MSC-CS

CRYPTOGRAPHY & NETWORK SECURITY

UNIT - 5

Unit-5: Network Access Control and Cloud Security:

Network Access Control – Extensible Authentication Protocol – IEEE 802.1X Port-Based Network Access Control – Cloud Computing – Cloud Security Risk and Counter measures – Data Protection in the Cloud – Cloud Security as a Service – addressing Cloud Computing Security Concerns

Network Access Control (NAC)

- An umbrella term for managing access to a network
- Authenticates users logging into the network and determines what data they can access and actions they can perform
- Also examines the health of the user's computer or mobile device

Elements of a Network Access Control System

NAC systems deal with three categories of components:

Access requester (AR)

- Node that is attempting to access the network and may be any device that is managed by the NAC system, including workstations, servers, printers, cameras, and other IP-enabled devices
- Also referred to as *supplicants,* or clients

Policy server

- Determines what access should be granted
- Often relies on backend systems

Network access server (NAS)

- Functions as an access control point for users in remote locations connecting to an enterprise's internal network
- Also called a *media gateway, remote access server (RAS), or policy server*
- May include its own authentication services or rely on a separate authentication service from the policy server

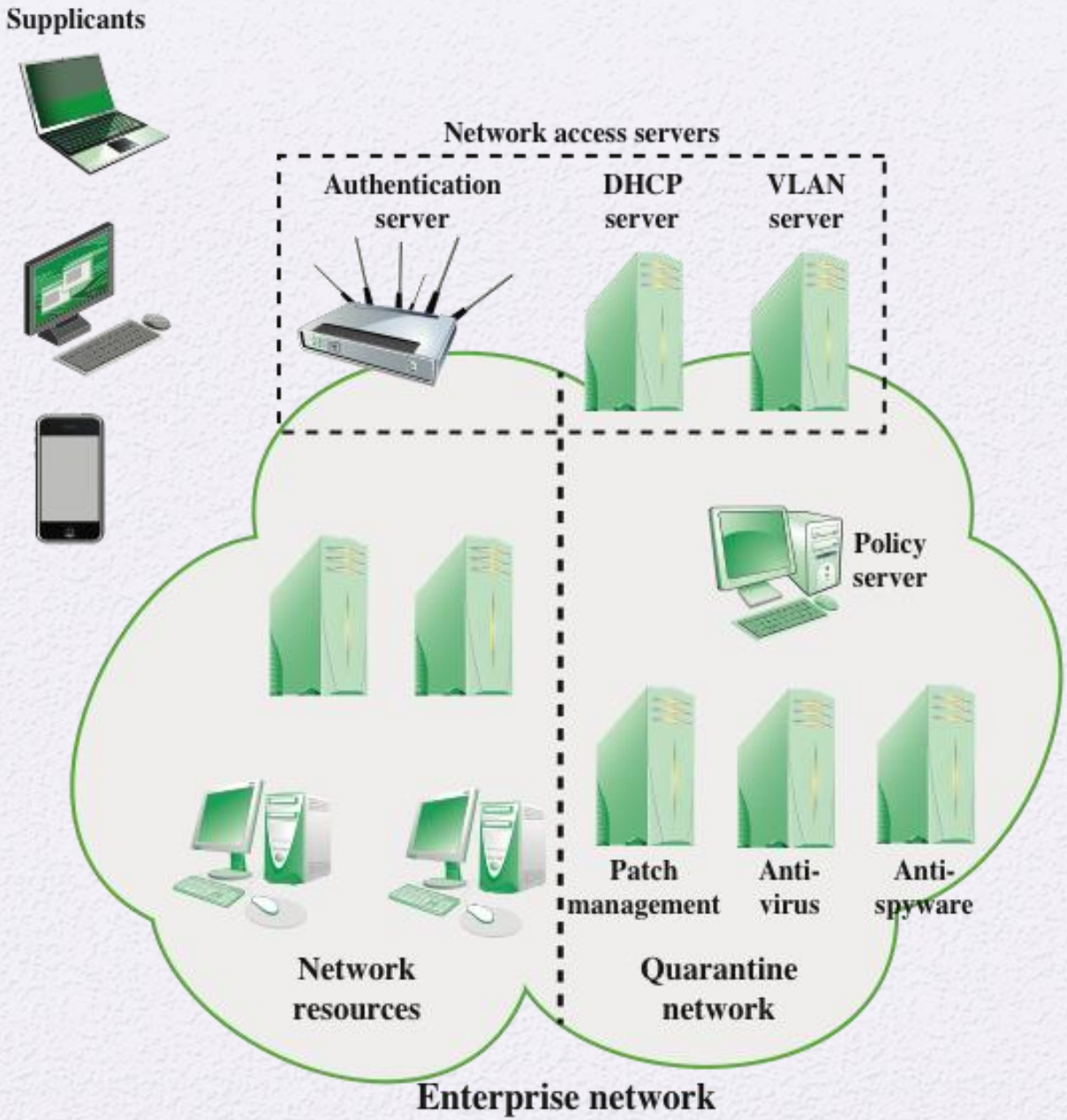


Figure 16.1 Network Access Control Context

Network Access Enforcement Methods

- The actions that are applied to ARs to regulate access to the enterprise network
  - Many vendors support multiple enforcement methods simultaneously, allowing the customer to tailor the configuration by using one or a combination of methods

Common NAC enforcement methods:

- IEEE 802.1X
- Virtual local area networks (VLANs)
- Firewall
- DHCP management

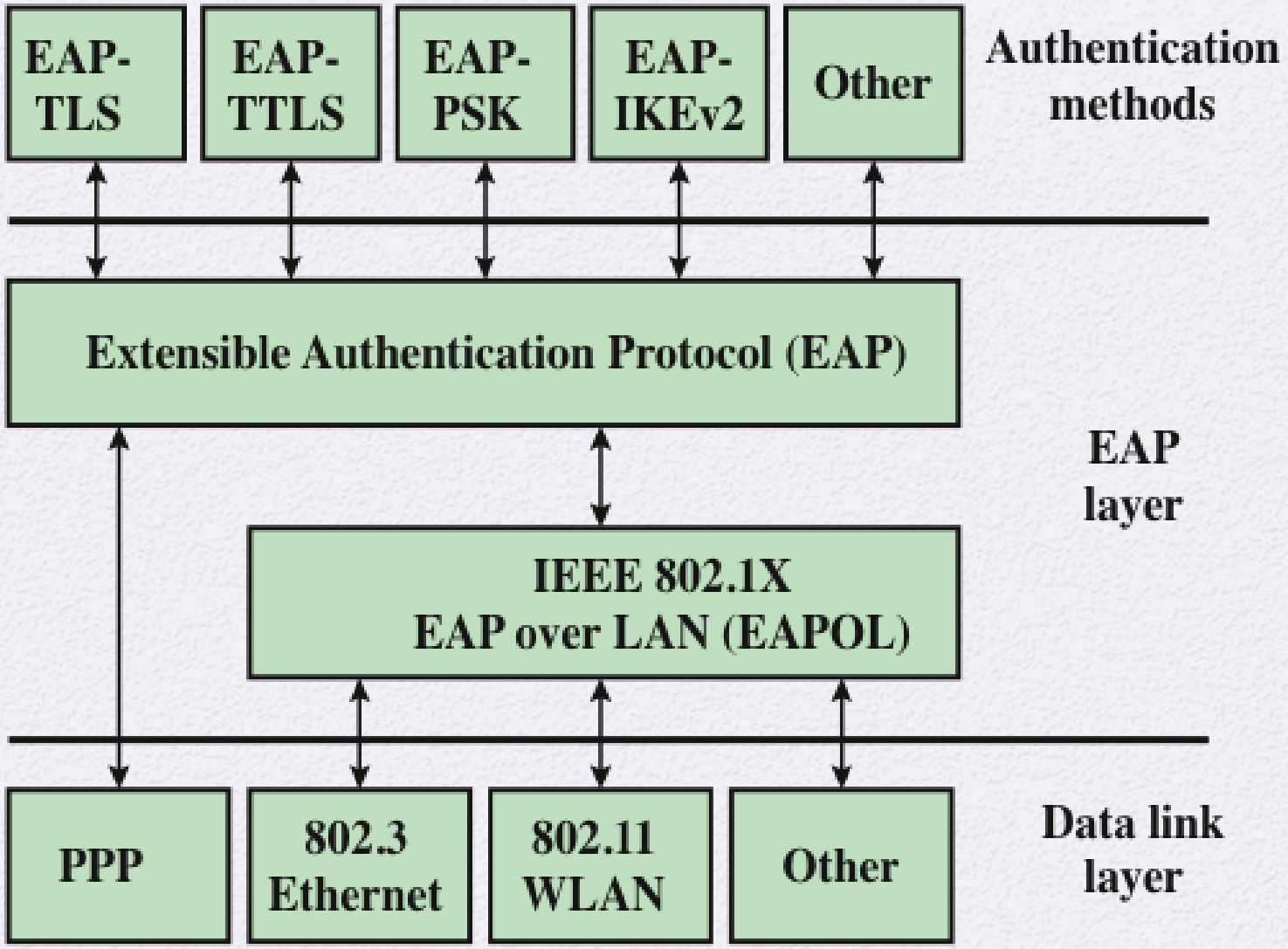


Figure 16.2 EAP Layered Context

Authentication Methods

- EAP provides a generic transport service for the exchange of authentication information between a client system and an authentication server
- The basic EAP transport service is extended by using a specific authentication protocol that is installed in both the EAP client and the authentication server

Commonly supported EAP methods:

- EAP Transport Layer Security
- EAP Tunneled TLS
- EAP Generalized Pre-Shared Key
- EAP-IKEv2

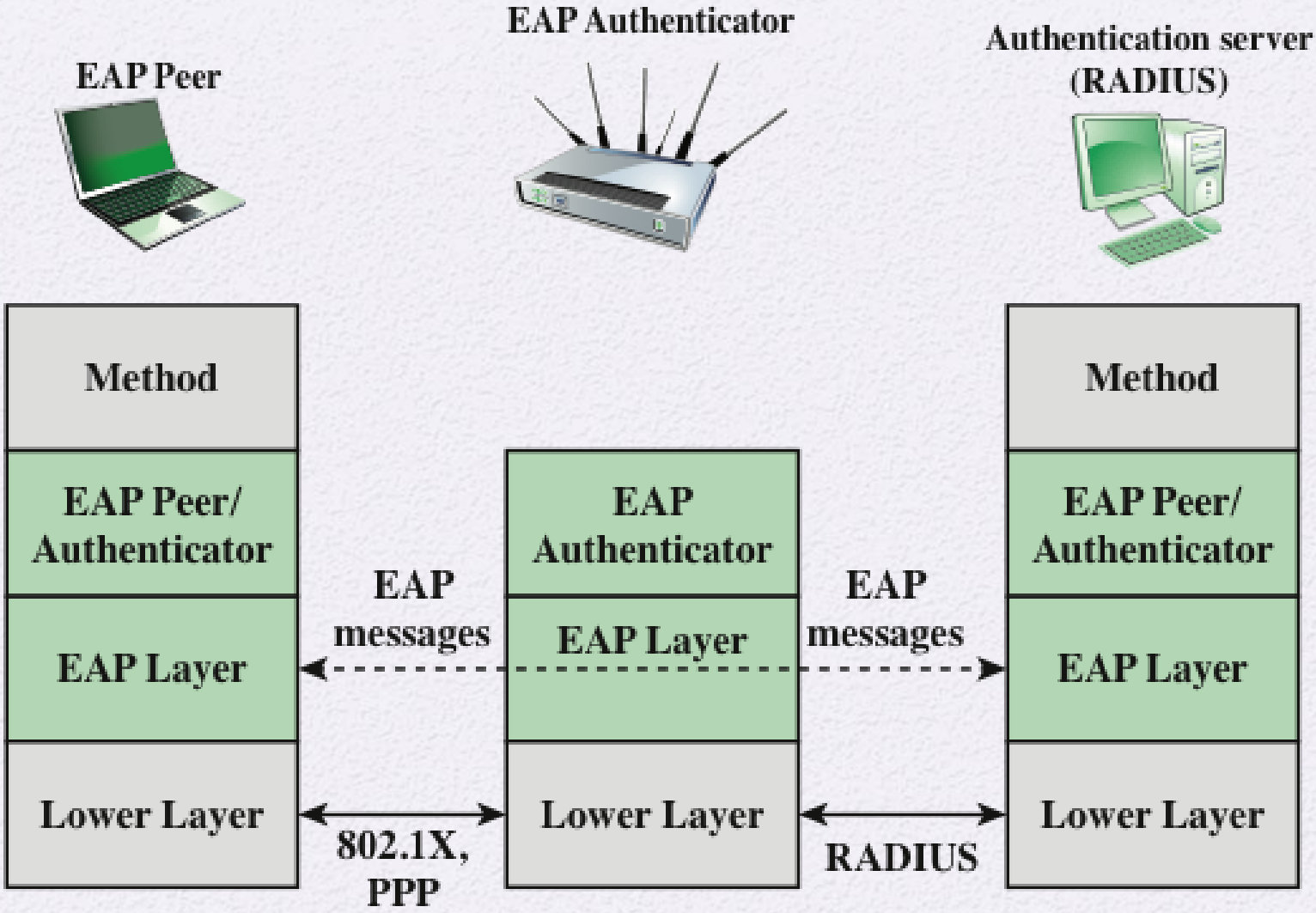


Figure 16.3 EAP Protocol Exchanges

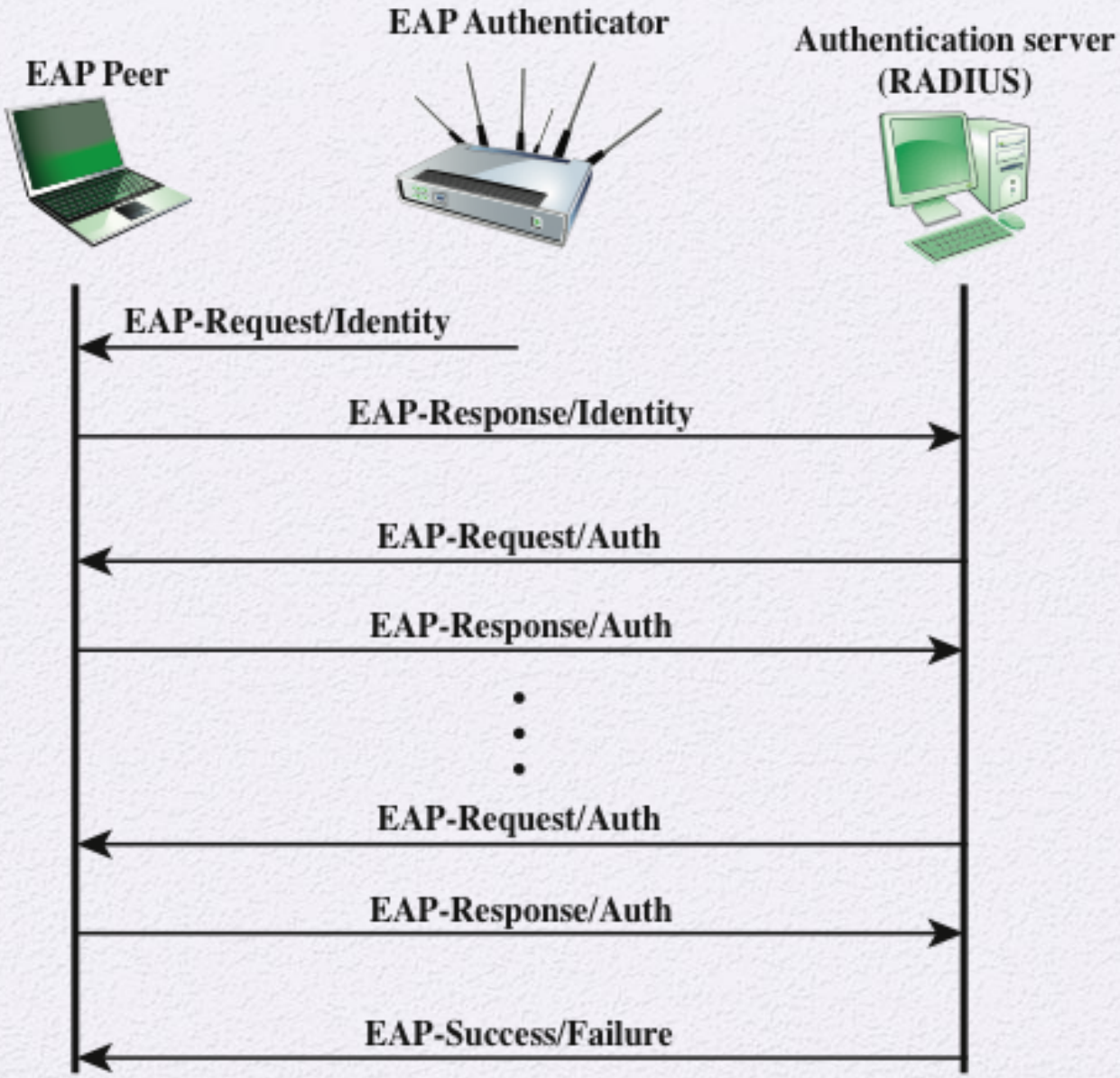


Figure 16.4 EAP Message Flow in Pass-Through Mode

Authenticator
An entity at one end of a point-to-point LAN segment that facilities authentication of the entity to the other end of the link.

Authentication exchange
The two-party conversation between systems performing an authentication process.

Authentication process
The cryptographic operations and supporting data frames that perform the actual authentication.

Authentication server (AS)
An entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by supplicant, whether the supplicant is authorized to access the services provided by the system in which the authenticator resides.

Authentication transport
The datagram session that actively transfers the authentication exchange between two systems.

Bridge port
A port of an IEEE 802.1D or 802.1Q bridge.

Edge port
A bridge port attached to a LAN that has no other bridges attached to it.

Network access port
A point of attachment of a system to a LAN. It can be a physical port, such as a single LAN MAC attached to a physical LAN segment, or a logical port, for example, an IEEE 802.11 association between a station and an access point.

Port access entity (PAE)
The protocol entity associated with a port. It can support the protocol functionality associated with the authenticator, the supplicant, or both.

Supplicant
An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an authenticator attached to the other end of that link.

Table 16.1

Terminology Related to IEEE 802.1X

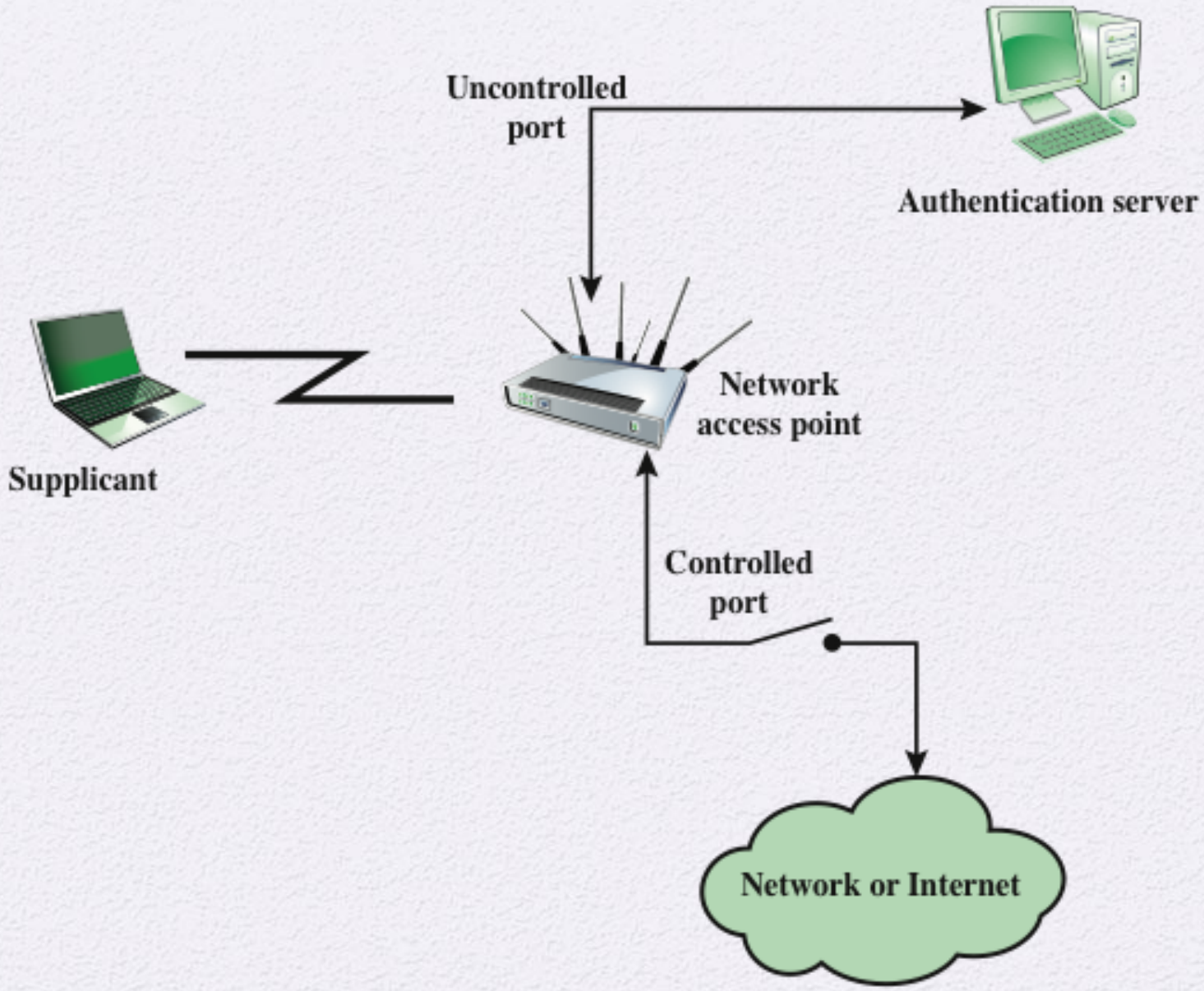


Figure 16.5 802.1X Access Control

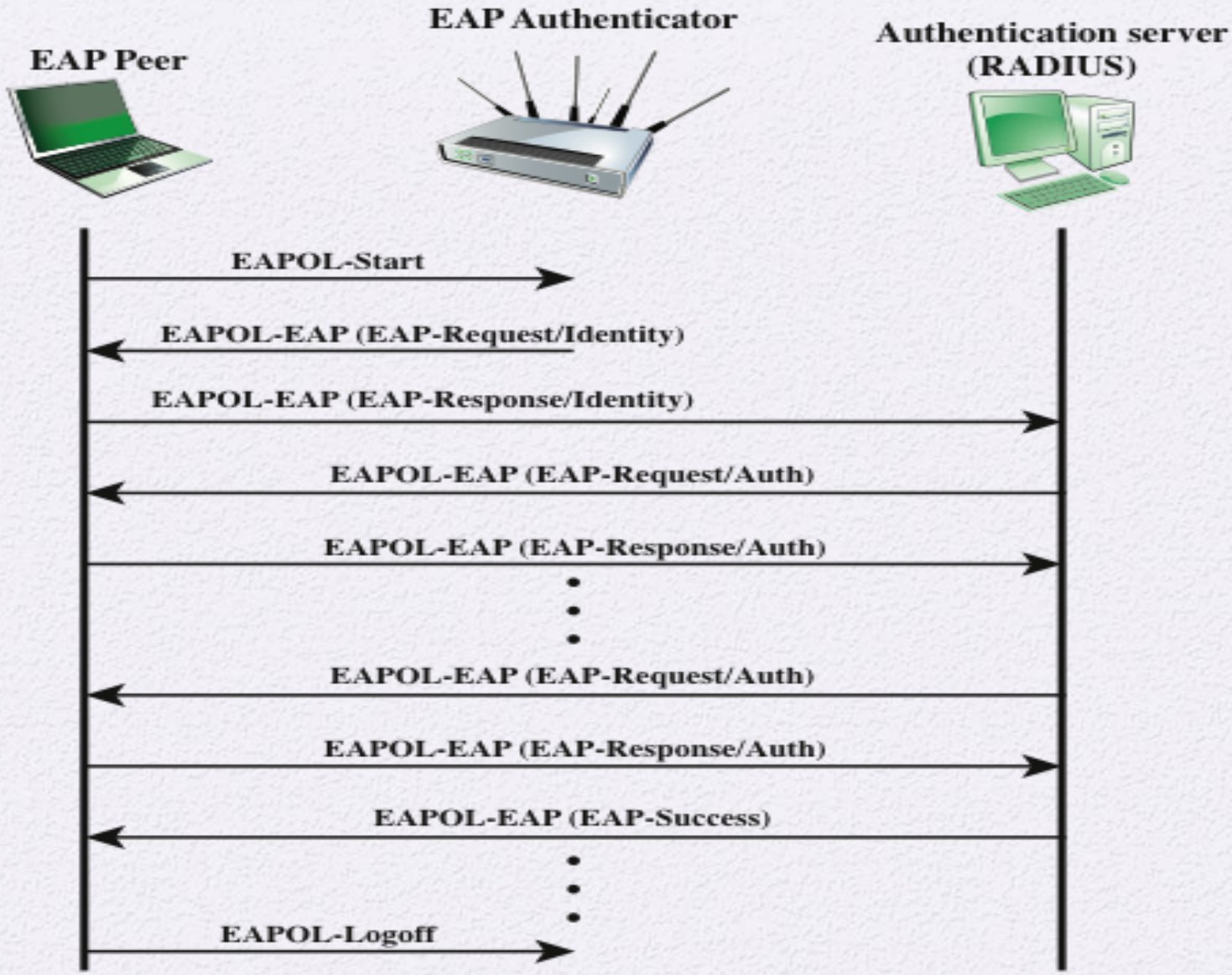


Figure 16.6 Example Timing Diagram for IEEE 802.1X

Cloud Computing

- NIST defines cloud computing, in NIST SP-800-145 (The NIST Definition of Cloud Computing), as follows:

  "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."

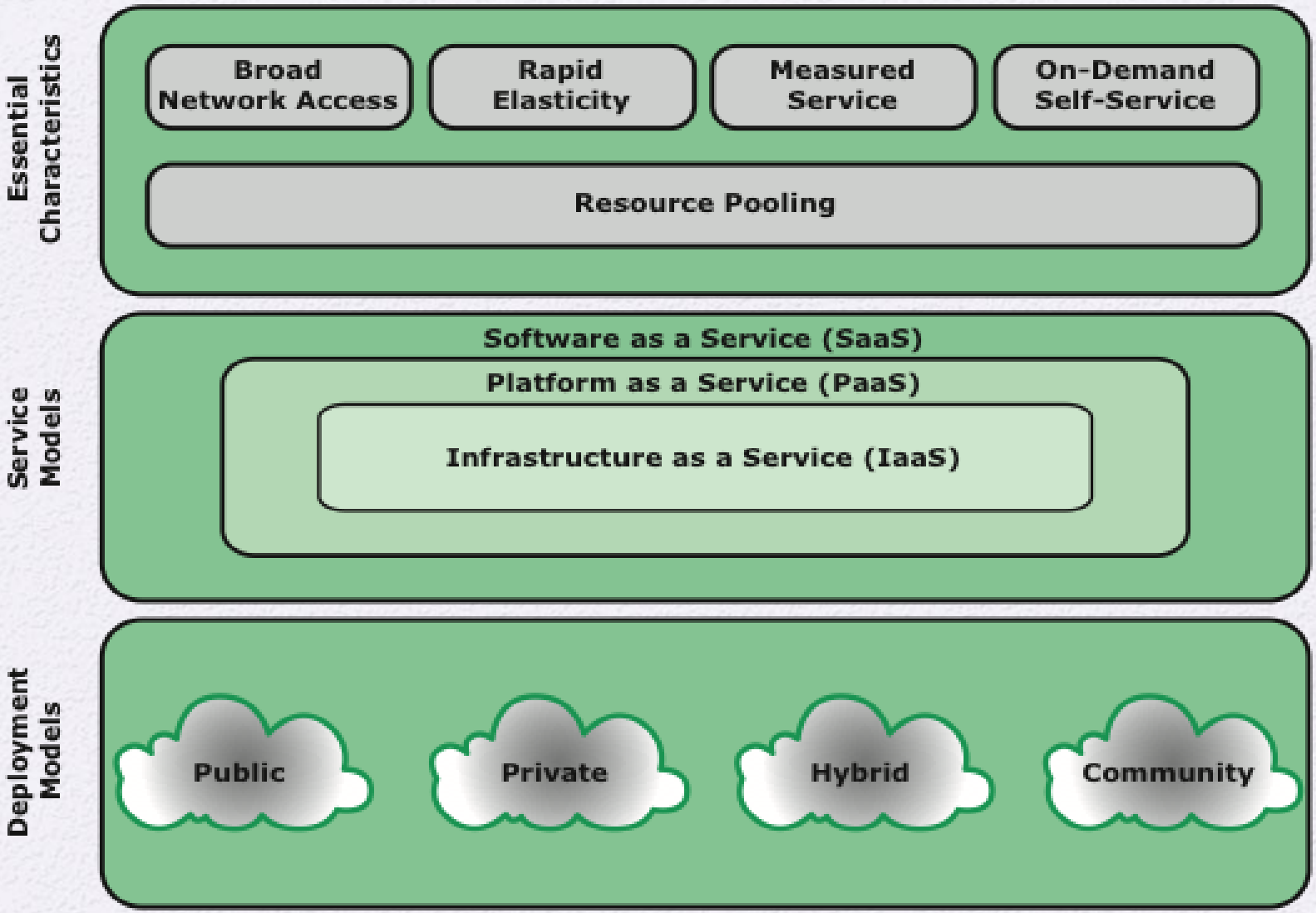


Figure 16.7 Cloud Computing Elements

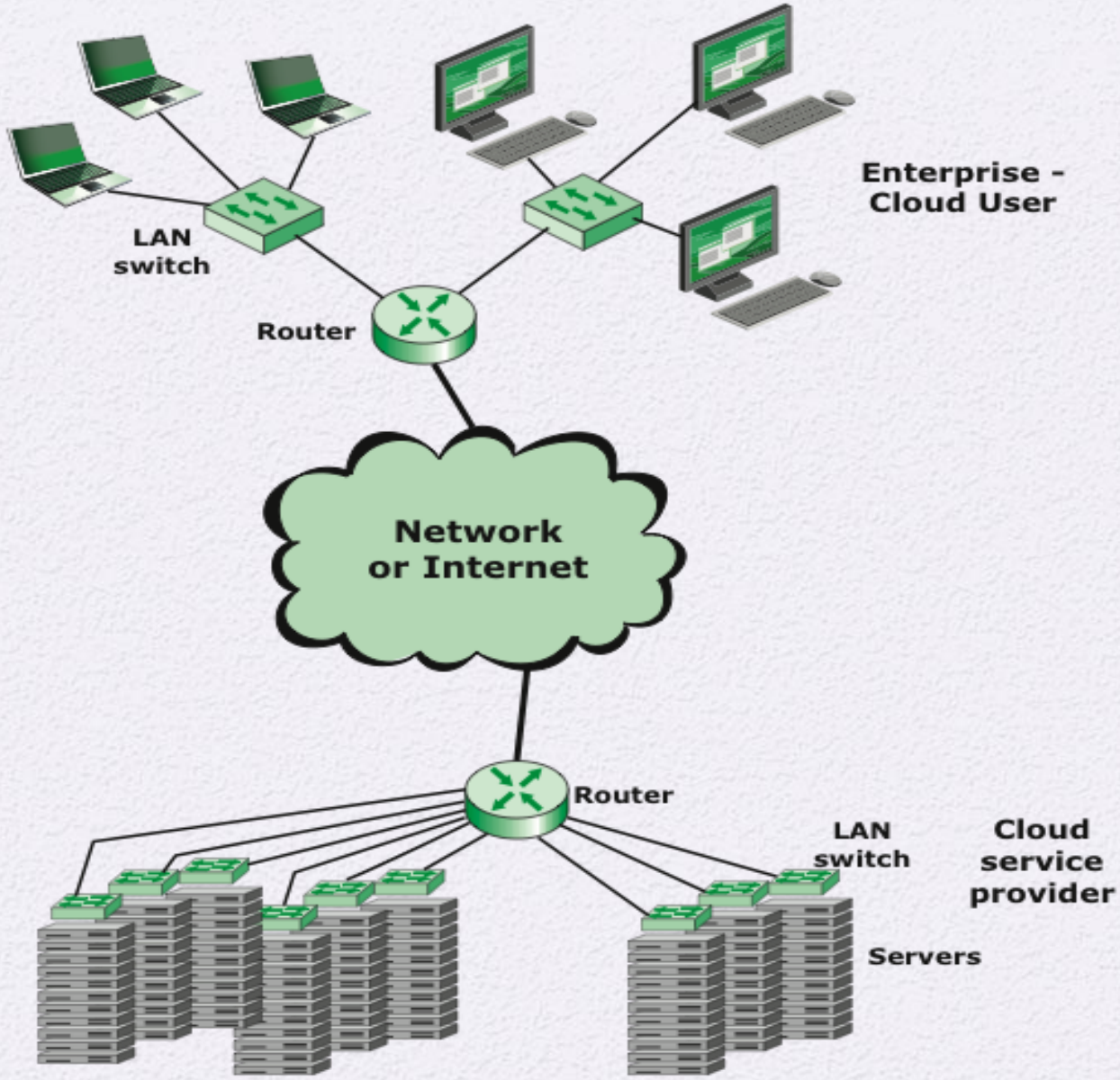
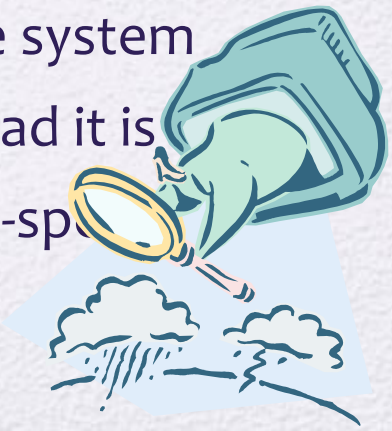


Figure 16.8 Cloud Computing Context

Cloud Computing Reference Architecture

- NIST SP 500-292 (NIST Cloud Computing Reference Architecture) establishes a 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."



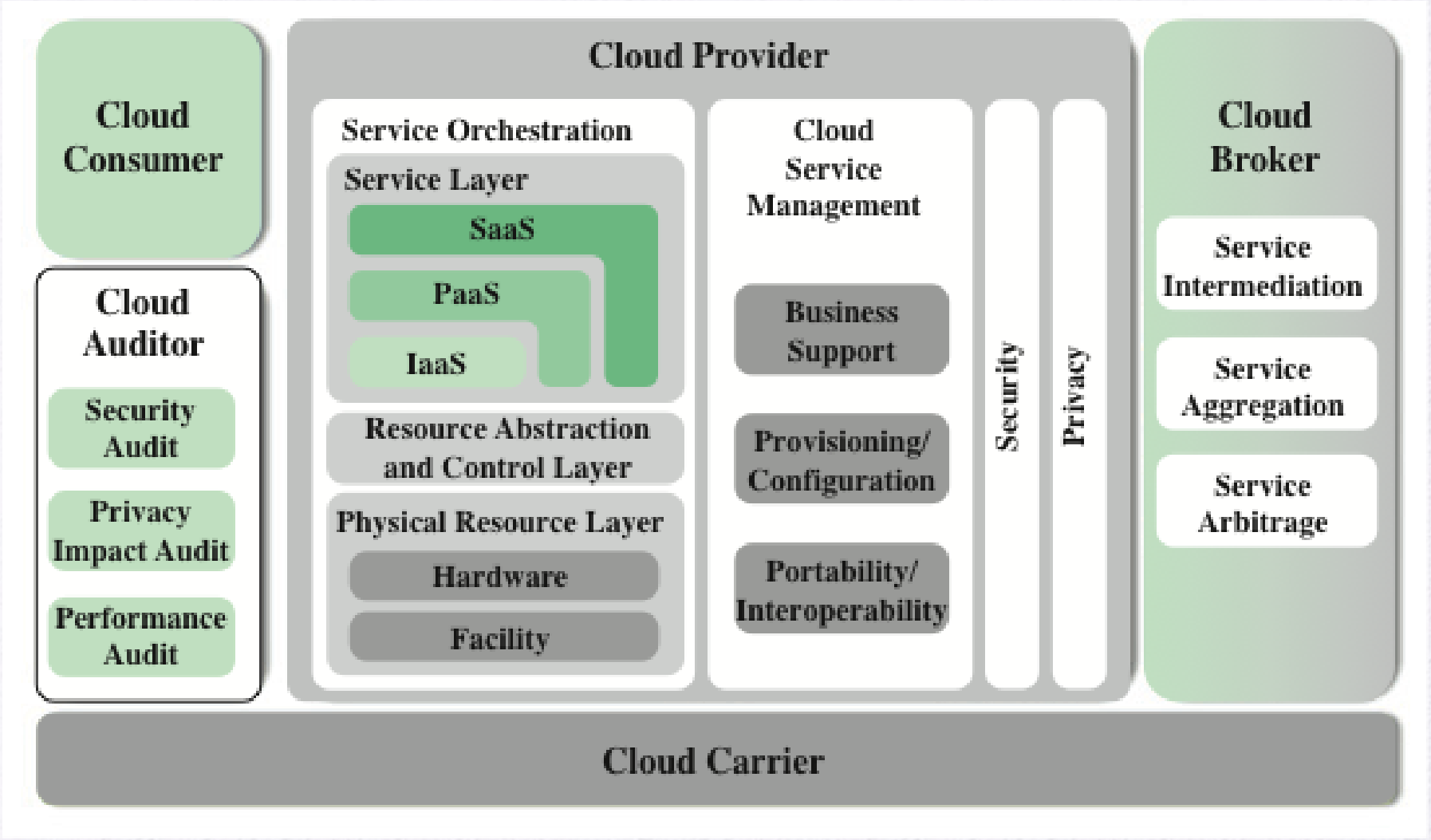
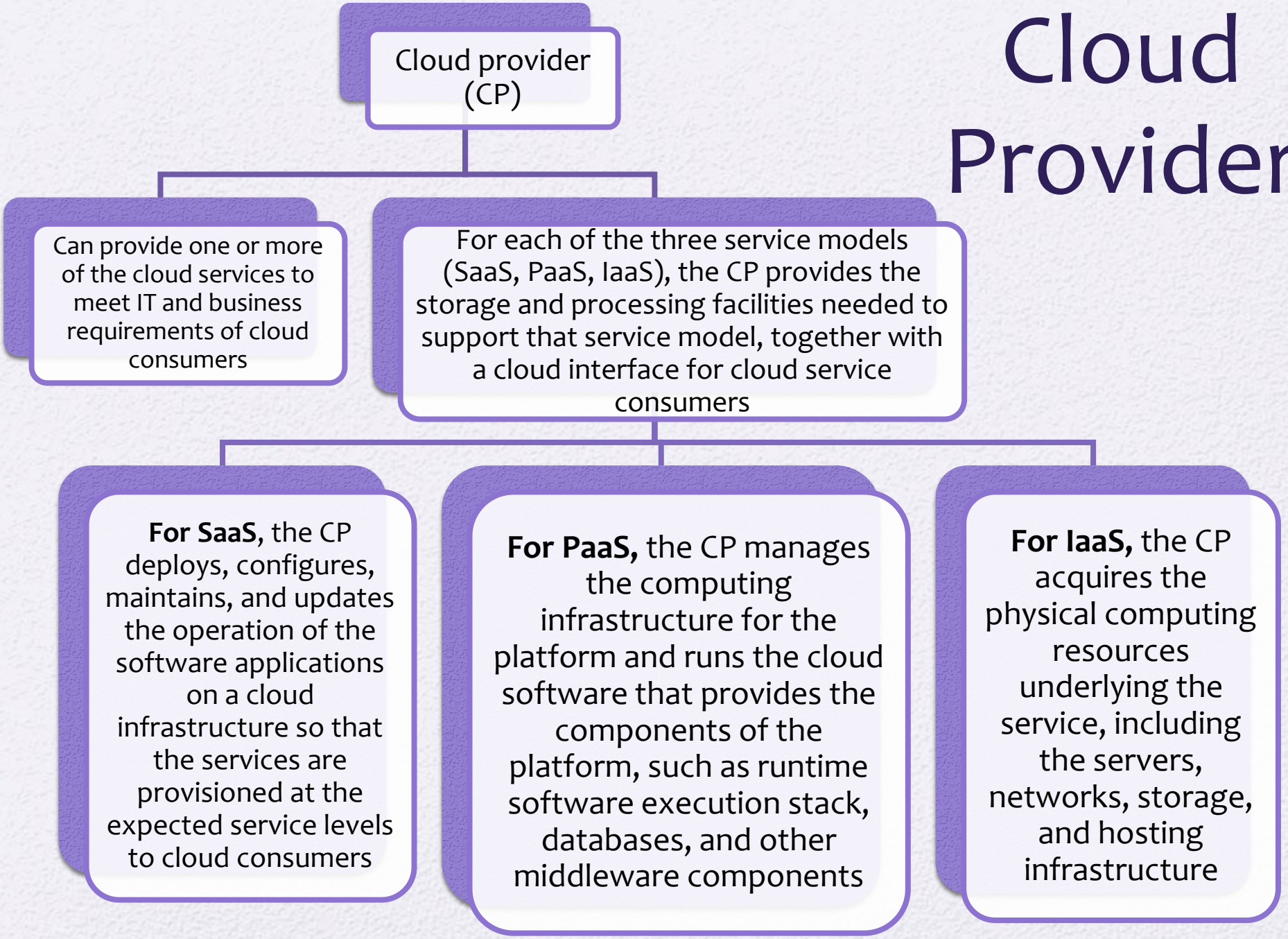


Figure 16.9 NIST Cloud Computing Reference Architecture

Cloud Provider



Roles and Responsibilities

Cloud carrier

- A networking facility that provides connectivity and transport of cloud services between cloud consumers and CPs

Cloud auditor

- An independent entity that can assure that the CP conforms to a set of standards

Cloud broker

- Useful when cloud services are too complex for a cloud consumer to easily manage
- Three areas of support can be offered by a cloud broker:
  - Service intermediation
    - Value-added services such as identity management, performance reporting, and enhanced security
  - Service aggregation
    - The broker combines multiple could services to meet consumer needs not specifically addressed by a single CP, or to optimize performance or minimize cost
  - Service arbitrage
    - A broker has the flexibility to choose services from multiple agencies

Cloud Security Risks and Countermeasures

- The Cloud Security Alliance [CSA10] lists the following as the top cloud specific security threats, together with suggested countermeasures:

Abuse and nefarious use of cloud computing

- Countermeasures: stricter initial registration and validation processes; enhanced credit card fraud monitoring and coordination; comprehensive introspection of customer network traffic; monitoring public blacklists for one's own network blocks

Malicious insiders

- Countermeasures: enforce strict supply chain management and conduct a comprehensive supplier assessment; specify human resource requirements as part of legal contract; require transparency into overall information security and management practices, as well as compliance reporting; determine security breach notification processes

Risks and Countermeasures (continued)

Insecure interfaces and APIs

Countermeasures:

analyzing the security model of CP interfaces; ensuring that strong authentication and access controls are implemented in concert with encryption machines; understanding the dependency chain associated with the API

Shared technology issues

Countermeasures:

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:

implement strong API access control; encrypt and protect integrity of data in transit; analyze data protection at both design and run time; implement strong key generation, storage and management, and destruction practices

Risks and Countermeasures (continued)

- Account or service hijacking
  - Countermeasures: 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 CP security policies and SLAs
- Unknown risk profile
  - Countermeasures: disclosure of applicable logs and data; partial/full disclosure of infrastructure details; monitoring and alerting on necessary information

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.

Table 16.3

NIST Guidelines on Security and Privacy Issues and Recommend ations

Data Protection in the Cloud

- The threat of data compromise increases in the cloud
- Database environments used in cloud computing can vary significantly
  - Multi-instance model
    - Provides a unique DBMS running on a virtual machine instance for each cloud subscriber
    - This gives the subscriber complete control over role definition, user authorization, and other administrative tasks related to security
  - Multi-tenant model
    - Provides a predefined environment for the cloud subscriber that is shared with other tenants, typically through tagging data with a subscriber identifier
    - Tagging gives the appearance of exclusive use of the instance, but relies on the CP to establish and maintain a sound secure database environment

Data Protection in the Cloud

- Data must be secured while at rest, in transit, and in use, and access to the data must be controlled
- The client can employ encryption to protect data in transit, though this involves key management responsibilities for the CP
- 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 CP having no access to the encryption key
- A straightforward solution to the security problem in this context is to encrypt the entire database and not provide the encryption/decryption keys to the service provider
  - The user has little ability to access individual data items based on searches or indexing on key parameters
  - The user would have to download entire tables from the database, decrypt the tables, and work with the results
  - To provide more flexibility it must be possible to work with the database in its encrypted form

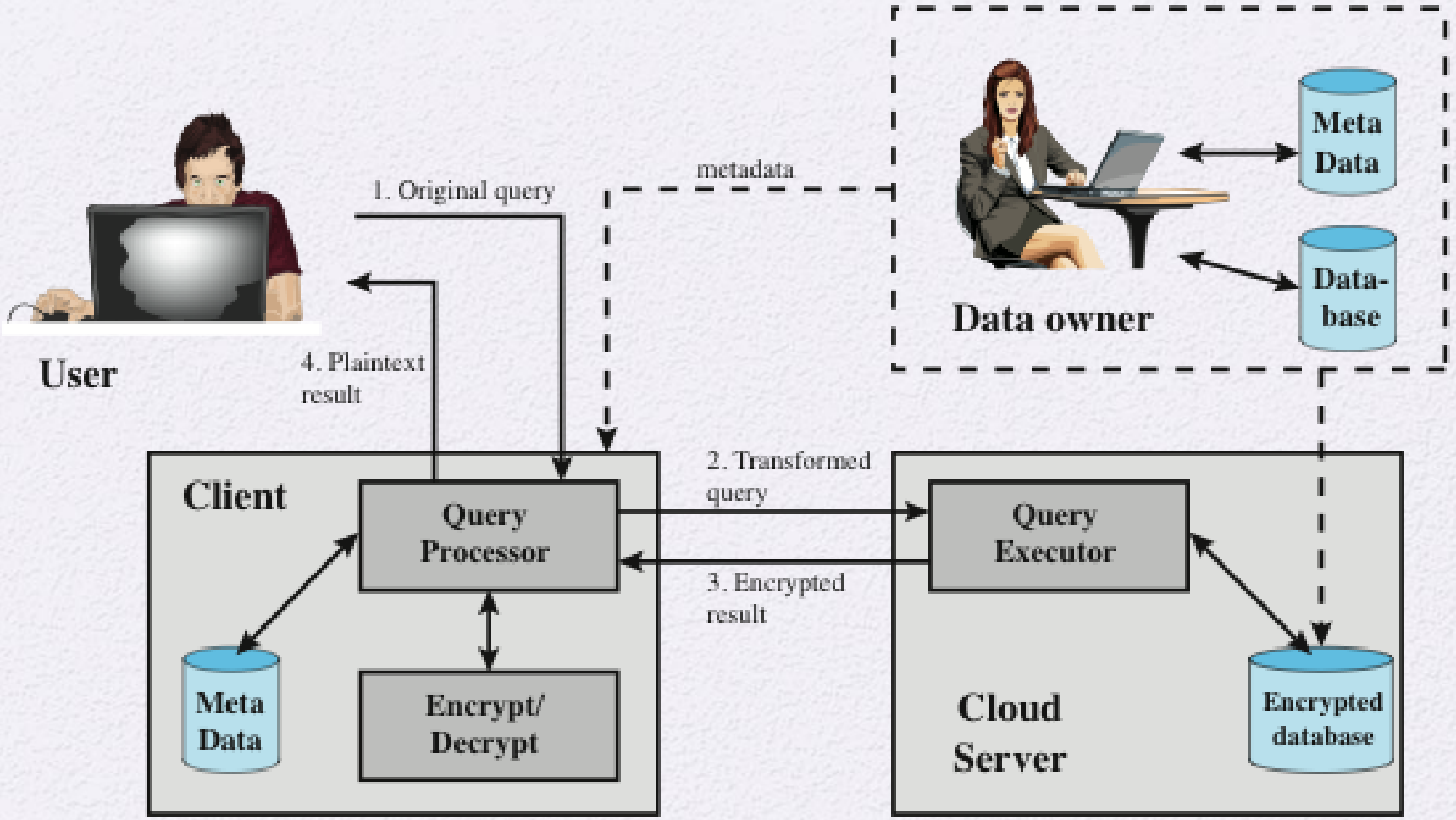


Figure 16.10 An Encryption Scheme for a Cloud-Based Database

Cloud Security as a Service (SecaaS)

- The Cloud Security Alliance 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

- The Cloud Security Alliance 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

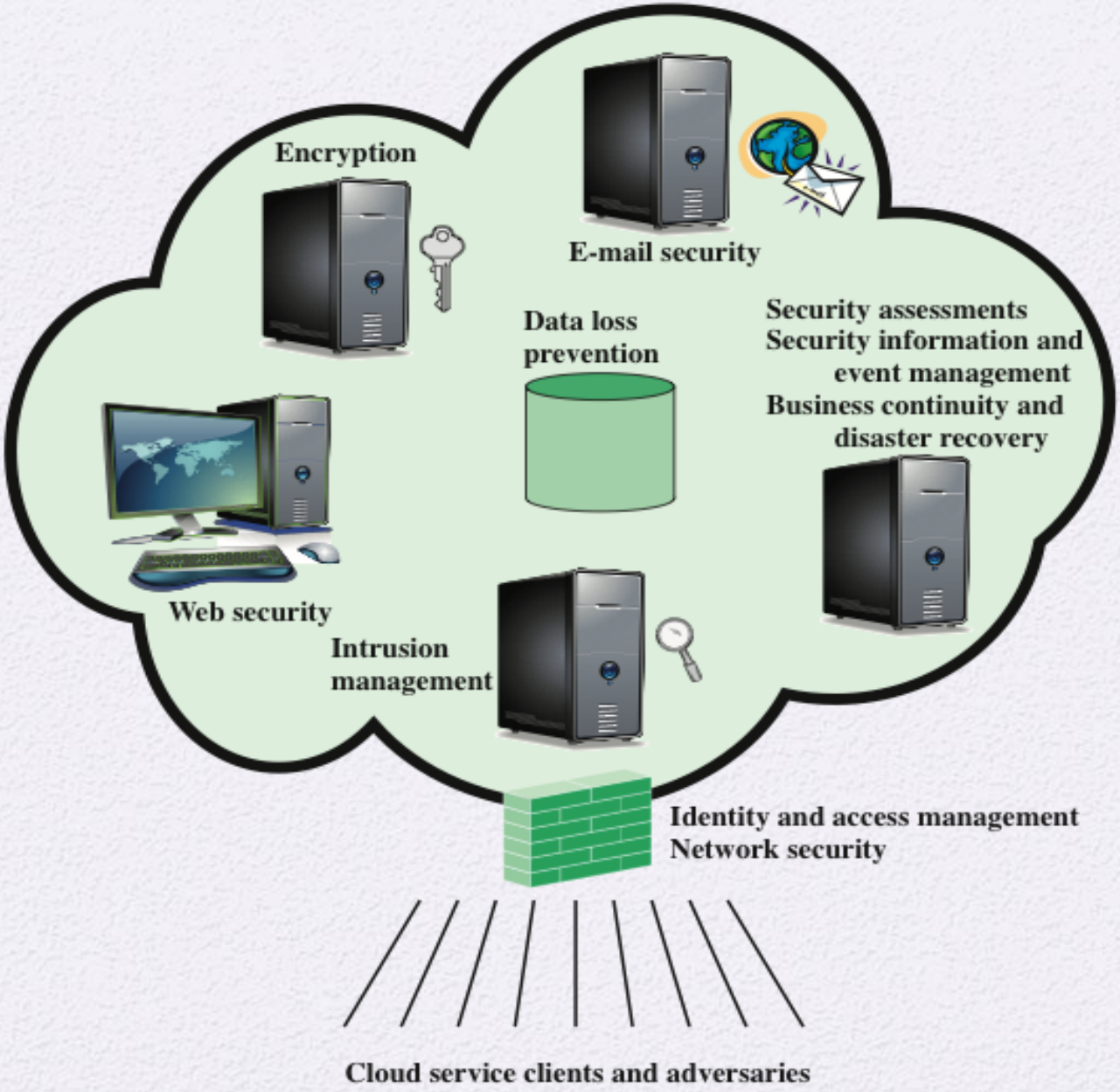


Figure 16.11 Elements of Cloud Security as a Service

Addressing cloud computing Security Concerns

Table 16.4 Control Functions and Classes

Technical	Operational	Management
Access Control	Awareness and Training	Certification, Accreditation, and Security Assessment
Audit and Accountability	Configuration and Management	Planning Risk Assessment
Identification and Authentication	Contingency Planning	System and Services Acquisition
System and Communication Protection	Incident Response	
	Maintenance	
	Media Protection	
	Physical and Environmental Protection	
	Personnel Security System and Information Integrity	