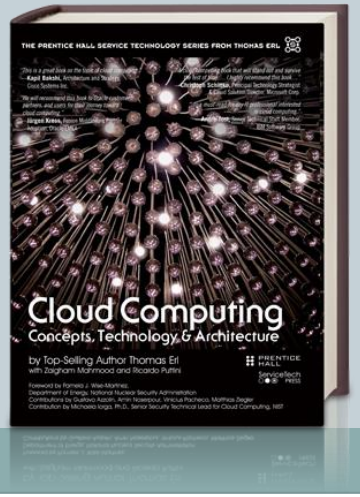
Cloud Computing

Concept, Technology & Architecture

Chapter 06

Fundamental Cloud Security

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



Contents

- Security topics and concepts relevant and distinct to cloud computing are introduced, including descriptions of common cloud security threats and attacks.
  - 6.1 Basic Terms and Concepts
  - 6.2 Threat Agents
  - 6.3 Cloud Security Threats
  - 6.4 Additional Considerations
  - 6.5 Case Study Example

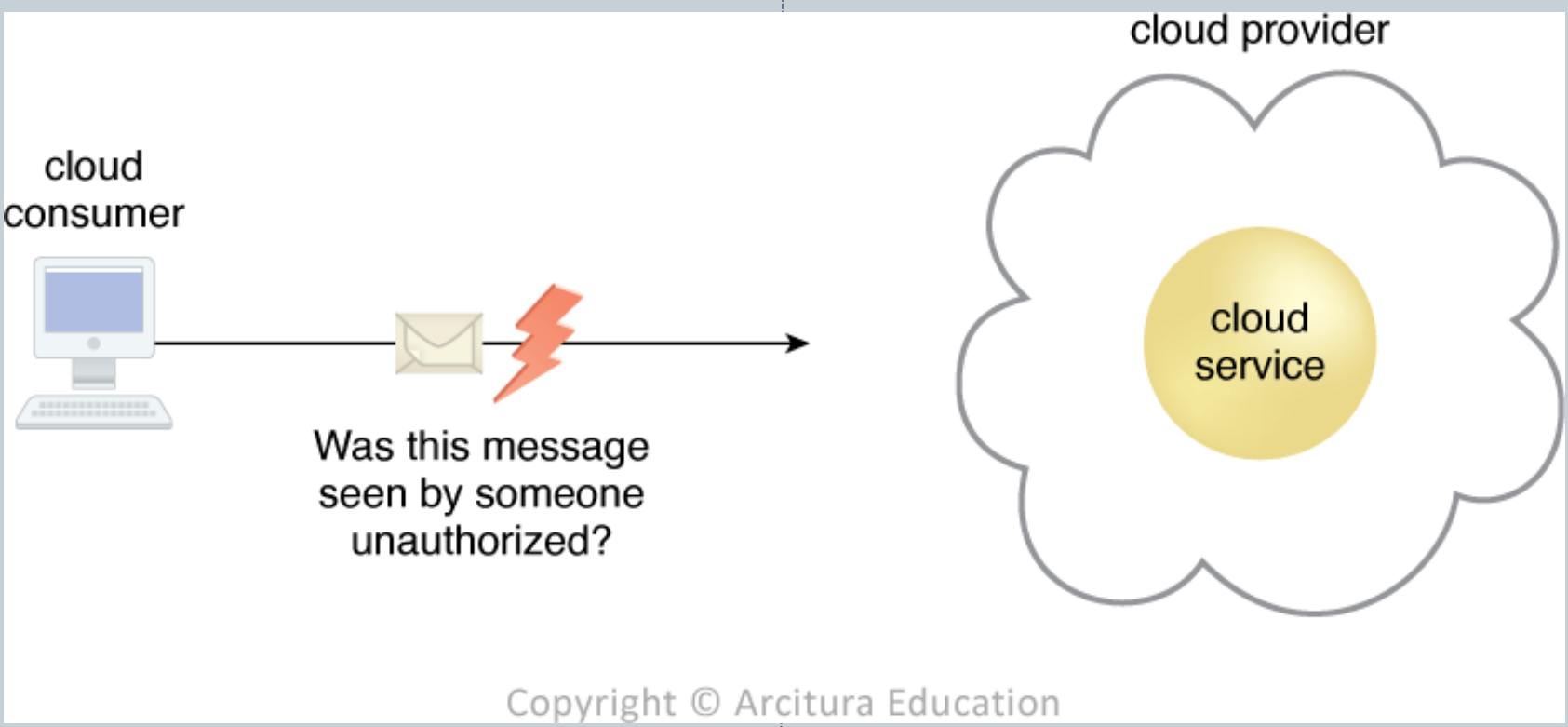
6.1 Basic Terms and Concepts (1/6)

- IT security measures aim to defend against threats and interference that arise from both malicious intent and unintentional user error.
- Basic terms include the followings:
  - Confidentiality, Integrity, Authenticity, Availability
    - Are associated with measuring security
  - Threat, Vulnerability, Risk
    - Are associated with measuring and assessing insecurity or the lack of security
  - Security Controls, Security Mechanisms, Security Policies
    - Are associated with establishing countermeasures and safeguards in support of improving security

6.1 Basic Terms and Concepts (2/6)

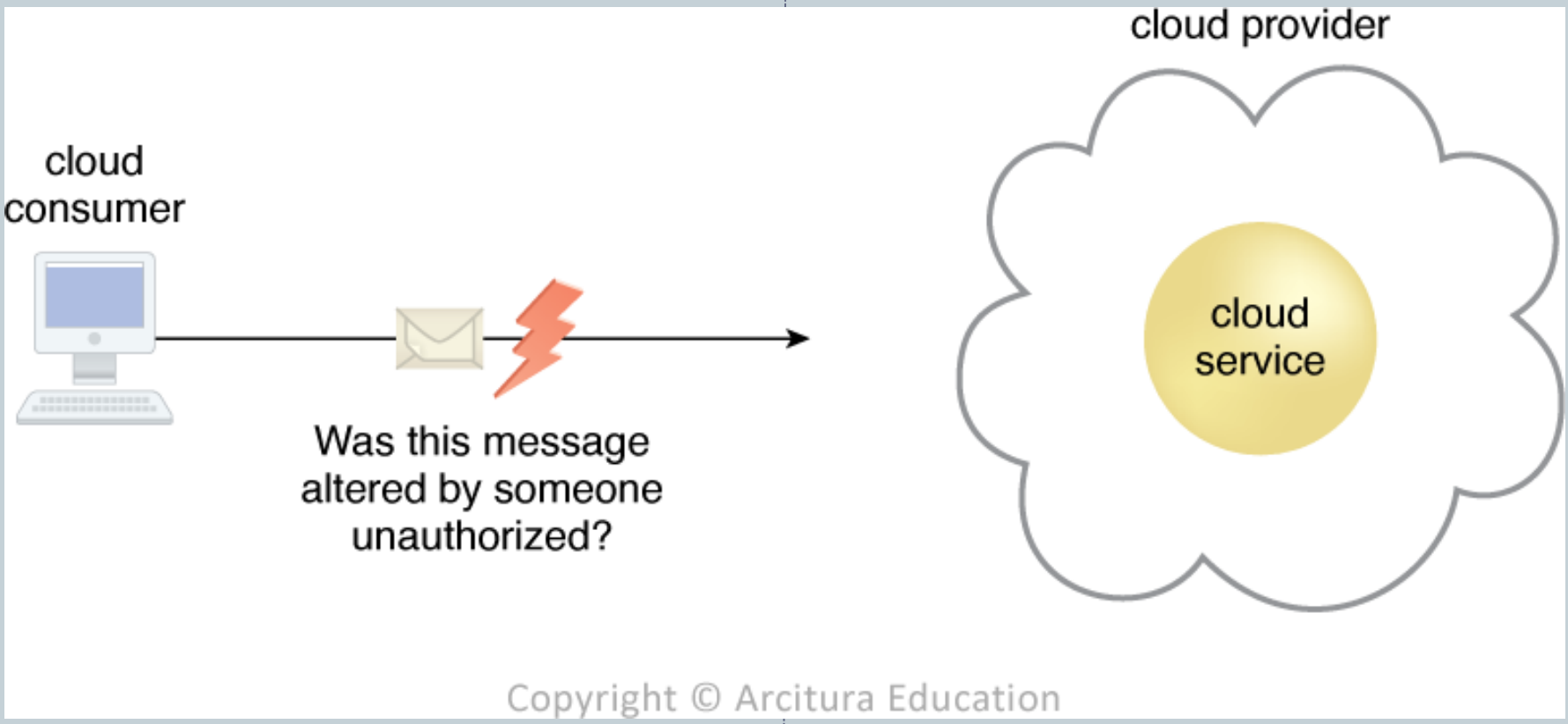
- Confidentiality
  - Confidentiality is the characteristics of something being made accessible only to authorized parties.
  - It primarily pertains to restricting access data in transit and storage.
- Integrity
  - Integrity is the characteristics of not having been altered by an unauthorized party.
  - Specifically, determine whether a cloud consumer can be guaranteed that the data it transmits to a cloud service matches the data received by cloud services and resources.

Figure 6.1



- *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.*

Figure 6.2



- *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.*

6.1 Basic Terms and Concepts (4/6)

- Authenticity
  - Authenticity is the characteristics of something having been provided by an authorized source.
  - Non-repudiation – the inability of a party to deny or challenge the authentication of an interaction.
- Availability
  - Availability is the characteristics of being accessible and usable during a specified time period.
- Threat
  - A threat is a potential security violation that can challenge defenses in an attempt to breach privacy and/or cause harm.

6.1 Basic Terms and Concepts (5/6)

- 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.
- Risk
  - Risk is the possibility of loss or harm arising from performing an activity.
  - 2 measures: the probability of a threat occurring and the expectation of loss upon the IT resource being compromised.

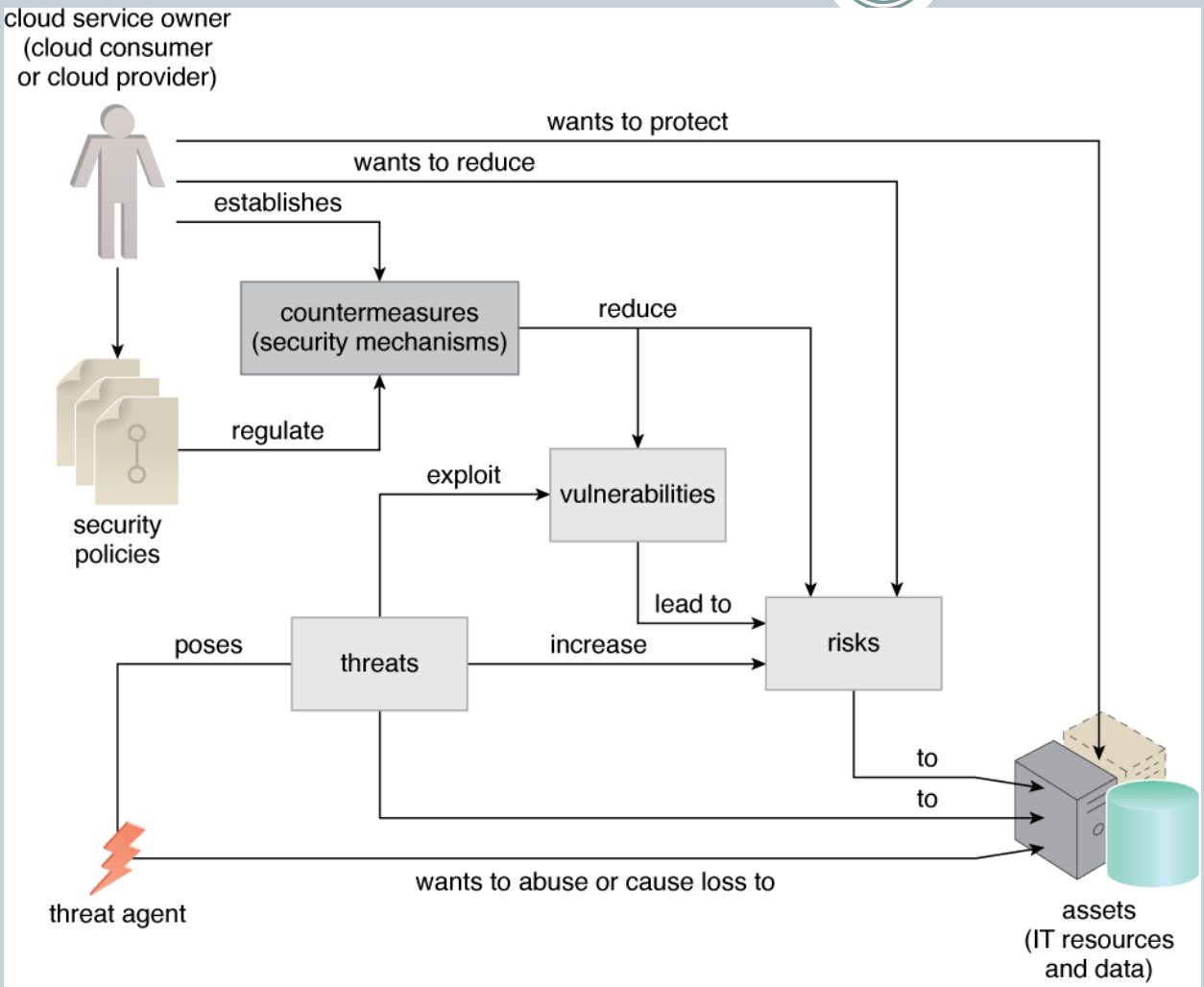
6.1 Basic Terms and Concepts (6/6)

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

6.2 Threat Agents (1/5)

- A threat agent is an entity that poses a threat because it is capable of carrying out an attack.
- A threat agent can originate either internally or externally, from humans or software programs.
- Among the various types of threat agents, trusted attackers (also called malicious tenants) and malicious insiders could cause most tremendous damage potential.

Figure 6.3



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

6.2 Threat Agents (2/5)

- 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.*

6.2 Threat Agents (3/5)

- Malicious Service Agent
  - A Malicious Service Agent is able to intercept and forward the networks traffic that flows within a cloud.

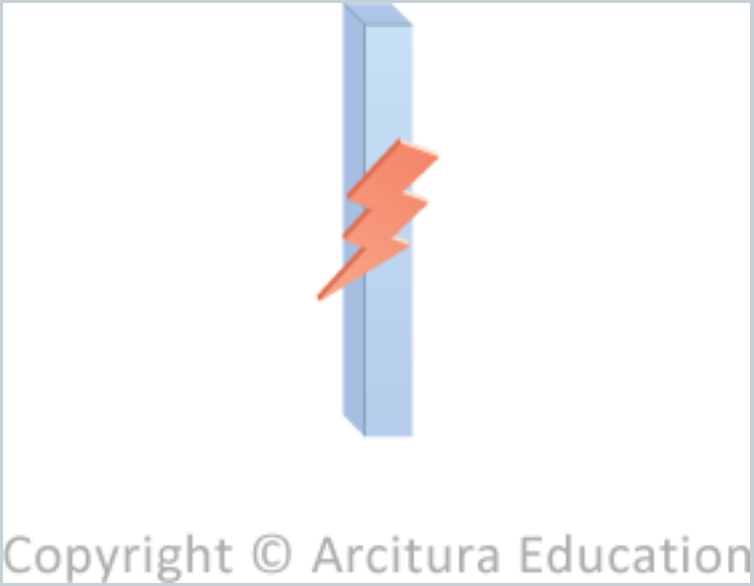


Figure 6.5 - The notation used for a malicious service agent.

6.2 Threat Agents (4/5)

- 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 provides and the cloud tenants with whom they share IT resources.

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

6.2 Threat Agents (5/5)

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

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

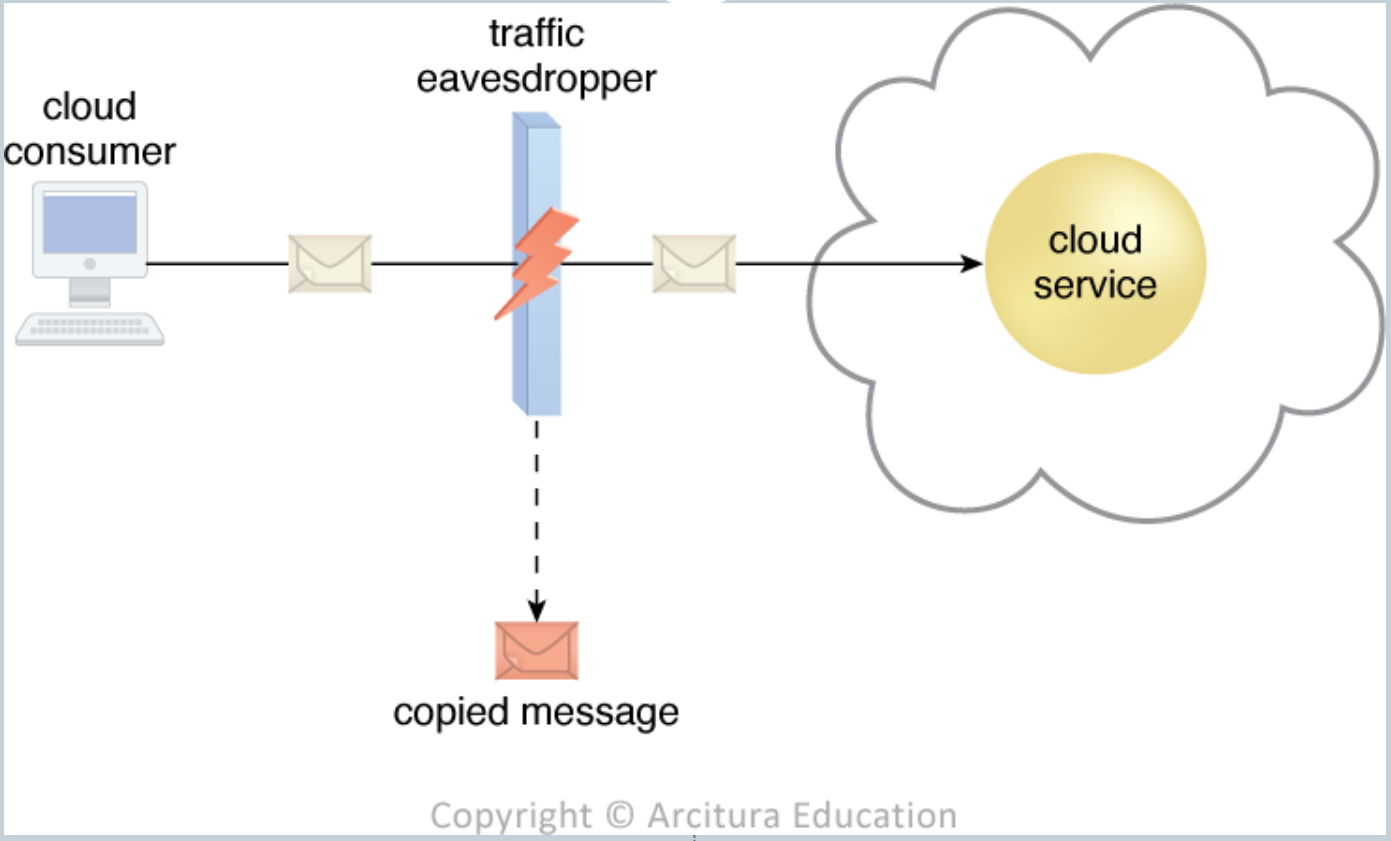
Summary of Threat Agents

- 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.

6.3 Cloud Security Threats (1/6)

- 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 indirectly compromise the confidentiality of the data and 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 period of time.

Figure 6.8

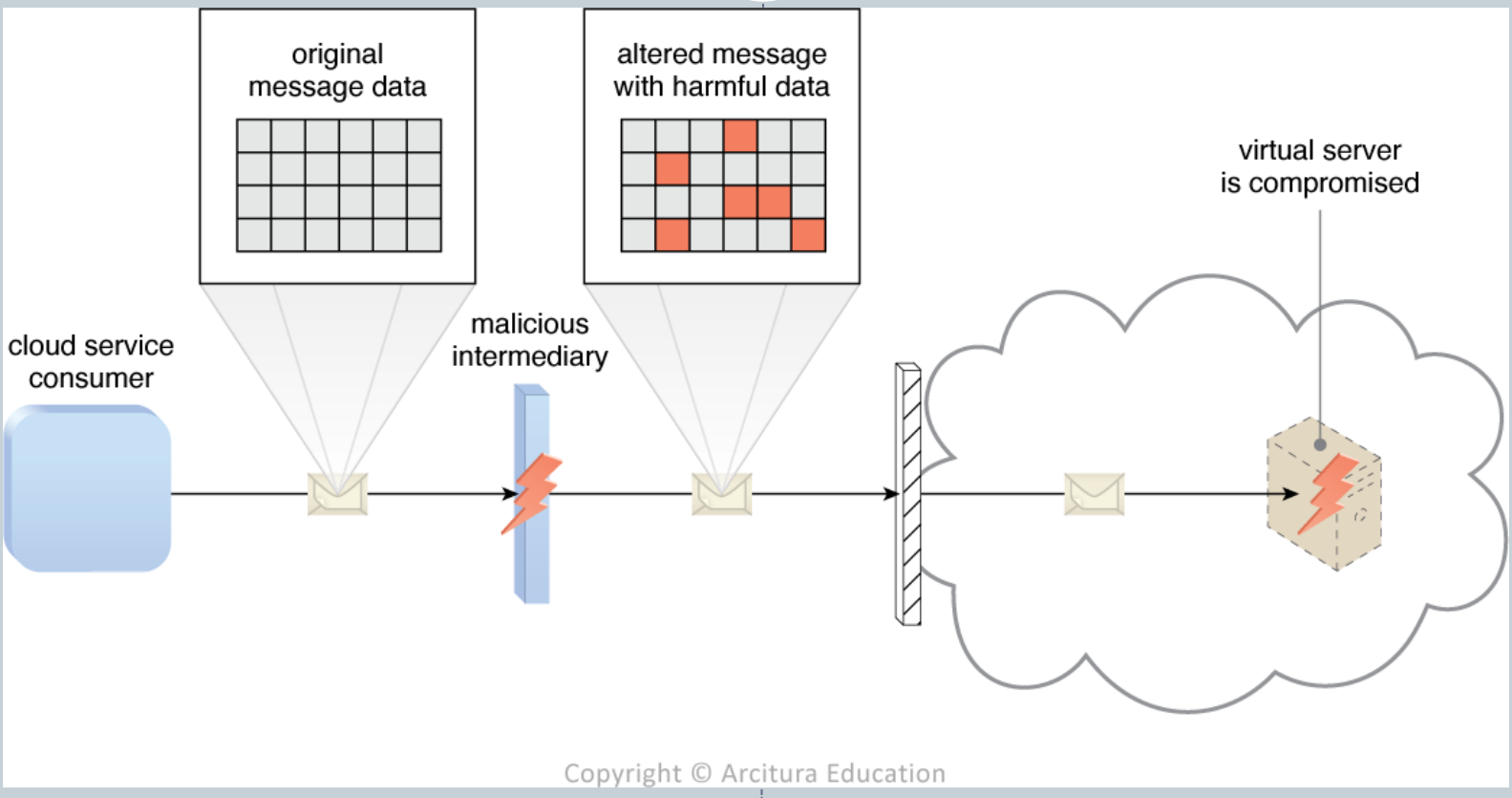


- *Figure 6.8 - An externally positioned malicious service agent carries out a traffic eavesdropping attack by intercepting a message sent by the cloud service consumer to the cloud service. The service agent makes an unauthorized copy of the message before it is sent along its original path to the cloud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

6.3 Cloud Security Threats (2/6)

- Malicious Intermediary
  - The malicious intermediary threat arises when messages are intercepted and altered by a malicious service agent, thereby potentially comprising the message's confidentiality and/or integrity.
  - It may also insert harmful data into the message before forwarding it to its destination.
  - The malicious intermediary attack can also be carried out by a malicious cloud service consumer program.

Figure 6.9

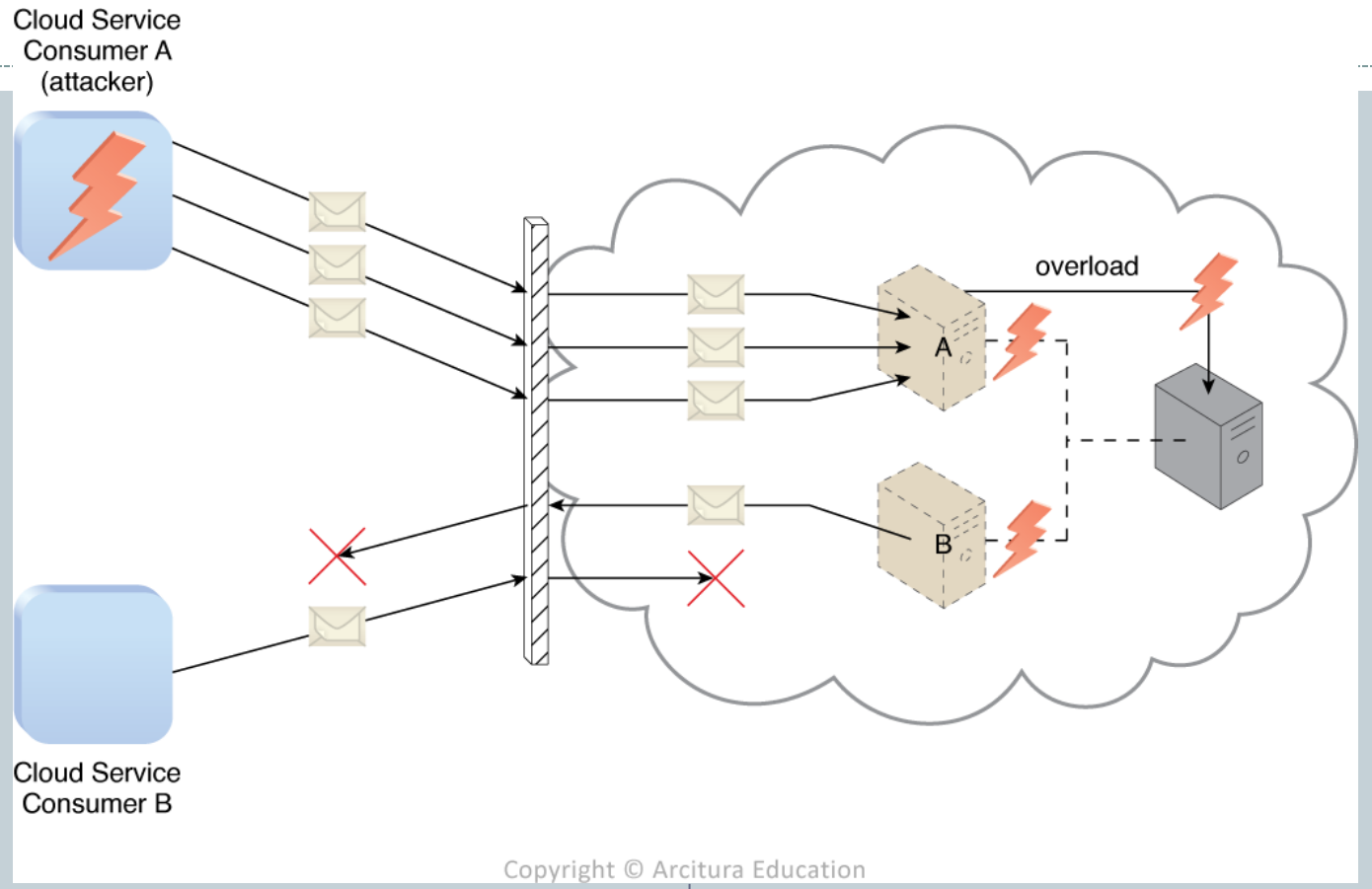


- *Figure 6.9 - The malicious service agent intercepts and modifies a message sent by a cloud service consumer to a cloud service (not shown) being hosted on a virtual server. Because harmful data is packaged into the message, the virtual server is compromised.*

6.3 Cloud Security Threats (3/6)

- Denial of Service
  - The objective of denial of service (DoS) attack is to overload IT resources to the point where they cannot function properly.
- DoS is commonly launched in the following ways:
  - The workload is artificially increased.
  - He network is overloaded with traffic.
  - Multiple service requests with excessive memory and processing resources are sent.
- Successfully DoS attacks produce server degradation and/or failure.

Figure 6.10

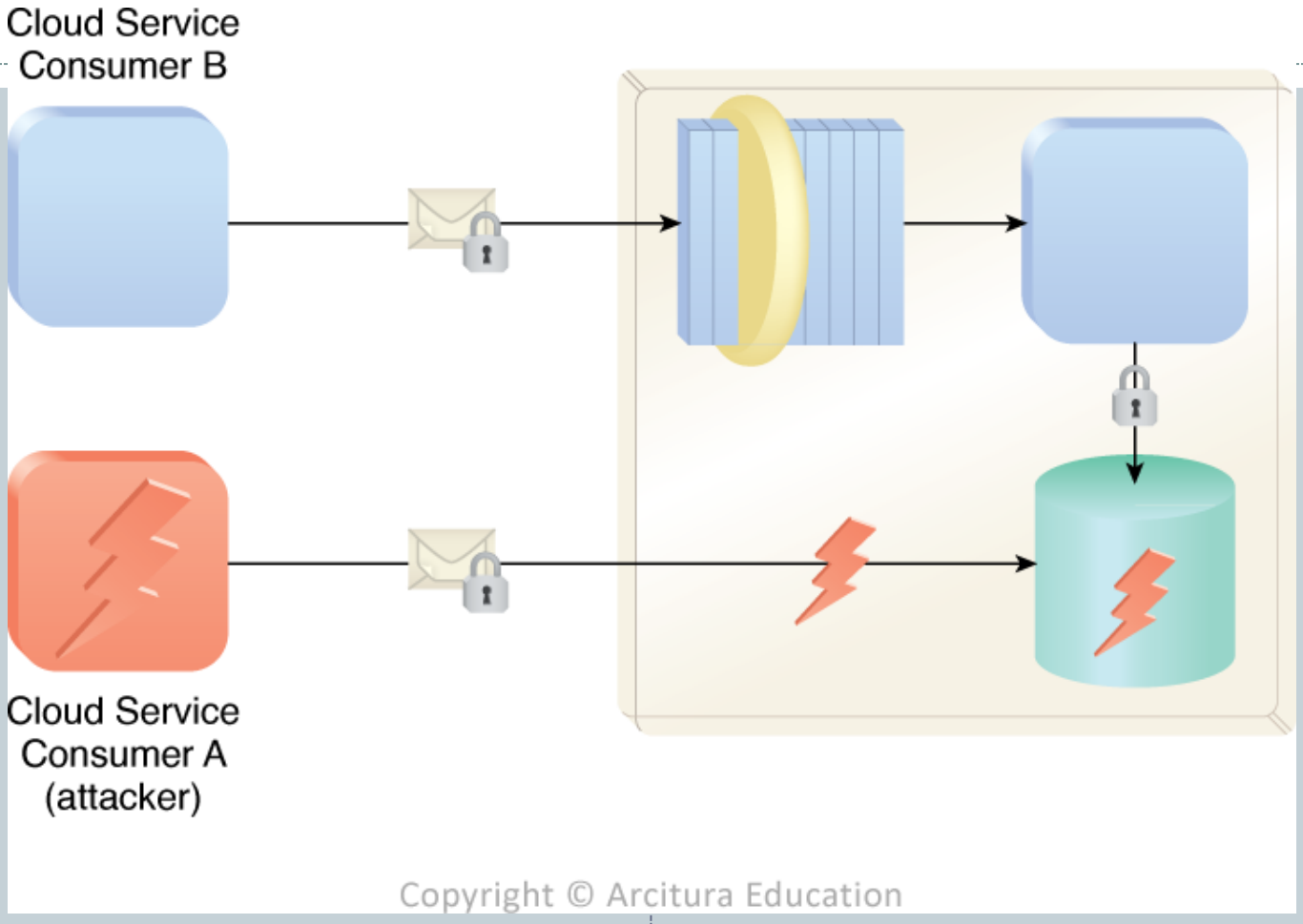


- *Figure 6.10 - Cloud Service Consumer A sends multiple messages to a cloud service (not shown) hosted on Virtual Server A. This overloads the capacity of the underlying physical server, which causes outages with Virtual Servers A and B. As a result, legitimate cloud service consumers, such as Cloud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

6.3 Cloud Security Threats (4/6)

- Insufficient Authorization
  - The insufficient authorization attack occurs when access is granted to an attack erroneously or too broadly, resulting in the attacker getting access to IT resources that are normally protected.
  - It 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.

Figure 6.11

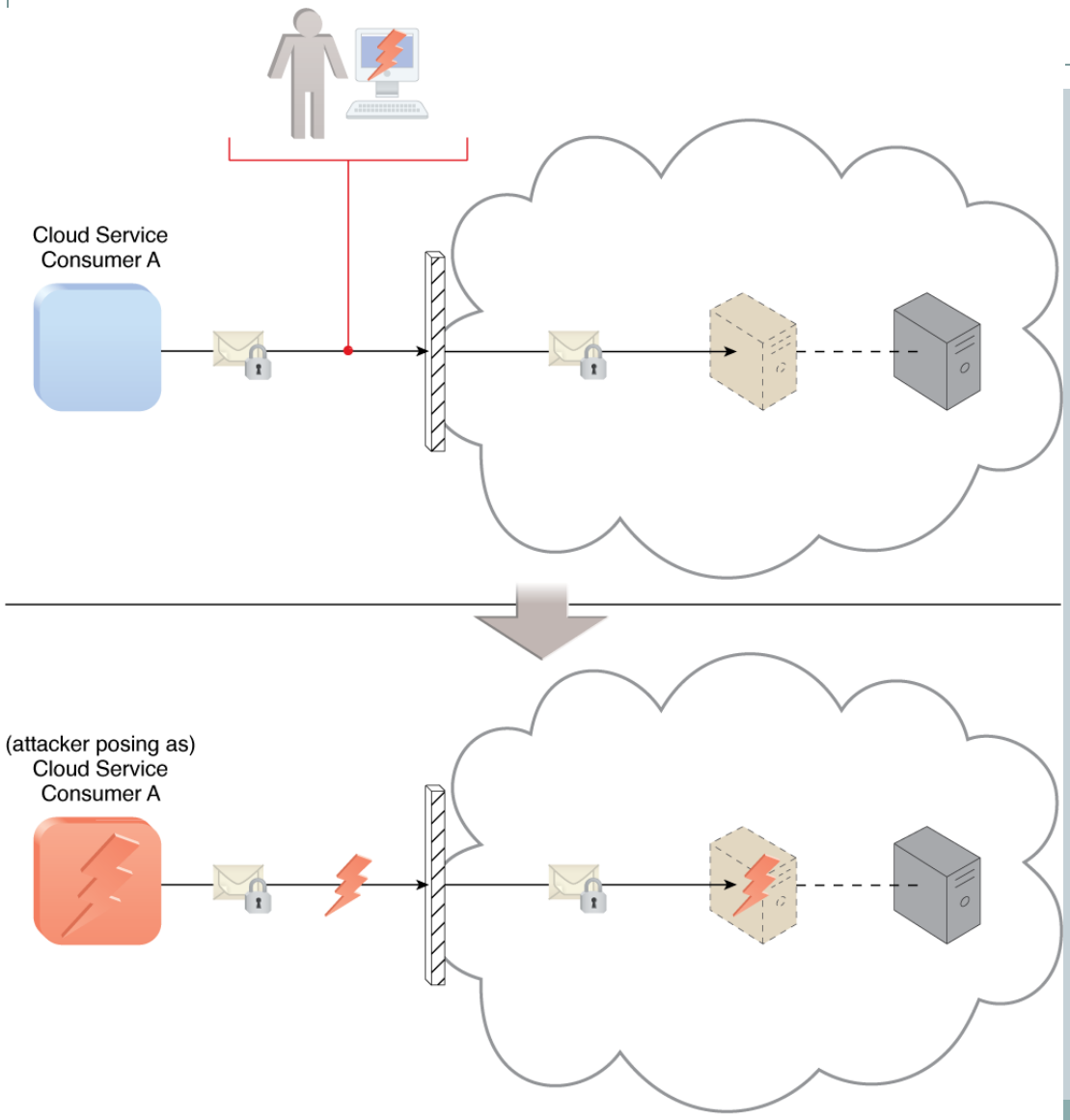


- *Figure 6.11 - Cloud Service Consumer A gains access to a database that was implemented under the assumption that it would only be accessed through a Web service with a published service contract (as per Cloud Service Consumer B).*

6.3 Cloud Security Threats (5/6)

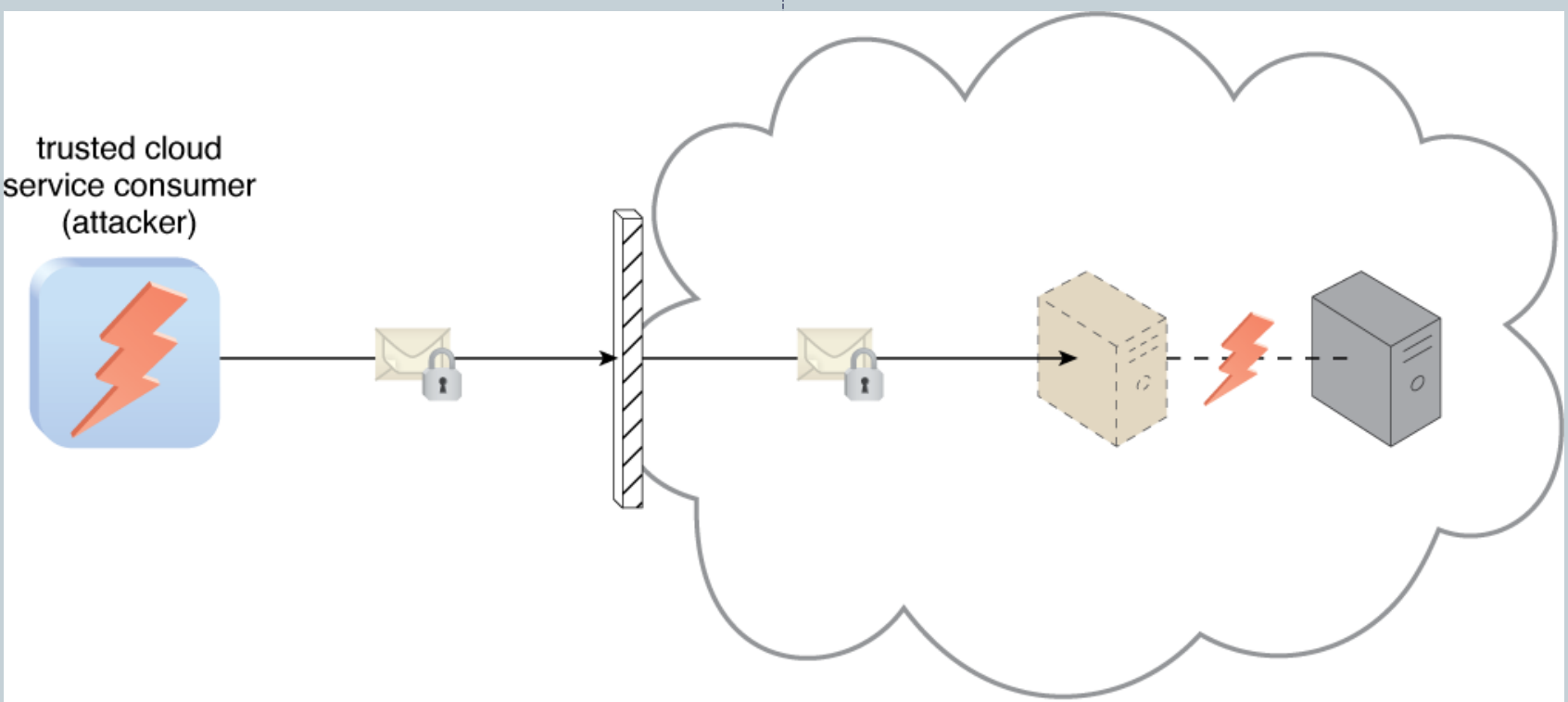
- Virtualization Attack
  - A virtualization attack exploits vulnerabilities in the virtualization platform to jeopardize its confidentiality, integrity, and/or availability.
  - Cloud provider could grant cloud consumers administrative access to virtualized IP resources, there is an inherent risk of abusing this access to attack the underlying physical IT resources.

Figure 6.12



- *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.*

Figure 6.13

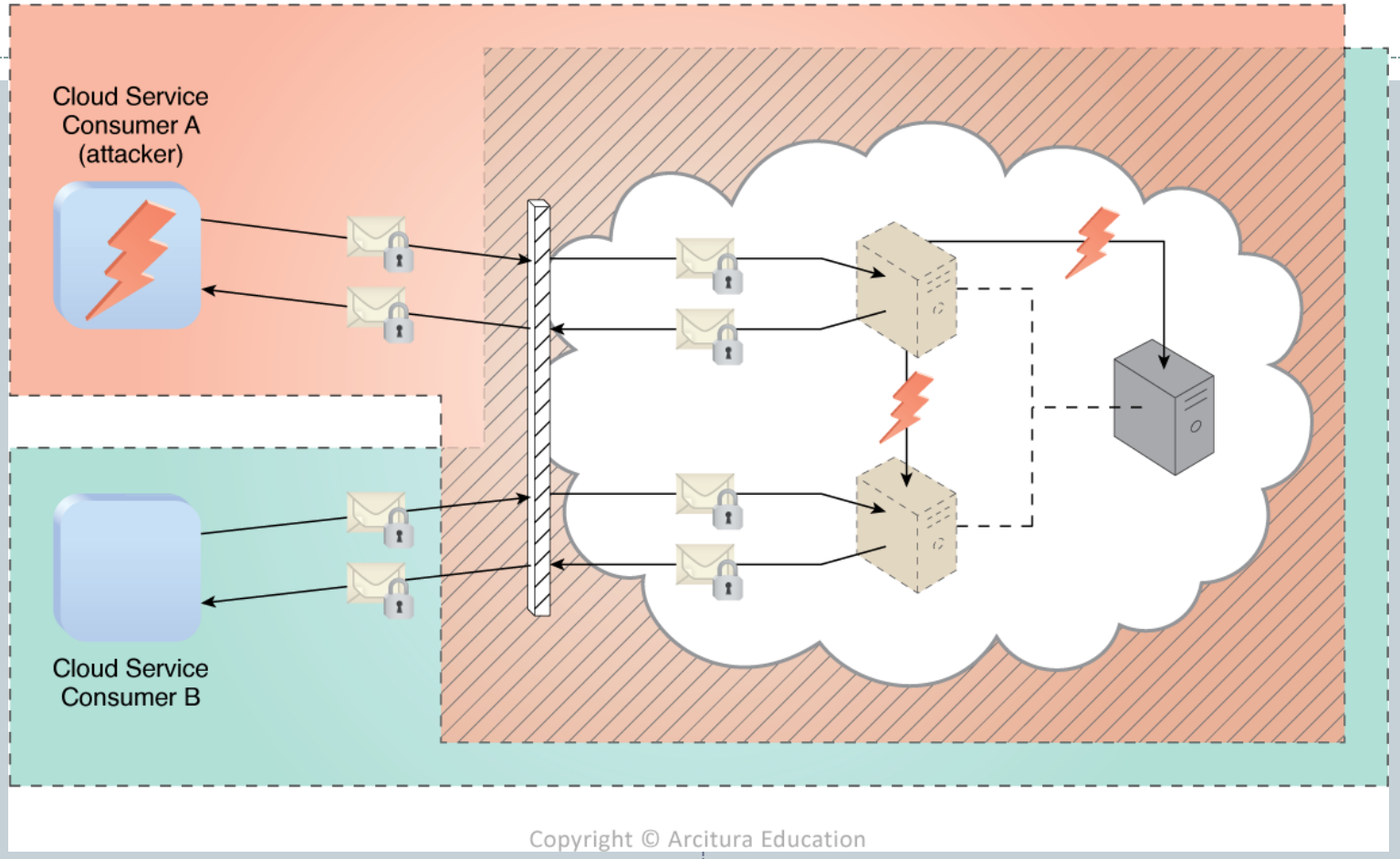


- *Figure 6.13 - An authorized cloud service consumer carries out a virtualization attack by abusing its administrative access to a virtual server to exploit the underlying hardware.*

6.3 Cloud Security Threats (6/6)

- 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.

Figure 6.14

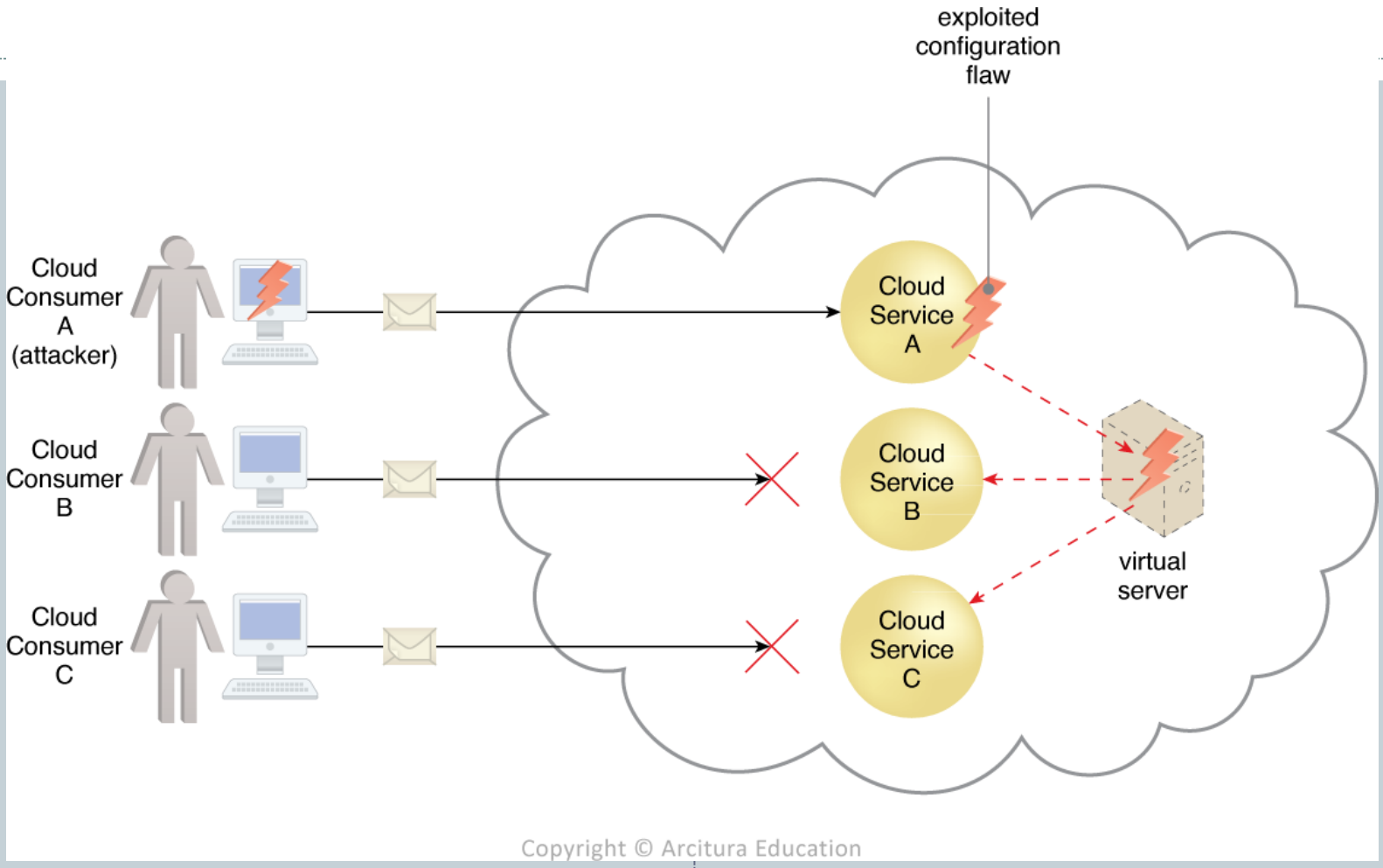


- *Figure 6.14 - Cloud Service Consumer A is trusted by the cloud and therefore gains access to its virtual server which it then attacks with the intention of attacking the underlying physical server and the virtual server used by Cloud Service Consumer B.*

6.4 Additional Considerations (1/4)

- Flawed Implementations
  - If the cloud provider's software and/or hardware have inherent security flaws or operational weakness, attackers can exploit these vulnerabilities to impair the integrity, confidentiality, and/or availability of cloud provider IT resources and cloud consumer IT resources hosted the cloud provider.
  - The flaw is exposed accidently by a legitimate cloud service consumer, it could have easily been discovered and exploited by an attacker.

Figure 6.15



- *Figure 6.15 - 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.*

6.4 Additional Considerations (2/4)

- Security Policy Disparity
  - 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.
- Contracts
  - 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.

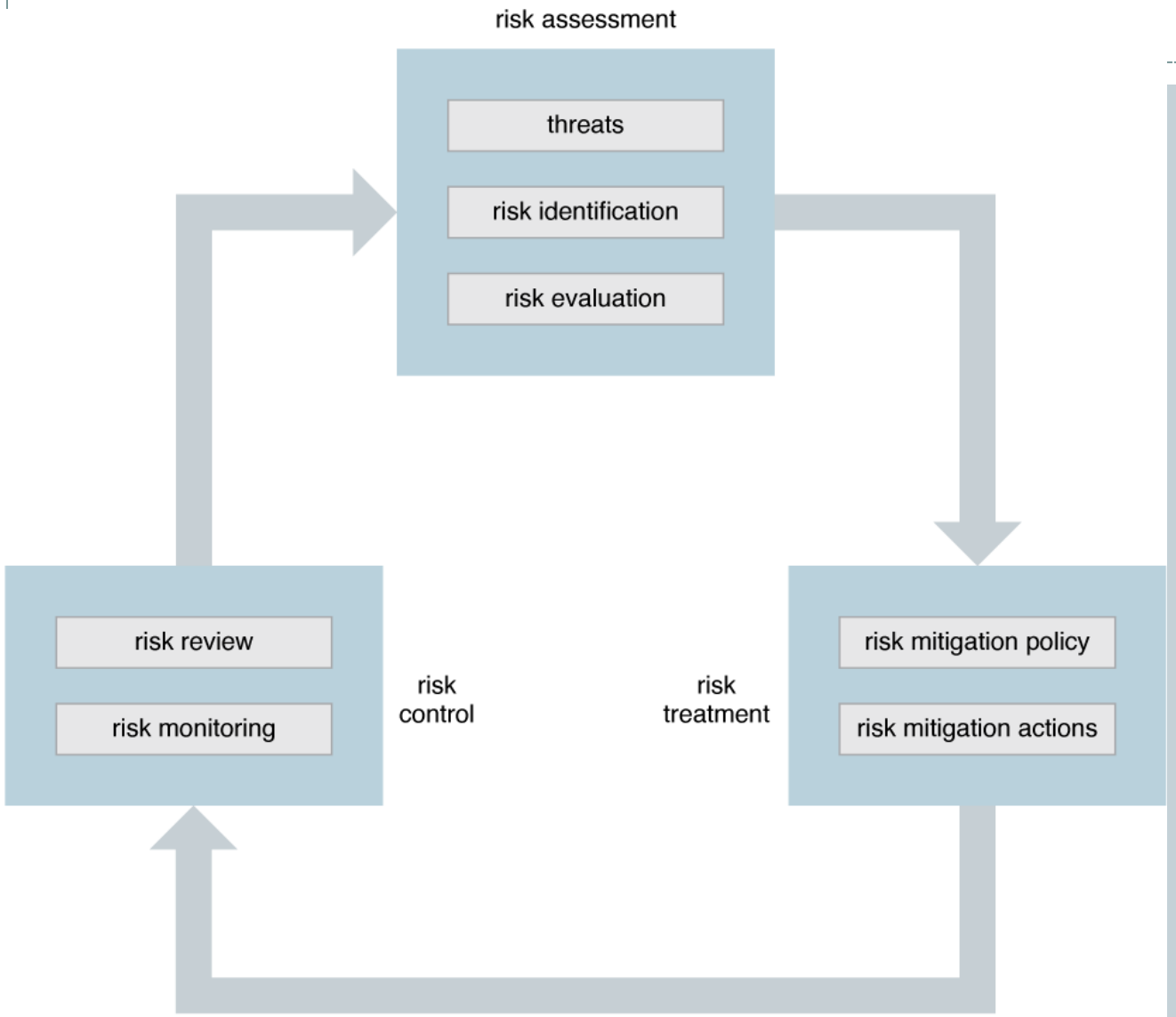
6.4 **Additional Considerations** (3/4)

- Risk Management
  - Risk management is comprised of a set of coordinated activities for overseeing and controlling risks. There are three main activities:
    1. Risk Assessment
    2. Risk Treatment
    3. Risk Control

6.4 Additional Considerations (4/4)

- Risk assessment
  - Risk management is comprised of a set of coordinated activities for overseeing and controlling risks: past threats information, risk identification, and risk evaluation.
- Risk treatment
  - Risk mitigation policy
  - Risk mitigation actions
- Risk control
  - Surveying related events, reviewing to determine the effectiveness of previous assessments and treatments, and identifying any policy adjustment needs.

Figure 6.16



- *Figure 6.16 - The ongoing risk management process, which can be initiated from any of the three stages.*