NETWORK ACCESS CONTROL AND CLOUD SECURITY

Tran Song Dat Phuc

SeoulTech 2015

Table of Contents

- Network Access Control (NAC)
- Network Access Enforcement Methods
- Extensible Authentication Protocol
- IEEE 802.1X Port-Based NAC
- Cloud Computing
- Cloud Security Risks and Countermeasures
- Cloud Security as a Service (SecaaS)

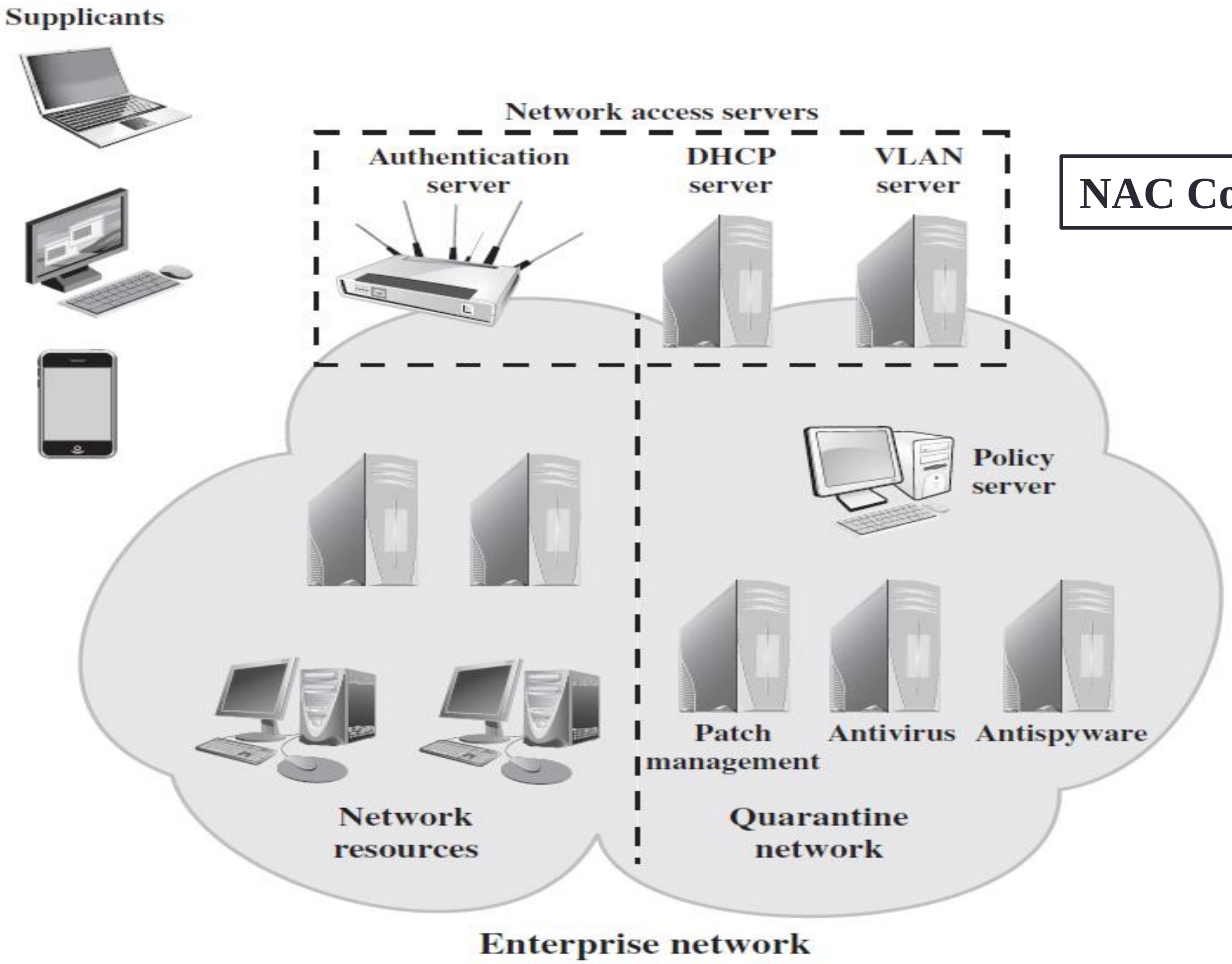
Network Access Control (NAC)

- “**Network Access Control (NAC)** is a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices when they initially attempt to access the network.” – wikipedia.
- “**NAC** is an approach to computer network security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.” – wikipedia.
- **NAC** authenticates users logging into the network and determines what data they can access and action they can perform.
- **NAC** examines the health of the user’s computer or mobile device (the endpoints).

Network Access Control (NAC)

- **Access requestor (AR)**: referred to as supplicants, or clients. The **AR** is the node that is attempting to access the network and may be any device that is managed by the NAC system.
- **Policy server**: Based on the **AR**'s posture and an enterprise's defined policy, the **policy server** determines what access should be granted.
- **Network access server (NAS)**: Also called a media gateway, a remote access server (**RAS**), or a policy server. The **NAS** functions as an access control point for users in remote locations connecting to an enterprise's internal network.

Network Access Control (NAC)



NAC Context

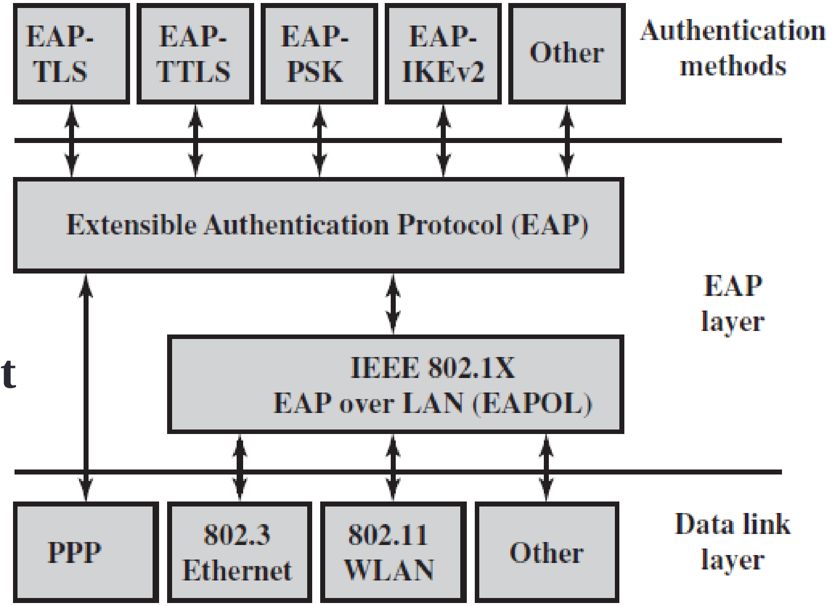
Network Access Enforcement Methods

- Enforcement methods are the actions that are applied to **AR**s to regulate access to the enterprise network.
  - **IEEE 802.1X**: enforces authorization before a port is assigned an IP address. IEEE 802.1X makes use of the Extensible Authentication Protocol for the authentication process.
  - **Virtual local area networks (VLANs)**: the enterprise network, consisting of an interconnected set of LANs, is segmented logically into a number of virtual LANs. The NAC system decides to which of the network's VLANs it will direct an AR.
  - **Firewall**: allow or deny network traffic between an enterprise host and an external user.
  - **DHCP management**: DHCP enables dynamic allocation of IP addresses to hosts. A DHCP server intercepts DHCP requests and assigns IP addresses. Thus, NAC enforcement occurs at the IP layer based on subnet and IP assignment.

Extensible Authentication Protocol

- The Extensible Authentication Protocol (**EAP**) acts as a framework for network access and authentication protocols.
- **EAP** provides a set of protocol messages, encapsulate various authentication methods to be used between a client and an authentication server.
- **EAP** can operate over a variety of network and link level facilities, including point-to-point links, LANs, and other networks, and can accommodate the authentication needs of the various links and networks.

EAP Layered Context



EAP Authentication

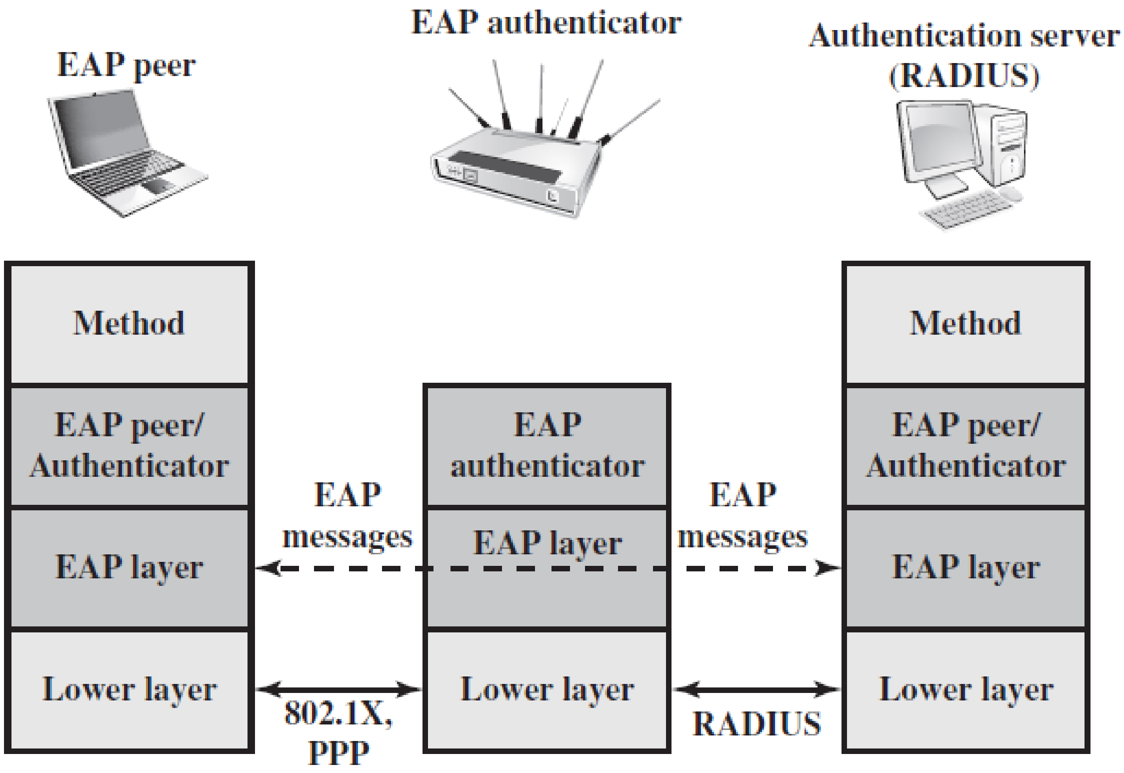
- **EAP-TLS (EAP Transport Layer Security)**: defines how the TLS protocol can be encapsulated in EAP messages. It uses the handshake protocol in TLS.
- **EAP-TTLS (EAP Tunneled TLS)**: like **EAP-TLS**, except only the server has a certificate to authenticate itself to the client first. In **EAP-TLS**, a secure connection (the "tunnel") is established with secret keys.
- **EAP-GPSK (EAP Generalized Pre-Shared Key)**: is an **EAP** method for mutual authentication and session key derivation using a pre-shared key (**PSK**). It specifies an **EAP** method based on **PSK**s and employs secret key-based cryptographic algorithms.
- **EAP-IKEv2**: based on the Internet Key Exchange protocol ver.2 (IKEv2). It supports mutual authentication and session key establishment using a variety of methods.

EAP Exchanges

The authentication information and authentication protocol information are carried in EAP messages.

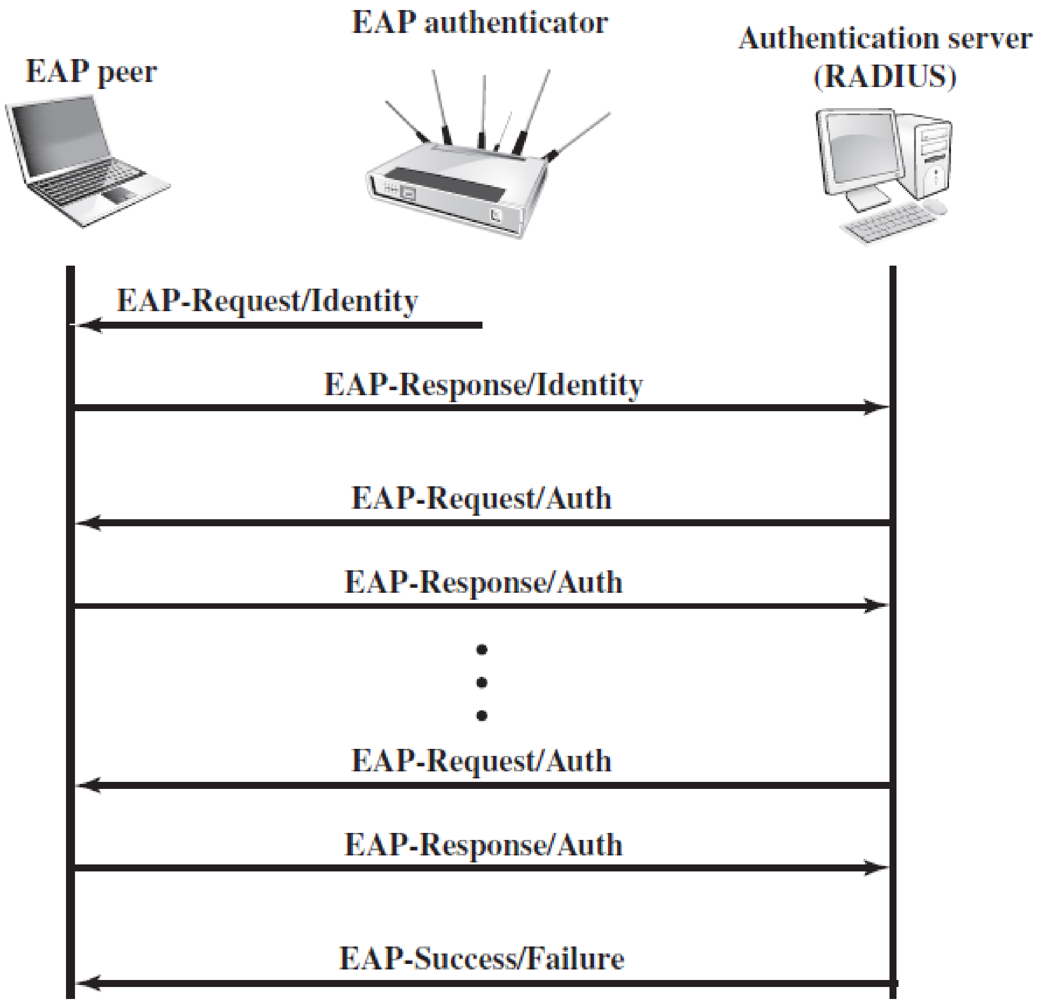
EAP Message
Code
Identifier
Length
Data

EAP Protocol Exchange



EAP Exchanges

EAP Message Flow in Pass-Through Mode



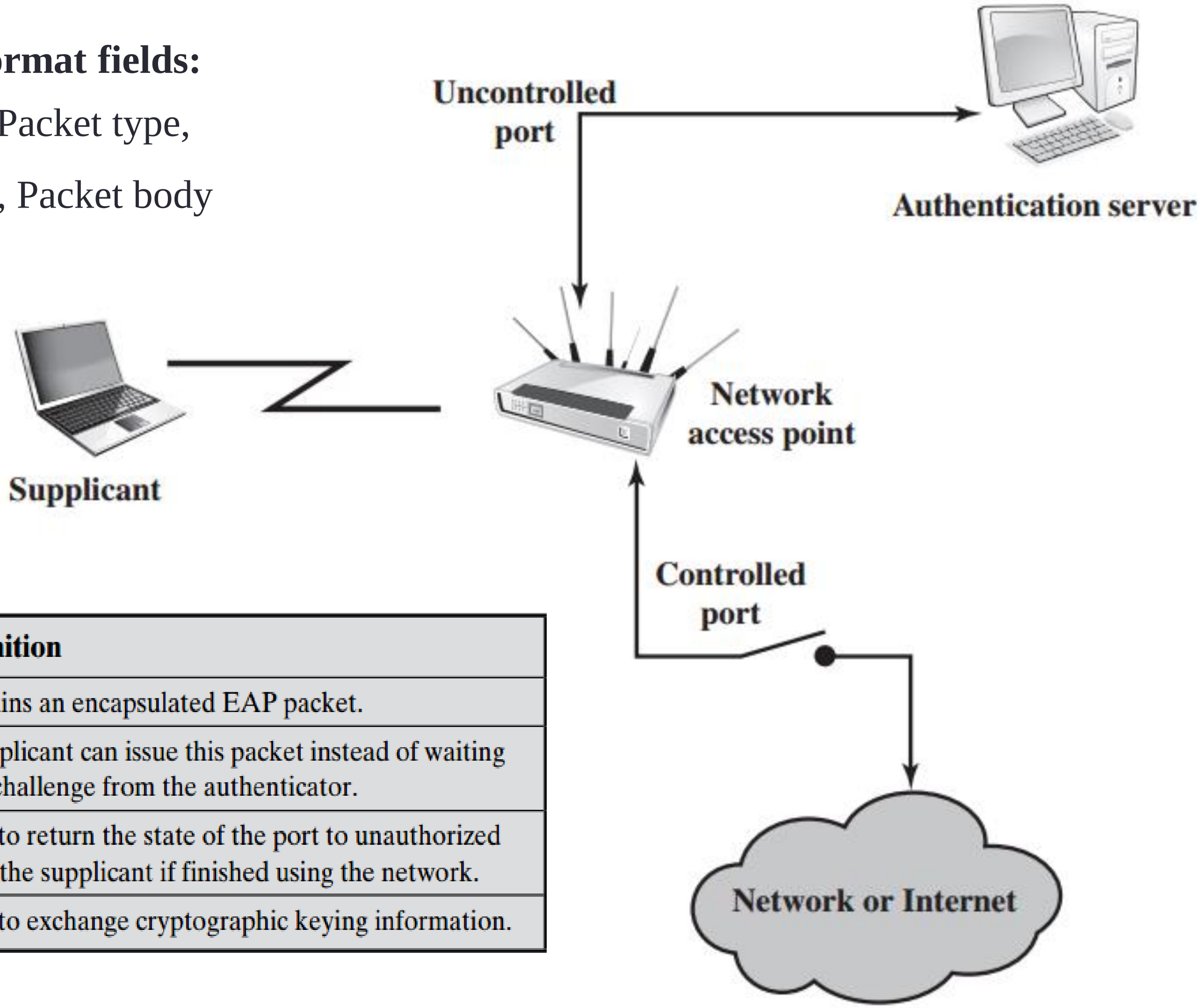
IEEE 802.1X Port-Based NAC

- Provide access control functions for LANs
- IEEE 802.1X Terminology:
  - Authenticator
  - Authentication exchange
  - Authentication process
  - Authentication server (AS)
  - Authentication transport
  - Bridge port
  - Edge port
  - Network access port
  - Port access entity (PAE)
  - Supplicant
- **EAPOL** (EAP over LAN) protocol operates at the network layers and makes use of an IEEE 802 LAN (Wifi or Ethernet), at the link layer.
- **EAPOL** enables a supplicant to communicate with an authenticator and support the exchange of EAP packets for authentication.

EAPOL packet format fields:

Protocol version, Packet type,

Packet body length, Packet body

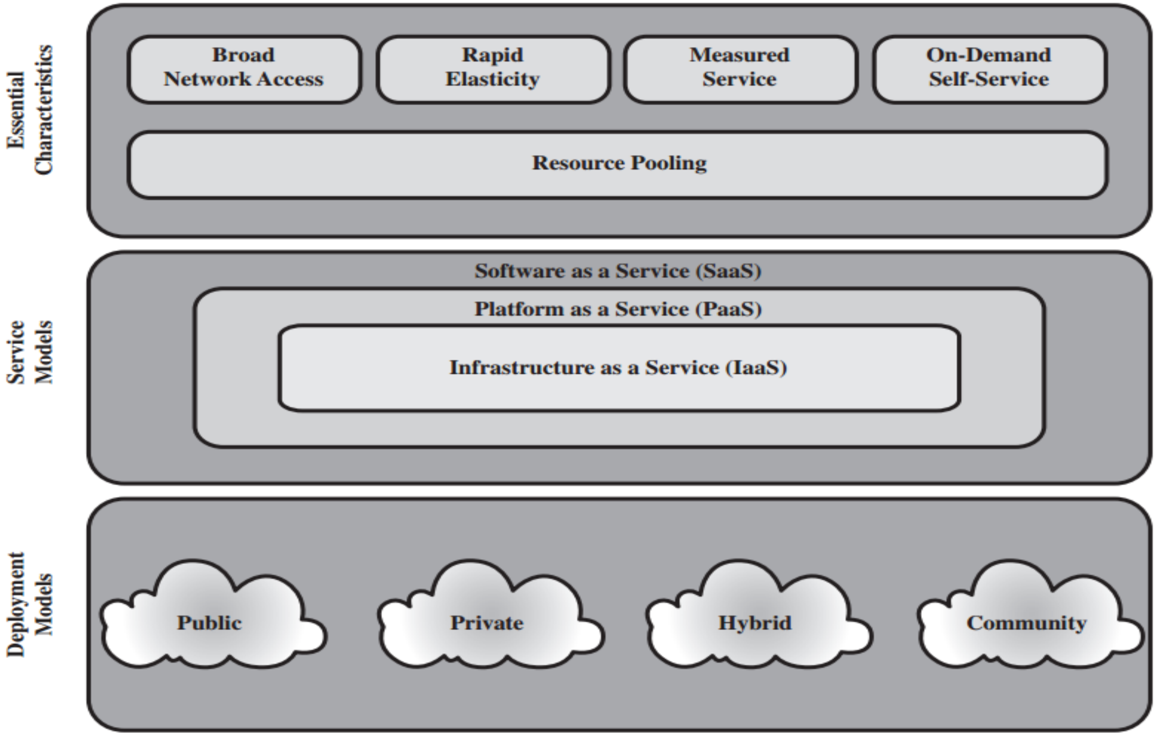


Frame Type	Definition
EAPOL-EAP	Contains an encapsulated EAP packet.
EAPOL-Start	A supplicant can issue this packet instead of waiting for a challenge from the authenticator.
EAPOL-Logoff	Used to return the state of the port to unauthorized when the supplicant if finished using the network.
EAPOL-Key	Used to exchange cryptographic keying information.

802.1X Access Control

Cloud Computing

- “A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, services) that can be released with minimal management effort or service provider interaction.” – NIST SP-800-145.



Cloud Computing Elements

Cloud Computing Characteristics

- **Resources** related to some aspects, such as storage, processing, memory, network bandwidth, and virtual machine.
- **Broad network access** - available over the network and accessed through standard mechanisms, use by client platforms or other cloud-based services.
- **Rapid elasticity** - ability to expand and reduce resources according to specific requirements.
- **Measured service** - control and optimize resource suitable to the appropriate type of service. Resource usage can be monitored, controlled, reported, provide clearly utilized service.
- **On-demand self-service** - ability to provision resource capabilities automatically, no need human interaction. The resources is temporary in IT infrastructure.
- **Resource pooling** - ability to serve multiple consumers using a multi-tenant model, with different physical and virtual resources, dynamically assigned and reassigned base on consumer demand.

Cloud Computing Service Models

- **Software as a Service (SaaS)** - the capability allows consumer to use the provider's application running on a cloud infrastructure. The applications are accessible from various client devices by just a thin client interface (Web browser). **SaaS** saves the complexity of software installation, maintenance, upgrades, patches.

- **Platform as a Service (PaaS)** - the capability allows consumer to deploy onto the cloud infrastructure consumer or acquired applications - created. Also, **PaaS** provides middleware-style services , such as database and component services use by apps. **PaaS** is such like an operating system in the cloud.

- **Infrastructure as a Service (IaaS)** - the capability allows consumer to provision processing, storage, networks, and other computing resources, that is used to deploy and run various software. **IaaS** enables customers to combine basic computing services to build highly adaptable computer systems.

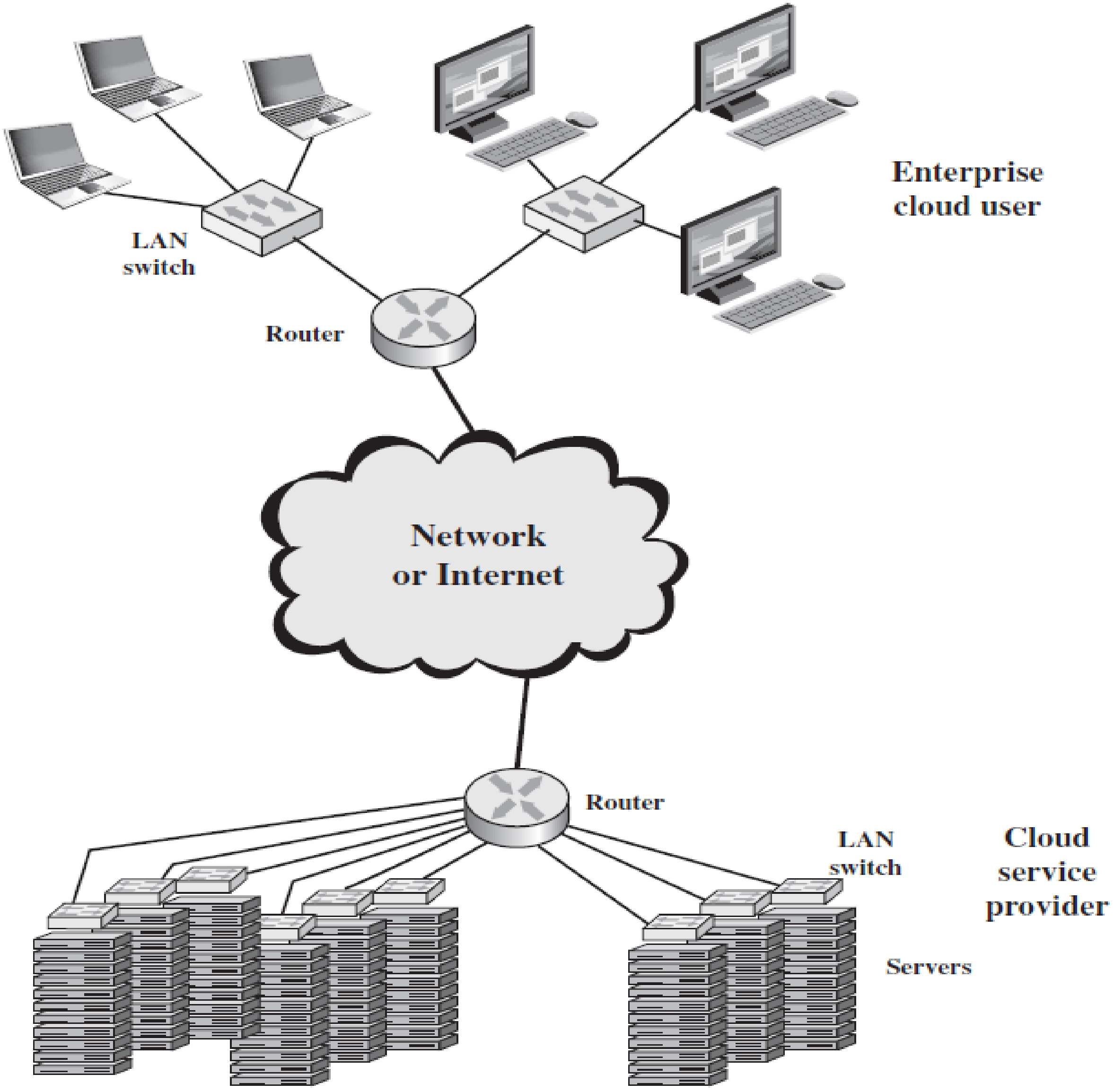
Cloud Computing Deployment Models

- **Public cloud** - available to the general public or a large industry group, is owned by an organization selling cloud services. The cloud provider (**CP**) is responsible for cloud infrastructure and for control data and operations within cloud.

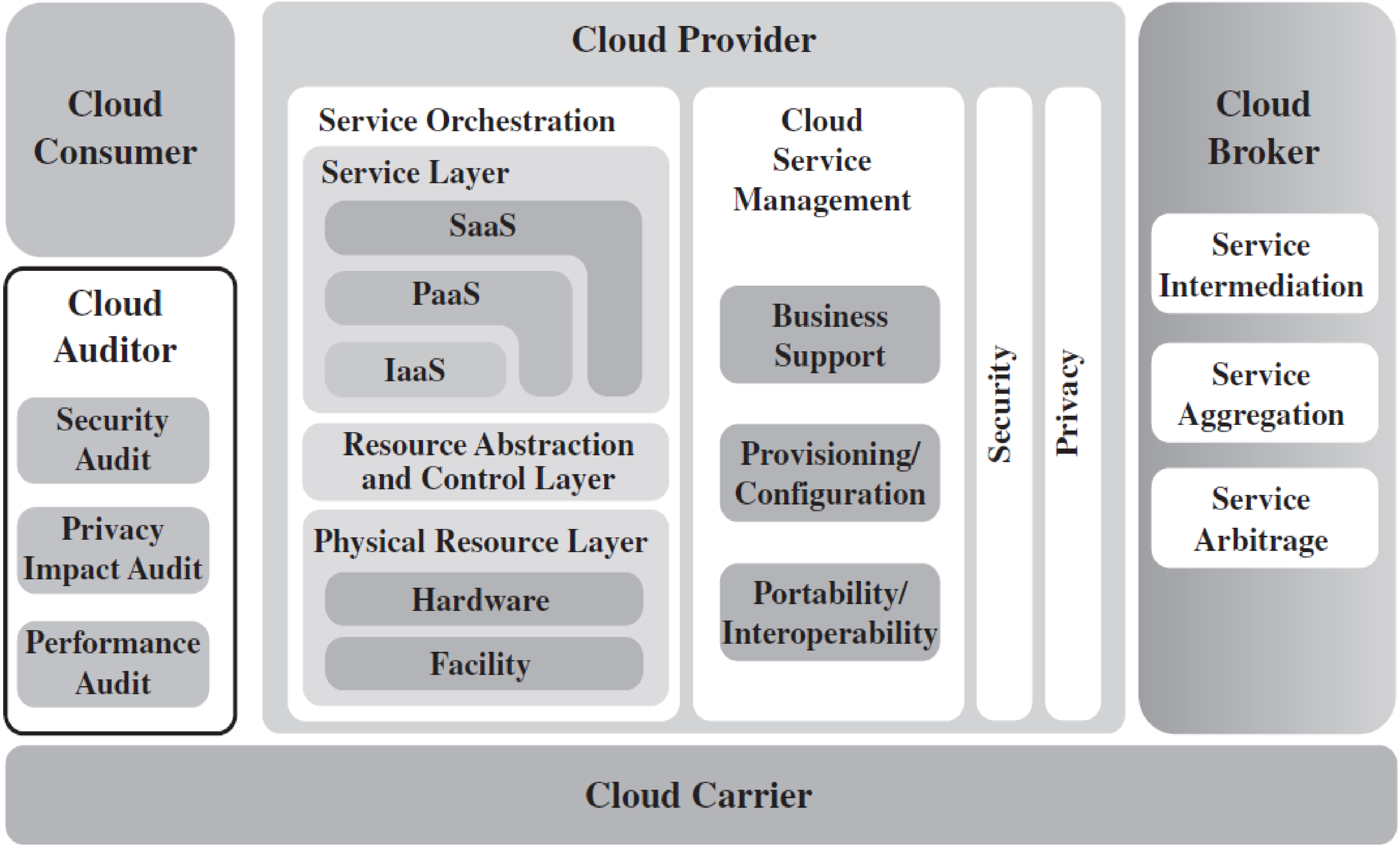
- **Private cloud** - operated solely for an organization, managed by organization or a third party. The **CP** is responsible only for the infrastructure.

- **Community cloud** - shared by several organizations and supports a specific community shared specific concerns (mission, policy, security …), managed by the organization or a third party.

- **Hybrid cloud** - is a composition of two or more clouds, remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).



Cloud Computing Context



NIST Cloud Computing Reference Architecture

Cloud Computing Reference Architecture

- **Cloud consumer -** a person or organization maintains a business relationship with, and uses service from, cloud providers.
- **Cloud provider -** a person, organization, or entity responsible for making a service available to interested parties.
- **Cloud auditor -** a party conducts independent assessment of cloud services, info. system operations, performance, and security of cloud implementation.
- **Cloud broker -** an entity manages the use, performance, and delivery of cloud services, and negotiates relationships between **CP** and consumers.
- **Cloud carrier -** an intermediary provides connectivity and transport of cloud services from **CP**s to consumers.

Cloud Security Risks and Countermeasures

- **Abuse and nefarious use of cloud computing -** The easy of register and use cloud service leads to high risks from attackers inside the cloud, such as spamming, malicious code attacks, or DOS attack.

  Countermeasures: (1) stricter initial registration and validation processes, (2) enhance credit card fraud monitoring and coordination, (3) comprehensive introspection of customer network traffic, (4) monitoring public blacklists for one's network blocks.

- **Insecure interfaces and APIs -** CPs expose a set of software interfaces or APIs customers use to manage and interact with cloud services. From authentication and access control, these interfaces need to be resisted against accidental and malicious attempts.

  Countermeasure: (1) analyzing the security model of CP interfaces, (2) ensuring that strong authentication and access control are implemented with encrypted transmission, (3) understanding the dependency chain associated with the API.

- **Malicious insiders –** risk of malicious insider activity. Cloud architectures necessitate roles that extremely high risk.

  Countermeasures: (1) enforce strict supply chain management and conduct a comprehensive supplier assessment, (2) specify human resource requirements as part of legal contract, (3) require transparency into overall infor. security and management practices, and compliance reporting, (4) determine security breach notification processes.

Cloud Security Risks and Countermeasures

- **Shared technology issues**: IaaS vendors deliver services by sharing infrastructure which is not strong enough in isolation properties for a multi-tenant architecture.

  Countermeasures: implement security best practices for installation/ configuration, (2) monitor environment for unauthorized changes/ activity, (3) promote strong authentication and access control for administrative access and operation.

- **Data loss and leakage -** for clients. The most devastating from security breach is the loss or leakage of data.

  Countermeasures: (1) implement strong API access control, (2) encrypt, protect integrity of data in transit, (3) analyze data protection at design and run-time, (4) implement strong keys generation, , storage and management, destruction practices.

- **Account or service hijacking -** usually with stolen credentials, attackers can access critical areas of cloud services, allowing to compromise the confidentiality, integrity, and availability (CIA).

  Countermeasures: (1) prohibit the sharing of account credentials between users and services, (2) leverage strong two-factor authentication techniques, (3) employ proactive monitoring to detect unauthorized activity, (4) understand CP security policies and SLAs.

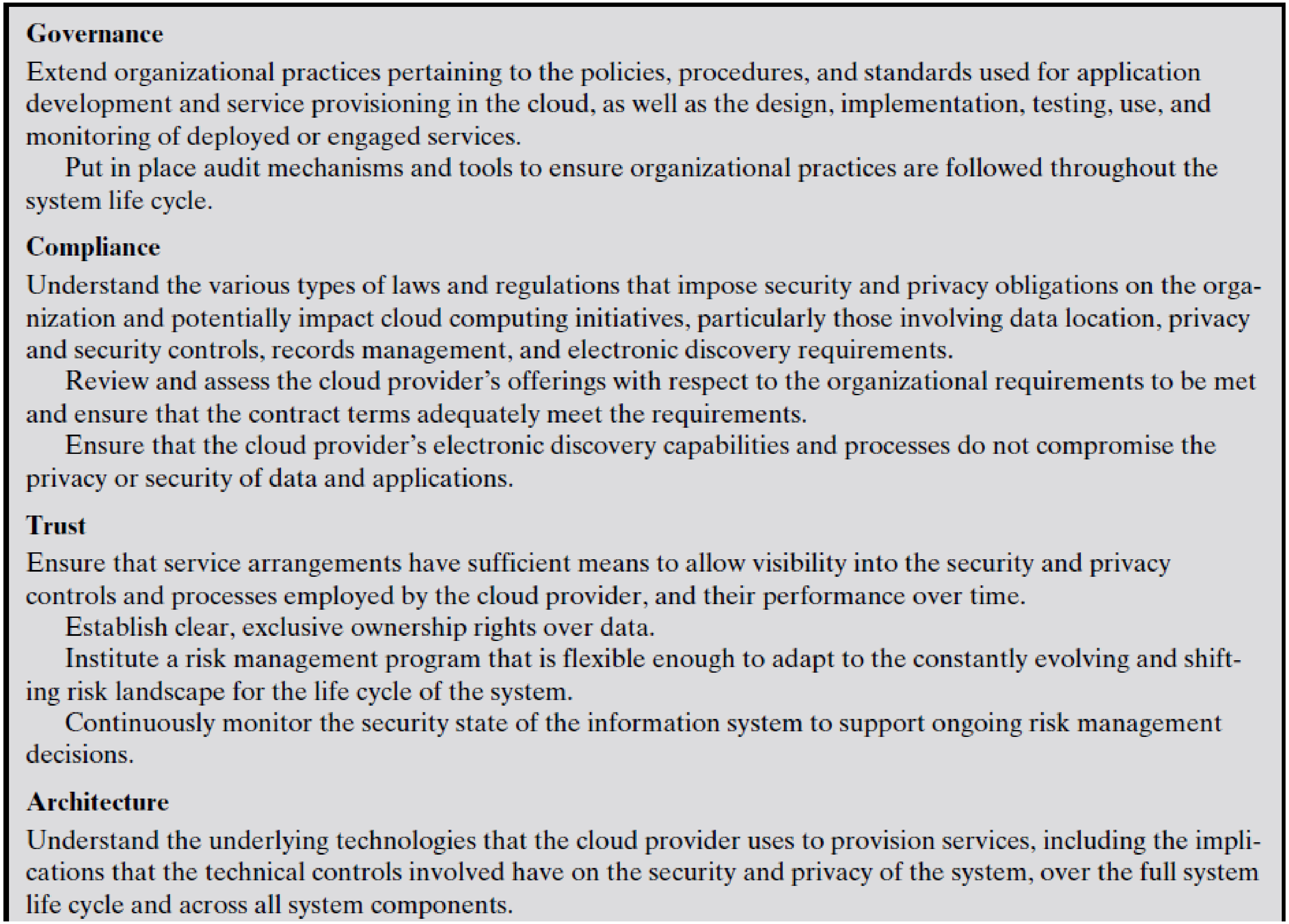
Cloud Security Risks and Countermeasures

- **Unknown risk profile -** in using cloud infrastructure, client should cedes control to the CP on a number of issues that may affect security, and pay attention, clearly define the roles and responsibilities involved for managing risks.

  Countermeasures: (1) disclosure of applicable logs and data, (2) partial/full disclosure of infrastructure details (patch levels and firewalls), (3) monitoring and alerting on necessary infor.

Data Protection in the Cloud

NIST Guidelines on Security and Privacy Issues and Recommendations



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 life cycle.

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.

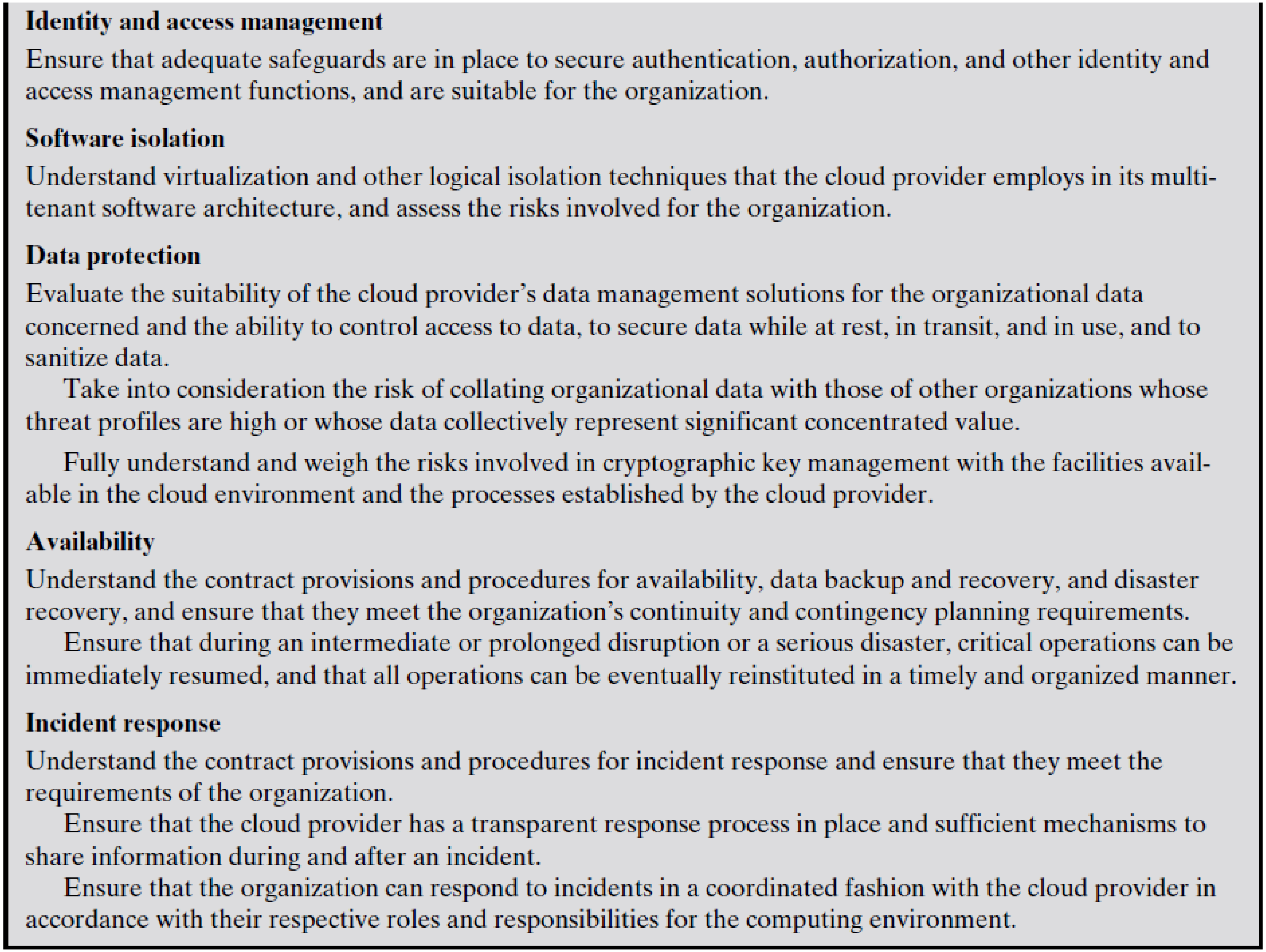
Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the life cycle of the system.

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 life cycle and across all system components.

Data Protection in the Cloud



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.

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.

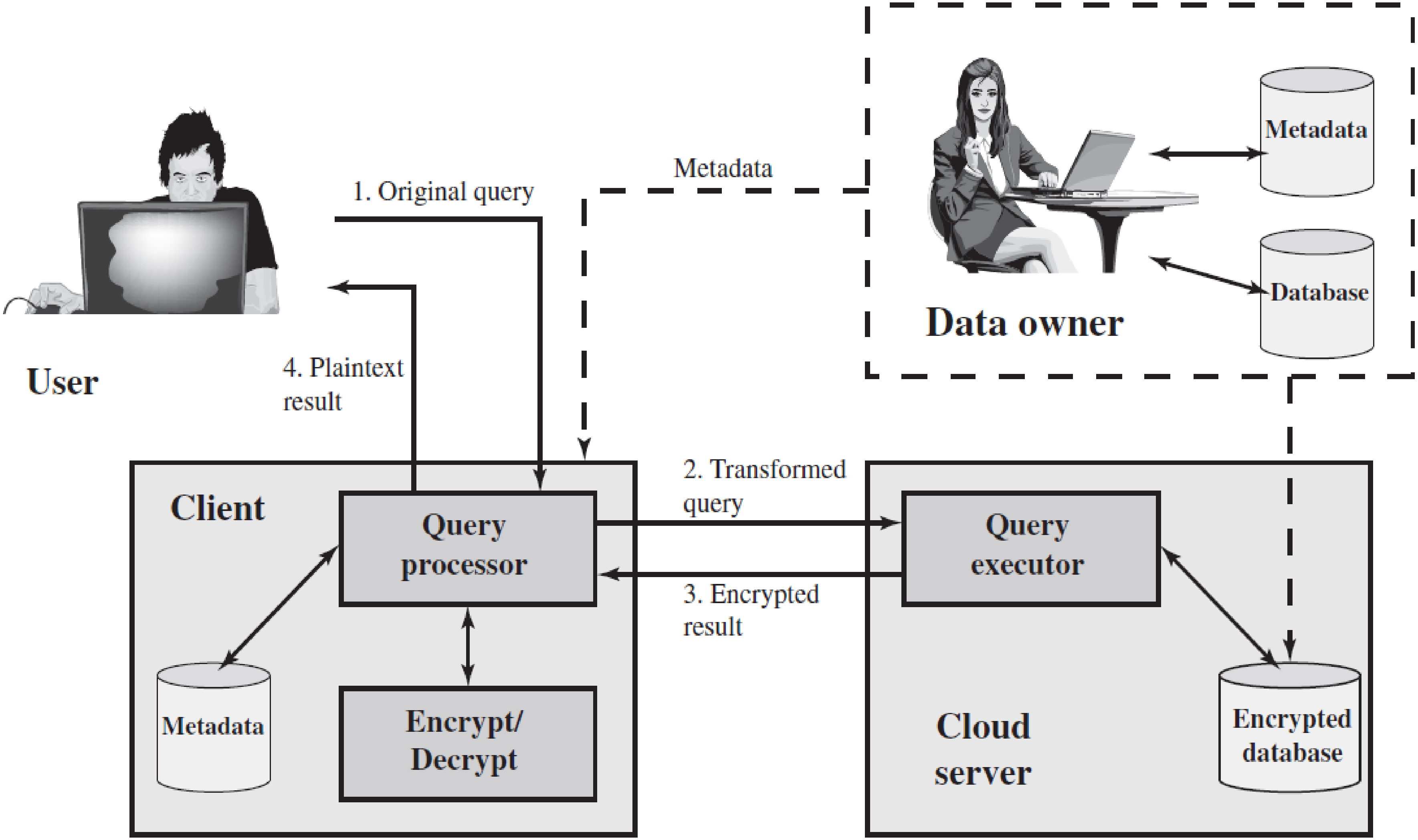
Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.

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.

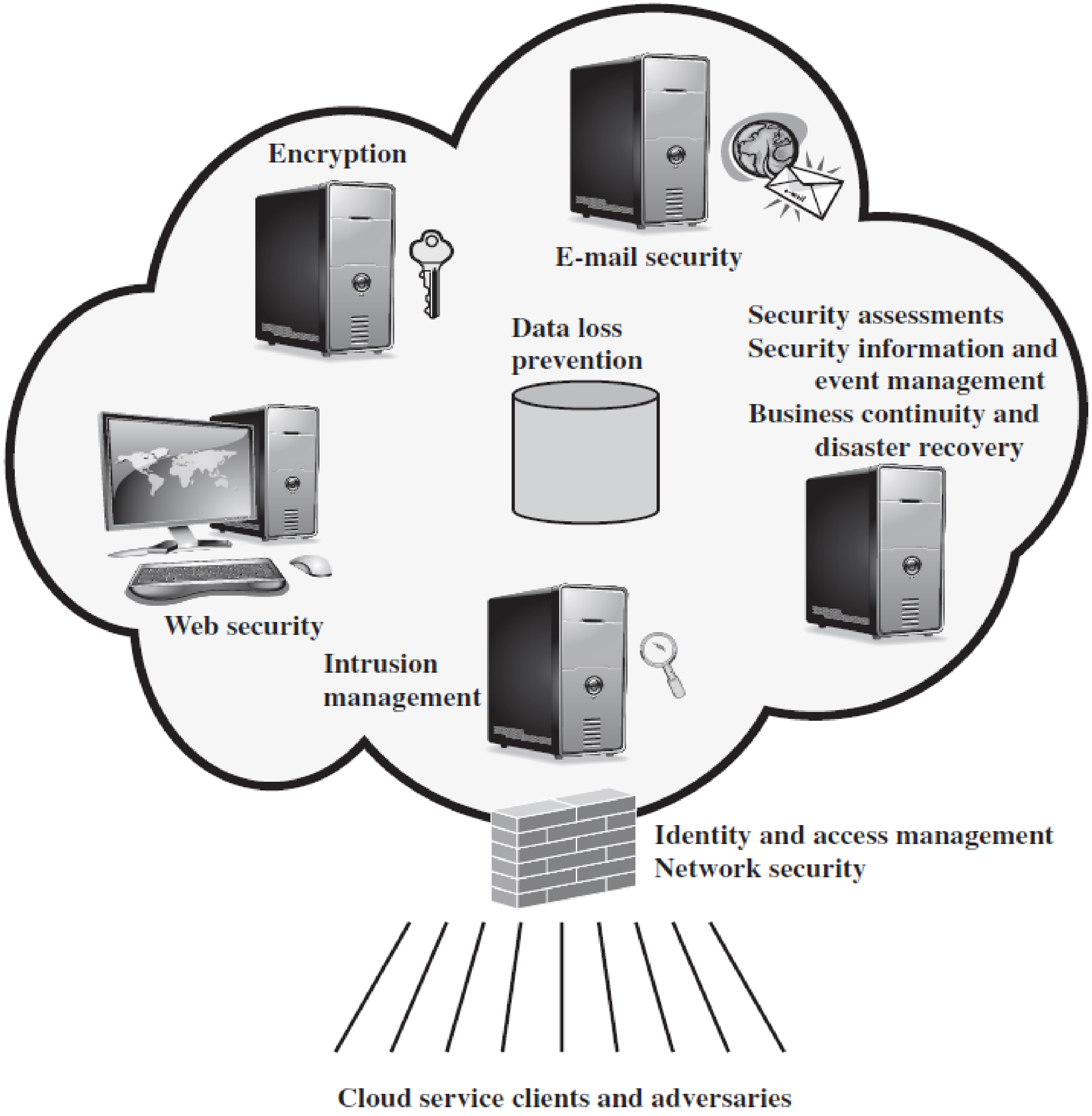
Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.



An Encryption Scheme for a Cloud-Based Database

Cloud Security as a Service (SecaaS)

- **SecaaS** is a segment of the **SaaS**, meant a package of security services offered by a service provider that offloads much of the security responsibility from an enterprise to the security service provider.
- The services: authentication, antivirus, antimalware-spyware, intrusion detection, security event management.
- **SecaaS** categories:
  - Identity and access management
  - Data loss prevention
  - Web security
  - Email security
  - Security assessments
  - Intrusion management
  - Security info. and event management
  - Encryption
  - Business continuity and disaster recovery
  - Network security


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

Cloud Security as a Service (SecaaS)

- **Identify and access management** - people, processes, and systems. Used to manage access to enterprise resources, assure the identity is verified, and grants correct level to access. It involves authentication and access control services.
- **Data loss prevention** - monitoring, protecting, and verifying the data, implemented by cloud client, make rules about what functions can be performed on data.
- **Web security** - real-time protection offered through software/appliance installation, or the cloud by proxying or redirecting web traffic to the **CP**. Antivirus, antimalware, usage policy enforcement, data backup, traffic control, web access control within it.
- **Email security** - provides control over inbound and outbound email, protects from phishing, malicious attachments, offers corporate policies, spam prevention, digital signatures and email encryption.
- **Security assessments** - third part audits of cloud services, provides tools and access points to facilitate assessment activities.

Cloud Security as a Service (SecaaS)

- **Intrusion management** - intrusion detection, prevention, and response, the core is intrusion detection systems (**IDS**s) and intrusion prevention systems (**IPS**s). **IDS** detects unauthorized accesses to host system, while **IPS** block traffic from intruders.

- **Security info. and event management** - aggregates log and event data from virtual and real networks, applications, and systems, provides real-time reporting and info./event alarming.

- **Encryption** - provides for data, as email traffic, client-specific network management info, and identifies info. Involves key management, application encryption, and data content access.

- **Business continuity and disaster recovery** - measures and mechanisms to ensure operational resiliency in the events or service interruptions. Includes flexible infrastructure, redundancy of functions and hardware, monitored operations, geographically distributed data centers, and network survivability.

- **Network security** - security services that allocate access, distribute, monitor, and protect resource services. Includes perimeter, server firewalls, DOS protection, in the network security service.

THANKS FOR WATCHING !!!

???