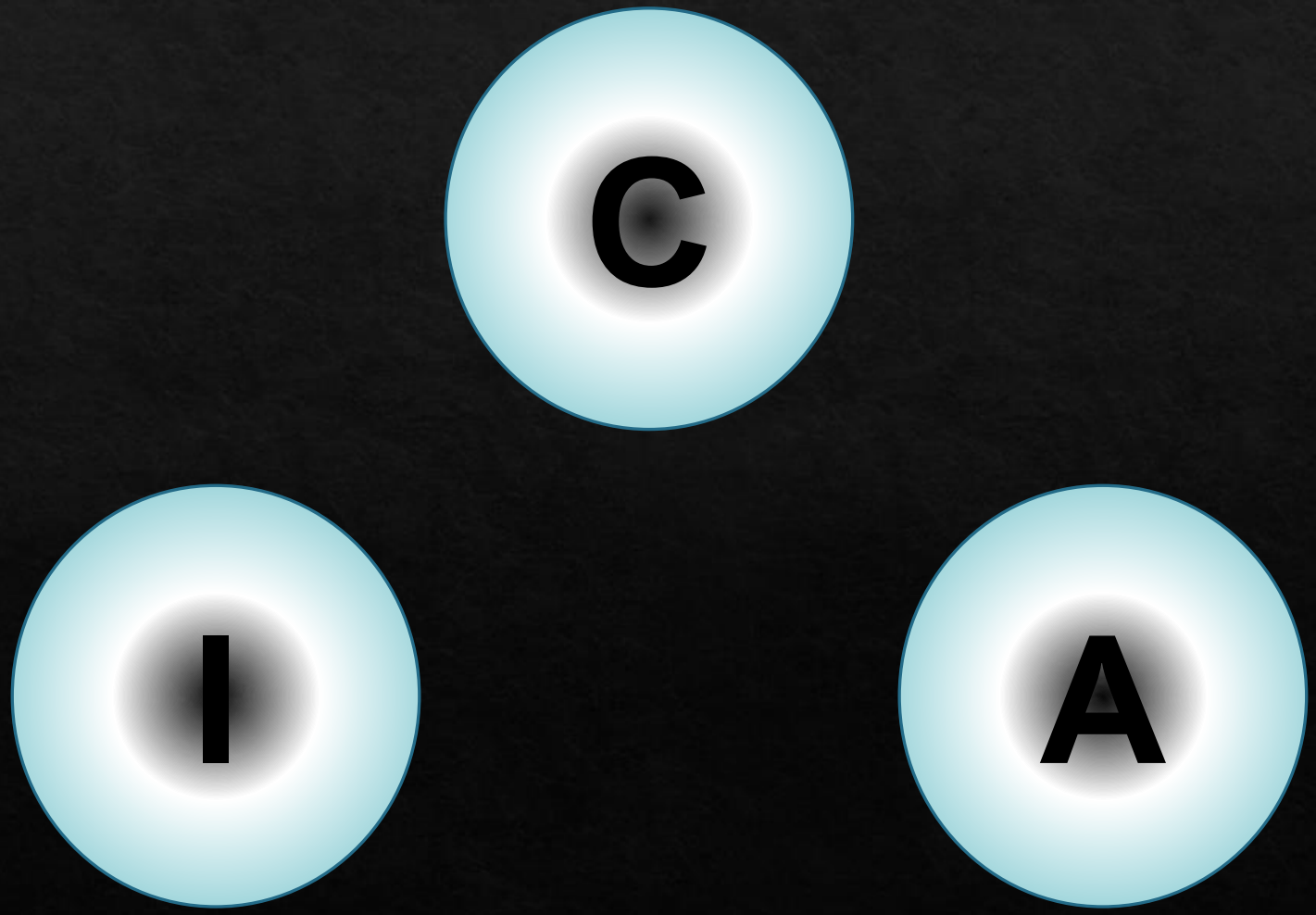
Cloud Security Fundamental

Basic Concepts

- Information security is a complex ensemble of
  - techniques,
  - technologies, regulations, and
  - behaviors

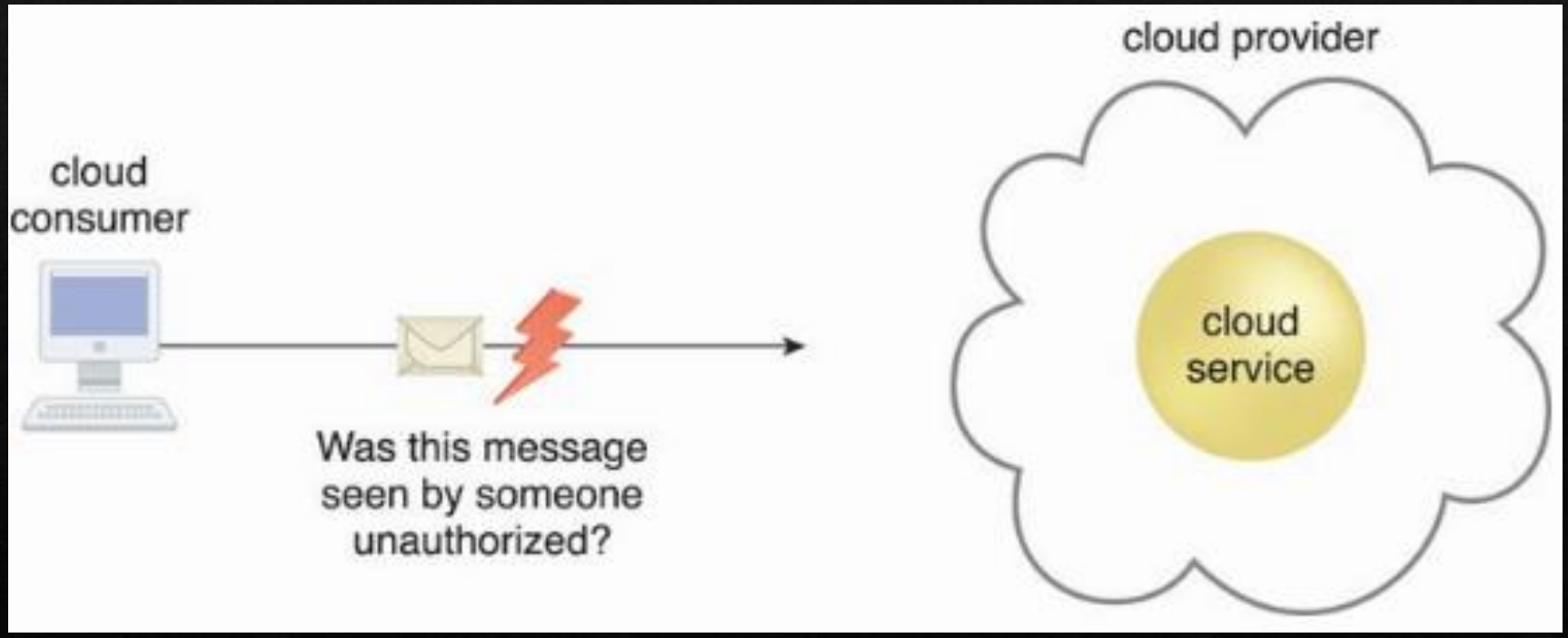
  that collaboratively protect the integrity of and access to computer systems and data.
- IT security measures aim to defend against threats and interference that arise from both malicious intent and unintentional user error.

Basic Concepts (2)



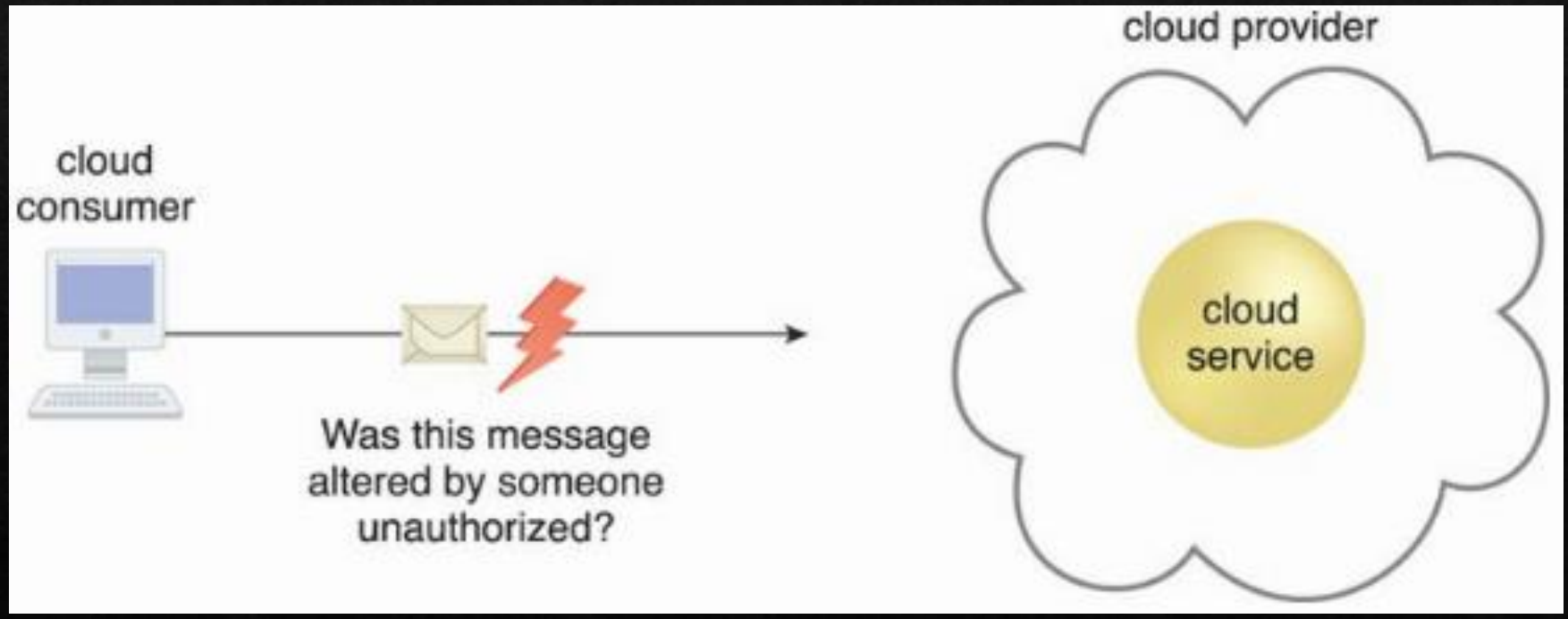
Confidentiality

- The characteristic of something being made accessible only to authorized parties.



Integrity

- The characteristic of not having been altered by an unauthorized party.



Authenticity

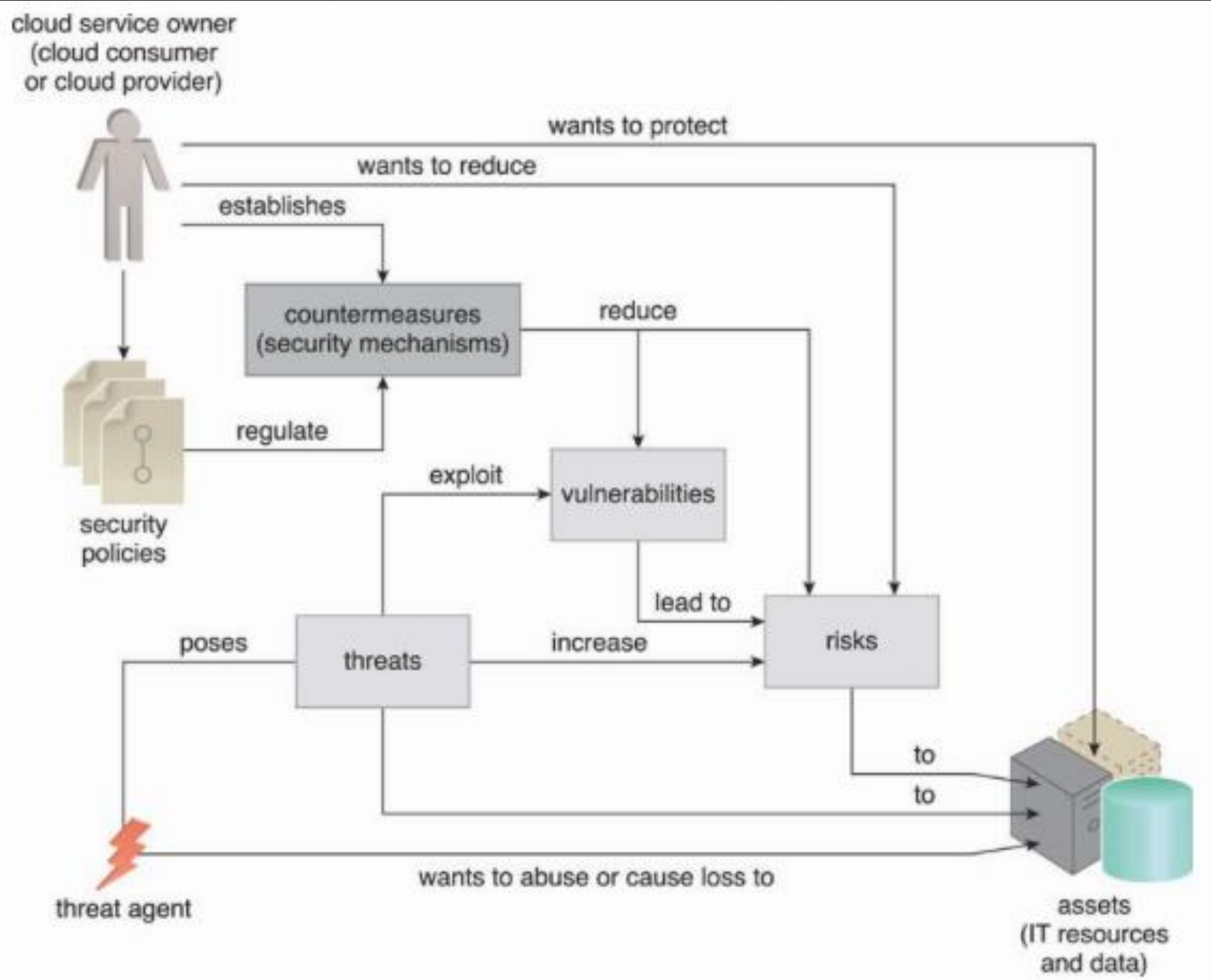
- The characteristic of something having been provided by an authorized source. This also encompasses non-repudiation.
- Non-repudiation?
  - The inability of a party to deny or challenge the authentication of an interaction.

Other Relevant Terms

- **Availability** - being accessible and usable during a specified time period.
- **Threat** - a potential security violation that can challenge defenses in an attempt to breach privacy and/or cause harm.
- Vulnerabilities - a weakness that can be exploited because it is protected by insufficient security controls.
- **Risk** - the possibility of loss or harm arising from performing an activity.

Other Relevant Terms (2)

- **Security Controls** - countermeasures used to prevent or respond to security threats and to reduce or avoid risk.
- **Security Mechanisms** - components comprising a defensive framework that protects IT resources, information, and services.
- **Security Policies** - a set of security rules and regulations that enforce security controls and mechanisms.


cloud service owner
(cloud consumer
or cloud provider)
wants to protect
wants to reduce
establishes
countermeasures
(security mechanisms)
reduce
regulate
security
policies
exploit
vulnerabilities
lead to
poses
threats
increase
risks
to
to
wants to abuse or cause loss to
threat agent
assets
(IT resources
and data)

Common Threat Agents

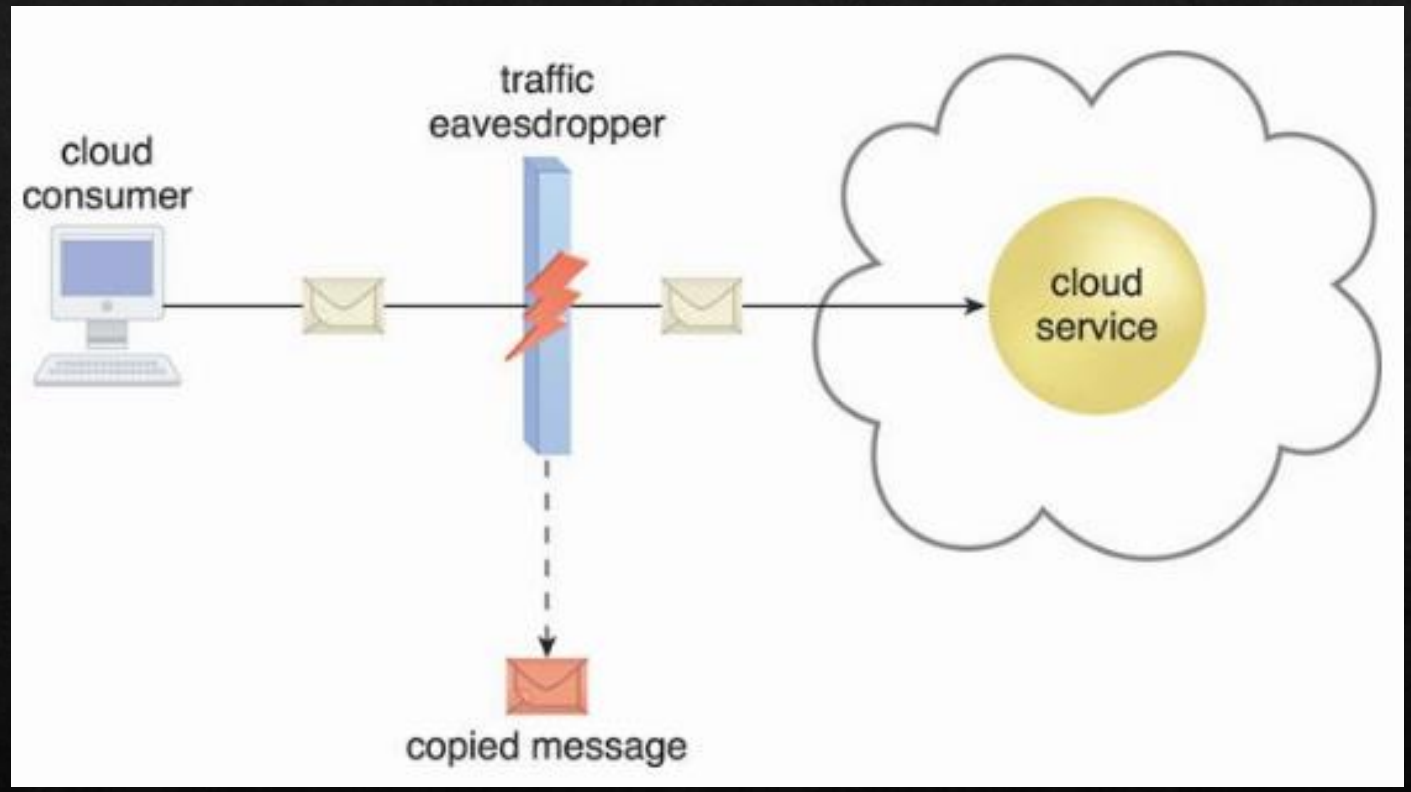
- A threat agent?
  - an entity that poses a threat because it is capable of carrying out an attack.
- Originated from?
  - either internally or externally, from humans or software programs.

Types of Threat Agents/Attackers

- **Anonymous Attackers** - a non-trusted cloud service consumer without permissions in the cloud (typically external software programs).
- **Malicious Service Agent** - a service agent (or a program pretending to be a service agent) with compromised or malicious logic.
- **Trusted Attacker** - attacks from within a cloud's trust boundaries by abusing legitimate credentials.
- **Malicious Insider** - 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.

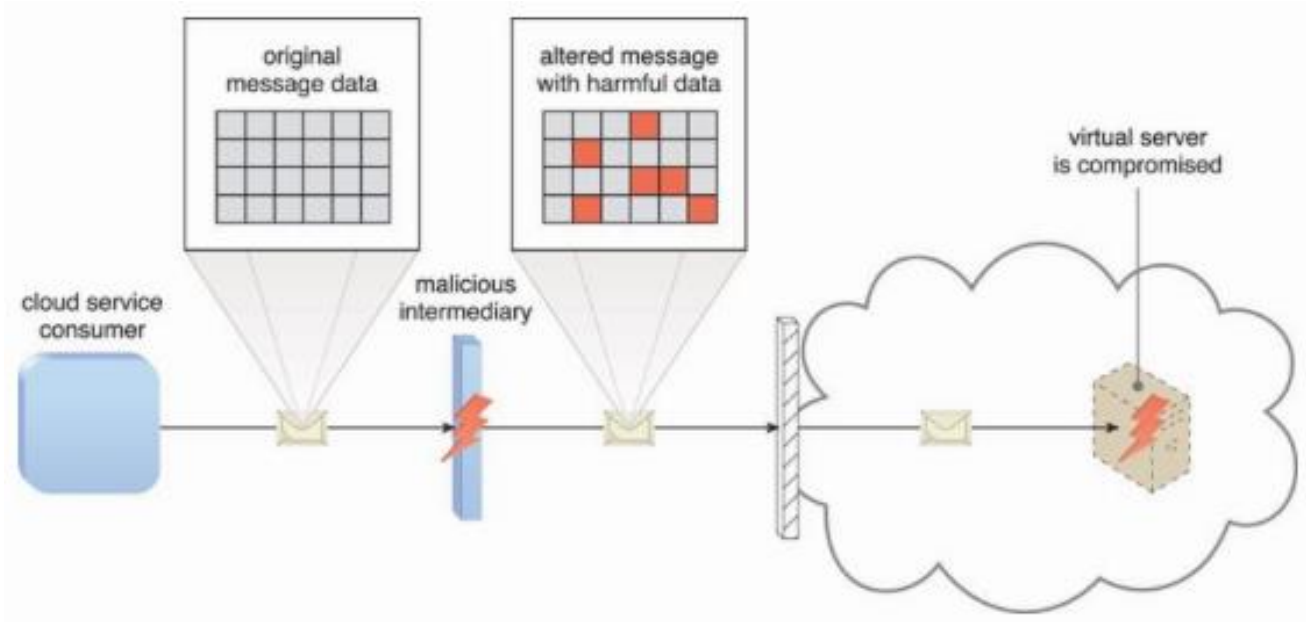
Cloud Security Threats

- **Traffic Eavesdropping** – data is passively intercepted by malicious service agents.
- Gather information to directly compromise confidentiality, e.g., username and password.



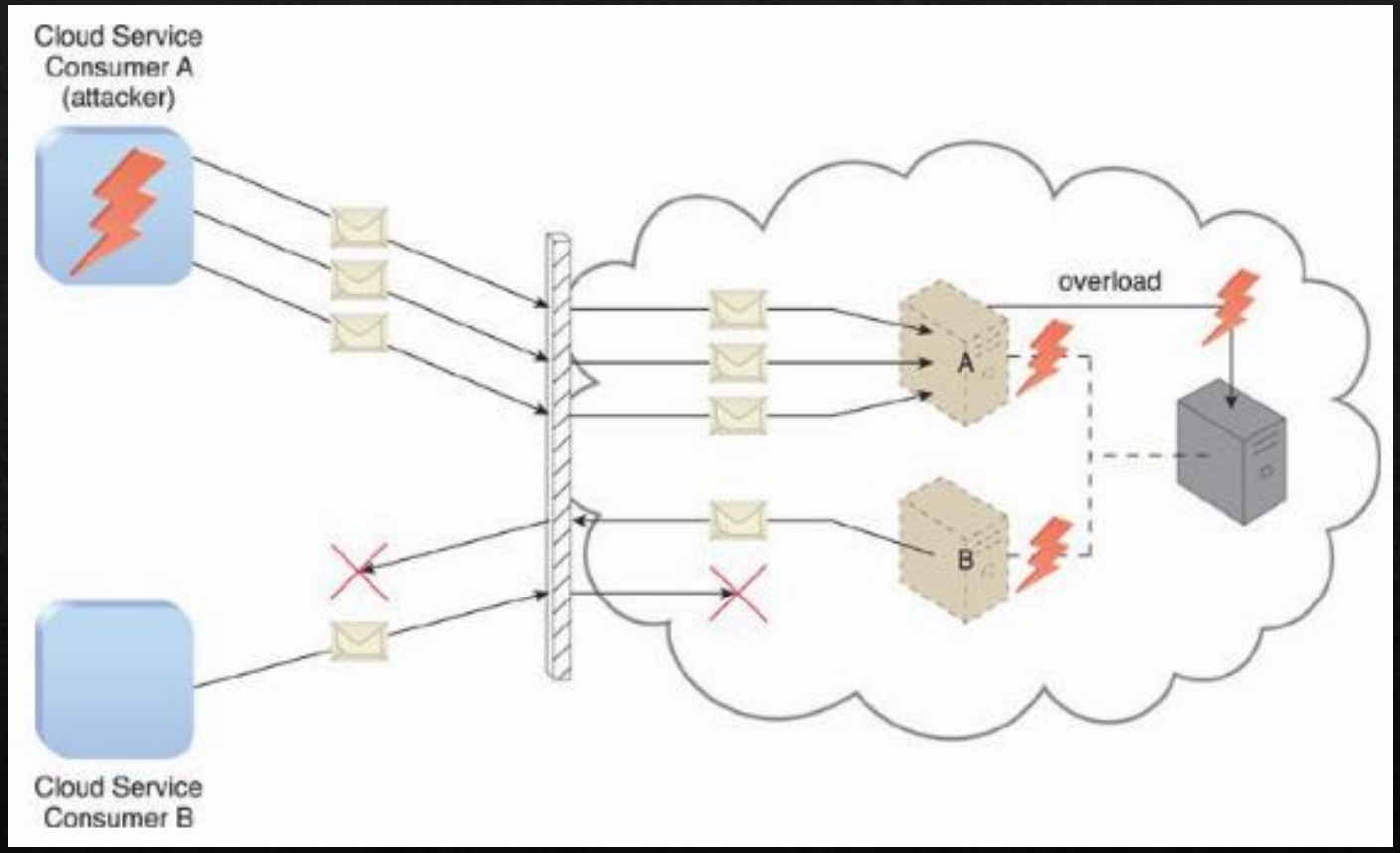
Malicious Intermediary

This attack arises when messages are intercepted and altered by a malicious service agent.



Denial of Service

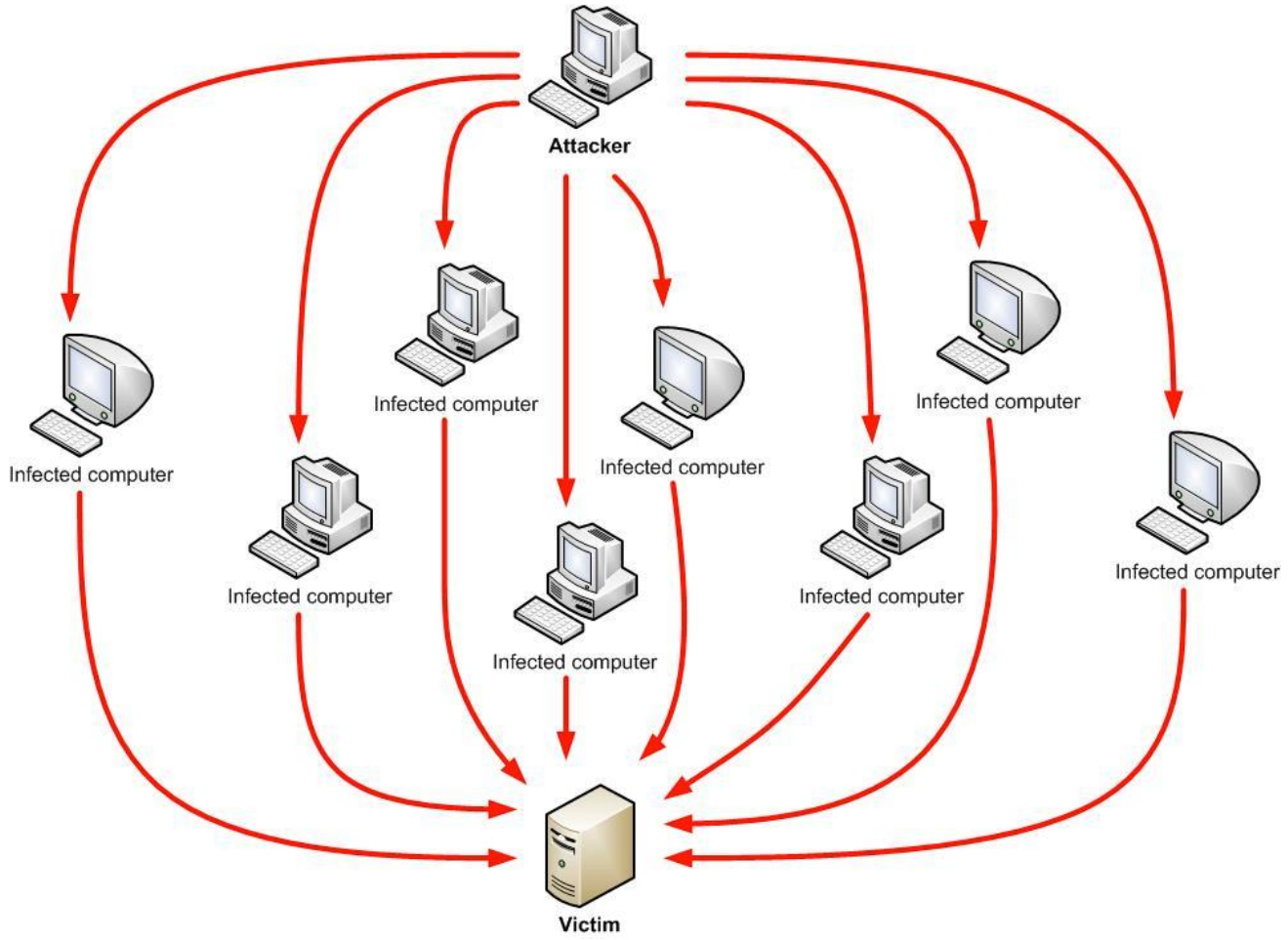
- To overload IT resources to the point where they cannot function properly.
  - Workload increased (CPU, memory loads)
  - Network traffic increased
- Successful DoS attacks produce server degradation and/or failure.



Distributed DoS (DDoS)

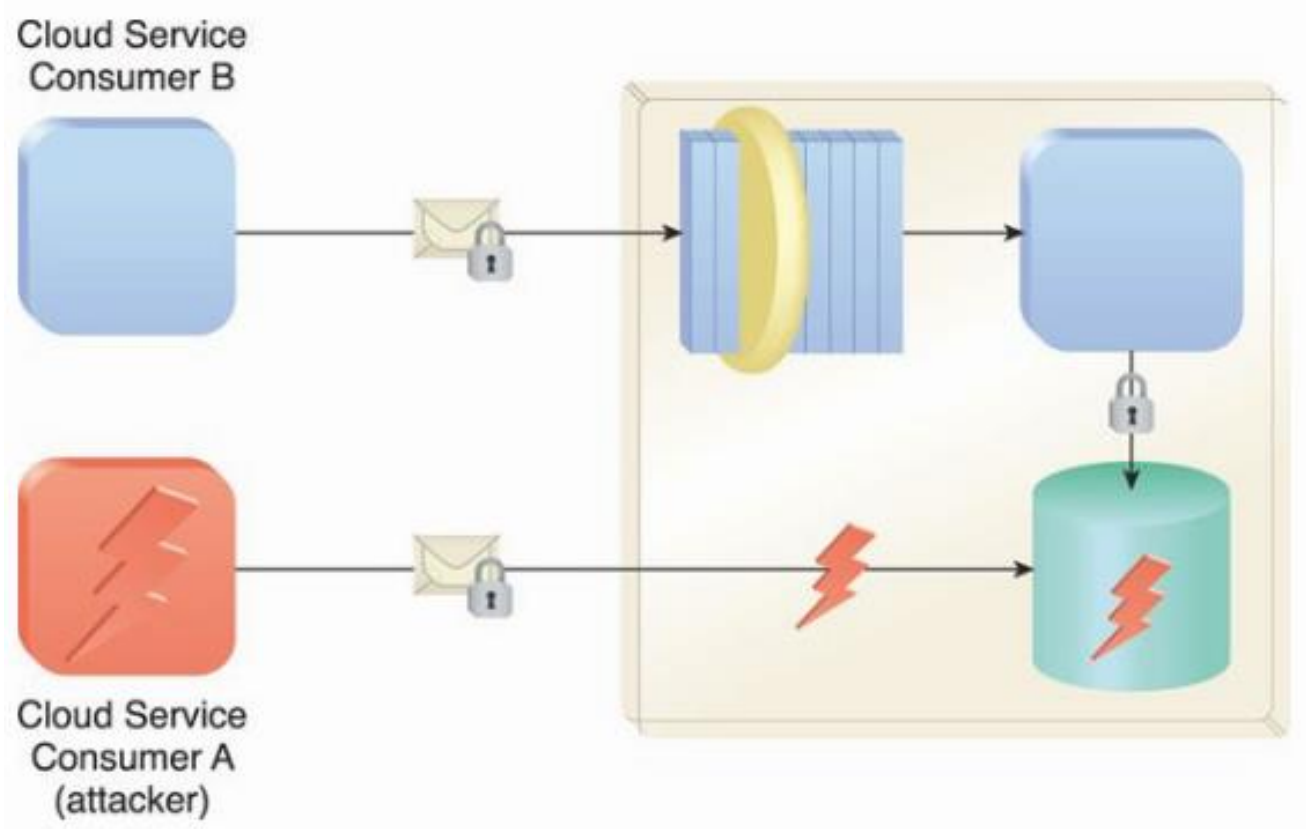
DoS is easy to detect (trace back) and mitigate.

DDoS on the opposite is harder to detect.



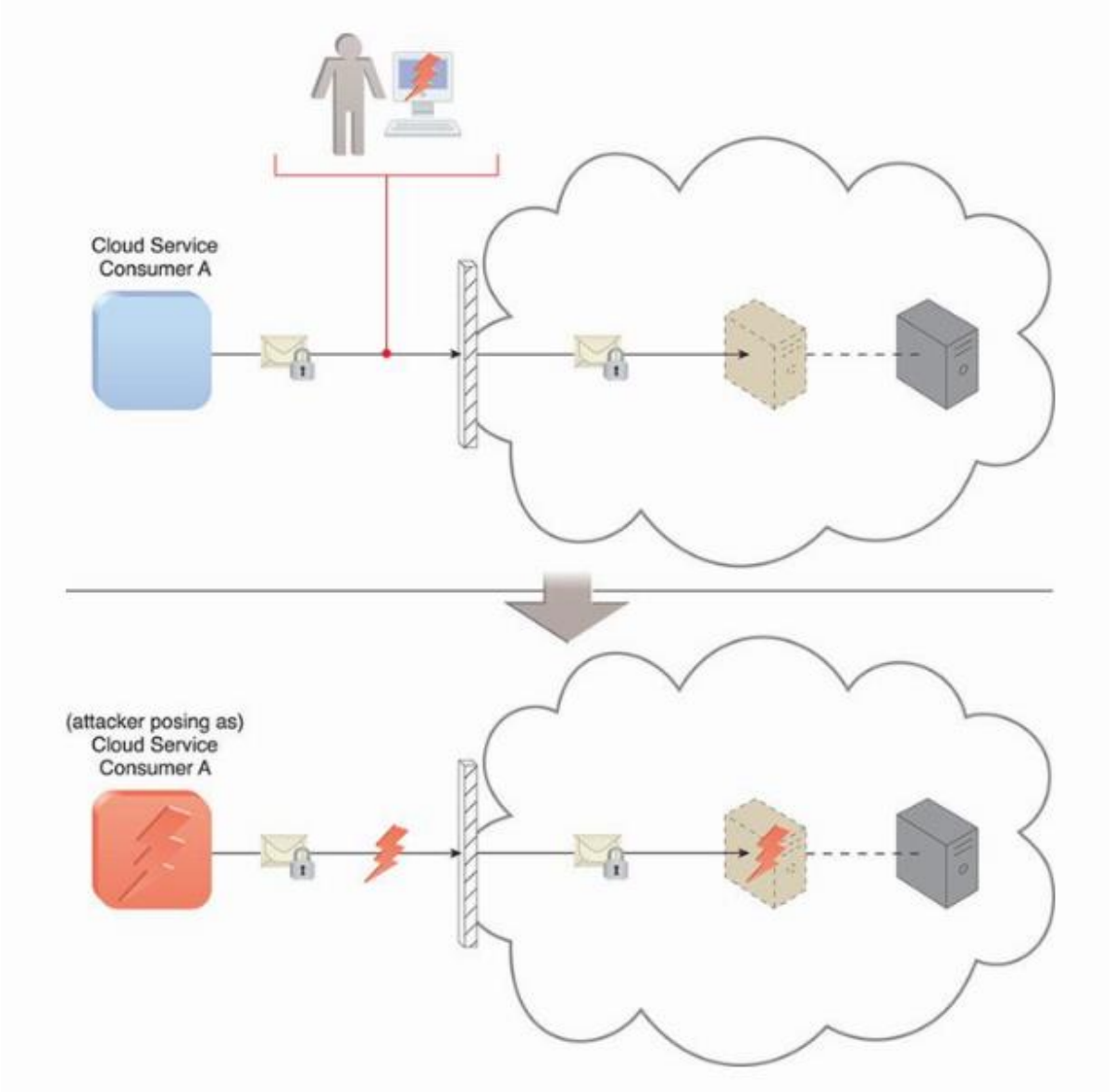
Insufficient Authorization

Attackers gain direct access to IT resources through poorly managed cloud API.



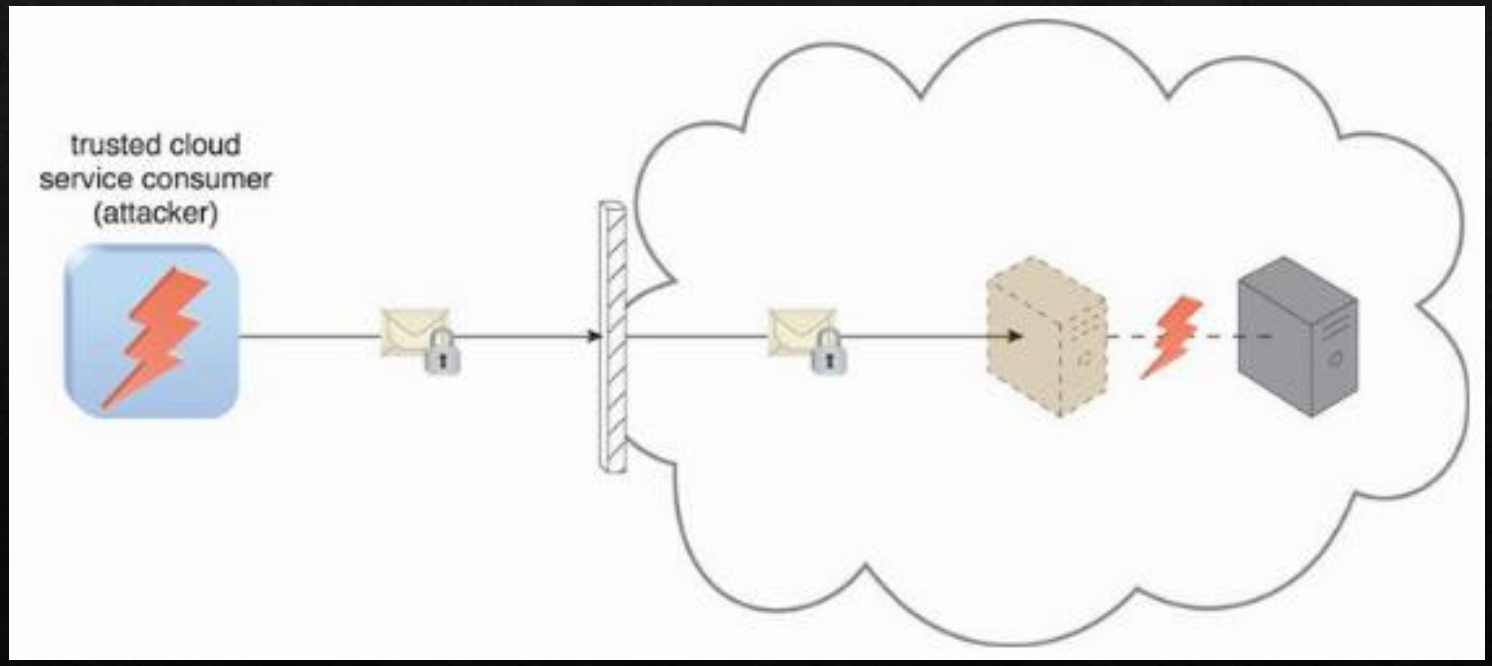
Weak Authentication

Cloud consumer A uses a weak password enabling an attacker to easily crack it.



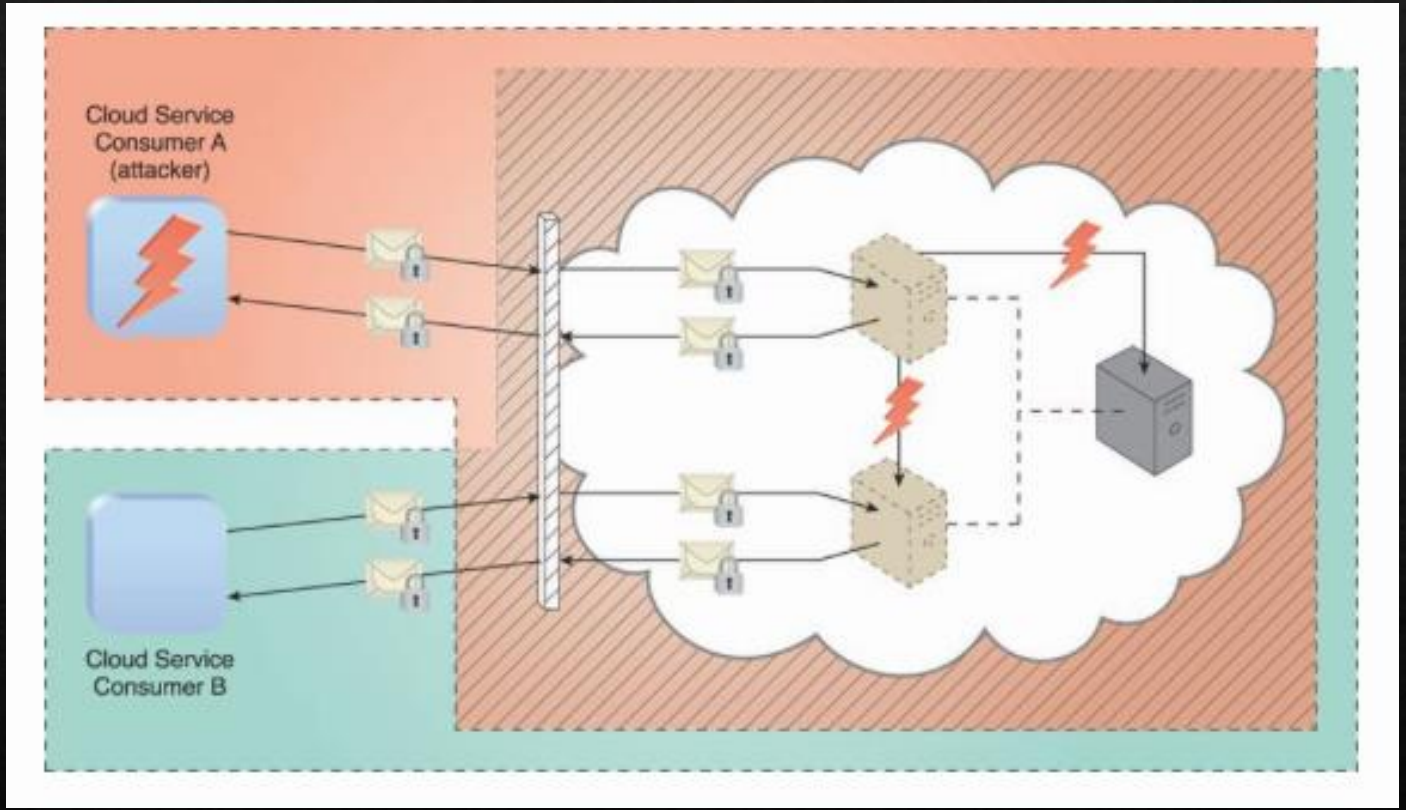
Virtualization Attack

- This attack exploits vulnerabilities in the virtualization platform to jeopardize its confidentiality, integrity, and/or availability.
- Accesses a virtual server to compromise its underlying physical server.



Overlapping Trusted Boundaries

- Physical IT resources shared by multiple cloud consumers, resulting in overlapping trusted boundaries.
- Malicious cloud consumers target shared IT resources with the intention of compromising cloud consumers or other IT resources that share the same trust boundary.



Another Considerations

FLAWED IMPLEMENTATION

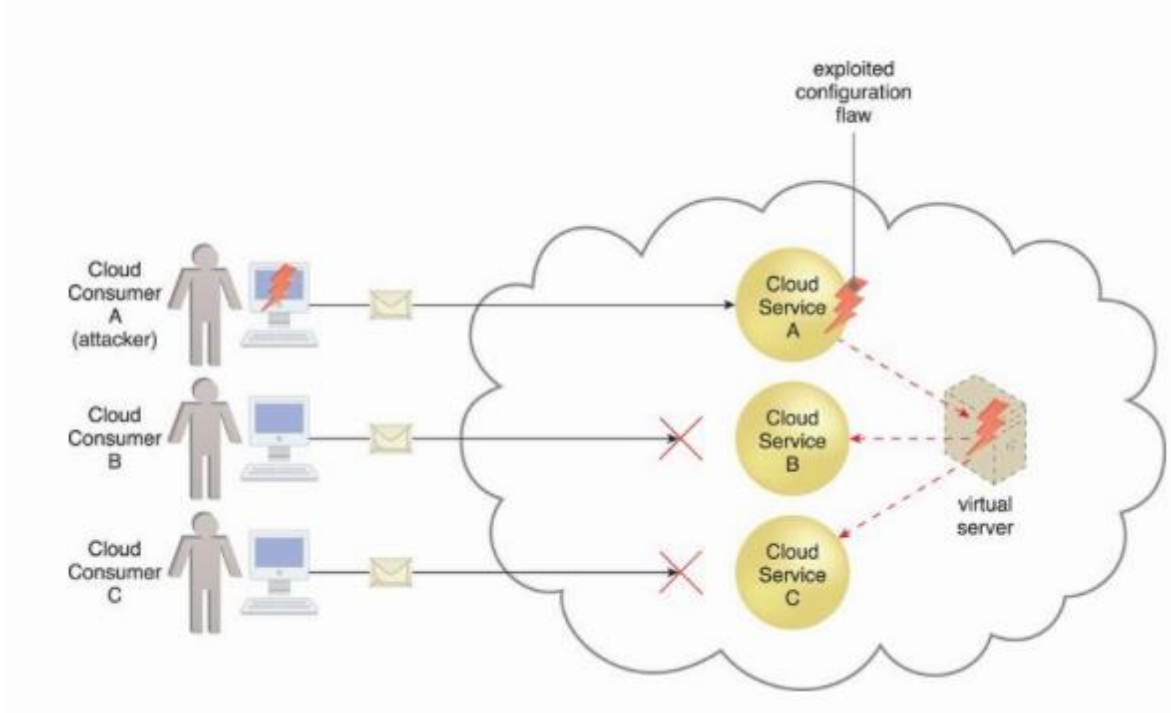
SECURITY POLICY DISPARITY

CONTRACTS

RISK MANAGEMENT

Flawed Implementation

- Substandard design, implementation, or configuration of cloud service deployments may lead to undesirable consequences.
- Attackers can exploit these vulnerabilities to impair the integrity, confidentiality, and/or availability of cloud provider IT resources.



Security Policy Disparity

- Our own implemented security mechanisms are different from that provided by cloud providers.
- Assessments are needed to ensure our IT resources being migrated to a cloud are sufficiently protected.
- Cloud consumers may not be granted sufficient administrative control (of course we are not the owner of the cloud infra).
- Some public clouds, additional third parties, such as security brokers and certificate authorities, may introduce their own distinct set of security policies and practices (make things more complicated).

Contracts

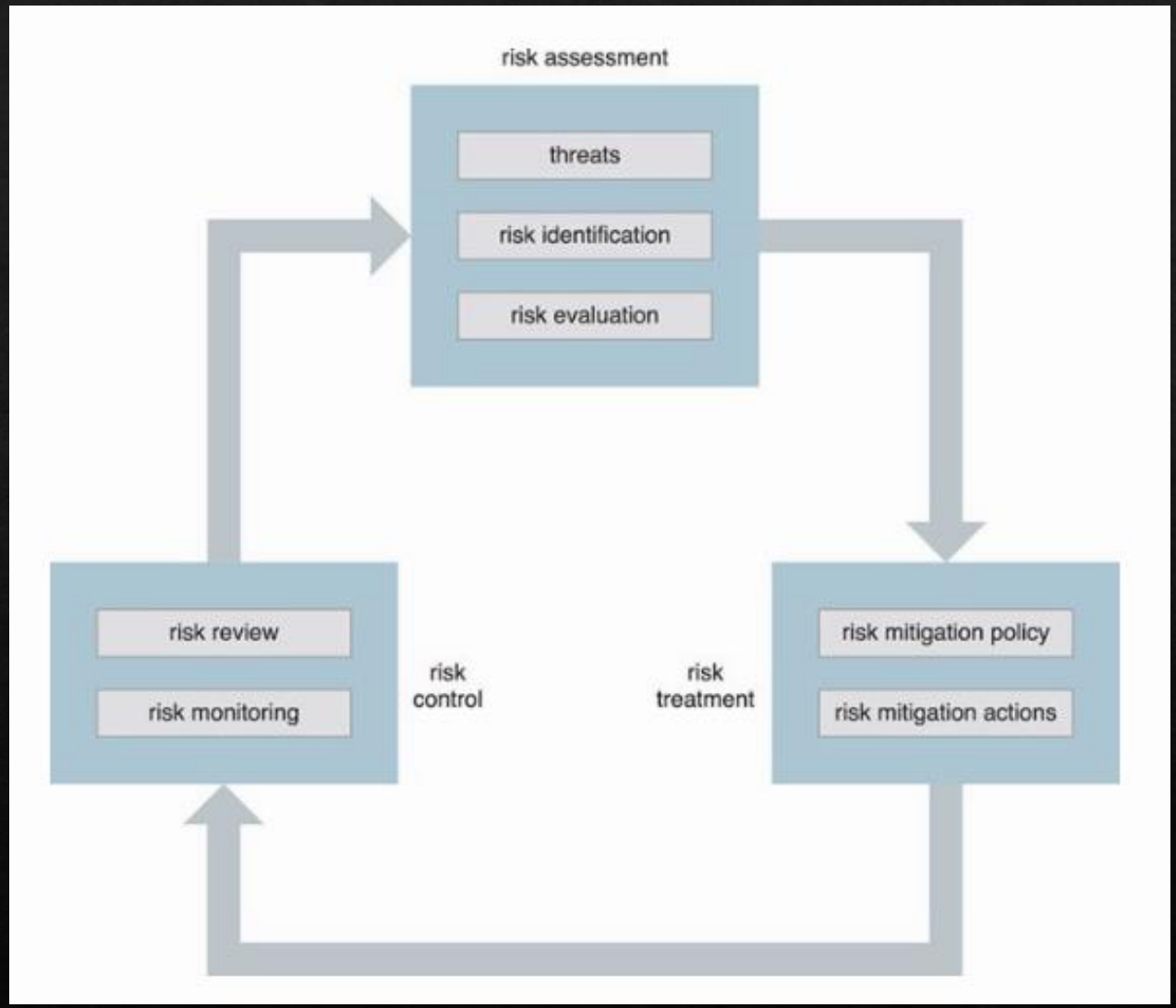
Examine contract and SLA.

Use 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.

Contractual obligations is where the lines are drawn between cloud consumer and cloud provider assets. In case of security breach, who to be blamed (us or cloud provider).

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. Process comprises
  - Risk assessment – to identify potential vulnerabilities and shortcomings.
  - Risk treatment – mitigation policies and plans to treat risks.
  - Risk control – risk monitoring
- Risk management is an on-going process.



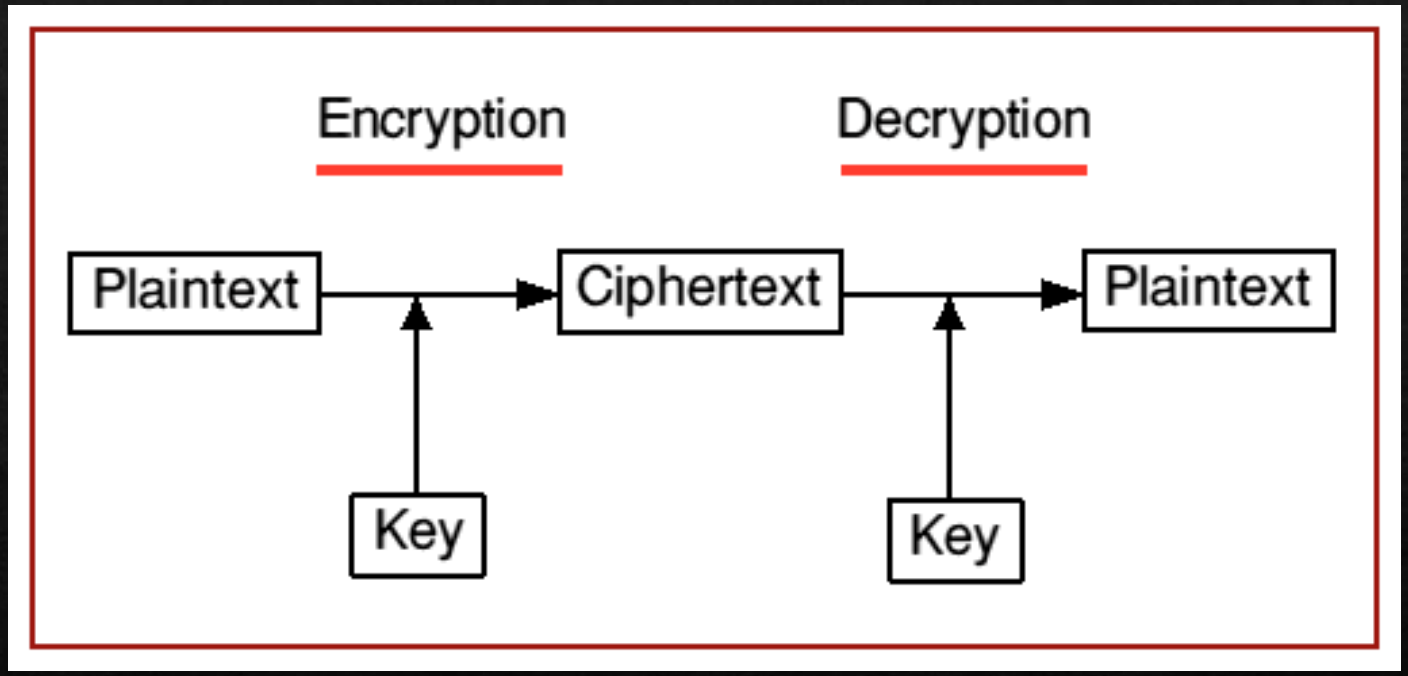
Cloud Security Mechanisms

Security Mechanisms

- Encryption
- Hashing
- Digital Signature
- Public Key Infrastructure (PKI)
- 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 (in some algorithms only) of data.



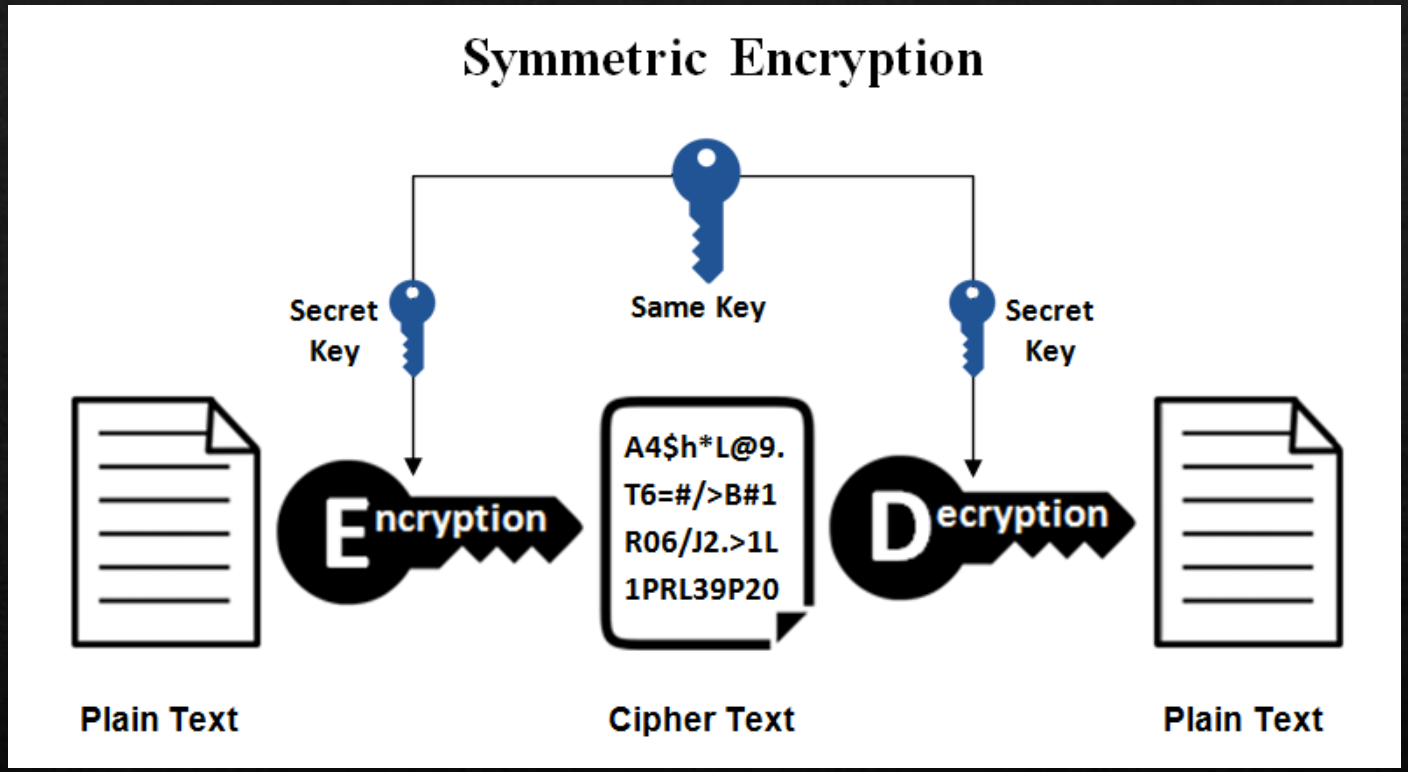
Key size (bits)	Number of alternative keys	Time required at 1 decryption/μs	Time required at 10^6 decryption/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \square 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \square 10^{38}$	2^{127} ns = $5.3 \square 10^{21}$ years	$5.3 \square 10^{17}$ years
168	Triple DES	$2^{168} \approx 3.7 \square 10^{50}$	2^{167} ns = $5.8 \square 10^{33}$ years	$5.8 \square 10^{29}$ years
192	AES	$2^{192} \approx 6.3 \square 10^{57}$	2^{191} ns = $9.8 \square 10^{40}$ years	$9.8 \square 10^{36}$ years
256	AES	$2^{256} \approx 1.2 \square 10^{77}$	2^{255} ns = $1.8 \square 10^{60}$ years	$1.8 \square 10^{56}$ years

Brute Force Search

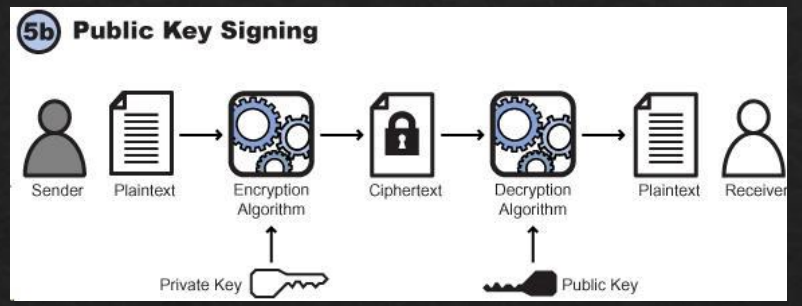
Symmetric Encryption

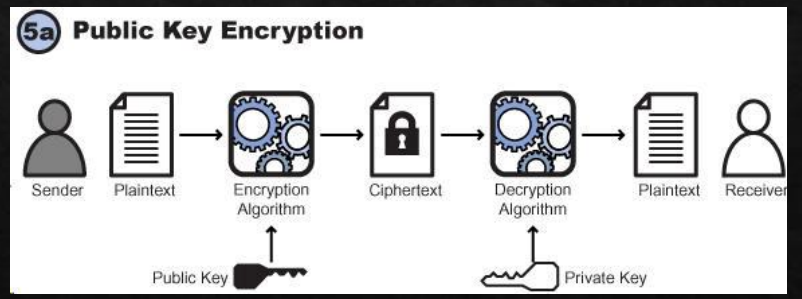
- Single key for both encryption/decryption processes.
- Non-repudiation is not possible if more than two parties share the same key.



Asymmetric Encryption

- Also known as public key encryption.
- A pair of keys, public and private keys, are utilized.
- Use cases
  - Public key encryption – confidentiality.
  - Private key signing – non-repudiation.



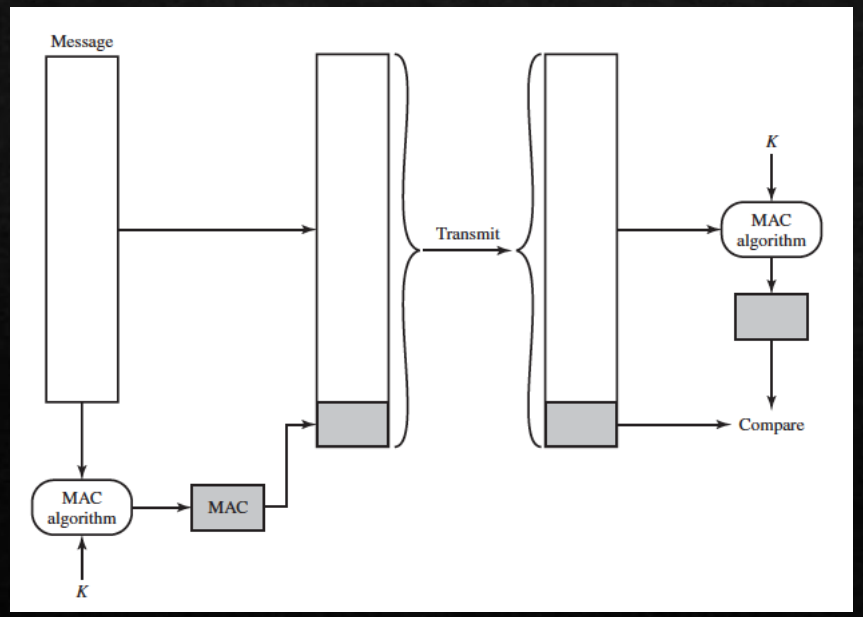


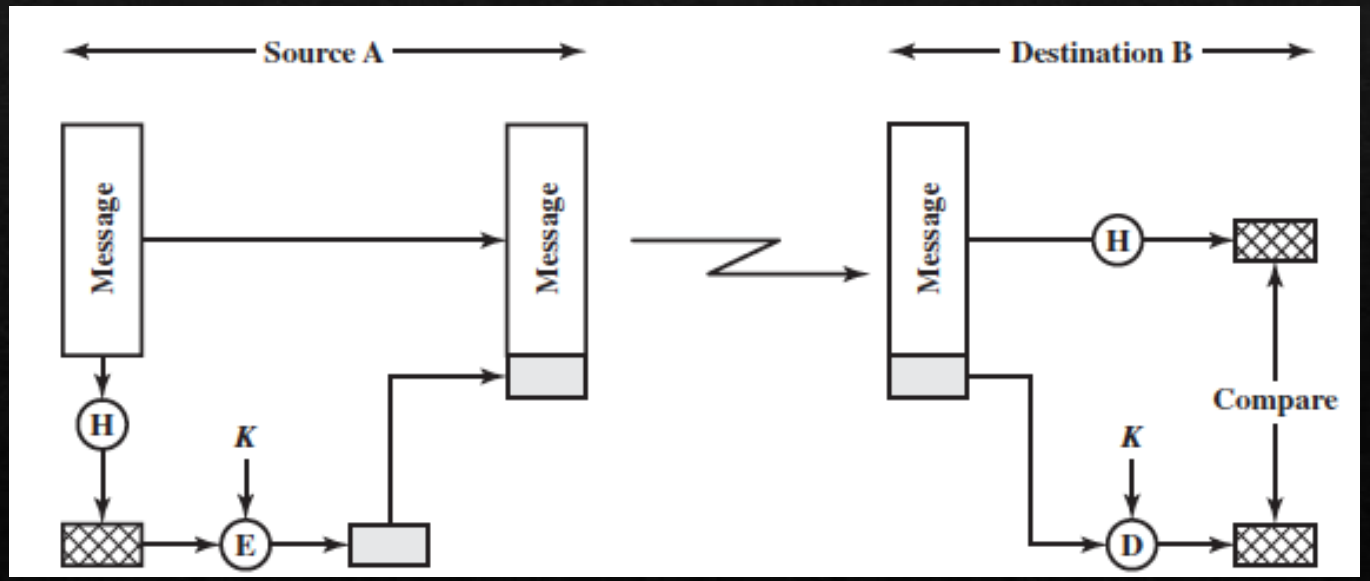
Hashing

Hashing mechanism is used to achieve data integrity.

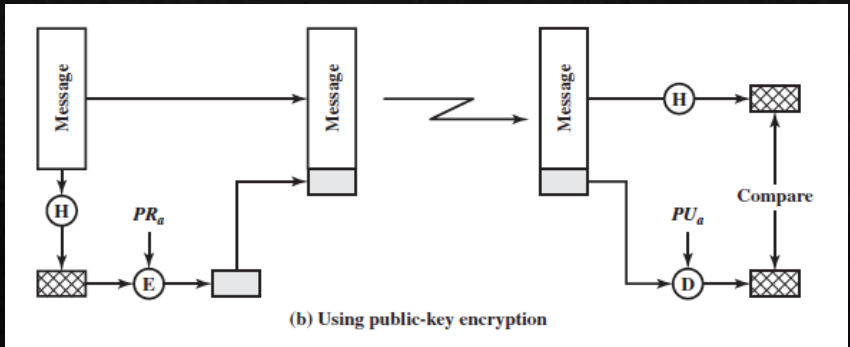
Hashing technology can be used to derive a hashing code or message digest from a message.

Message Digest vs. Hashing Code

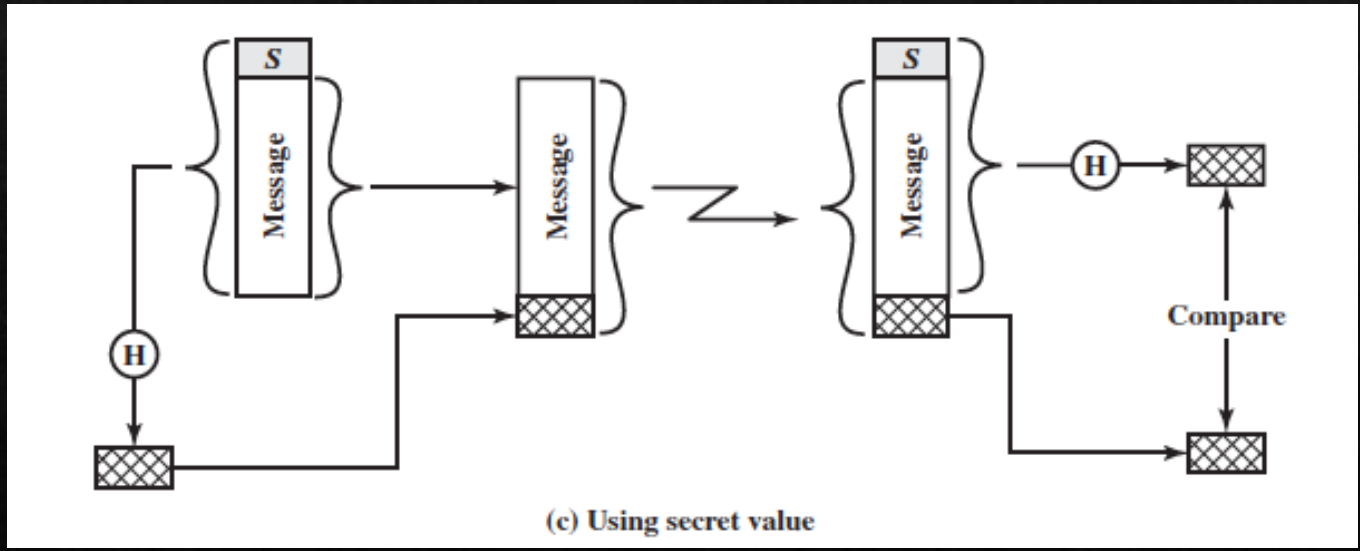




Alternative Hashing Approaches



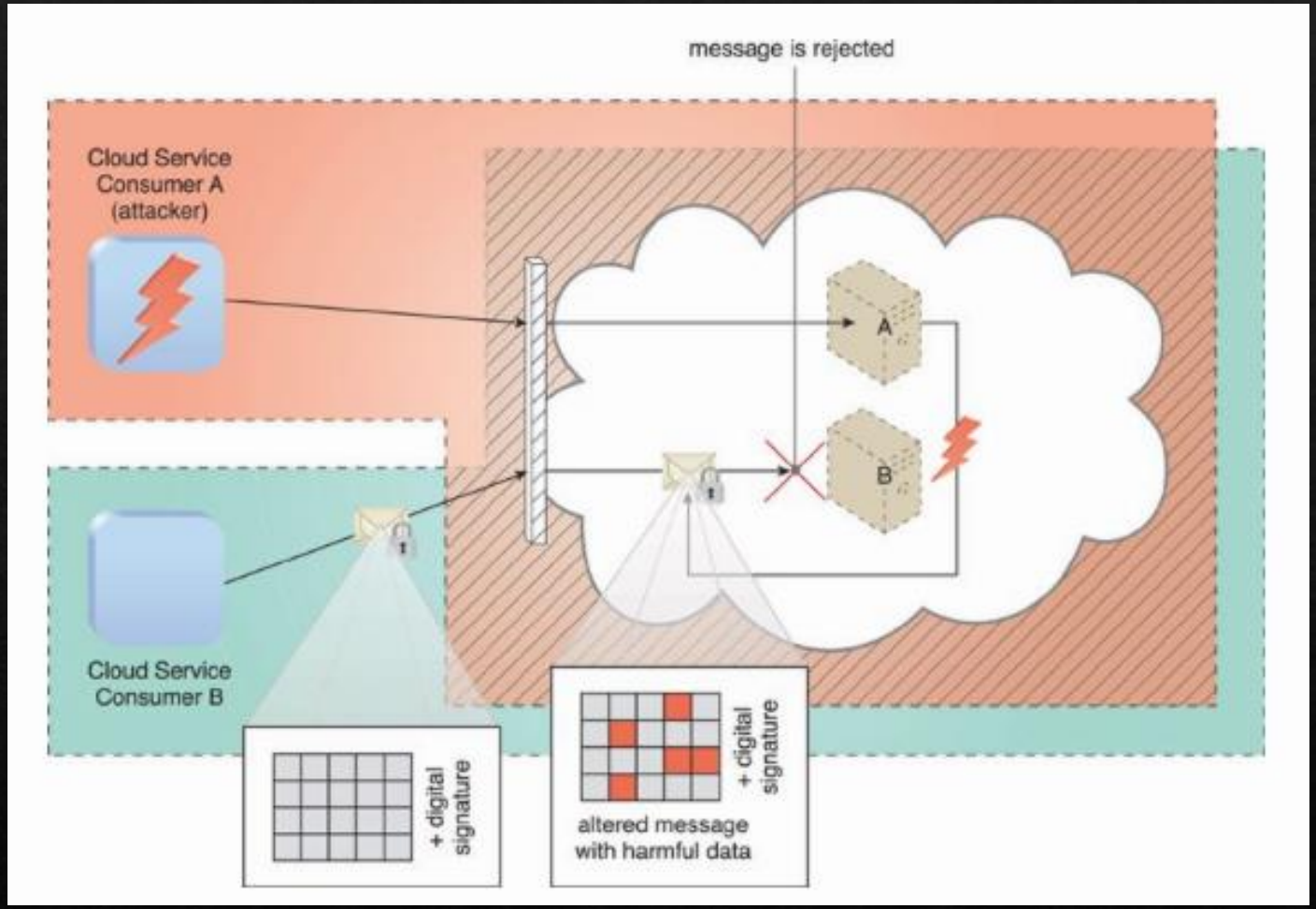
(b) Using public-key encryption

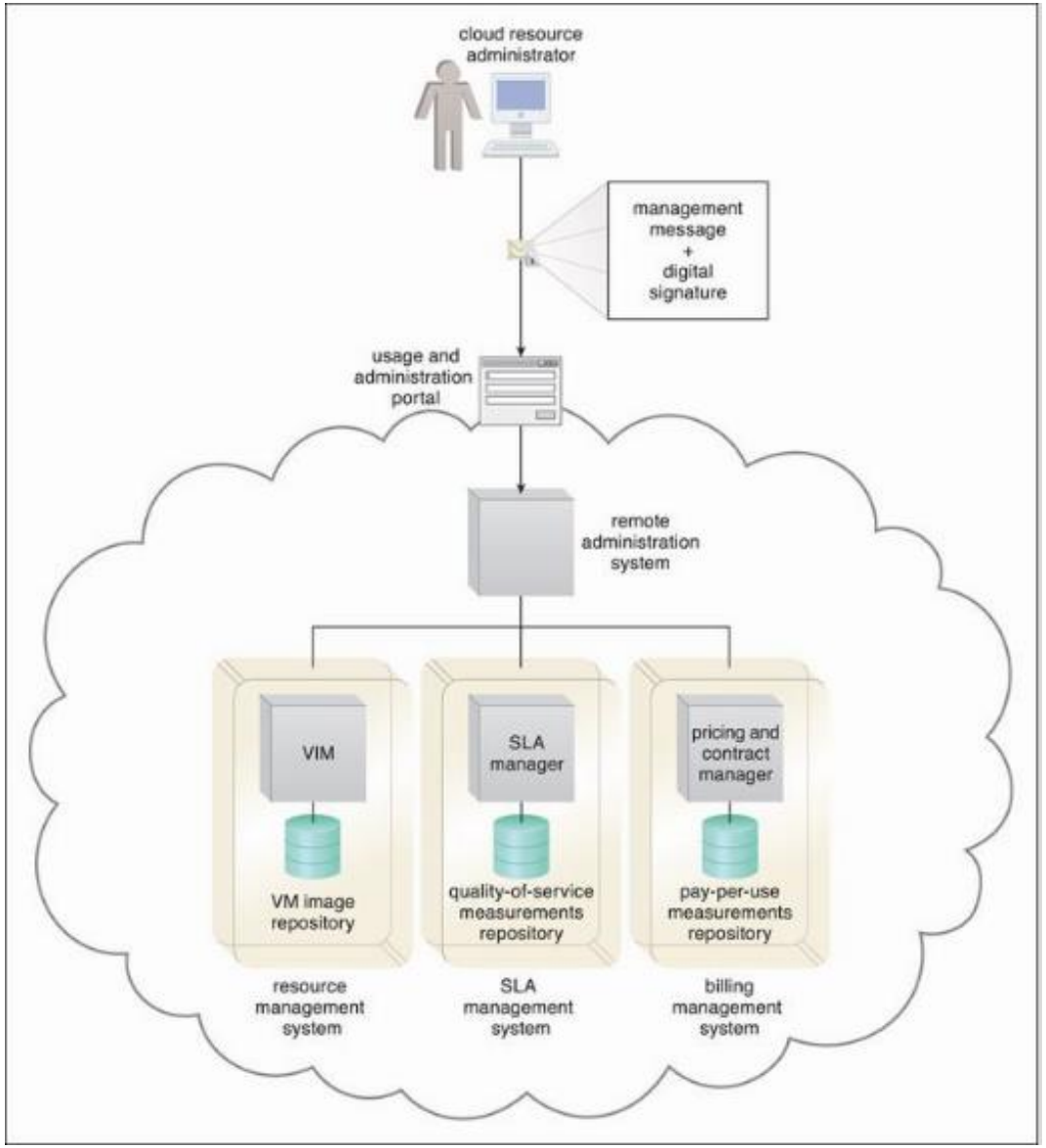


(c) Using secret value

Digital Signature

- Means of providing data authenticity and integrity through authentication and non-repudiation.
- Asymmetric encryption and hashing mechanisms are involved in the process.



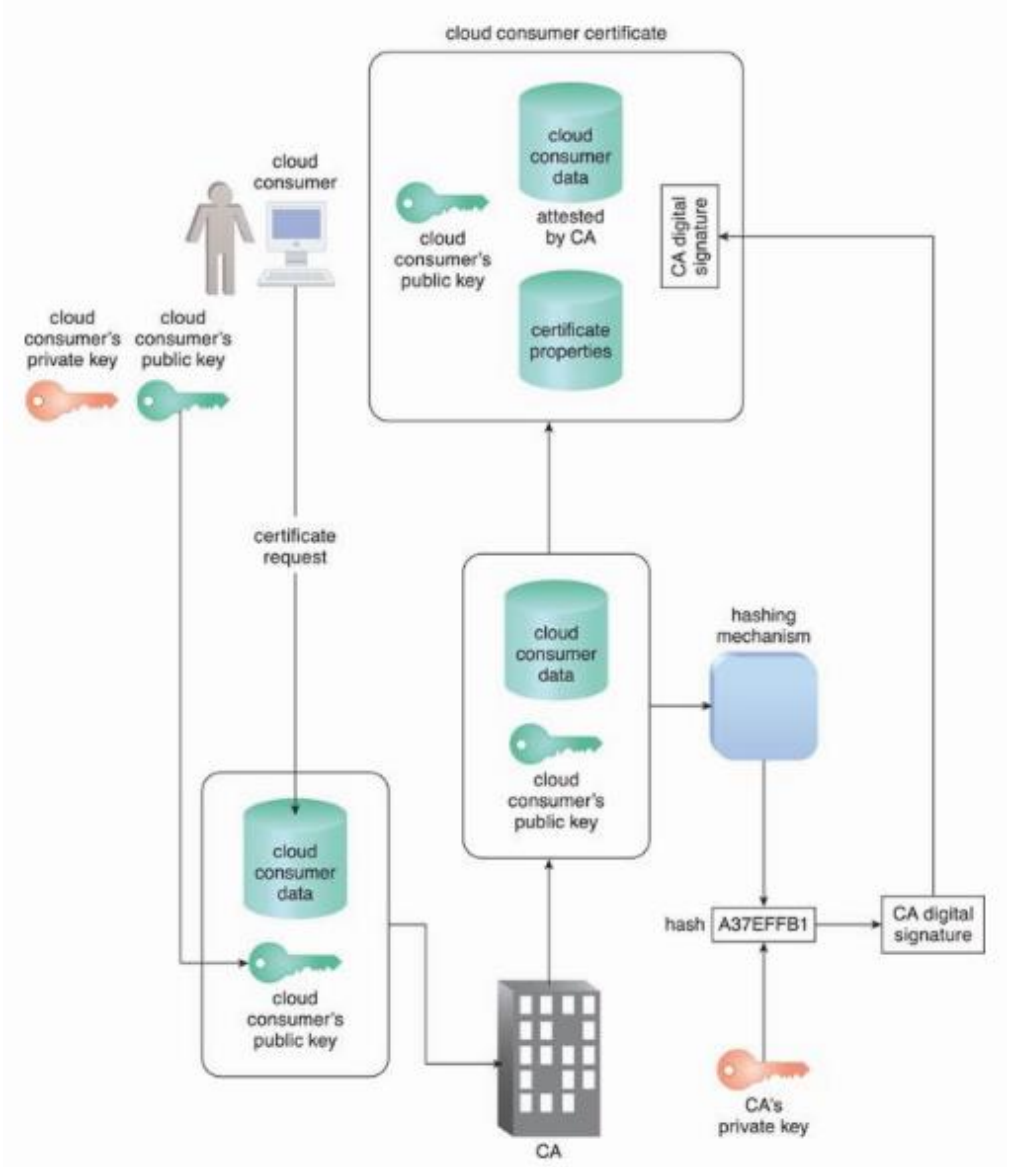

cloud resource administrator
management message + digital signature
usage and administration portal
remote administration system
VIM
VM image repository
SLA manager
quality-of-service measurements repository
pricing and contract manager
pay-per-use measurements repository
resource management system
SLA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

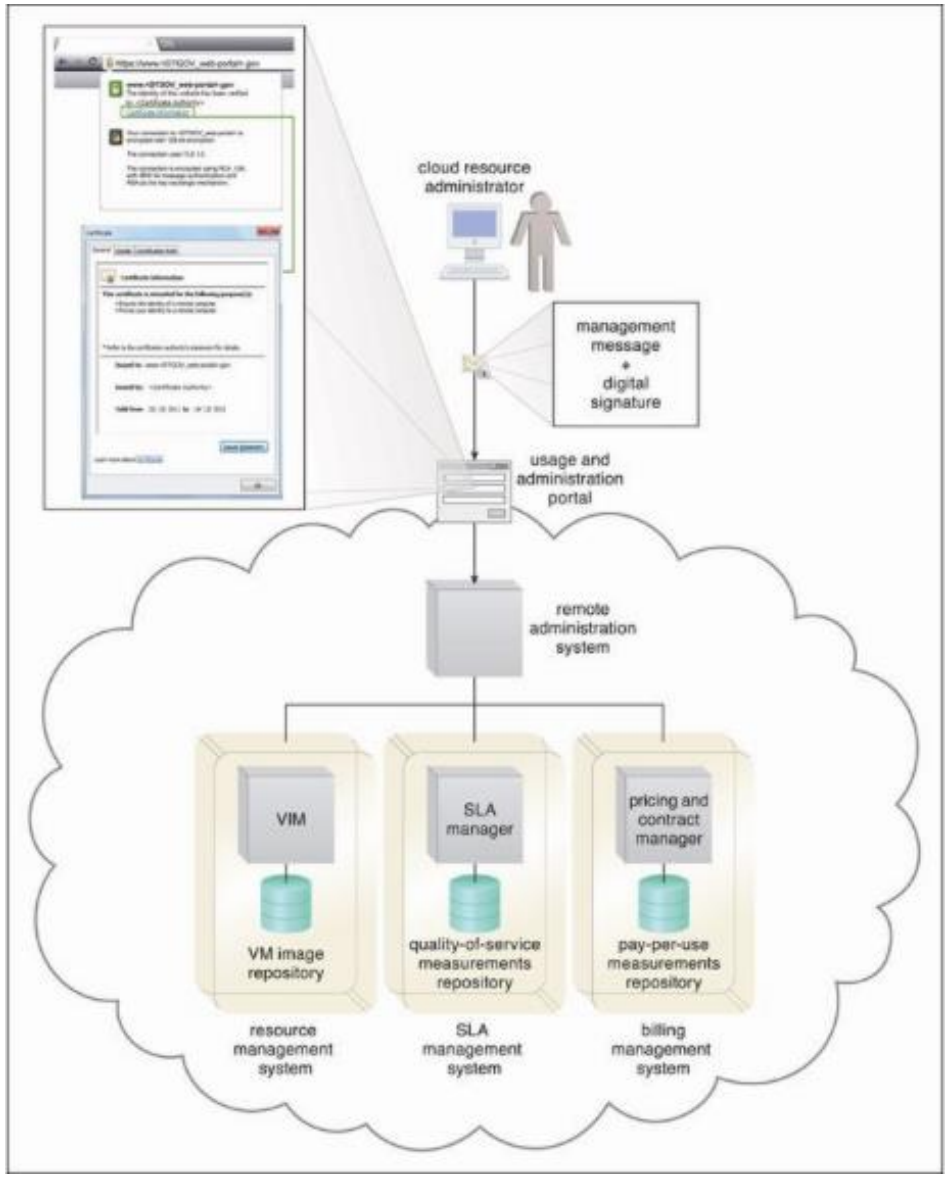
Public Key Infrastructure (PKI)

Management the issuance of asymmetric keys.

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.

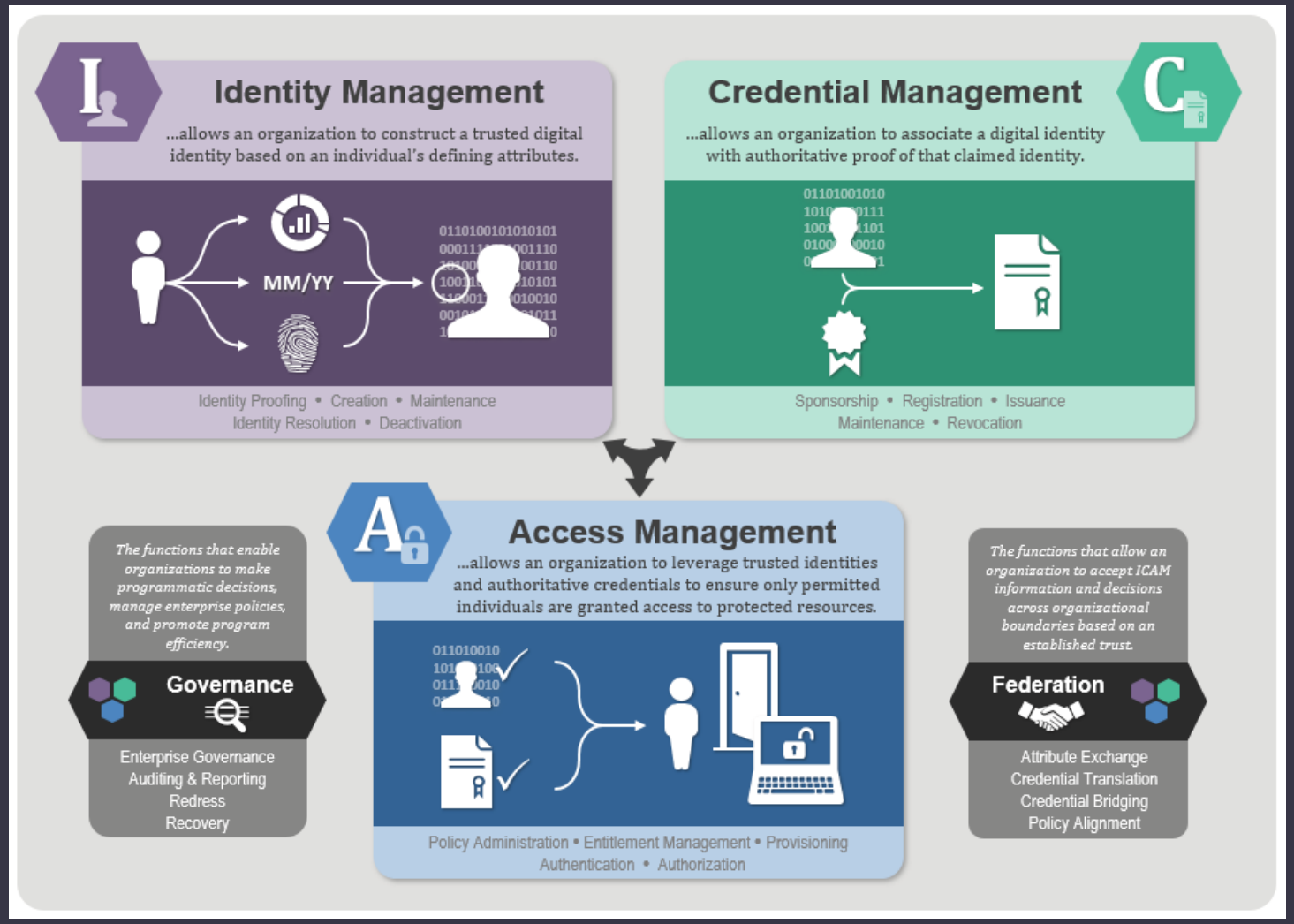
Digital certificates are usually digitally signed by a third-party certificate authority (CA).


cloud consumer certificate
cloud consumer data
attested by CA
cloud consumer's public key
CA digital signature
certificate properties
cloud consumer
cloud consumer's private key
cloud consumer's public key
certificate request
cloud consumer data
cloud consumer's public key
hashing mechanism
cloud consumer data
cloud consumer's public key
hash
A37EFFB1
CA digital signature
CA's private key
CA


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

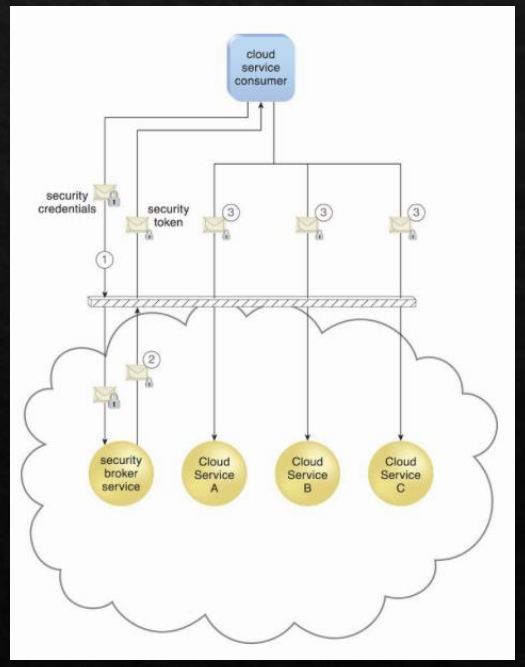
Identity and Access Management (IAM)

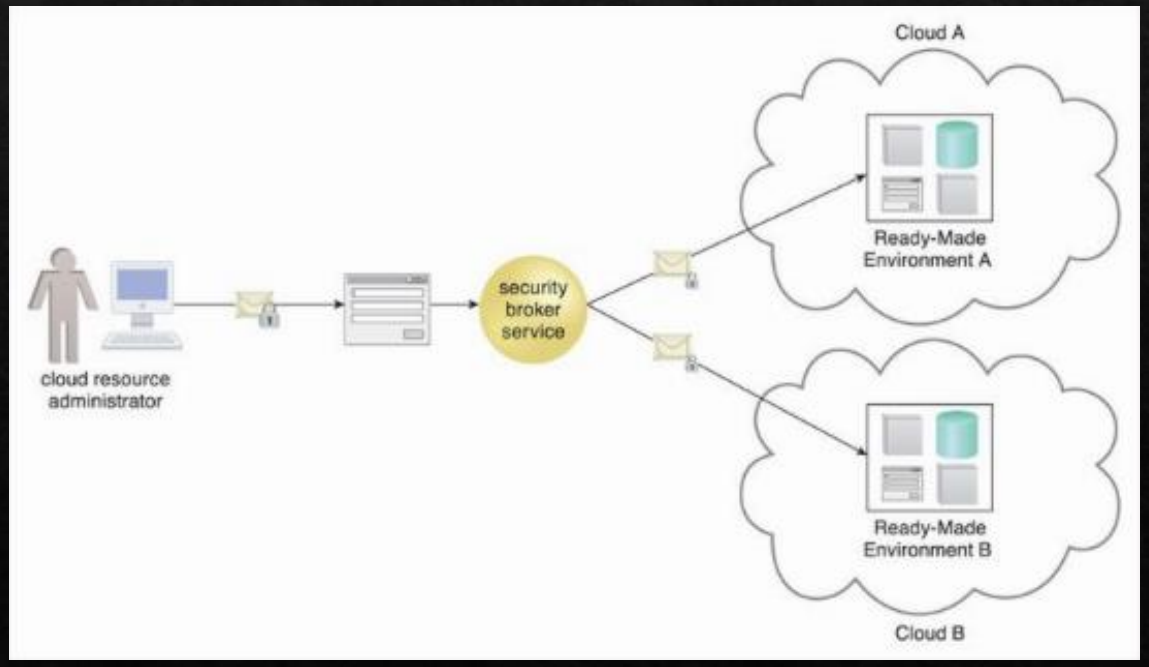
- Encompasses the components and policies necessary to control and track user identities and access privileges for IT resources
  - Authentication – username/password, biometric, digital signatures, your blood, etc.
  - Authorization – correct granularity for access controls and the relationships between identities, access control rights, and IT resource availability.
  - User management – create, modify, delete, group management.
  - Credential management - establishes identities and access control rules for defined user accounts.

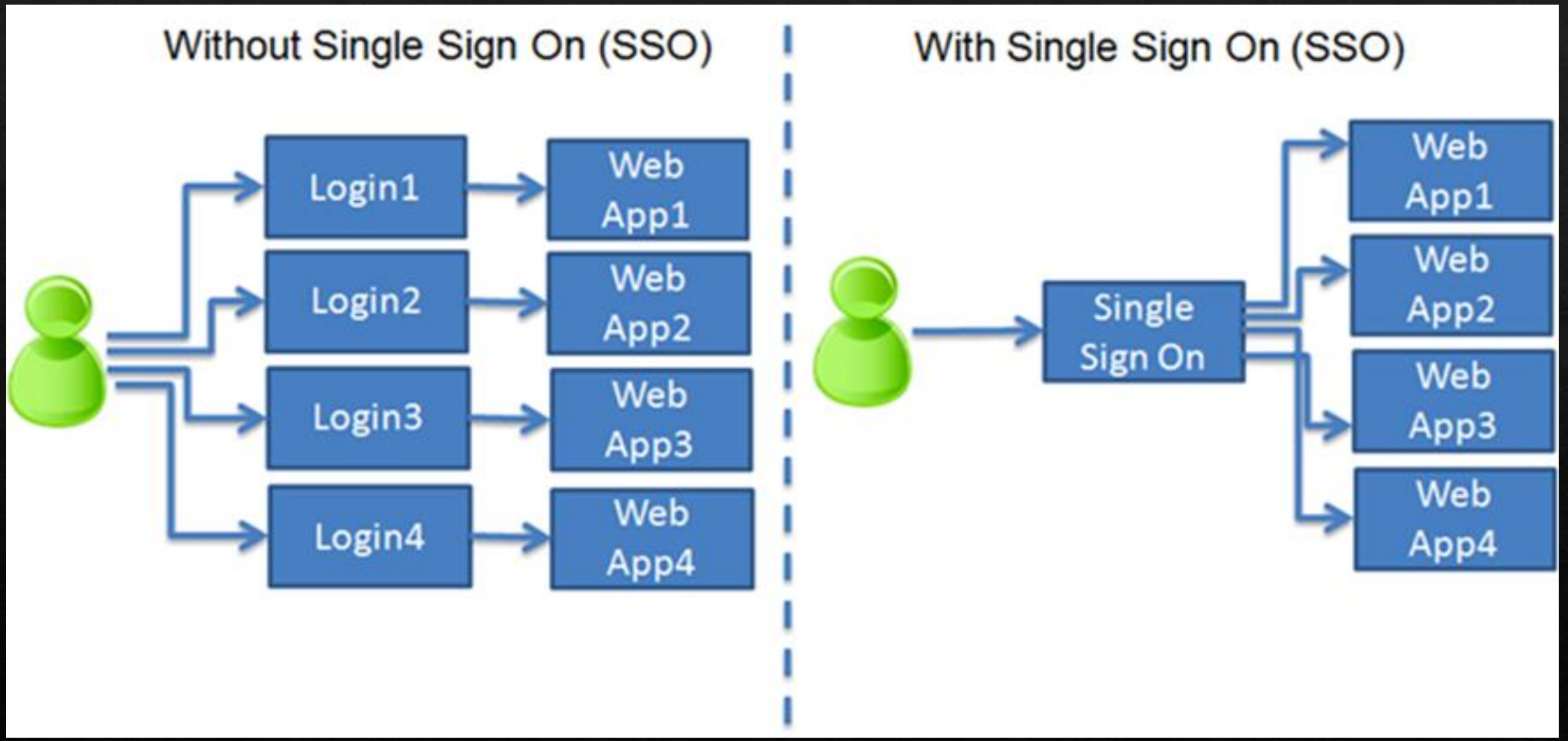

Identity Management
...allows an organization to construct a trusted digital identity based on an individual's defining attributes.
MM/YY
Identity Proofing • Creation • Maintenance
Identity Resolution • Deactivation
Credential Management
...allows an organization to associate a digital identity with authoritative proof of that claimed identity.
Sponsorship • Registration • Issuance
Maintenance • Revocation
Access Management
...allows an organization to leverage trusted identities and authoritative credentials to ensure only permitted individuals are granted access to protected resources.
Policy Administration • Entitlement Management • Provisioning
Authentication • Authorization
The functions that enable organizations to make programmatic decisions, manage enterprise policies, and promote program efficiency.
Governance
Enterprise Governance
Auditing & Reporting
Redress
Recovery
The functions that allow an organization to accept ICAM information and decisions across organizational boundaries based on an established trust.
Federation
Attribute Exchange
Credential Translation
Credential Bridging
Policy Alignment

Single Sign-On (SSO)

- Authenticated once, access all services.
- Authenticated by a security broker.
- Credentials remain valid for the duration of a session.






Without Single Sign On (SSO)
Login1
Login2
Login3
Login4
Web App1
Web App2
Web App3
Web App4
With Single Sign On (SSO)
Single Sign On
Web App1
Web App2
Web App3
Web App4

SSO Advantages & Disadvantages

SSO reduces password fatigue.

SSO reduces password exposure.

SSO simplifies user and password management.

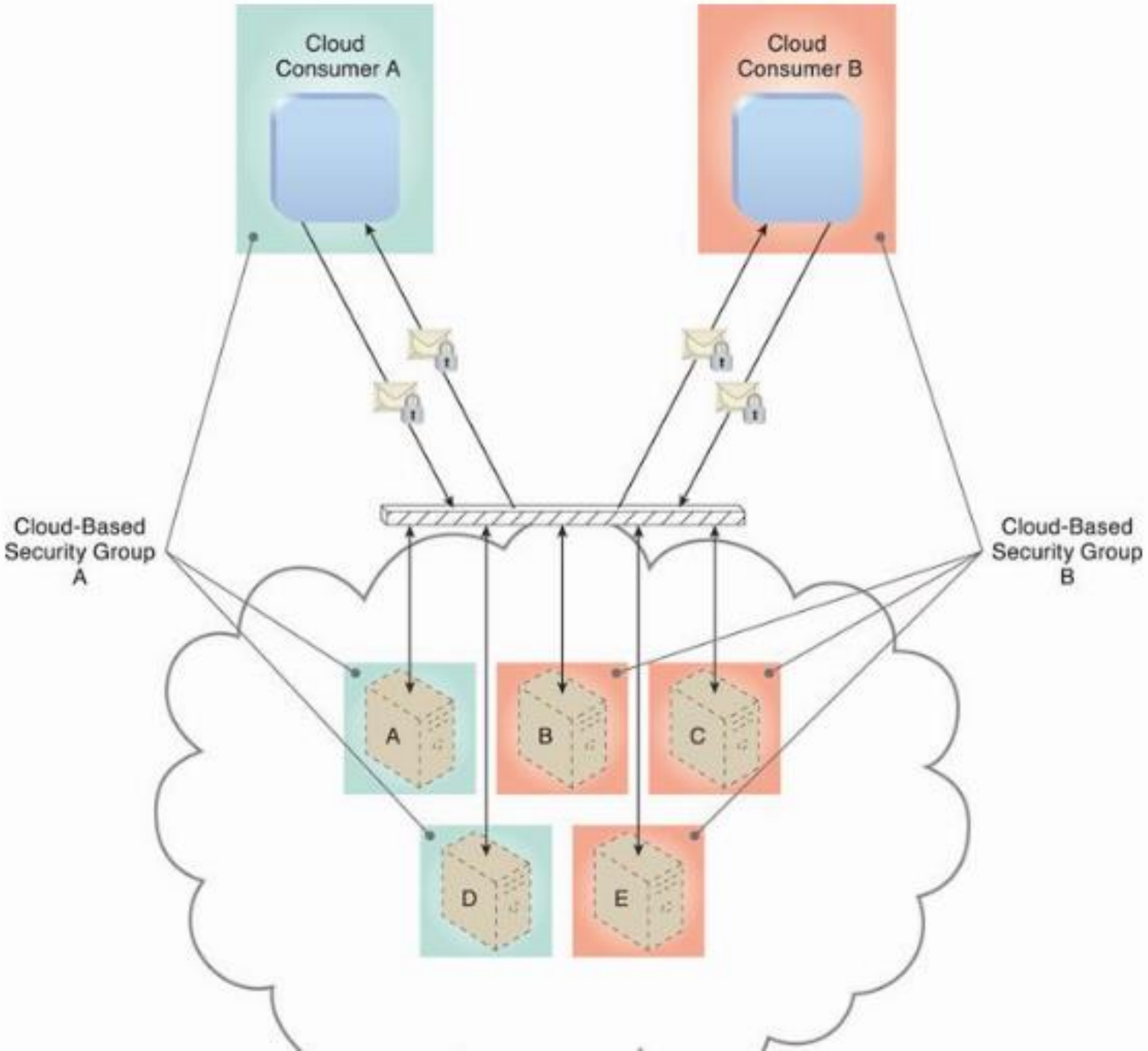
SSO opens up new possibilities.

How about disadvantages?

- SSO gives you the keys to the castle.
- SSO does not work when your identity provider is down.
- SSO takes a little bit of investment to set up.

Cloud-Based Security Groups

- Segment IT resources hence different security mechanisms can be provided to different segments.
- Network – multiple segments each with different security policies and mechanisms.
- Virtual servers –multiple types such as public/private groups, development/production groups.



Hardened Virtual Server Images

- The process of stripping unnecessary software from a system to limit potential vulnerabilities that can be exploited by attackers.
  - Remove redundant programs.
  - Close unnecessary server ports.
  - Disable unused services, root accounts, guest accounts, etc.