CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Wireless, IoT, and Cloud Security

Cloud Security

Video summary

- Cloud Computing Reference Architecture
- Cloud Computing Security Issues
- Risk and Countermeasures
- Cloud Security As A Service (SecaaS)
- Open Stack

Cloud Computing Reference Architecture

- NIST SP-500-292 (*NIST Cloud Computing Reference Architecture)* establishes reference architecture, described as follows:

> "The NIST cloud computing reference architecture focuses on the requirements of "what" cloud services provide, not a "how to" design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference."

Objectives

NIST developed the reference architecture with the following objectives in mind:

- To illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model
- To provide a technical reference for CSCs to understand, discuss, categorize, and compare cloud services
- To facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations

NIST Cloud Computing Major Actors

- **Cloud service consumer** (CSC): A person or organization that maintains a business relationship with, and uses service from, cloud providers.

- **Cloud service provider (CSP):** A person, organization, or entity responsible for making a service available to interested parties.

- **Cloud auditor:** A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.

- **Cloud broker:** An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between CSPs and cloud consumers.

- **Cloud carrier:** An intermediary that provides connectivity and transport of cloud services from CSPs to cloud consumers.

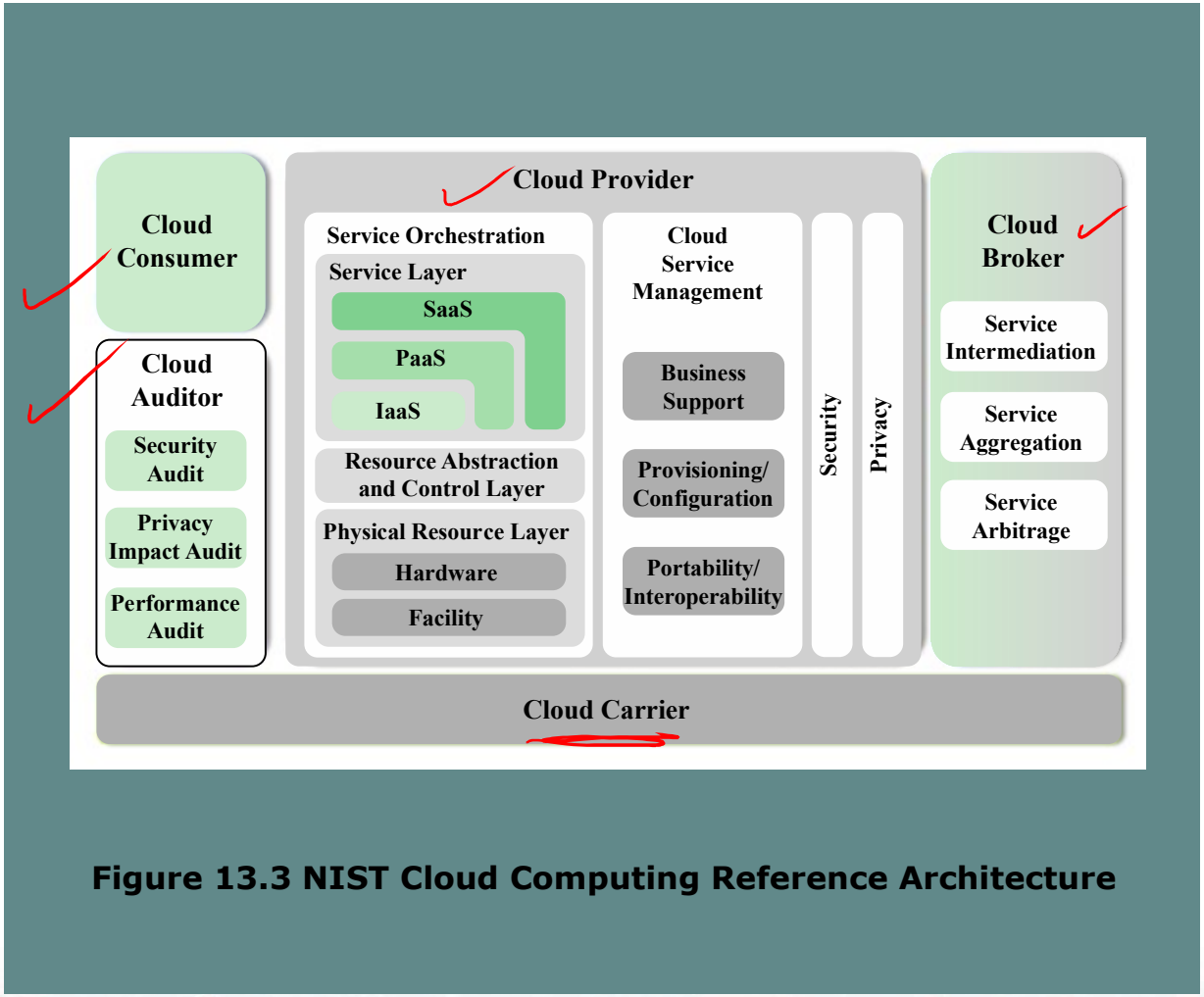


Figure 13.3 NIST Cloud Computing Reference Architecture

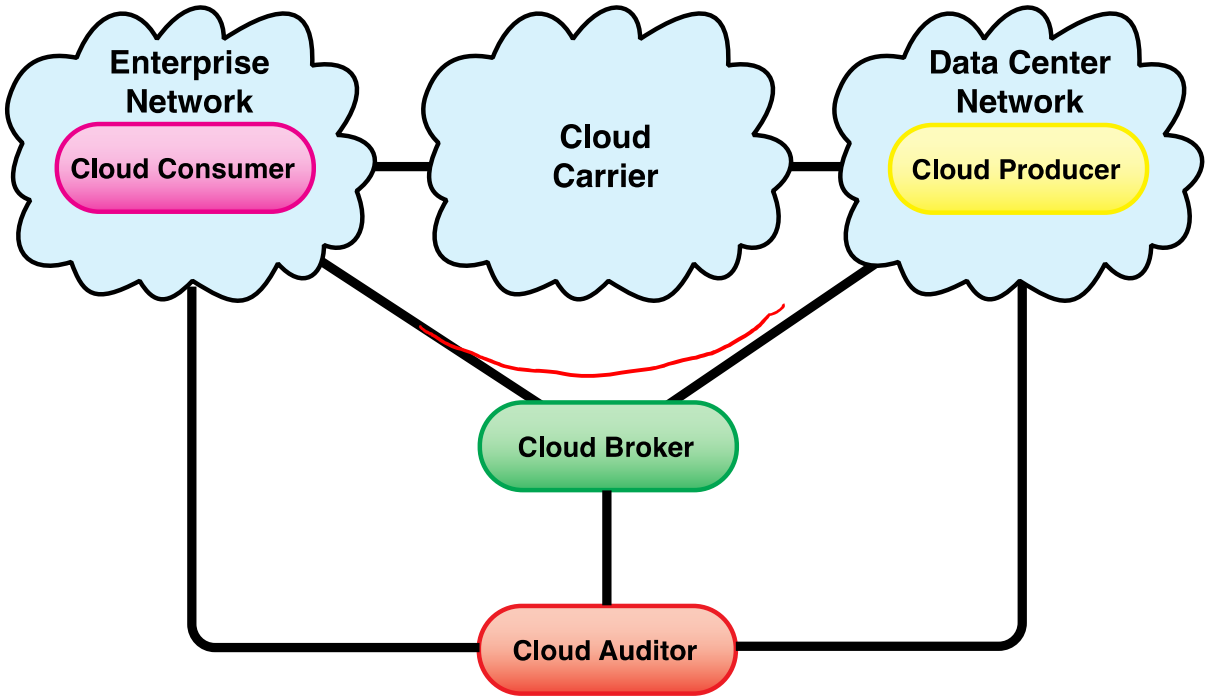


Figure 13.4 Interactions Between Actors in Cloud Computing

Governance

Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services.

Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.

Compliance

Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements.

Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements.

Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.

Trust

Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time.

Establish clear, exclusive ownership rights over data.

Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system.

Continuously monitor the security state of the information system to support ongoing risk management decisions.

Architecture

Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.

Identity and access management

Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.

Software isolation

Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.

Data protection

Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.

Take into consideration the risk of collating organizational data with those of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value.

Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.

Table 13.2

NIST Guidelines on Cloud Security and Privacy Issues and Recommendations

(Table is on pages 433-434 in the textbook)

Availability

Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements.

Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.

Incident response

Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization.

Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.

Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

Table 13.2

NIST Guidelines on Cloud Security and Privacy Issues and Recommendations

Security Issues for Cloud Computing

- Availability is a major concern 99.999%
- Auditability of data must be ensured
- Businesses should take actions on security threats both from outside and inside the cloud
  - Cloud users are responsible for application-level security
  - Cloud vendors are responsible for physical security and some software security
- Cloud providers must guard against theft or denial-of-service attacks by their users and users need to be protected from one another
- Businesses should consider the extent to which subscribers are protected against the provider, especially in the area of data loss

Risks and Countermeasures

The Cloud Security Alliance (CSA) lists the following as the top cloud-specific security threats:

- Abuse and nefarious use of cloud computing
  - Countermeasures include:
    - Stricter initial registration and validation processes
    - Comprehensive inspection of customer network traffic
    - Monitoring public blacklists for one's own network blocks

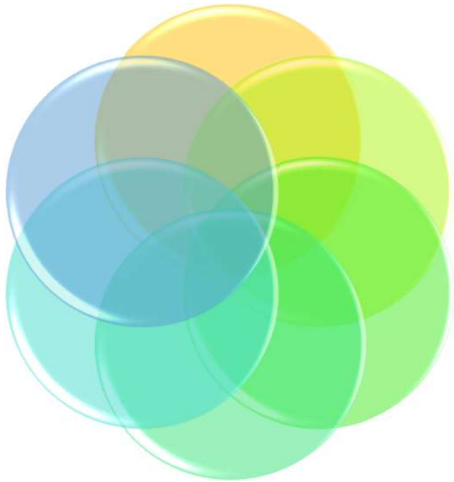
- Insecure interfaces
  - Countermeasures include:
    - Analyzing the security model of CSP interfaces
    - Ensuring that strong authentication and access controls are implemented in concert with encrypted transmission

- Malicious insiders
  - Countermeasures include:
    - Specify human resource requirements as part of legal contract
    - Require transparency into overall information security and management practices
    - Determine security breach notification processes (by law)
- Shared technology isolation issues (CPUs, GPUs)
  - Countermeasures include:
    - Implement security best practices for installation/configuration
    - Monitor environment for unauthorized changes/activity
    - Promote strong authentication and access control for administrative access and operations
    - Enforce SLAs for patching and vulnerability remediation
    - Conduct vulnerability scanning and configuration audits

- Data loss or leakage
  - Countermeasures include:
    - Implement strong access control
    - Encrypt and protect integrity of data in transit and at rest
    - Analyze data protection at both design and run time
    - Implement strong key generation, storage and management, and destruction practices
- Account or service hijacking
  - Countermeasures include:
    - Prohibit the sharing of account credentials between users and services
    - Leverage strong two-factor authentication techniques where possible
    - Employ proactive monitoring to detect unauthorized activity
    - Understand CSP security policies and SLAs

Data Protection in the Cloud

The threat of data compromise increases in the cloud, due to the number of, and interactions between, risks and challenges that are unique to the cloud



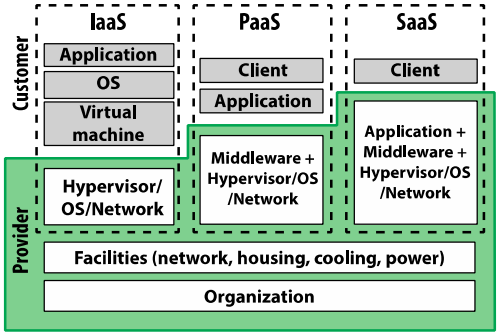
Even with these precautions, corruption and other denial-of-service attacks remain a risk

Data must be secured while at rest, in transit, and in use, and access to the data must be controlled

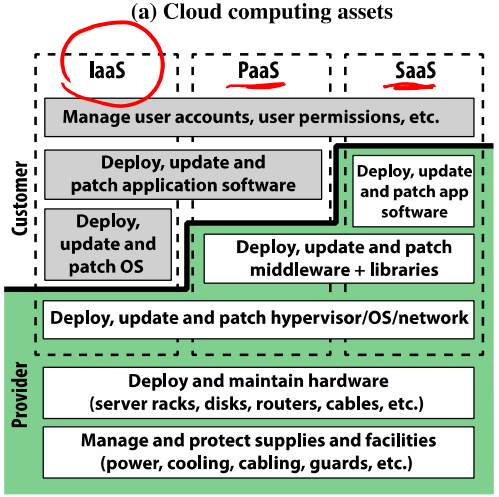
For data at rest, the ideal security measure is for the client to encrypt the database and only store encrypted data in the cloud, with the CSP having no access to the encryption key

The client can employ encryption to protect data in transit, though this involves key management responsibilities for the CSP

The client can enforce access control techniques, but CSP is involved to some extent depending on the service model used



(a) Cloud computing assets



(b) Cloud computing management tasks

Figure 13.5 Security Considerations for Cloud Computing Assets

Cloud Security as a Service

- In the context of cloud computing, cloud security as a service, (SecaaS) is a segment of the SaaS offering of a CSP
- The CSA defines SecaaS as the provision of security applications and services via the cloud either to cloud-based infrastructure and software, or from the cloud to the customers' on-premise systems
- CSA has identified the following SecaaS categories of service:
  - Identity and access management
  - Data loss prevention
  - Web security
  - E-mail security
  - Security assessments
  - Intrusion management
  - Security information and event management
  - Encryption
  - Business continuity and disaster recovery
  - Network security

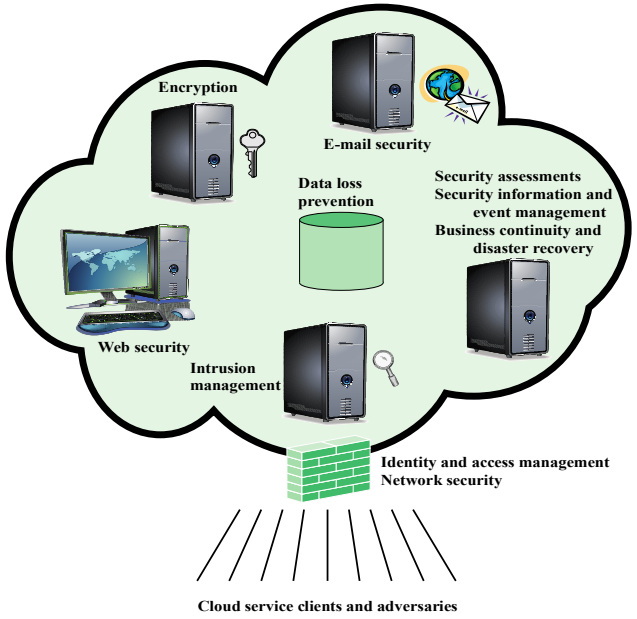


Figure 13.6 Elements of Cloud Security as a Service

OpenStack

Open-source software project of the OpenStack Foundation that aims to produce an open-source cloud operating system

The principal objective is to enable creating and managing huge groups of virtual private servers in a cloud computing environment

OpenStack is embedded, to one degree or another, into data center infrastructure and cloud computing products

It provides multi-tenant IaaS, and aims to meet the needs of public and private clouds, regardless of size, by being simple to implement and massively scalable

OpenStack

- The security module for OpenStack is called Keystone
- Keystone provides the shared security services essential for a functioning cloud computing infrastructure

Video summary

- Cloud Computing Reference Architecture
- Cloud Computing Security Issues
- Risk and Countermeasures
- Cloud Security As A Service (SecaaS)
- Open Stack