2. Failover system mechanism

1. **Purpose of Failover System:**
   - Technique in cloud computing to enhance IT resource reliability and availability.
   - Utilizes clustering technology for redundant IT resource implementations.
   - Automatically switches to standby instance on active resource unavailability.

2. **Common Usage:**
   - Deployed for mission-critical programs & reusable services to avoid single points of failure.
   - Can span multiple geographical regions for redundancy[5].

3. Failover System Configurations:

a. Active-Active:

- Redundant IT resources actively serve workload synchronously.
- Requires load balancing among active instances.

(Figure 6.8.2). Whichever IT resource remains operational when a failure is detected takes over the processing (Figure 6.8.3).

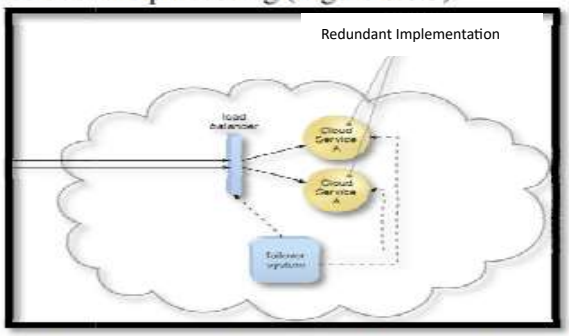


Fig 6.8.1 The failover system monitors the operational status of Cloud Service A.

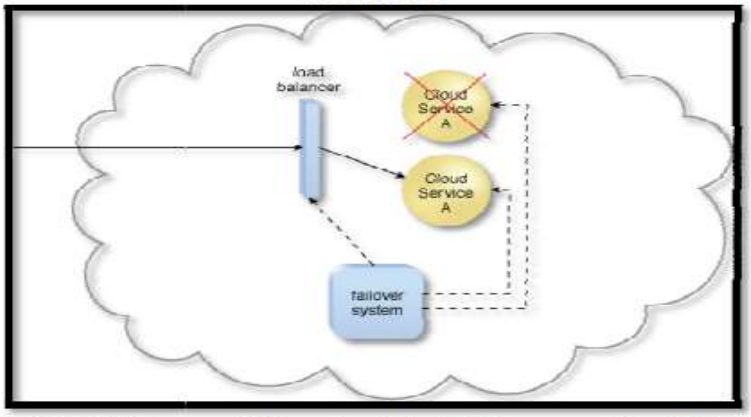


Figure 6.8.2 When a failure is detected in one Cloud Service A implementation, the failover system commands the load balancer to switch over the workload to the redundant Cloud Service A implementation.

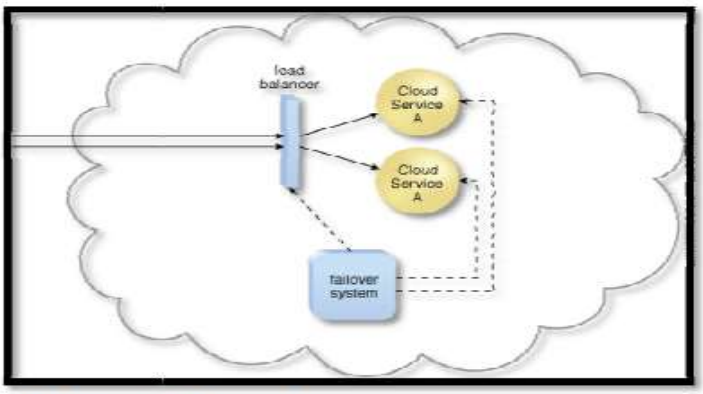


Figure 6.8.3 The failed Cloud Service A implementation is recovered or replicated into an operational cloud service. The failover system now commands the load balancer to distribute the workload again

b. *Active-Passive:*

- Redundant or standby IT resource implementations operate independently.
- Suitable for stateless processing IT resources without state sharing.

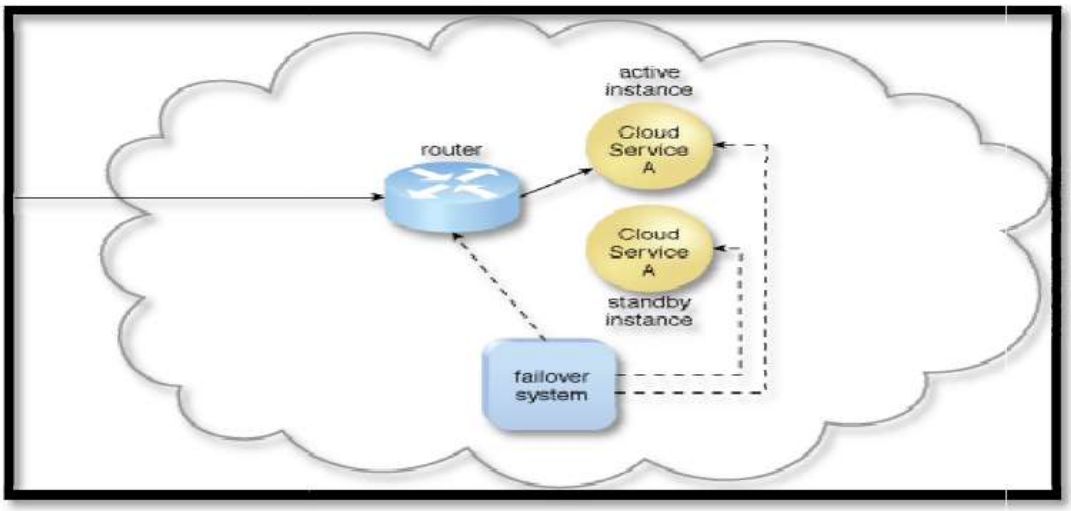


Figure 6.8.4 The failover system monitors the operational status of Cloud Service A. The Cloud Service A implementation acting as the active instance is receiving cloud service consumer requests.

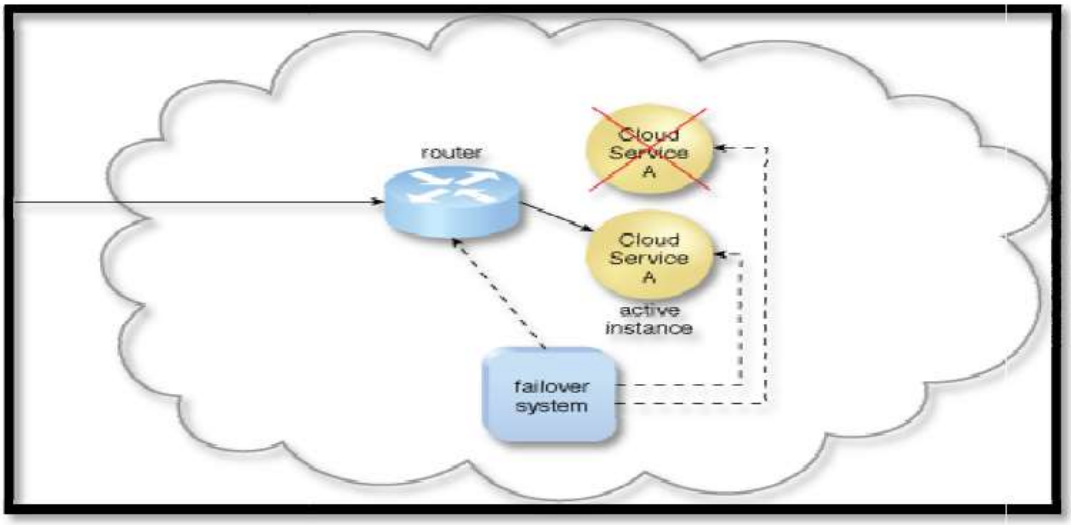


Figure 6.8.5 The Cloud Service An implementation acting as the active instance encounters a failure that is detected by the failover system, which subsequently activates the inactive Cloud Service A implementation and redirects the workload toward it. The newly invoked Cloud Service A implementation now assumes the role of active instance.

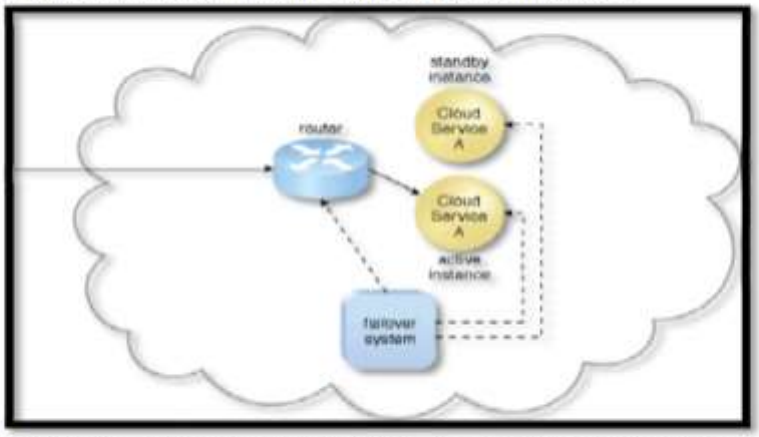
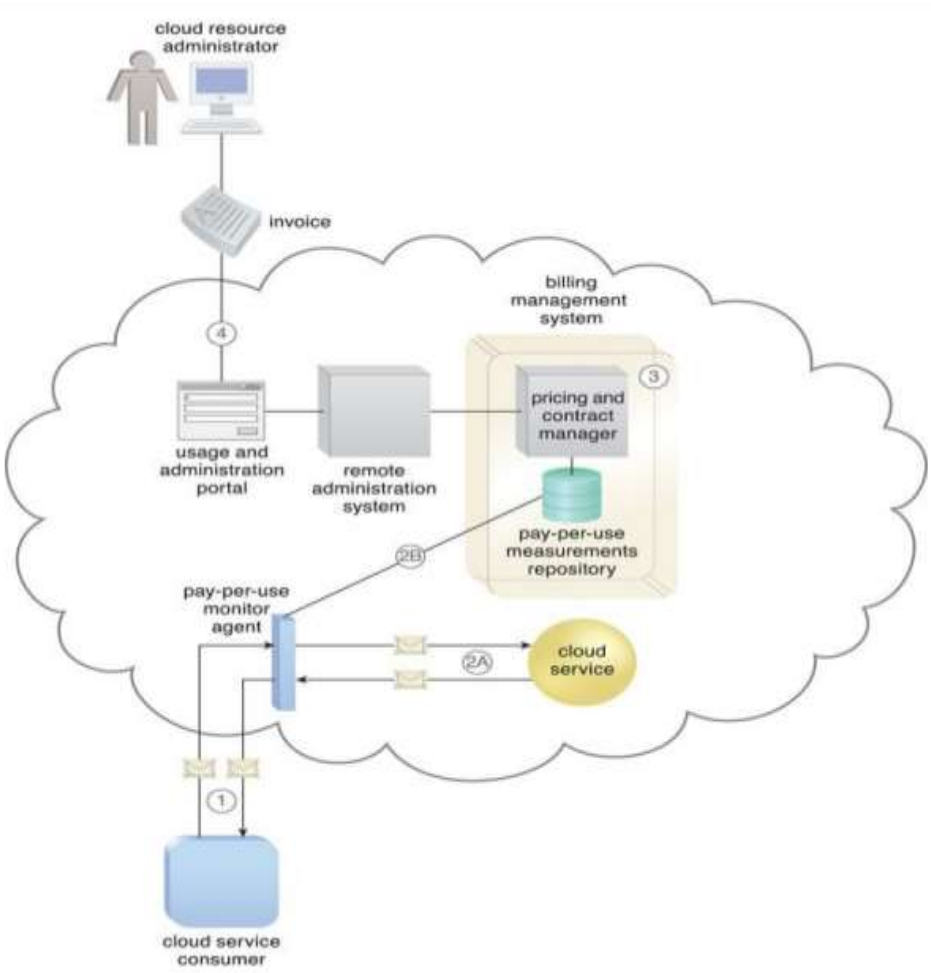


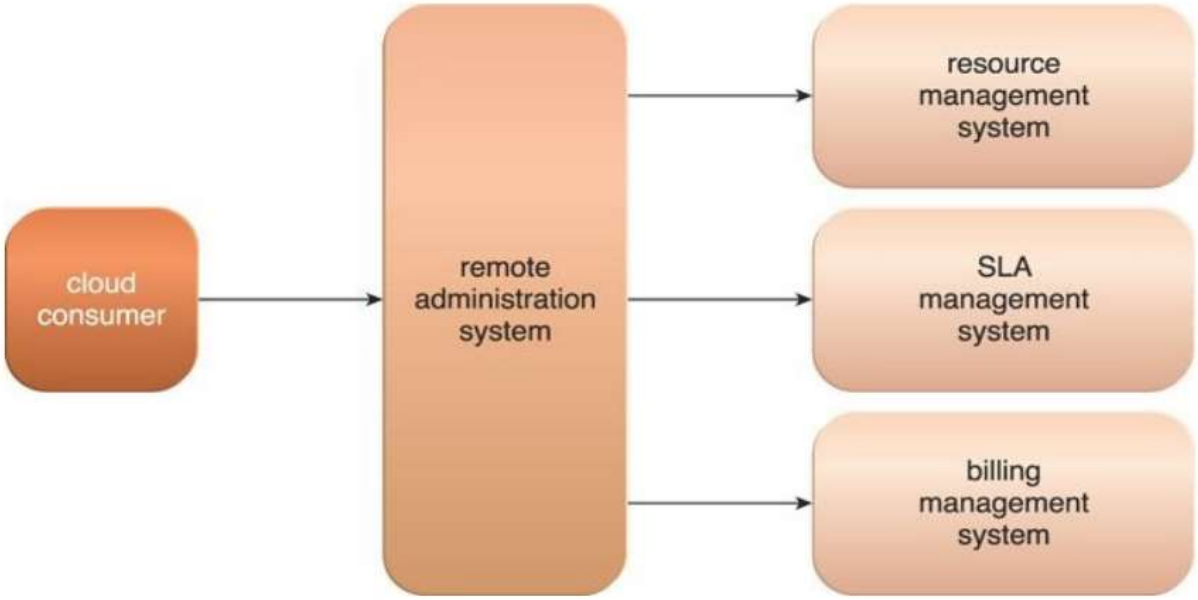
Figure 6.8.6 The failed Cloud Service A implementation is recovered or replicated into an operational cloud service, and is now positioned as the standby instance, while the previously invoked Cloud Service A continues to serve as the active instance.

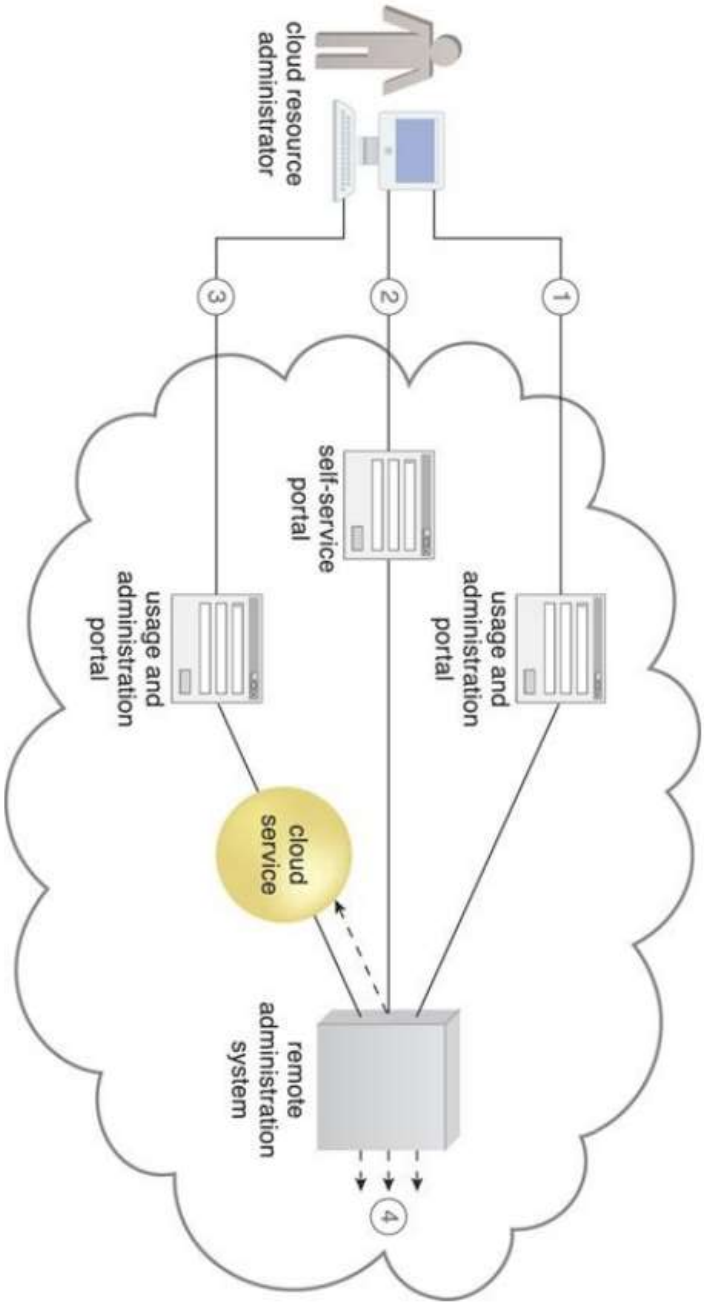
3. Billing Management System



- **Overview:**
  - The Billing Management System in cloud computing is a dedicated mechanism for collecting and processing usage data related to cloud provider accounting and consumer billing.
  - It utilizes pay-per-use monitors to gather runtime data stored in a repository, utilized by system components for billing, reporting, and invoicing purposes.
- **Functionality:**
  - The system tracks cloud resource usage by consumers, generating accurate bills to enable providers to charge for consumed resources and consumers to manage costs.
- **Example Scenario:**
  - A company subscribes to a cloud service provider for hosting. The provider charges based on resources used, tracked by the Billing Management System.
  - Usage data from monitors (e.g., virtual machines, network, storage) is stored for billing purposes.
  - At the billing cycle end, the system generates a detailed bill, including virtual machines, storage, and bandwidth usage, facilitating transparent cost review and payment.
- **Technical Details:**
  - The Billing Management System relies on pay-per-use monitors for runtime usage data, encompassing request/response metrics, data volume, and bandwidth.
  - This data is stored in a repository, supporting the generation of invoices, reports, and payment fee calculations for cloud consumers.

4. Remote Administration





1. **Definition and Function:**
    - Remote Administration is a mechanism in cloud computing that provides tools and user-interfaces for external administrators to configure and administer cloud-based IT resources[1].
    - Cloud service providers use Remote Administration Systems to manage infrastructure and provide controls to customers.
2. **Example Scenario:**
    - A company subscribes to a cloud service provider for hosting. The provider offers resources like virtual machines and storage.
    - The company uses the Remote Administration System to configure resources via a web-based portal from anywhere[1].
3. **Key Features:**
    - Remote Administration Systems include tools, user-interfaces, and APIs for customization[1].
    - Cloud service providers may develop self-service portals for customers to manage resources[1].
4. **Remote Administration in Cloud Environments:**
    - Refers to managing and controlling cloud-based IT resources from a remote location.
    - Tasks include configuring cloud services, provisioning and releasing resources, monitoring service status and performance, managing user accounts and access control, tracking leased service access, planning IT resource provisioning, and capacity planning[6].
5. **Benefits:**
    - Enables efficient resource utilization, optimal performance monitoring, and secure access management in cloud environments.

- Remote administration refers to the process of managing and controlling computer systems or networks from a remote location.
- It allows administrators to perform various tasks and operations on the systems without physically being present at the location.
- Remote administration is commonly used in cloud computing environments, where administrators can remotely configure, monitor, and manage cloud-based IT resources.

Examples of remote administration tasks include:

1. Configuring and setting up cloud services: Administrators can remotely configure and customize cloud services according to the specific requirements of the organization.

2. Provisioning and releasing IT resources: Administrators can remotely allocate and release IT resources as needed, ensuring efficient resource utilization.

3. Monitoring cloud service status, usage, and performance: Administrators can remotely monitor the status, usage, and performance of cloud services to ensure optimal performance and identify any issues or bottlenecks.

4. Managing user accounts, security credentials, authorization, and access control: Administrators can remotely manage user accounts, security credentials, and access control policies to ensure secure and authorized access to cloud resources.

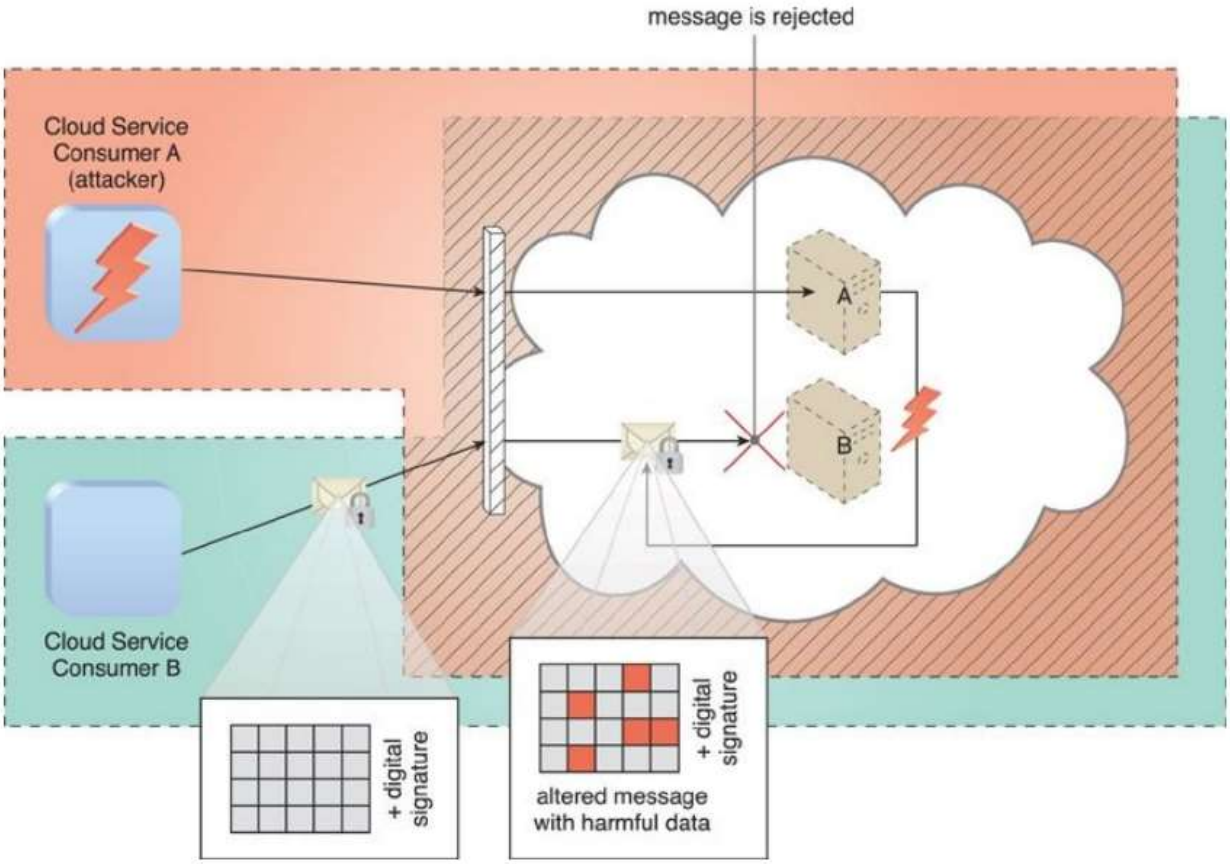
5. Tracking internal and external access to leased services: Administrators can monitor and track the access and usage of leased services by both internal and external users, ensuring compliance and security.

6. Planning and assessing IT resource provisioning: Administrators can remotely plan and assess the provisioning of IT resources based on the organization's needs and future requirements.

7. Capacity planning: Administrators can remotely analyze and plan for the capacity needs of the cloud infrastructure, ensuring scalability and efficient resource allocation.

Remote administration systems often provide tools and user interfaces that allow administrators to perform these tasks. These systems may also offer standardized APIs, allowing organizations to develop their own front-end interfaces and easily switch between different cloud providers that support the same API.

5. Digital Signature



Digital Signature Mechanism

• Digital Signature in cloud computing ensures data authenticity, integrity, and non-repudiation.

• It guarantees that a received message matches the one created by the rightful sender without tampering.

• Example: A company uses Digital Signature to securely send a confidential document over the internet.

How Digital Signature Works

1. The company creates a message digest of the document using a hashing algorithm.
2. The message digest, representing the document, is encrypted with the company's private key, creating a digital signature.
3. The digital signature is appended to the original document, and the message is sent to the recipient.
4. The recipient verifies the digital signature using the company's public key.
5. By decrypting the signature, the recipient obtains the message digest.
6. The recipient creates a message digest of the received document using the same hashing algorithm.
7. If the two message digests match, it confirms the document's integrity, ensuring it was sent by the rightful sender.

Applications of Digital Signatures

1. **Financial Sector**: Used for secure online transactions, electronic fund transfers, and digital contracts[2].

2. **Healthcare**: Ensures integrity of electronic health records, prescriptions, and medical reports[5].
3. **Government and Legal**: Employed for secure online communication, digital documents, e-voting systems, and signing legal documents[3][4].
4. **Supply Chain Management**: Verifies authenticity and integrity of shipping documents, invoices, and purchase orders[3].
5. **Intellectual Property Protection**: Protects authorship and ownership in digital content distribution, software licensing, and copyright protection[2].
6. **Cloud Computing**: Ensures security and integrity of data in the cloud, verifying the authenticity of service providers[6].

Conclusion

Digital signatures play a crucial role in various industries, ensuring secure communication, data integrity, and non-repudiation.

6. Identity and Access Management

1. **Authentication**
    - Common credentials: IAM manages username and password combinations as the primary authentication method.
    - Support for various credentials: IAM also supports digital signatures, certificates, biometric hardware (e.g., fingerprint readers), specialized software (e.g., voice analysis programs), and the ability to lock user accounts to specific IP or MAC addresses [1].
2. **Authorization**
    - Granularity control: The authorization component determines the appropriate level of access control granularity.
    - Relationship oversight: It oversees the relationships between identities, access control rights, and the availability of IT resources [2].
3. **User Management**
    - Administrative capabilities: User management is responsible for creating new user identities and access groups.
    - Password management: It includes resetting passwords, defining password policies, and managing user privileges [6].
4. **Credential Management**
    - Establishment of identities: Credential management establishes identities and access control rules for defined user accounts.
    - Mitigation of authorization threats: It helps mitigate the threat of insufficient authorization.

Ignore

➢ *Here are some examples of how IAM is used:*

1. Healthcare Industry: In the healthcare sector, IAM ensures secure access to patient records and sensitive medical information. It helps healthcare providers manage user identities, control access privileges, and enforce strict authentication measures to protect patient data from unauthorized access.

2. Financial Services: IAM plays a vital role in the financial services industry to safeguard sensitive financial information and prevent fraudulent activities. It enables banks and financial institutions to manage user identities, implement strong authentication methods, and enforce access controls to ensure that only authorized individuals can access financial systems and perform transactions.

3. Government Sector: IAM is extensively used in government organizations to manage user identities, control access to sensitive government data, and protect critical infrastructure. It helps government agencies enforce strict authentication measures, manage user roles and permissions, and ensure compliance with security regulations.

4. E-commerce: IAM is essential in e-commerce platforms to manage user identities, secure customer accounts, and protect personal and financial information. It enables online retailers to implement multi-factor authentication, manage user profiles, and ensure secure access to customer data and payment systems.

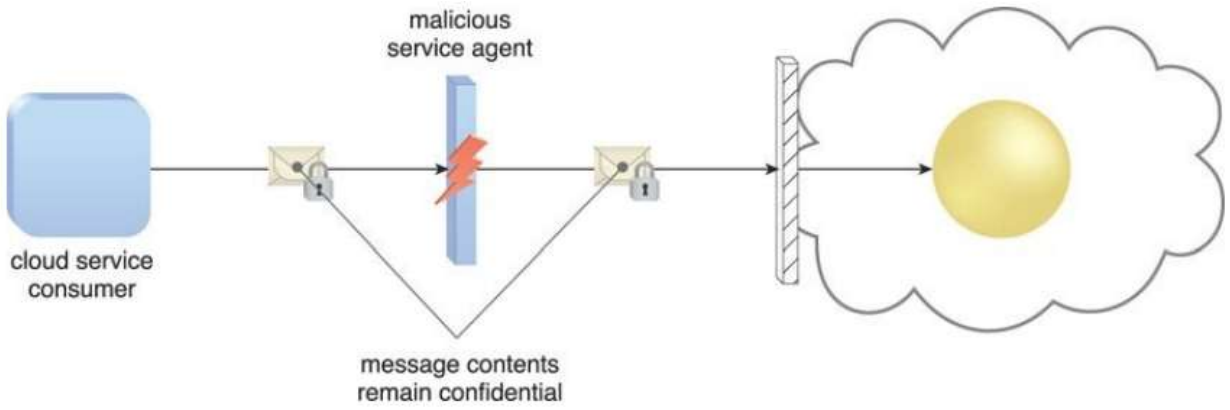
5. Education Sector: IAM is utilized in educational institutions to manage user identities, control access to educational resources, and protect student and faculty data. It helps schools and universities enforce access controls, manage user roles, and ensure secure authentication for online learning platforms and student information systems.

6. Cloud Computing: IAM is a fundamental component of cloud computing services. It enables cloud providers to manage user identities, control access to cloud resources, and ensure secure authentication and authorization for cloud-based applications and data storage.

These are just a few examples of how IAM is used in different industries and applications. IAM plays a crucial role in ensuring secure access to resources, protecting sensitive data, and maintaining regulatory compliance.

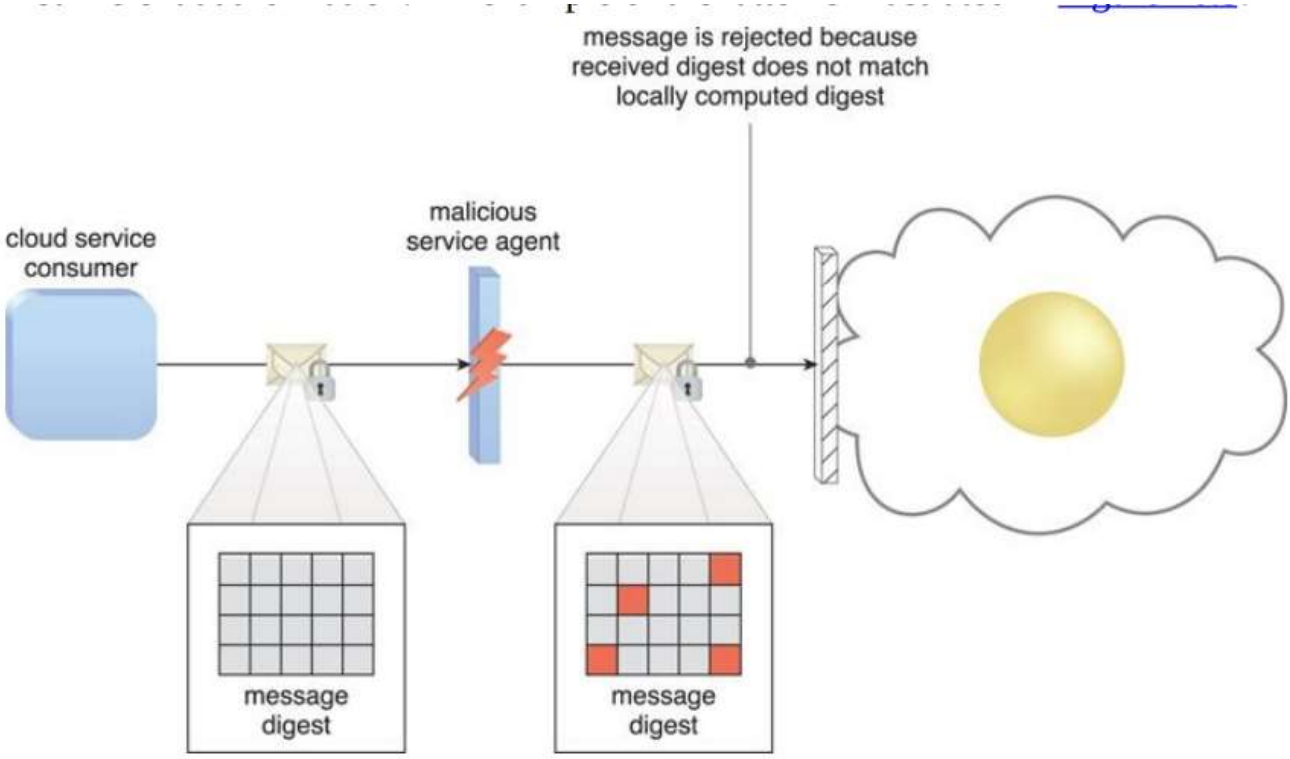
7. Hashing & Encryption

1. Encryption



- **Data Vulnerability**: Default data, known as plaintext, is vulnerable during transmission, risking unauthorized access.
- **Encryption Mechanism**: Utilizes a digital coding system to encode plaintext into protected ciphertext, preserving data confidentiality and integrity.
- **Cipher Algorithm**: Standardized algorithms, like ciphers, transform plaintext into ciphertext, keeping original data hidden.
- **Encryption Key**: Paired with plaintext, an encryption key, a secret message shared among authorized parties, decrypts ciphertext.
- **Security Threats**: Counters security threats like traffic eavesdropping, malicious intermediaries, insufficient authorization, and overlapping trust boundaries.
- **Symmetric Encryption**:
  - Uses a single key for encryption and decryption.
  - Known as secret key cryptography.
  - Provides evidence of rightful decryption but lacks nonrepudiation.
- **Asymmetric Encryption**:
  - Uses private and public keys.
  - Private key known only to the owner, while the public key is available.
  - Slower than symmetric encryption due to two keys.
  - Security level depends on key usage.
  - Private key offers integrity and authenticity, public key provides confidentiality but lacks integrity and authenticity protection.

2. Hashing



Hashing is a crucial mechanism for one-way, non-reversible data protection, commonly used for password storage.

- **Locking Mechanism:**
  - Applied to a message, hashing locks it without providing a key for unlocking.
- **Message Digest:**
  - Hashing generates a fixed-length message digest from the original message, used for verification.
- **Verification Process:**
  - Sender attaches the message digest to the message.
  - Recipient applies the same hash function to verify the identical message digest.
- **Tampering Detection:**
  - Any alteration to the original data results in a different message digest, indicating tampering.
- **Cloud Security:**
  - Hashing mitigates cloud threats such as malicious intermediaries and insufficient authorization.
  - Example: Figure 10.3 illustrates hashing protecting a message altered by a malicious service agent.

- Ignore
- here's an example of how Hashing and Encryption work:
- Hashing and Encryption are mechanisms in cloud computing that provide data protection and security . Hashing is used when a one-way, non-reversible form of data protection is required, while Encryption is used when two-way reversible data protection is required.
- Let's say a company wants to store user passwords securely in their database. To ensure that the passwords are not stored in plain text and are protected from unauthorized access, the company can use Hashing.
- First, the company creates a message digest of the password using a hashing algorithm. The message digest is a fixed-length string of bits that represents the password. The company then stores the message digest in their database instead of the actual password. When a user logs in, the company creates a message digest of the entered password and compares it with the stored message digest. If the two message digests match, it means that the entered password is correct.
- In this way, Hashing helps to protect user passwords from unauthorized access and ensures that even if the database is compromised, the actual passwords cannot be obtained.
- Now let's say the company wants to send a confidential document to another company over the internet. To ensure that the document is not intercepted and read by unauthorized parties during transmission, the company can use Encryption.
- First, the company encrypts the document using a symmetric encryption algorithm and a secret key. The encrypted document is sent to the recipient. When the recipient receives the document, they decrypt it using the same secret key to obtain the original document.
- In this way, Encryption helps to protect confidential documents from interception and ensures that only authorized parties can read the document.
- Overall, Hashing and Encryption are important mechanisms in cloud computing that provide data protection and security. Hashing is used when one-way, non-reversible data protection is required, while Encryption is used when two-way reversible data protection is required.

➢ Hashing and encryption are widely used in various industries and applications to ensure data security and protect sensitive information. Here are some examples:

1. Banking and Financial Services: Hashing and encryption techniques are used to secure online banking transactions, protect customer data, and prevent unauthorized access to financial systems.

2. Healthcare: In the healthcare industry, hashing and encryption are used to safeguard patient records, medical data, and personal health information (PHI). This ensures that sensitive information remains confidential and protected from unauthorized access.

3. E-commerce: Hashing and encryption are crucial for securing online transactions, protecting customer payment information, and ensuring the integrity of data exchanged between buyers and sellers.

4. Government and Defense: Government agencies and defense organizations use hashing and encryption to secure classified information, communications, and sensitive data. This helps prevent unauthorized access and ensures the confidentiality and integrity of critical information.

5. Cloud Computing: Hashing and encryption techniques are employed to secure data stored in the cloud, ensuring that only authorized users can access and decrypt the data. This helps protect against data breaches and unauthorized access to sensitive information.

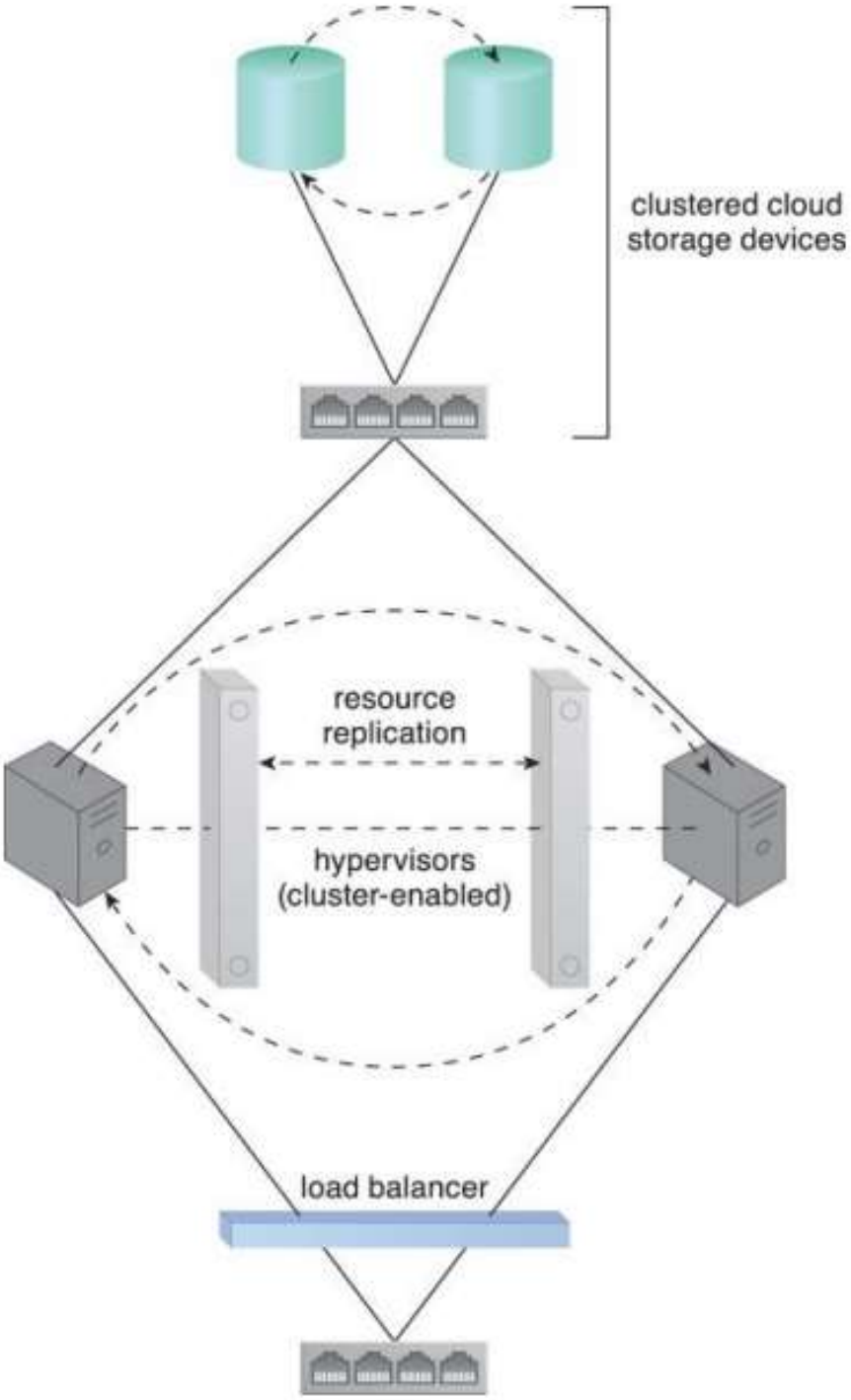
6. Communication and Messaging: Hashing and encryption are used to secure email communications, instant messaging platforms, and other forms of electronic communication. This ensures that messages remain confidential and protected from interception or tampering.

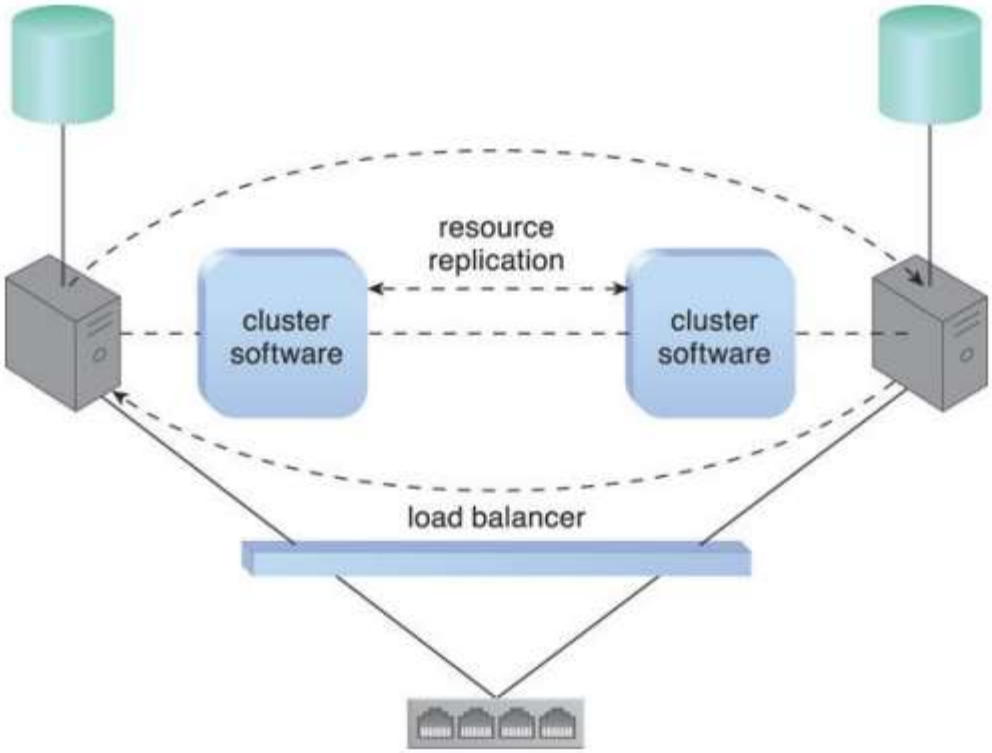
7. Password Storage: Hashing is commonly used to store passwords securely. Instead of storing the actual passwords, a hash value is stored. When a user enters their password, it is hashed and compared to the stored hash value for authentication.

8. Digital Signatures: Encryption and hashing techniques are used to create digital signatures, which provide authentication, integrity, and non-repudiation for digital documents and transactions. This is commonly used in industries such as legal, finance, and e-commerce.

These are just a few examples of how hashing and encryption are used in various industries and applications to ensure data security and protect sensitive information.

8. Resource cluster





➢ Common Resource Cluster Types

A. **Server Cluster:**

- Clusters physical or virtual servers to enhance performance and availability.
- Hypervisors on different servers can share virtual server execution state for live-migration.
- Enables transparent live-migration of virtual servers for scalability.
- Often requires access to shared storage.

B. **Database Cluster:**

- Enhances data availability with synchronization across different storage devices.
- Employs active-active or active-passive failover systems for redundancy.

C. **Large Dataset Cluster:**

- Implements data partitioning for efficient distribution without compromising integrity.
- Each node processes workloads independently, reducing communication.

Additional Information:

- Resource clusters may require nodes with similar computing capacity.
- High-availability clusters need common storage access and often have two-layer communication.
- Some clusters have loosely coupled IT resources requiring only network layer communication.

➢ Basic Types of Resource Clusters

A. **Load Balanced Cluster:**

- Specializes in distributing workloads among nodes to increase IT resource capacity.
- Implements a load balancer mechanism.

B. **High-Availability (HA) Cluster:**

- Ensures system availability in case of multiple node failures.
- Employs redundant implementations of clustered IT resources.
- Implements failover systems to redirect workload away from failed nodes.

- here's an example of how a Resource Cluster works:
- A Resource Cluster is a mechanism in cloud computing that provides high availability and scalability for IT resources by grouping them together into a cluster . Resource clusters are designed to improve data availability and increase IT resource capacity while preserving the centralization of IT resource management.
- Let's say a company has subscribed to a cloud service provider to host their e-commerce website. The website receives a large number of visitors, and the company needs to ensure that the website is always available and can handle the traffic. To do this, the company can use a Resource Cluster provided by the cloud service provider.
- The Resource Cluster includes multiple nodes, each with identical computing capacity and characteristics. The nodes are connected to a shared storage device and communicate with each other to maintain the synchronization of data being stored at different storage devices used in the cluster. The redundant capacity is usually based on an active-active or active-passive failover system committed to maintaining the synchronization conditions.
- When a user accesses the website, the Resource Cluster distributes the workload among the cluster nodes to increase IT resource capacity. Each cluster node processes workloads without communicating with other nodes as much as in other cluster types. This ensures that the website is always available and can handle the traffic.
- In this way, a Resource Cluster helps the company to improve data availability and increase IT resource capacity while preserving the centralization of IT resource management. It ensures that the website is always available and can handle the traffic, providing a better user experience for the website visitors.

- A resource cluster is a mechanism used in cloud computing to group multiple IT resource instances together so that they can be operated as a single IT resource. It aims to improve the allocation and use of hardware resources such as processor power, memory, and I/O.
- Resource cluster architectures rely on high-speed dedicated network connections between IT resource instances to facilitate workload distribution, task scheduling, data sharing, and system synchronization. A cluster management platform, running as distributed middleware in all cluster nodes, is responsible for coordinating these activities. It allows distributed IT resources to appear as one IT resource and executes IT resources within the cluster.
- There are different types of resource clusters, including:

1. Server Cluster: Physical or virtual servers are clustered to increase performance and availability. Hypervisors running on different physical servers can be configured to share virtual server execution state, allowing for the establishment of clustered virtual servers. This configuration requires access to shared storage and enables live migration of virtual servers between physical servers to increase scalability.

2. Database Cluster: This type of cluster is designed to improve data availability. It utilizes a synchronization feature to maintain data consistency across different storage devices in the cluster. Redundant capacity is typically based on an active-active or active-passive failover system to ensure synchronization.

3. Large Dataset Cluster: This cluster focuses on efficient data partitioning and distribution. It partitions target datasets without compromising data integrity or computing accuracy. Each cluster node processes workloads independently, minimizing communication with other nodes.

- Resource clusters often require cluster nodes to have similar computing capacity and characteristics to simplify design and maintain consistency. High-availability cluster architectures require access to shared storage IT resources, necessitating communication for both storage access and IT resource orchestration.

- There are two basic types of resource clusters:

i. Load Balanced Cluster: This cluster specializes in distributing workloads among nodes to increase IT resource capacity while maintaining centralized management. It incorporates a load balancer mechanism either within the cluster management platform or as a separate IT resource.
ii. HA Cluster: A high-availability cluster ensures system availability in the event of multiple node failures. It includes redundant implementations of most or all clustered IT resources and employs a failover system to monitor failure conditions and redirect workloads away from failed nodes.

The provisioning of clustered IT resources can be more expensive than individual resources with equivalent computing capacity.