

CSCI 5409 Cloud Computing – Fall, 2023  
Week 10 – Lecture 1 (Nov 6, 2023)

## Security – Part 1

Dr. Lu Yang  
Faculty of Computer Science  
Dalhousie University  
luyang@dal.ca

## Housekeeping and Feedback

- Start recording
- Starting working on the term project. Ask Purvesh and Rahul questions.
- PIER tour tomorrow.

## Objectives

- Understand and develop risk mitigation plans for cloud-specific security threats

## Contents

- Section 1.** Key Security Terms
- Section 2.** Threat Agents
- Section 3.** Cloud-Specific Security Threats



# 1

## **Key Security Terms**

1. Key Security Terms
  2. What are We Trying to Protect?
- 

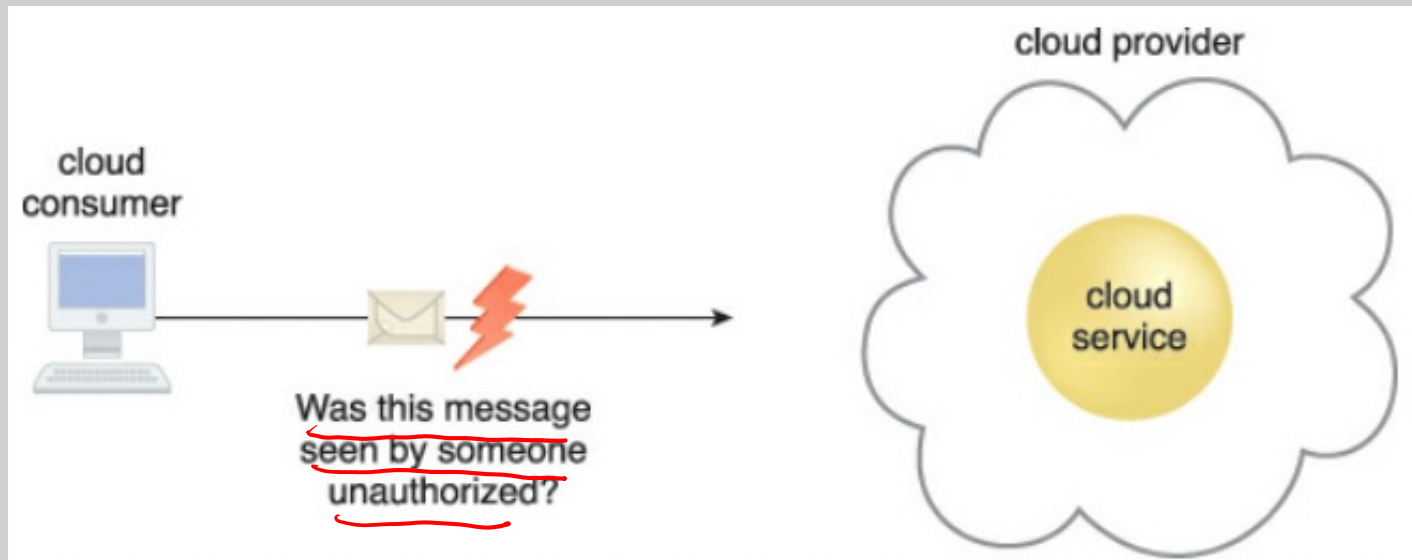
We have a lot security courses:

- CSCI5001 Privacy & IT ✓
- CSCI2201 Introduction to Info Security ✓
- CSCI4116 Cryptography ✓
- CSCI4174 Network Security ✓
- CSCI6708 Advanced Topics in Network Security ✓

## Key Security Terms<sup>[1]</sup> (1/6)

- **Confidentiality:**

- "The characteristic of something being made accessible only to authorized parties."
- Within cloud environments, confidentiality primarily pertains to restricting access to data in transit and storage.

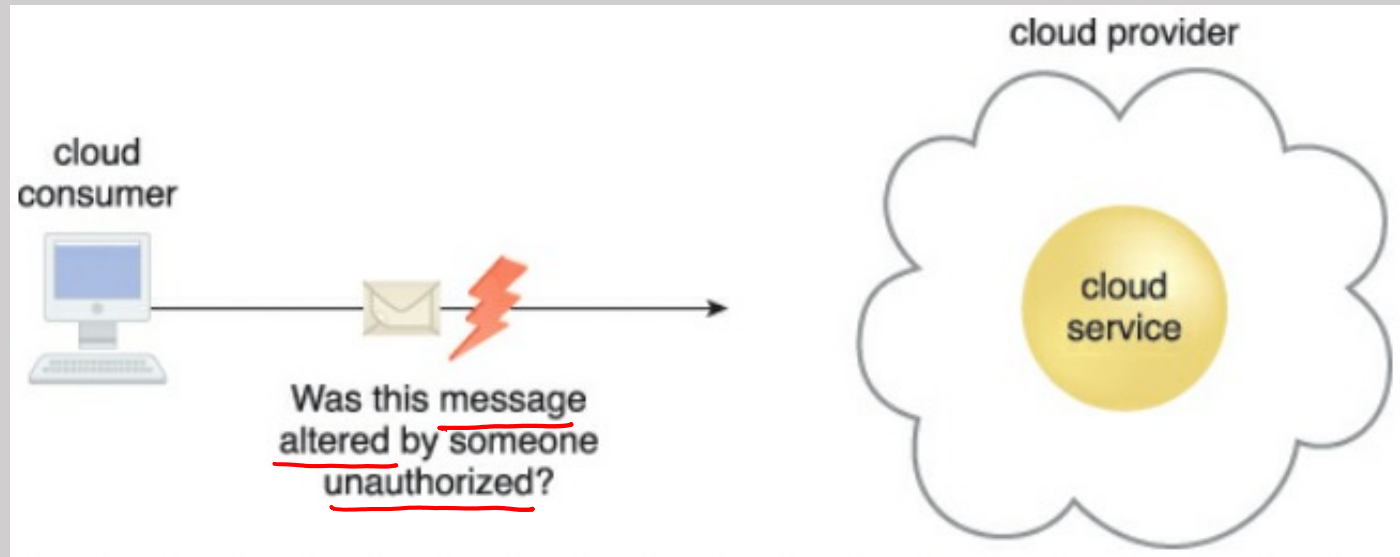


The message issued by the cloud consumer to the cloud service is considered confidential only if **it is not accessed or read by an unauthorized party**

## Key Security Terms<sup>[1]</sup> (2/6)

- **Integrity**

- "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



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



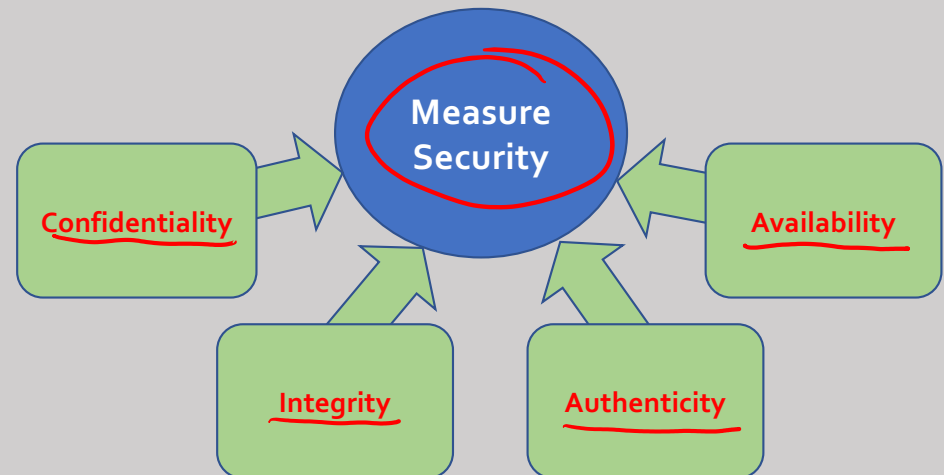
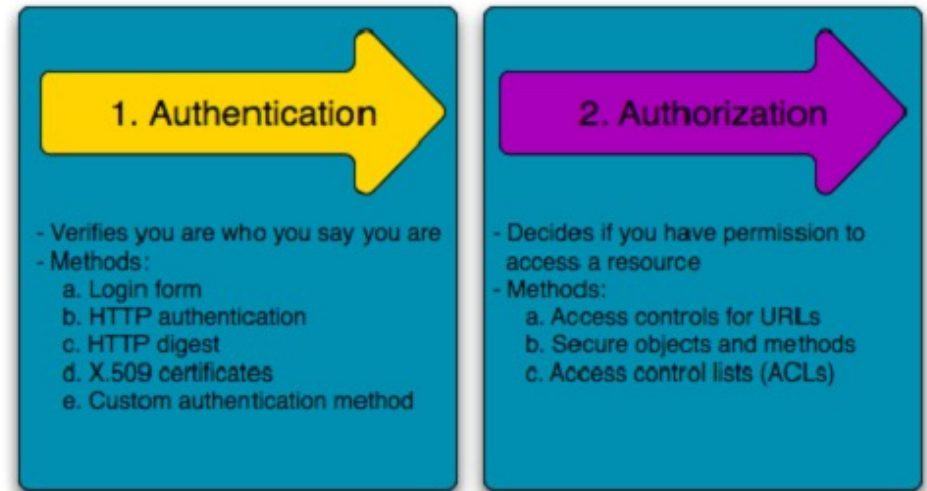
## Key Security Terms<sup>[1]</sup> (3/6)

- **Authenticity**

- "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.

- **Availability**

- "The characteristic of being accessible and usable during a specified time period."



## Key Security Terms<sup>[1]</sup> (4/6)

- **Threat**

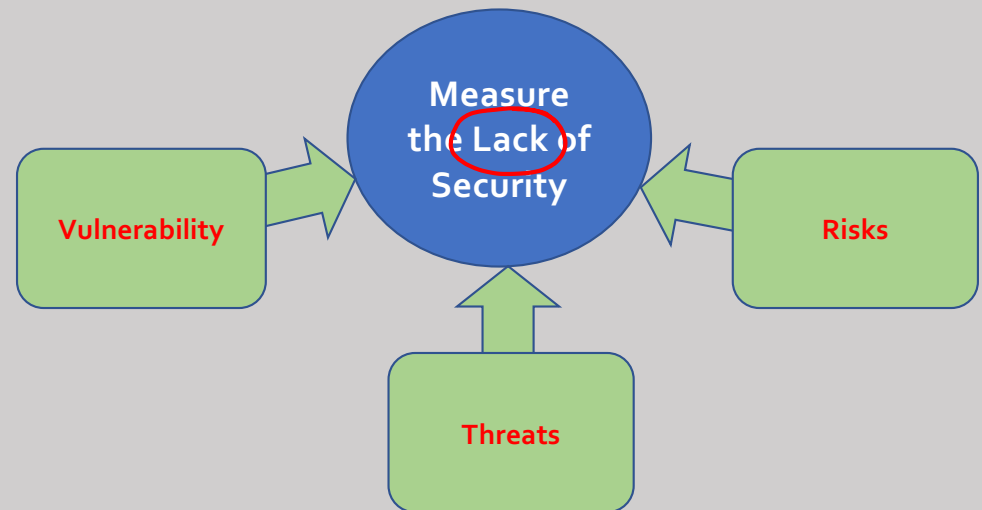
- "A potential security violation that can challenge defenses in an attempt to break privacy and/or cause harm." A threat carried out is an attack.

- **Vulnerability**

- "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.

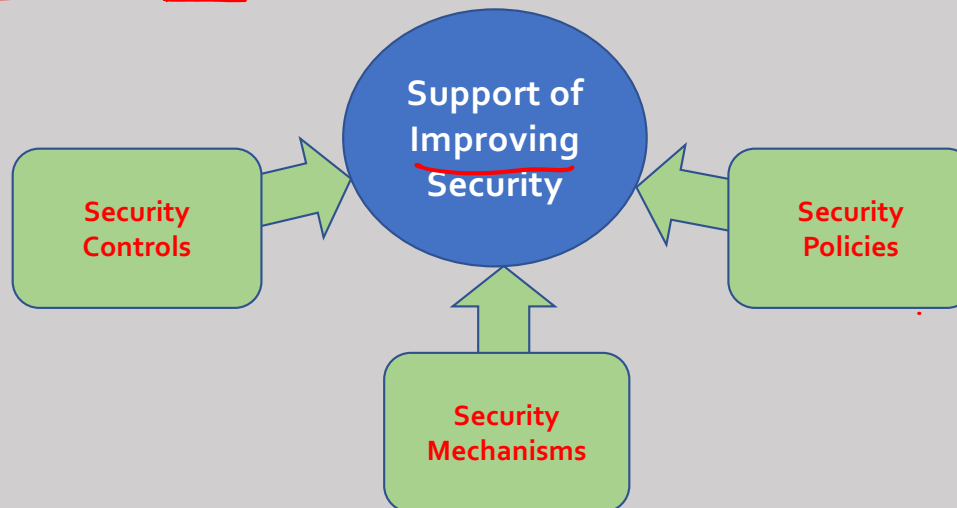
- **Risk**

- "The possibility of loss or harm arising from performing an activity." (From 3130: measured by likelihood and severity)
- Risk is typically measured according to its threat level and the number of possible or known vulnerabilities. Two metrics that can be used to determine risk for an IT resource are:
  - The probability of a threat occurring to exploit vulnerabilities in the IT resource
  - The expectation of loss upon the IT resource being compromised

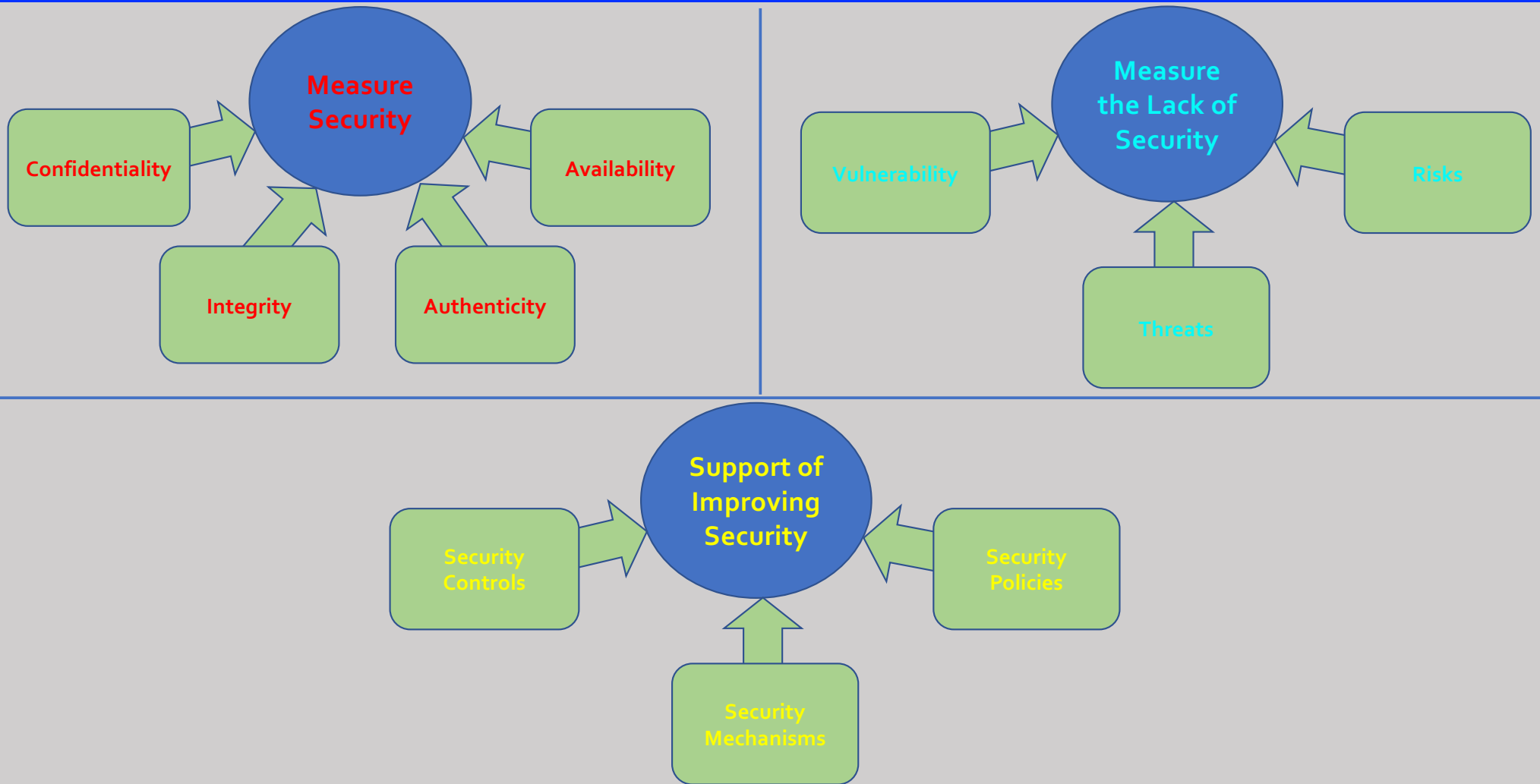


## Key Security Terms<sup>[1]</sup> (5/6)

- **Security Controls**
  - "Countermeasures used to prevent or respond to security threats and to reduce or avoid risk."
- **Security Mechanisms**
  - "Countermeasures are typically described in terms of security mechanism, which are components comprising a defensive framework that protects IT resources, information, and services."
- **Security Policies**
  - "Establishes a set of security rules and regulations."
  - Security policies will further define how these rules and regulations are implemented and enforced.
  - Includes the positioning and usage of security controls and mechanisms.

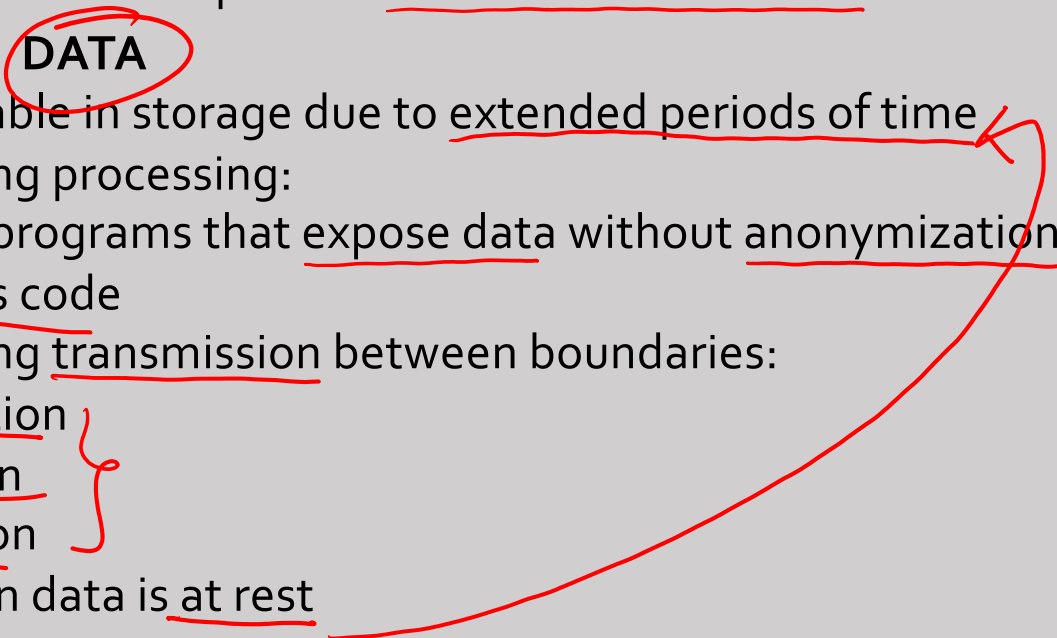


## Key Security Terms<sup>[1]</sup> (6/6)



[1] Cloud Computing (T. Erl, Z. Mahmoud, R. Puttini / 2013) pg. 120 - 121

## What are we trying to protect?

- IT Resources: We must keep them available to our consumers.
  - Most important: **DATA**
    - Most vulnerable in storage due to extended periods of time
    - Threats during processing:
      - Flaws in programs that expose data without anonymization (e.g. logging)
      - Malicious code
    - Threats during transmission between boundaries:
      - Interception
      - Alteration
      - Corruption
    - Threats when data is at rest
- 



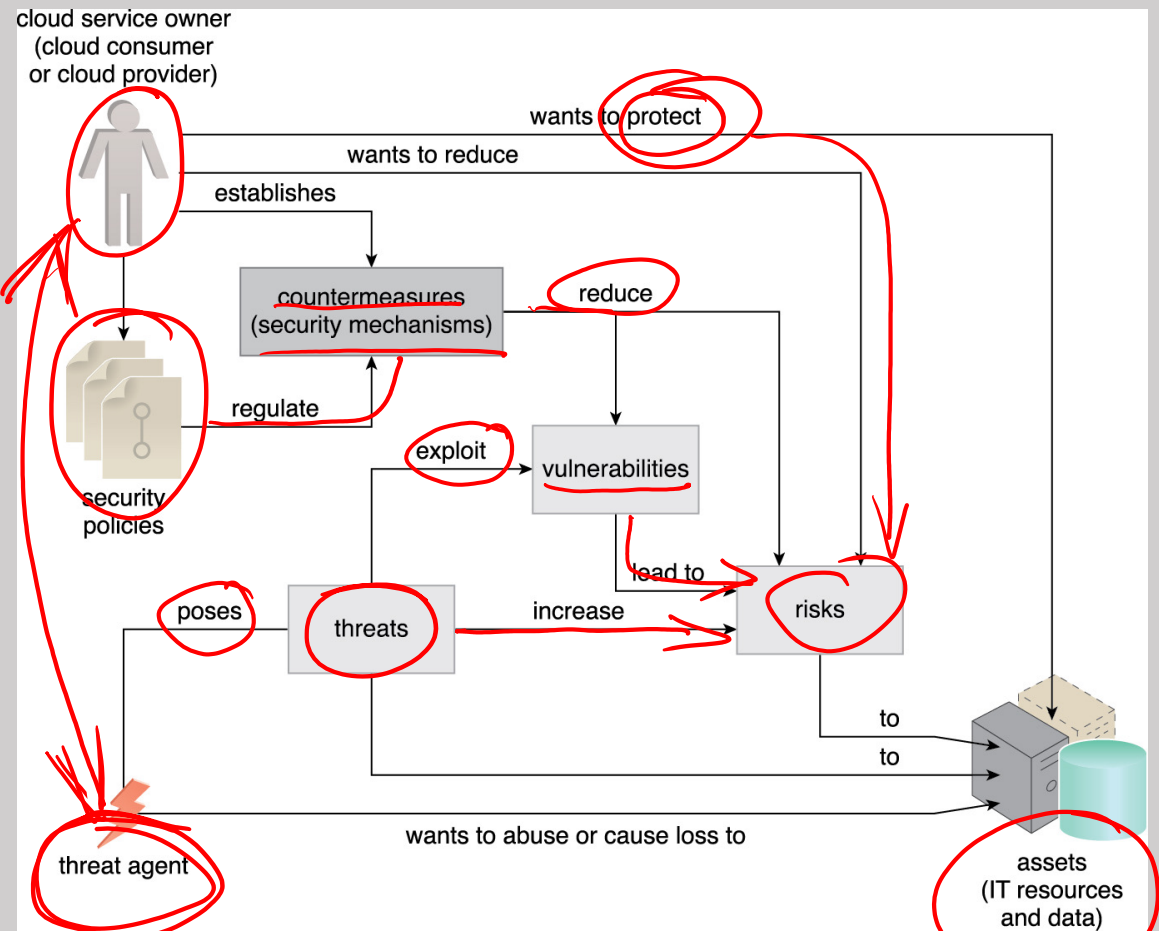
2

## Threat Agents



# Overview

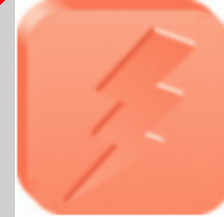
- "A **threat agent** is an entity that poses a threat because it is capable of carrying out an attack."<sup>[1]</sup>
- Cloud security threats can originate either internally or externally, from humans or software programs.



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."<sup>[1]</sup>
- Typically exists as an external software program that launches network-level attacks through public networks
- Usually resorts to acts like bypassing user accounts or stealing user credentials
- Actively uses methods that either ensure anonymity or require substantial resources for prosecution



The notation used for an anonymous attacker



## Threat Agents – Malicious Service Agent

- A **malicious service agent** is "able to intercept and forward the network traffic that flows within a cloud."
- Typically exists as a service agent (or a program pretending to be a service agent) with compromised or malicious logic
- May also be an external program able to remotely intercept and potentially corrupt message contents



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." [1]
- Usually launch their attacks within a cloud's trust boundaries by abusing legitimate credentials
- Trusted attackers (also known as malicious tenants) can use cloud-based IT resources for a wide range of exploitations, including the hacking of weak authentication processes, the breaking of encryption, the spamming of e-mail accounts, or to launch common attacks, such as denial of service campaigns.



The notation used for a trusted attacker

## Threat Agents – Malicious Insider

- Malicious insiders are "human threat agents acting on behalf of or in relation to the cloud provider." [1]
- Typically, current or former employees or third parties with access to the cloud provider's premises
- Carries tremendous damage potential as they may have administrative privileges for accessing cloud consumer IT resources



The notation used for a malicious insider. The human symbol is optional.



[1] Cloud Computing (T. Erl, Z. Mahmoud, R. Puttini / 2013) pg. 123

[Image] <https://cdn2.unrealengine.com/egs-amongus-innersloth-s6-1200x1600-675403712.jpg>

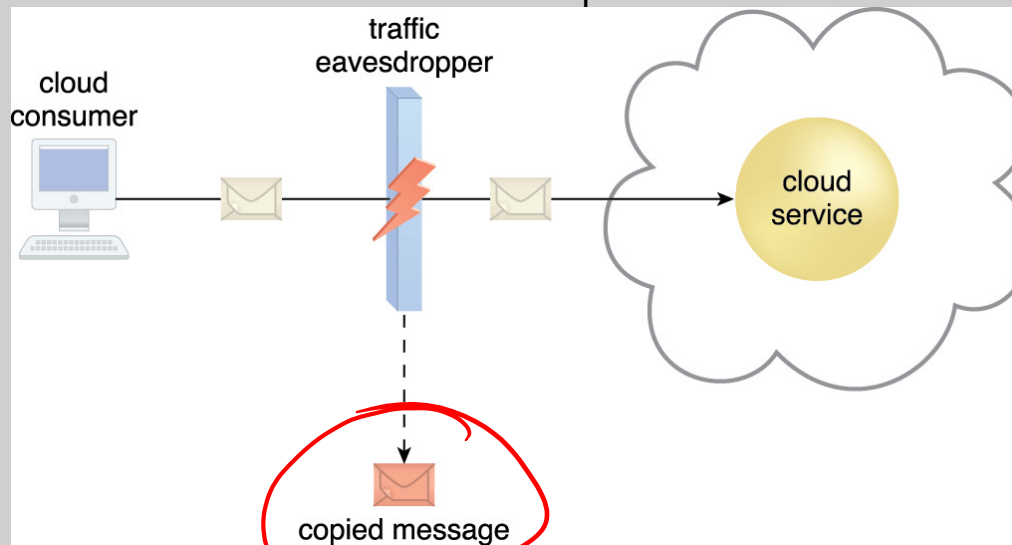


3

## **Cloud-Specific Security Threats**

## Traffic Eavesdropping

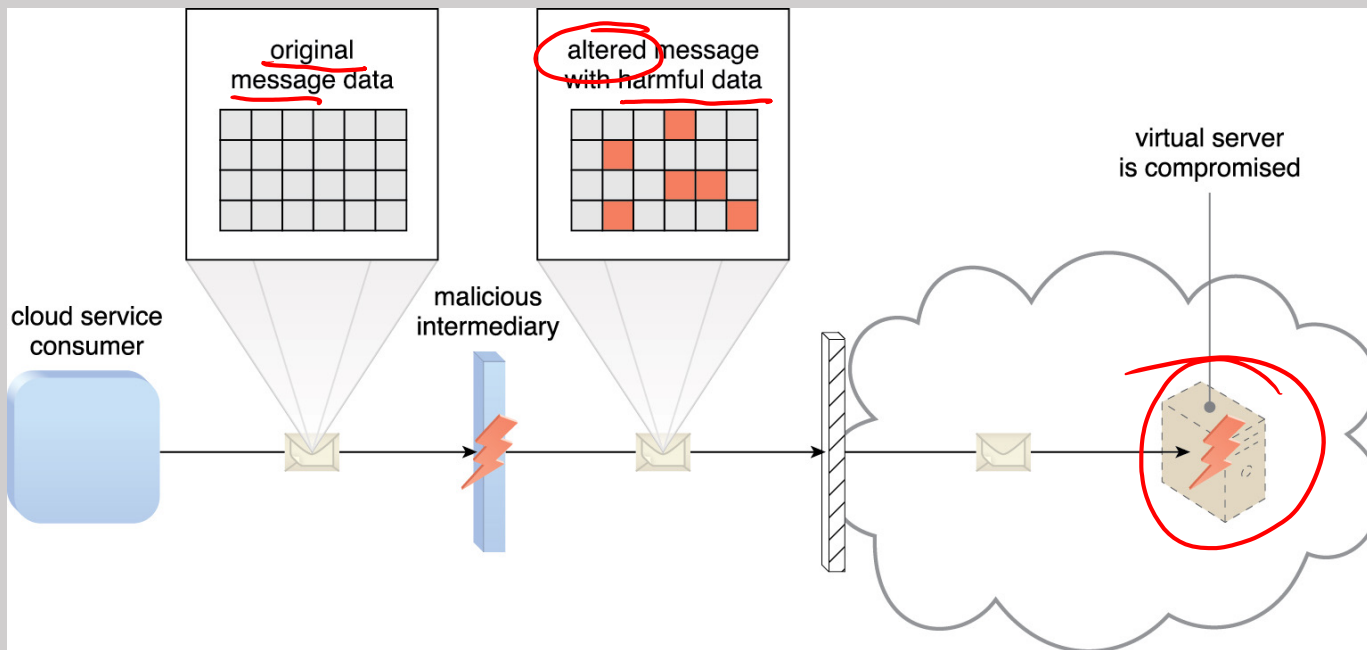
- **Traffic eavesdropping** "occurs when data being transferred to or within a cloud is passively intercepted by a malicious service agent for illegitimate information gathering purposes."
- Difficult to detect due to the passive nature
- The severity of this threat depends on the data intercepted, if account credentials or financial could be extremely high
- 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.



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

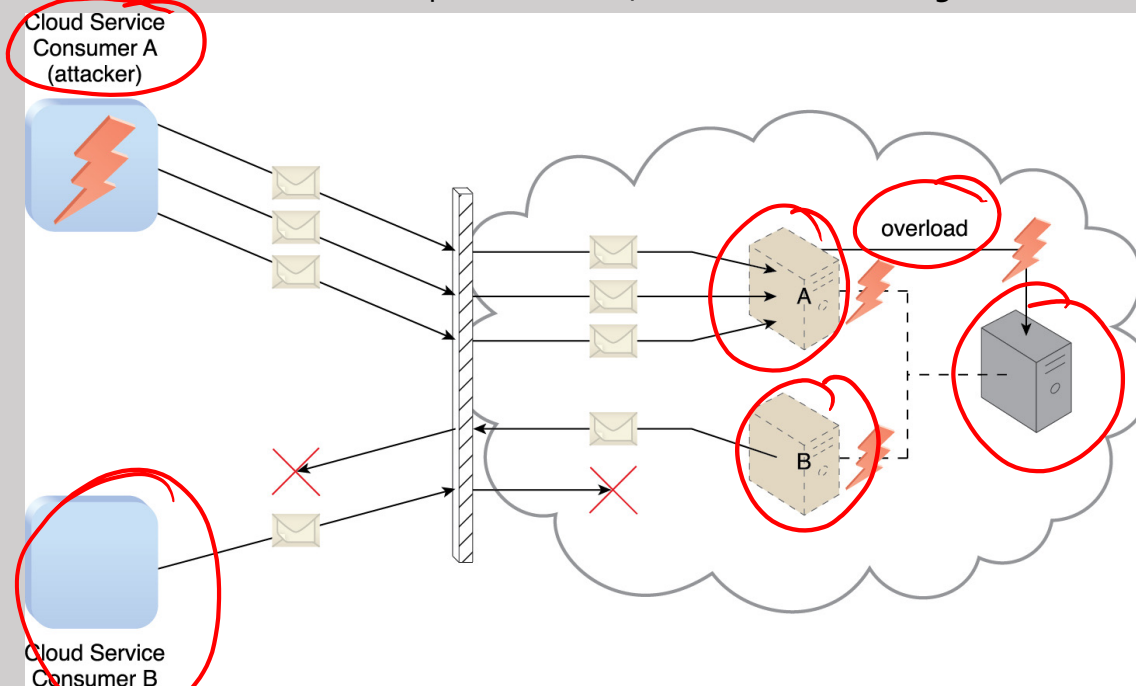
- The **malicious intermediary** "threat arises when messages are intercepted and altered by a malicious service agent, thereby potentially compromising the message's confidentiality and/or integrity." [1]
- The potential to insert harmful data (e.g. viruses) into the message before forwarding it to its destination makes this threat very dangerous



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

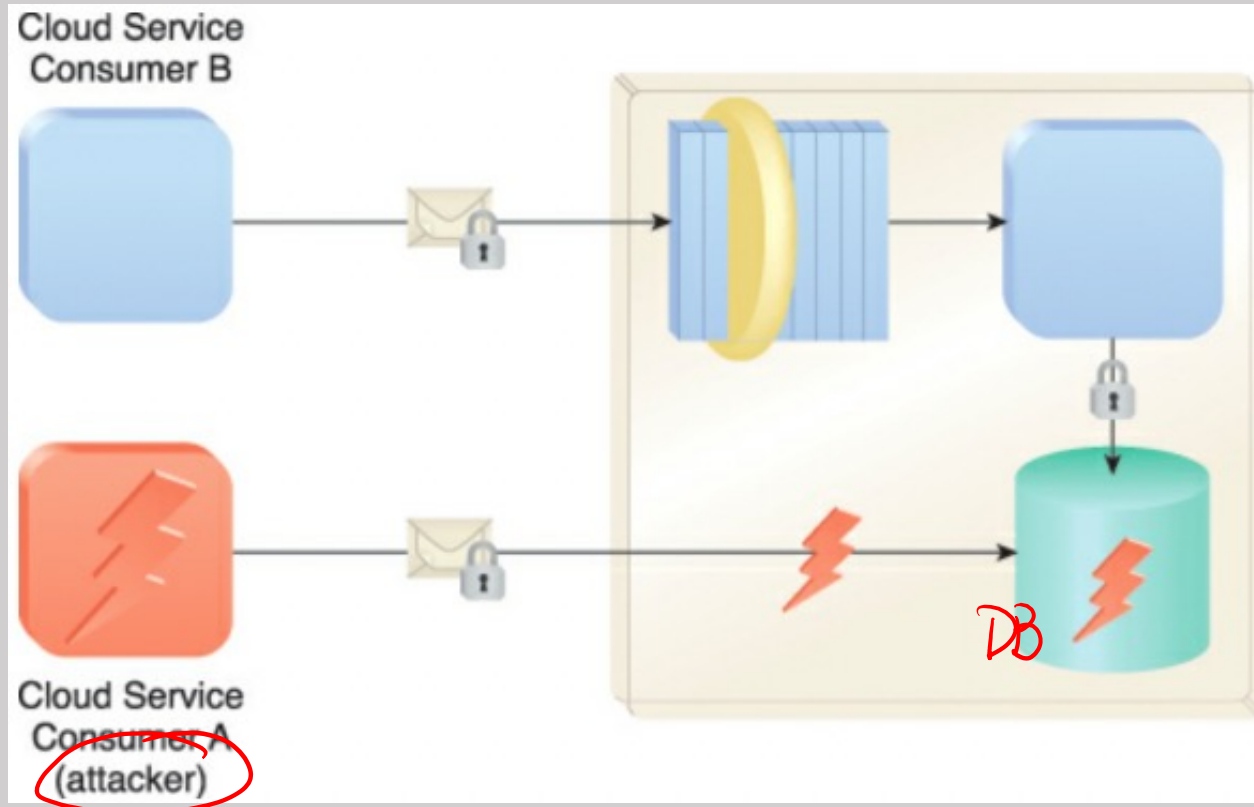
- "The objective of the **denial of service** (DoS) attack is to overload IT resources to the point where they cannot function properly." [1]
- Techniques: **DDoS**
  - Bombarding with duplicate / imitation messages
    - The workload on cloud services is artificially increased with imitation messages or repeated communication requests.
  - Overloading network traffic
    - The network is overloaded with traffic to reduce its responsiveness and cripple its performance.
  - Bombarding with service requests, each designed to consume excessive memory and processing resources
    - Multiple cloud service requests are sent, each of which is designed to consume excessive memory and processing resources.



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 (1/2)

- 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.

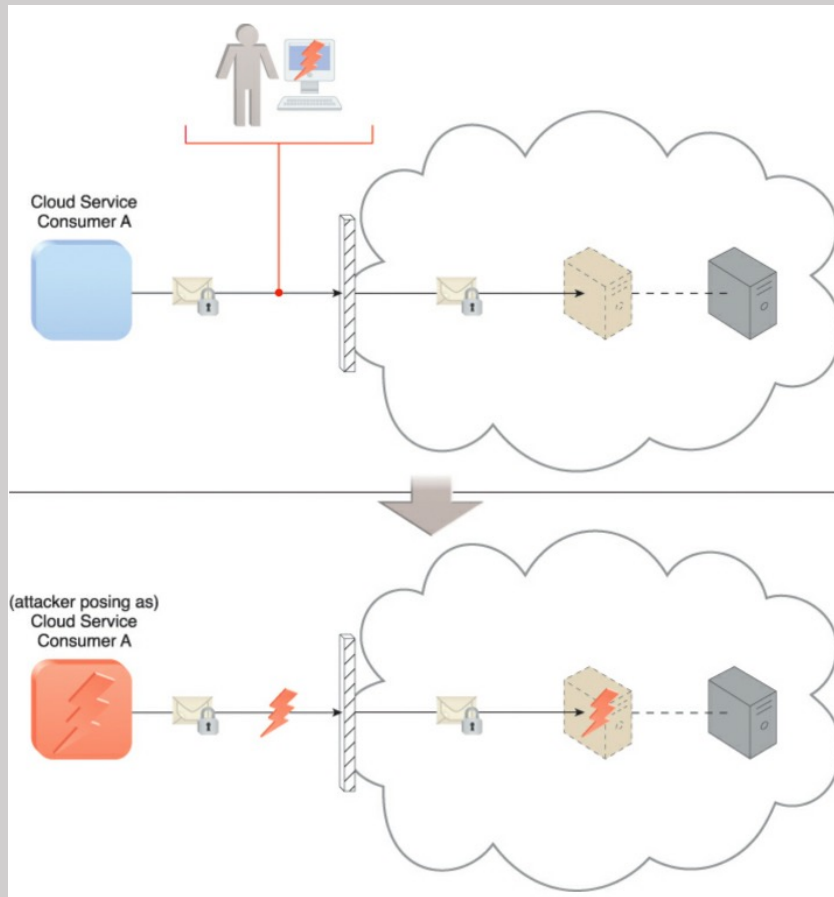


Cloud Service Consumer A gains access to a database that was implemented under the assumption that it would only be accessed through a Web service with a published service contract (as per Cloud Service Consumer B).



## Insufficient Authorization Attack (2/2)

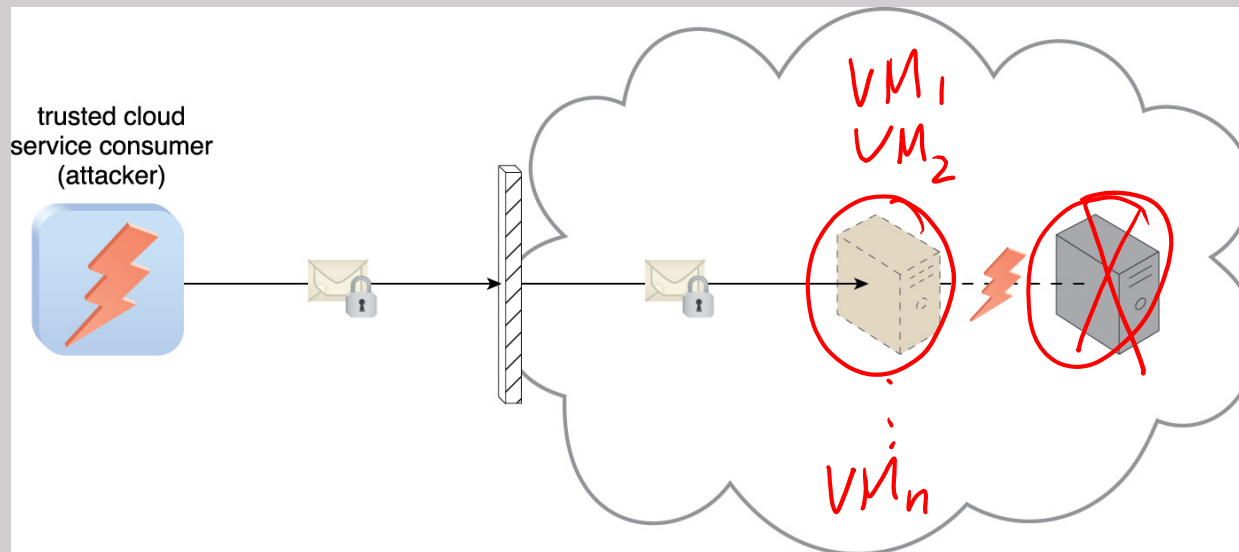
- Weak authentication attack: can result when weak passwords or shared accounts are used to protect IT resources.
- Within cloud environments, these types of attacks can lead to significant impacts depending on the range of IT resources and the range of access to those IT resources the attacker gains.



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

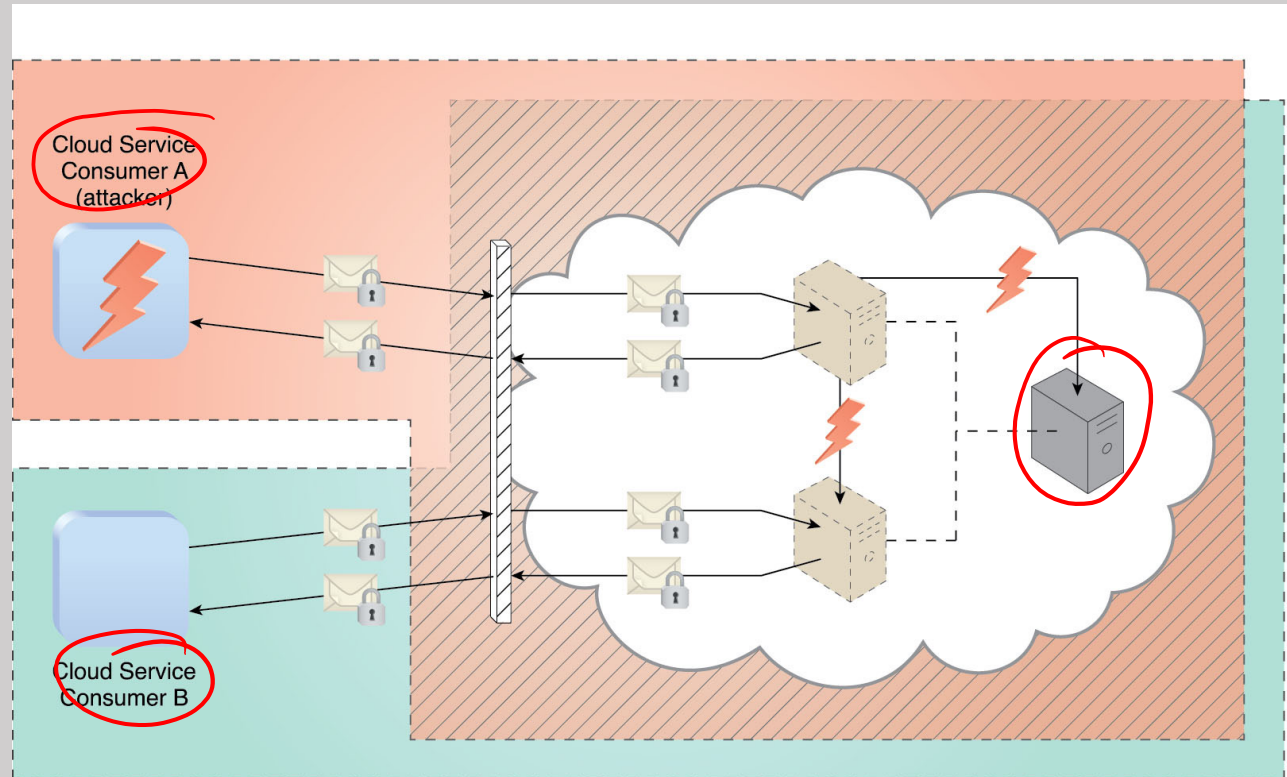
- A **virtualization attack** "exploits vulnerabilities in the virtualization platform to jeopardize its confidentiality, integrity, and/or availability." [1]
- After accessing a virtual server within the cloud, the trusted attacker can compromise or undermine the underlying physical server which may be providing virtual IT resources to multiple cloud consumers.
- 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.



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

- Essentially overlapping trust boundaries means that all cloud consumers of the cloud provider could be potential trusted attackers
- 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.



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

## Additional Considerations

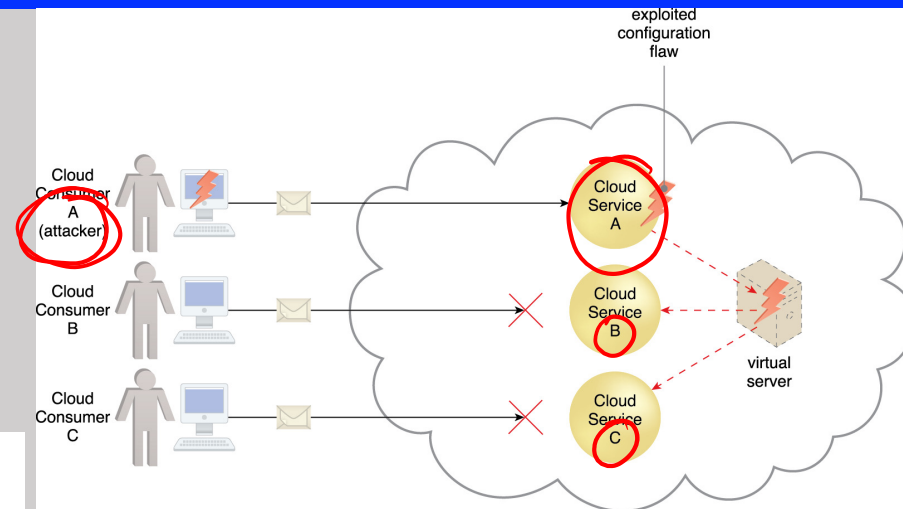
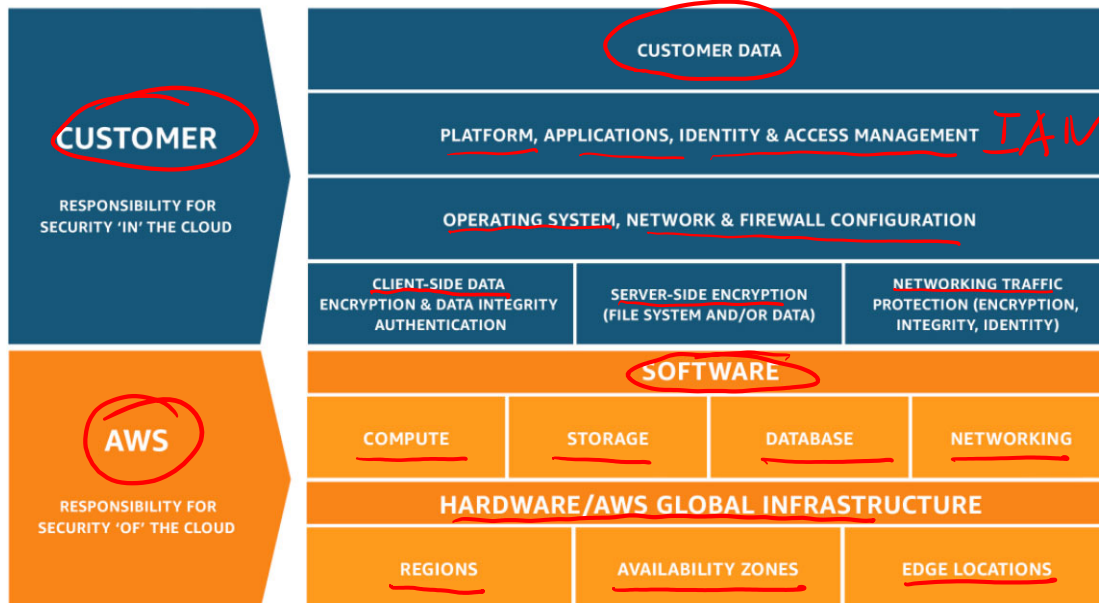
- Cloud consumers need to be aware that they may be introducing security risks by deploying flawed cloud-based solutions.
- An understanding of how a cloud provider defines and imposes proprietary, and possibly incompatible, cloud security policies is a critical
- Liability, indemnity, and blame for potential security breaches need to be clearly defined and mutually understood in the legal agreements signed by cloud consumers and cloud providers.
- It is important for cloud consumers, subsequent to gaining an understanding of the potential security-related issues specific to a given cloud environment, to perform a corresponding assessment of the identified risks.

[1] <https://aws.amazon.com/compliance/shared-responsibility-model/>

# Additional Considerations – Flawed Implementation

## Flawed Implementations – 50/50 Model

- Modern cloud providers have a 50/50 shared model for security [1]:
  - YOU**: Responsible for security **IN** the cloud.
  - PROVIDER**: Responsible for security **OF** the cloud.
- Flawed implementations in your layers expose vulnerabilities to your systems and data



The above figure depicts a poorly implemented cloud service that results in a server shutdown. Although in this scenario the flaw is exposed accidentally by a legitimate cloud service consumer, it could have easily been discovered and exploited by an attacker. 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.

[1] <https://aws.amazon.com/compliance/shared-responsibility-model/>

## Additional Considerations Security – Policy Disparity

- As soon as you include public cloud in your architecture you must share a trust boundary with your cloud provider:
  - Their security policies may vary significantly from yours, either more restrictive or less restrictive
  - This incompatibility must be assessed and accounted for in your architecture or disparity could leave vulnerabilities
- Examples:
  - Government implementing hybrid cloud solutions with cloud bursting, potentially with classified data having much higher restrictions than most cloud providers
  - An organization with no security experience transitioning to the cloud and being forced to adapt their application to more stringent security requirements by the cloud provider's services

The background of the image is a stylized world map divided into four quadrants by a vertical and a horizontal line. The top-left quadrant is red, the top-right is blue, the bottom-left is yellow, and the bottom-right is green. The word "Kahoot!" is written in a large, white, bold, sans-serif font across the center of the image, spanning all four quadrants.

**Kahoot!**