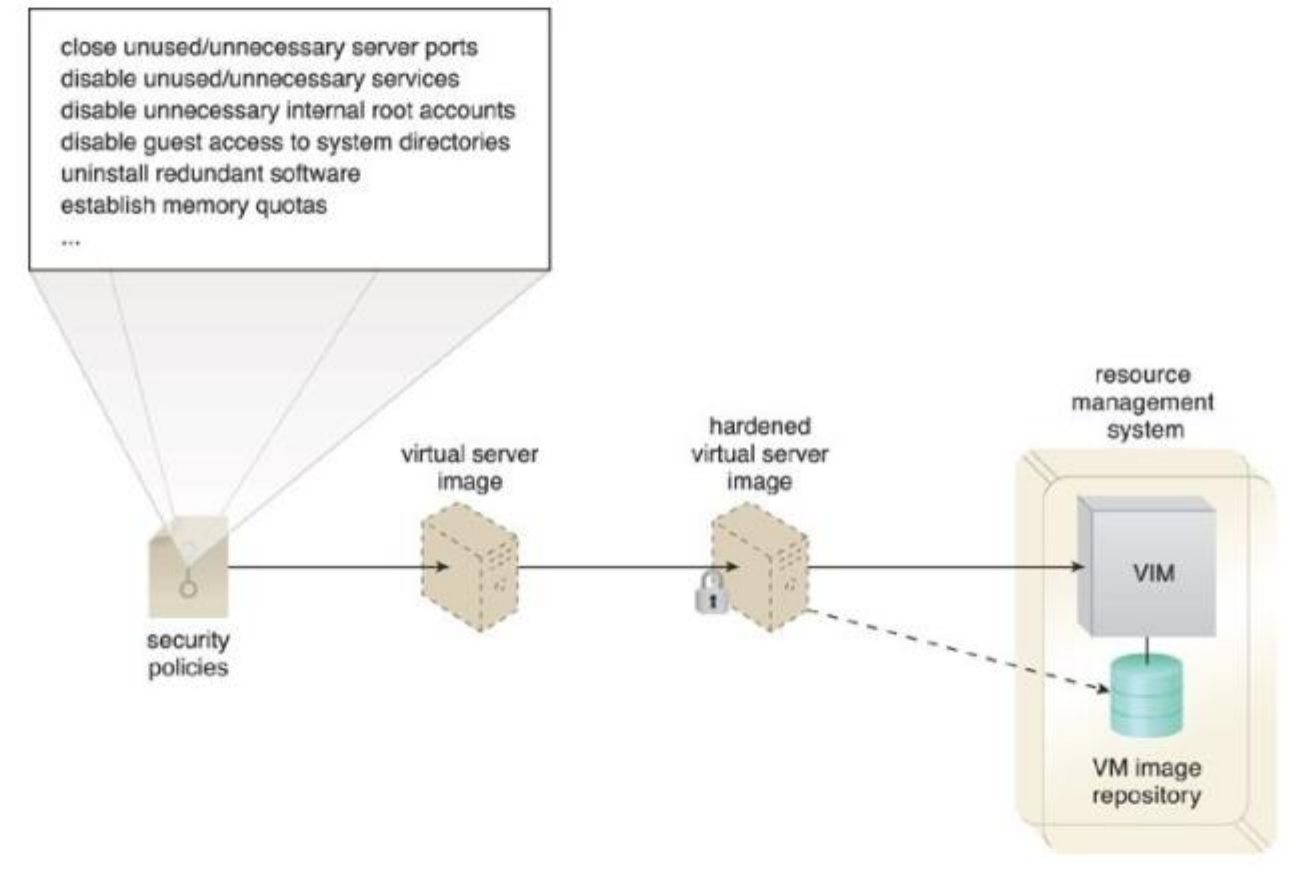
Cloud-Based Security Groups

- Cloud resource segmentation is a process by which separate physical and virtual IT environments are created for different users and groups.
- The cloud-based resource segmentation process creates cloud-based security group mechanisms that are determined through security policies.



Hardened Virtual Server Images

- 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.



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
...

I HAVE A PARTICULAR SET OF SKILLS...
NETWORK SECURITY, CLOUD SOLUTIONS, DATA RECOVERY, AND 24/7 MANAGED SERVICES
imgflip.com