NEW YORK INSTITUTE OF TECHNOLOGY

INCS 775
Data Center Security

Cloud Security – Part 2

Dr. Zakaria Alomari
zalomari@nyit.edu

Security and Privacy Issues and Challenges

Cloud Security Risks

- ❑ According to the Cloud Security Alliance, the following represent the most critical cloud-specific security threats:
  - Abuse and malicious use of cloud computing resources
  - Insecure interfaces and application programming interfaces (APIs)
  - Insider threats posed by malicious individuals
  - Vulnerabilities arising from shared technology infrastructure
  - Risks of data loss or unintentional data leakage
  - Account or service hijacking incidents
  - Lack of transparency regarding risk posture and threat exposure

Cloud Security As A Service (SECaaS)

- It refers to the delivery of security service over the internet or cloud infrastructure.

- It enables organizations to delegate the management of their security needs to third-party providers that specialize in protecting *cloud-based systems*, *applications*, and *data*.

Cloud Security As A Service (SECaaS)

- ❑ **Zscaler** falls under the category of **Security as a Service (SECaaS)** providers.
- ❑ It delivers cloud-based security solutions that replace traditional on-premises hardware. Zscaler's platform offers a variety of services such as:
  - ○ Secure Web Gateway (SWG)
  - ○ Cloud-based Firewall
  - ○ Zero Trust Network Access (ZTNA)
  - ○ Cloud Access Security Broker (CASB)
  - ○ Data Loss Prevention (DLP)
  - ○ Advanced threat protection and sandboxing
- ❑ **Since all of these services are delivered via the cloud and follow a subscription-based model**, Zscaler is a strong example of SECaaS in action.

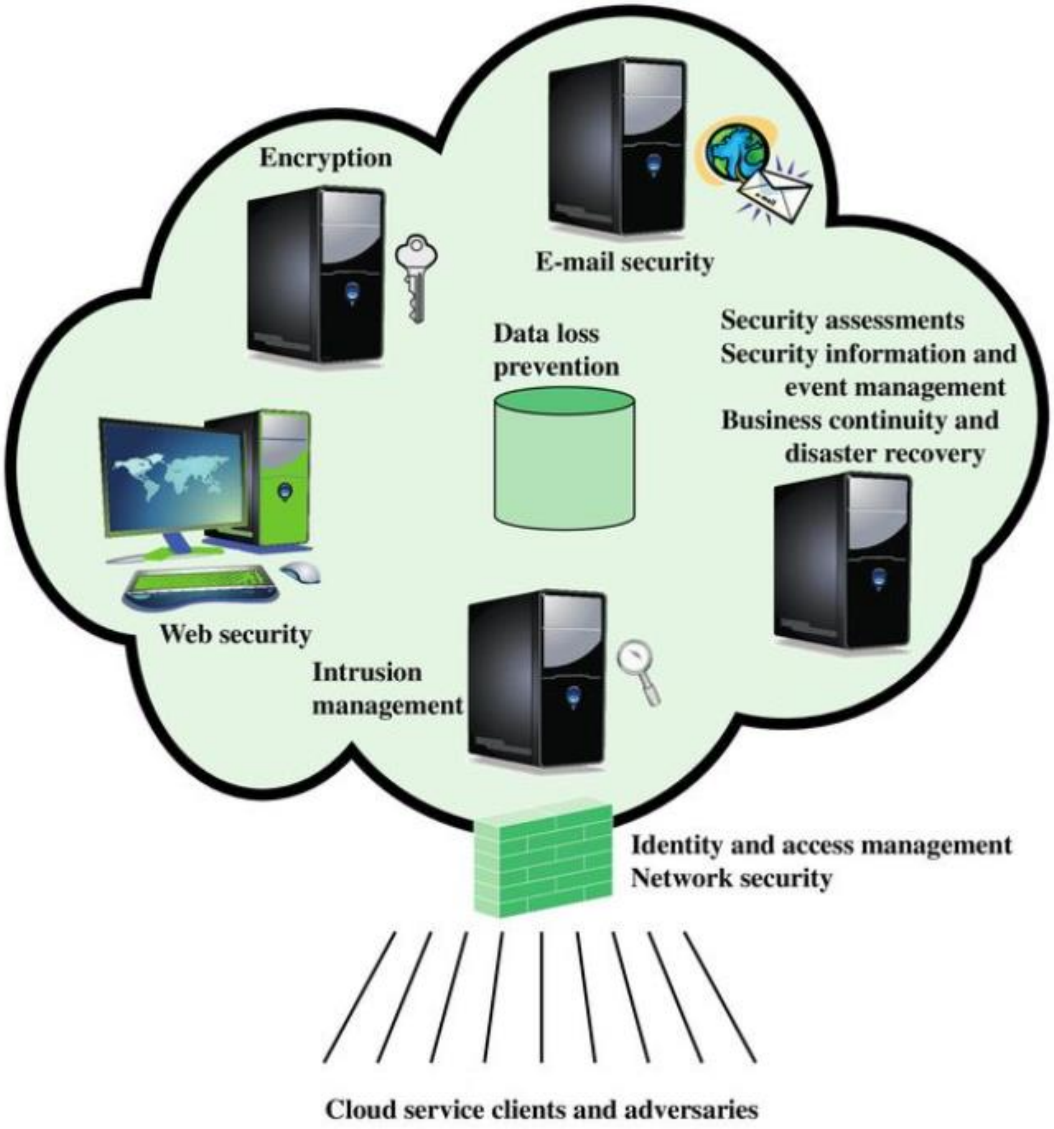
Cloud Security As A Service (SECaaS)

❑ **Some Key Components of SECaaS typically include:**

1. **Identity and Access Management:** Managing user identities, access controls, and permissions within the cloud environment to ensure only authorized individuals have access to resources.

2. **Data Encryption:** Encrypting data both in transit and at rest to protect it from unauthorized access or interception.

3. **Network Security:** Implementing firewalls, intrusion detection/prevention systems, and other network security measures to safeguard against unauthorized access and malicious activities.


Encryption
E-mail security
Data loss prevention
Security assessments
Security information and event management
Business continuity and disaster recovery
Web security
Intrusion management
Identity and access management
Network security
Cloud service clients and adversaries

Elements of Cloud Security as a Service

Traditional Systems Security vs Cloud Computing Security

- ❑ **Traditional System Security:**
  - ○ Security measures applied to **on-premises infrastructure** where organizations own and fully control their physical servers, network, and data centers.

- ❑ **Cloud Computing Security**
  - ○ Security practices for **cloud-based environments**, following **a shared responsibility model** where cloud providers secure the infrastructure, and customers secure their data, applications, and configurations

Comparison: Traditional Systems Security vs Cloud Computing Security

Aspect	Traditional System Security	Cloud Computing Security
Infrastructure Ownership and Control	Organizations **own and manage** their own **physical infrastructure** (servers, networks, storage). They have **full control** over security configurations.	Infrastructure is **owned and managed by third-party providers**. Organizations use **virtualized resources** and have **limited control** over physical infrastructure.
Security Responsibility	Organizations are **entirely responsible** for securing **all layers**: hardware, software, and networks.	Follows a **shared responsibility model**: - **Cloud provider** secures physical infrastructure and core services. - **Customer** secures data, applications, access, and configurations.

Comparison: Traditional Systems Security vs Cloud Computing Security

Aspect	Traditional System Security	Cloud Computing Security
Security Paradigm	**On-premises model** with internal IT teams implementing and managing security measures.	**Cloud-based model** with collaborative security between provider and customer, often involving **cloud-native tools** and practices.
Control Over Security Measures	**Complete control** over every aspect of system security, including firewalls, access controls, and patch management.	**Partial control**—while customers configure security within their environment, the cloud provider handles core infrastructure protection.

Traditional Systems Security vs Cloud Computing Security

Analogy

Securing a house

Securing a motel

Owner and user are often the same entity

Owner and users are almost invariably distinct entities

Traditional Systems Security vs Cloud Computing Security

Securing a house

Securing a motel

Biggest user concerns
Securing perimeter
Checking for intruders
Securing assets

Biggest user concern
Securing room against
(the bad guy in next
room | hotel owner)

Why Cloud Computing brings new threats?

- Traditional system security mostly means keeping bad guy out.
- The attacker needs to either compromise the auth/access control system, or impersonate existing users

Why Cloud Computing brings new threats?

- But clouds allow co-tenancy.
- Multiple independent users share the same physical infrastructure.
- So, an attacker can legitimately be in the same physical machine as the target

Who is the attacker

- **Insider Threats?**
  - Malicious Employee at the Client Organization :
    - An employee within the client company engaging in harmful activities.
  - Malicious employee at the Cloud Provider:
    - A dishonest employee working for the cloud service provider
  - Cloud provider Itself:
    - Security risks originating from the cloud service provider as an entity.

Who is the attacker

- **Outsider?**
  - Intruders:
    - This term refers to any individual or entity that gains unauthorized access to a computer system, network, or application.
  - Network attackers?
    - Network attackers are individuals or entities who engage in specific actions or employ techniques to compromise or disrupt the operation of a network.
  - **Summary**: Intruders are individuals or entities attempting unauthorized access, while network attacks refer to the specific techniques or actions they utilize to compromise or disrupt network systems and services.

Attacker Capability: Malicious Insider

- **A Malicious Insider** refers to an individual with legitimate access to either the **client's systems** or the **cloud provider's infrastructure**, who exploits this access for malicious purposes.

- **At the Client**
  - **Exfiltration of Passwords/Authentication Information:** The **malicious insider** can collect sensitive data, such as *passwords* or *authentication credentials*, through *unauthorized access* or *social engineering tactics*.
  - **Compromise of Virtual Machines (VMs):** The **insider** may exploit their access to seize control of virtual machines within the client's environment, enabling them to *manipulate or disrupt services*, *access confidential data*, or *initiate further attacks*.

Attacker Capability: Malicious Insider

- ✓ **At the Cloud Provider**
  - ○ **Intercepting and Logging Client Communication:** A **malicious insider** within the cloud provider's infrastructure may monitor and log communication between the client and cloud services. This includes *intercepting data transmissions*, *capturing sensitive information*, or *exploiting vulnerabilities in communication channels*.
  - ○ **Access to Unencrypted Data:** With access to the underlying infrastructure, the **malicious insider** could potentially read unencrypted data, including sensitive information such as *personal data*, *financial records*, or *proprietary business information*.

Attacker Capability: Malicious Insider

- **Accessing or Cloning Virtual Machines (VMs):** With administrative privileges, the **insider** might access or duplicate virtual machines hosted on the cloud provider's infrastructure, gaining unauthorized access to the *contents, including data and applications*.

- **Monitoring Network and Application Behavior:** The cloud provider can observe network traffic and application usage patterns within their infrastructure, enabling them to *gather insights into client service usage*, *data transmission*, and *potentially sensitive interactions*.

Attacker Capability: Malicious Insider

- **Acquiring Client Data and Behavior Insights:** The **malicious insider** can gain information regarding client data and usage patterns, which may provide valuable insights into client behavior.

- **Monetization or Exploitation of Information:** The **insider** may sell or misuse the acquired data and behavioral insights, either by **selling it to third parties for profit**, **utilizing it to enhance the provider's own services**, or **leveraging it for competitive advantage in the market**.

Attacker Capability: Outside attacker

❑ **Description:**

- ○ Passive monitoring of network traffic
- ○ Injection of malicious traffic (active)
- ○ Probing of cloud architecture (active): This refers to the deliberate attempt to assess or evaluate the structure, vulnerabilities, or security mechanisms of a cloud infrastructure. The process involves scanning the cloud environment to gather information that may be exploited for malicious purposes.
- ○ Launching a Denial of Service (DoS) attack

Novel attacks on cloud

- **Question:** can you attack a cloud or other users, without violating any law?
- **Answer:** Yes!! By launching side channel attacks, while not violating Acceptable User Policy.
  - A Side Channel is a passive attack in which attacker gains information about target through indirect observations.

Challenges for the attacker

- How to find out where the target is located.

- How to be co-located with the target in the same (physical) machine

- How to gather information about the target

More on attacks

1. Can one determine where in the cloud infrastructure an instance is located?
2. Can one easily determine if two instances are co-resident on the same physical machine?
3. Can an adversary launch instances that will be co-resident with other user instances?
4. Can an adversary exploit cross-VM information leakage once co-resident?

Answer: Yes to all

Cloud Cartography Strategy

❑ **Cloud Cartography Strategy:**

- It refers to a structured methodology for mapping and analyzing the intricate landscape of cloud computing environments.
- It involves creating visual diagrams or maps that represent the *various components*, *relationships*, and *interactions within the cloud infrastructure*.

Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, Ristenpart et al., CCS 2009

Cloud Cartography Strategy

❑ **Cloud Infrastructure Mapping and Security Testing Strategy**

1. **Mapping the Cloud Infrastructure to Identify the Target Location**

- This process entails understanding the architecture and configuration of the cloud environment to accurately identify the position of the target resource or component.

2. **Utilizing Heuristics to Determine Co-residency of Two Virtual Machines (VMs)**

- This involves applying a range of techniques to assess whether two VMs are operating on the same physical host in a cloud environment. These techniques may include *analyzing network traffic patterns*, *monitoring resource utilization metrics*, *examining performance data*, or *performing timing-based analysis to infer co-residency*.

Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, Ristenpart et al., CCS 2009

Cloud Cartography Strategy

3. **Deploying Probe VMs to Co-locate with Target VMs**

- This step involves launching VMs with the aim of co-locating them on the same physical hardware as specific target VMs within a cloud environment. *The goal is typically for security testing, research, or investigative purposes*.

4. **Exploiting Cross-VM Leakage to Extract Information from the Target**

- This technique involves exploiting vulnerabilities in virtualized environments to gather sensitive information from a target VM. This is achieved by leveraging shared resources or interactions with other VMs running on the same physical hardware. Such attacks pose significant risks to the confidentiality and integrity of data in cloud environments, highlighting the need for comprehensive security measures.

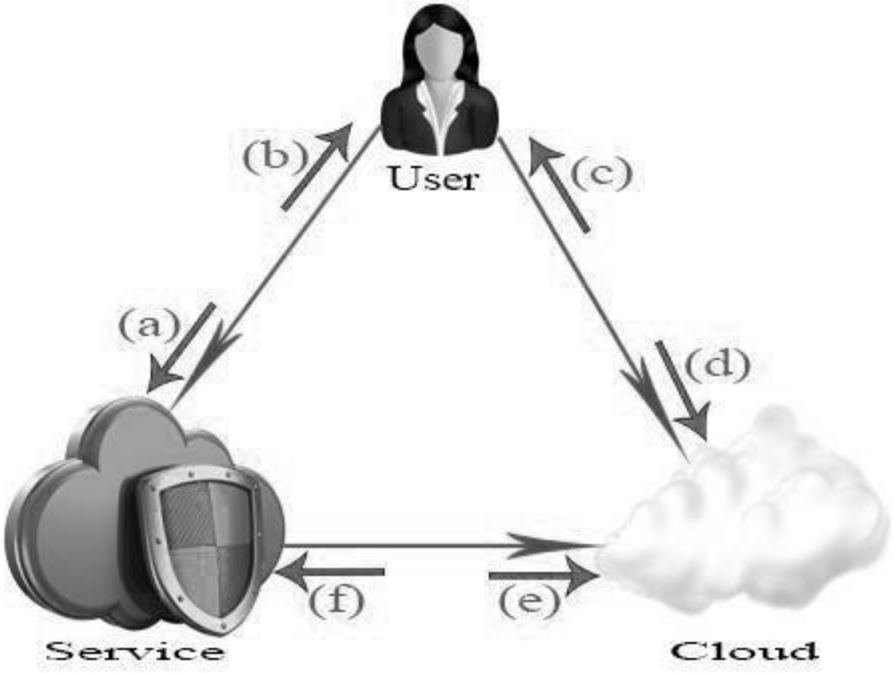
Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, Ristenpart et al., CCS 2009

Clouds extend the attack surface

- An **attack surface** is a vulnerability in a system that malicious users may utilize

- How?
  - By requiring users to communicate with cloud over a public/insecure network
  - By sharing the infrastructure among multiple users

Analyzing Attack Surfaces in Clouds



Cloud attack surfaces can be modeled using 3 entity model (**User**, **Service**, and **Cloud**)

With 3 participants, there are 6 such interfaces to consider.

Analyzing Attack Surfaces in Clouds

- The concept of **attack surfaces refers to potential vulnerabilities**, which can be analyzed through a **three-entity model consisting** of *User*, *Service*, and *Cloud*.

- This approach is particularly effective for identifying potential threats and vulnerability vectors. Each entity interacts with the others in different ways, resulting in interfaces that may be exploited by attackers.

- In the next slide, we will examine the six key interfaces, accompanied by relevant examples:

The attack surfaces mean vulnerability to:

1) **User-to-Service Interface:**

- **Description:** This interface involves direct interactions between users (customers or clients) and the services hosted in the cloud.

- **Example:** When users log in to a web application hosted on a cloud platform, they authenticate through this interface. Potential attacks here include **credential stuffing, phishing,** and **session hijacking**. For example, if a user logs in with weak credentials, attackers could use brute force attacks to gain unauthorized access.

The attack surfaces mean vulnerability to:

2) **Service-to-User Interface:**

- **Description:** This interface includes any data or responses sent back to users from the cloud service, often as part of an interactive session or notification.

- **Example:** Consider a cloud-hosted email service that sends notification emails to users. If the email service is compromised, it might send **phishing emails** or **malicious attachments** to users, leading to malware infection. Data leakage through **improperly configured API responses** is also a risk.

The attack surfaces mean vulnerability to:

3) User-to-Cloud Interface:

- **Description:** Here, users interact directly with the cloud infrastructure to manage resources or configure services.

- **Example:** A user may access the cloud provider's management console to configure virtual machines, storage, or networks. An attack could involve **compromising the user's cloud credentials** or launching a **Denial of Service (DoS)** attack on this interface to disrupt legitimate access.

The attack surfaces mean vulnerability to:

4) **Cloud-to-User Interface:**

- **Description:** This involves the cloud provider sending information, alerts, or responses to users, often for security notifications or billing.

- **Example:** If the cloud provider's alerting system is compromised, attackers could send fake billing alerts asking users to update their payment information on a malicious site, a classic **phishing attack** scenario. Poorly secured alert systems can also expose sensitive details, creating an additional attack vector.

The attack surfaces mean vulnerability to:

5) **Cloud-to-Service Interface:**

- **Description:** In this interface, the cloud infrastructure provides resources, scaling, and security controls to the hosted services.

- **Example:** A common example is a cloud service automatically scaling up resources for an application based on user demand. If this scaling function is misconfigured or exploited, attackers might cause **resource exhaustion** or inflate costs through forced scaling, a tactic known as a **resource consumption attack**.

The attack surfaces mean vulnerability to:

6) **Service-to-Cloud Interface:**

- **Description:** Services running in the cloud use this interface to access cloud infrastructure components (e.g., storage, databases, or compute resources).

- **Example:** Suppose a web service on the cloud accesses a database to retrieve user information. If the **API calls** between the service and the cloud database are not properly authenticated or encrypted, attackers could intercept these calls, leading to data leakage or unauthorized access. Misconfigured IAM (Identity and Access Management) policies can also expose sensitive resources.

Challenges in Cloud Computing Security

- The majority of security challenges in cloud computing arises from the following factors
  - Loss of control
  - Lack of trust
  - Multi-tenancy

- These **issues** are predominantly associated with third-party managed cloud models. While self-managed clouds also face security concerns, these are not typically linked to the factors mentioned above.

Loss of Control in the Cloud

- **Loss of Control in the Cloud** refers to the reduced ability of organizations to manage their *IT infrastructure*, *data*, or *services* when *migrating to the cloud*.

- Consumer's Loss of Control
  - Data, applications, and resources are managed by the **cloud provider**.
  - Identity management and access control are handled by the **provider**.
  - The **provider** ensures data security, privacy, resource availability, and service monitoring.

Lack of Trust in Cloud Computing

- **The lack of trust in cloud services** stems from concerns about *security*, *data privacy*, and *reliability*. **Organizations worry about** *data safety in shared environments*, *privacy risks from off-premises storage*, and *the cloud's ability to ensure consistent service availability*.
- **Trusting third-party services inherently involves risk.**

- **Trust and Risk:**
  - Trust and risk are **interconnected**.
  - Trust is built when it **proves beneficial**.
  - Trust becomes essential in **high-risk situations**.

Multi-Tenancy Issues in Cloud Computing

- **Multi-tenancy** involves hosting multiple tenants on the same physical infrastructure, with logical isolation between them. While it offers *resource optimization* and *cost efficiency*, it also presents challenges:
  - **Data Security and Privacy**: Increased risk of unauthorized access to sensitive data.
  - **Performance and Resource Contention**: Competition for resources like CPU and bandwidth can impact performance.
  - **Conflicting Tenant Objectives**: Opposing goals among tenants sharing resources may lead to conflicts.
  - **Handling Conflicts**: Can tenants coexist peacefully, or should isolation be implemented?
  - **Tenant Separation**: Ensuring proper isolation to avoid cross-tenant impact.
  - **Security Risks**: Shared infrastructure increases the risk of attackers being on the same physical machine as a target.

Cloud Security Concerns

- **Confidentiality**
  - Confidentiality is a core principle in cloud security, emphasizing the protection of sensitive information from unauthorized access or disclosure.
  - A **major concern among organizations** is the potential loss of control over their data once it is stored in the cloud. **Key questions that arise include**:
    - Will sensitive data stored in the cloud remain truly confidential?
    - Could a security breach in the cloud compromise the confidentiality of client information?
    - Can the cloud service provider be fully trusted to uphold privacy and refrain from accessing or viewing client data?

Cloud Security Concerns

- **Integrity**
  - Integrity in cloud computing refers to maintaining the accuracy, consistency, and trustworthiness of data throughout its entire lifecycle.
  - **Ensuring data** integrity involves *safeguarding information from unauthorized modification*, *loss*, or *corruption*.
  - Key considerations include:
    - How can one verify that the cloud service provider is performing computations correctly and as expected?
    - What mechanisms are in place to confirm that the provider has stored the data accurately and without unauthorized alterations?

Cloud Security Concerns

- **Availability**
  - Availability pertains to the **continuous accessibility and reliability** of IT *systems*, *services*, and *data.*
  - In the context of cloud computing, it is essential to ensure that applications, platforms, and tools are consistently available to both customers and employees—*anytime*, *anywhere*, and *from any internet-enabled device*.

Cloud Security Concerns

- **Availability**
  - Key considerations include:
    - **Resilience Against Denial of Service (DoS) Attacks:** Can critical systems at the client's end remain operational if the cloud service provider becomes the target of a DoS attack?
    - **Provider Viability**: What contingencies are in place if the cloud service provider discontinues operations or goes out of business?
    - **Scalability**: Is the cloud infrastructure capable of scaling efficiently to meet growing or fluctuating demand?

Cloud Security Concerns

- **Privacy**
  - Refers to individuals' right to keep personal information and activities confidential.
  - Involves control over access to data and how it is used.
  - Cloud providers manage data from numerous clients, **increasing the potential for privacy violations**.
  - Large-scale data mining by cloud providers may lead to unintended or unauthorized information disclosure.

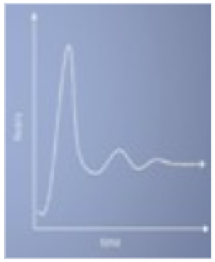
Cloud Security Concerns

- **Expanded Attack Surface**
  - Data is stored and processed by third-party cloud providers, increasing exposure to external threats.
  - Communication channels between clients and cloud providers become potential attack vectors.
  - Cloud provider employees may be targeted through phishing or social engineering attacks.
  - Insider threats and misconfigurations may also lead to security breaches.

Cloud Security Concerns

Cloud Computing is **a security nightmare** and it can't be handled in traditional ways.

John Chambers
CISCO CEO



- Security is one of the most difficult task to implement in cloud computing.
  - Different forms of attacks in the application side and in the hardware components
- Attacks with catastrophic effects only needs one security flaw

Possible Solutions

Minimize Loss of Control: Monitoring

- Enhancing Control Through Monitoring
  - To address potential loss of control in cloud environments, both **cloud providers** and **consumers** should be equipped with **mechanisms that allow them to detect and respond to threats within their respective domains of responsibility**.

- Provider-Side Capabilities:
  - **Infrastructure Remapping:** Enable **dynamic reconfiguration** by creating new fault domains or relocating existing ones to mitigate the impact of attacks.
  - **Component Shutdown:** Allow the provider to isolate or deactivate compromised components or targets. Support should also be offered to tenants for application or workload migration, if necessary.
  - **Automated Repairs:** Implement systems that can autonomously initiate recovery and repair procedures following a detected incident.

Minimize Loss of Control: Monitoring

- Consumer-Side Capabilities:
  - **Application-Level Monitoring:** Equip consumers with tools to monitor their applications for suspicious behavior or anomalies.
  - **Risk-Adaptive Access Control (RAdAC):** Employ access control mechanisms that adjust dynamically based on the assessed level of risk.
  - **Virtual Machine (VM) Porting with Remote Attestation:** Facilitate secure migration of VMs by verifying the integrity of the target host before transfer.
  - **Cross-Cloud Portability**: Provide users with the capability to move applications across cloud providers when required for security or resilience.

Minimize Loss of Control: Utilize Different Clouds

- Enhancing Control and Reducing Risk through Multi-Cloud Strategies
  - Embrace the principle of "**Don’t put all your eggs in one basket**" by adopting a multi-cloud or intra-cloud architecture.
  - Consumers can **leverage services from multiple cloud providers to**:
    - Distribute operational risk more effectively
    - Enhance redundancy at the task or application level
    - Improve the likelihood of mission success, especially for critical applications

Minimize Loss of Control: Utilize Different Clouds

- Considerations and Challenges:
  - **Policy Incompatibility:** Integrating different cloud services may result in conflicting policies—what overarching governance model applies?
  - **Data Interdependencies:** Applications spanning multiple clouds may introduce complex data dependencies that must be managed.
  - **Redundancy Management:** Effective use of redundancy requires robust monitoring tools to determine when and how to activate backup resources.
  - **Security and Privacy Risks:** Distributing sensitive data across multiple clouds could increase the risk of exposure—organizations must assess whether the benefits of redundancy outweigh potential vulnerabilities.

Minimize Loss of Control: Access Control

- Multiple layers of access control can be implemented:
  - For instance, access to the **cloud**, **servers**, **services**, **databases** (both direct access and through web service queries**), virtual machines (VMs)**, and **objects within a VM**.
  - Depending on the deployment model, some of these access controls may be managed by the provider, while others are controlled by the consumer.

- Regardless of the deployment model, **it is essential for the provider to oversee user authentication and access control procedures for the cloud environment**.
  - This places a significant amount of trust in the provider, as they are responsible for the *security*, *management*, and *maintenance of access control policies*.
  - This can be particularly burdensome when multiple users from various organizations with differing access control policies are involved.

Minimize Lack of Trust in the cloud

- **Enhanced Security Protocols:** Cloud service providers should prioritize the implementation of comprehensive security protocols, such as *encryption*, *access management controls*, *intrusion detection systems*, and *routine security audits to safeguard data integrity*.

- **Data Privacy Governance:** Cloud providers should offer customizable data privacy governance options, enabling clients to establish specific *access policies*, *encryption criteria*, and *data residency preferences tailored to their individual requirements*.

Minimize Multi-tenancy

- It is not **feasible to mandate that the provider accept fewer tenants**.
- However, efforts can be made to enhance isolation between tenants:
  - Employ robust isolation techniques (e.g., Virtual Private Cloud, to some extent).
  - Ensure that Quality of Service (QoS) requirements are met.
  - Define and enforce policy specifications.
- Alternatively, increasing trust among tenants could be considered:
  - Clearly define the security boundary and identify trusted individuals or entities.
  - Utilize Service Level Agreements (SLAs) to enforce trusted behavior.