8: Cloud Security

IT6406 – Network Security and Audit

Level III - Semester 6

Overview

This lecture aims at providing the fundamentals of information security in the context of cloud computing. It provide the details on what risks are available to cloud environments and what strategies can be used to minimise or eliminate them.

Intended Learning Outcomes

At the end of this lesson, you will be able to;

- Describe key concepts of cloud computing and its elements.
- Describe the reference architecture introduced by NIST.
- Describe different security risk available to cloud environments and potential countermeasures against them.
- Discuss the potential of providing cloud security as a service.

List of sub topics

8.1 Cloud computing

- 8.1.1 Cloud Computing Elements
- 8.1.2 Cloud Computing Reference Architecture

8.2 Cloud Security Risks and Countermeasures

8.3 Data Protection in the Cloud

8.4 Cloud Security as a Service

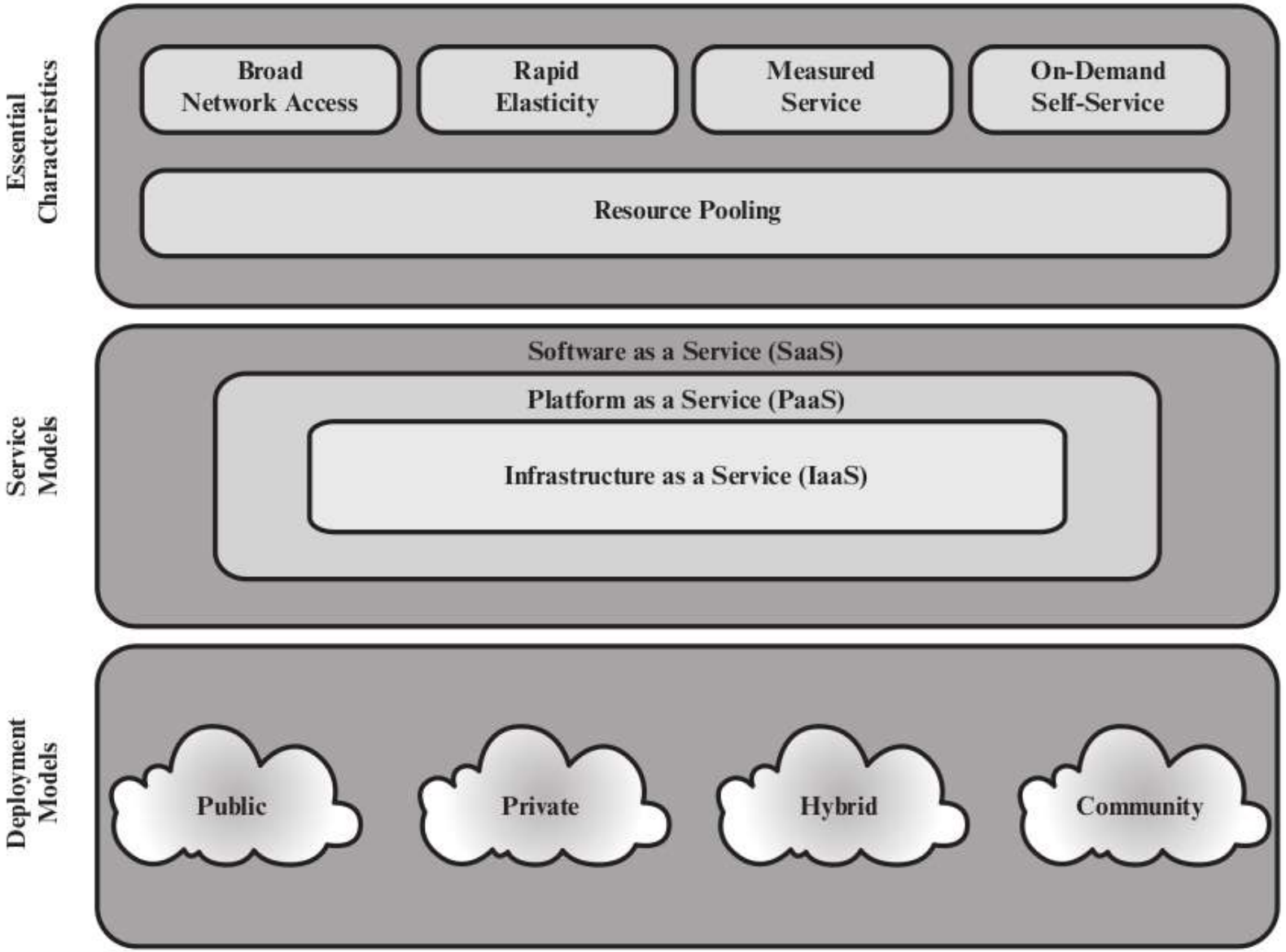
8.5 Addressing Cloud Computing Security Concerns

8.1 Cloud Computing

- Many organizations are moving a substantial portion of or even all information technology (IT) operations to an Internet-connected infrastructure: **cloud computing**.

- The NIST definition of cloud computing:
  - 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.

8.1 Cloud Computing



8.1 Cloud Computing

Essential characteristics of cloud computing:

- Broad network access
- Rapid elasticity
- Measured service
- On-demand self-service
- Resource pooling

8.1 Cloud Computing

Essential characteristics of cloud computing (cont.):

- **Broad network access:**

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloud-based software services.

8.1 Cloud Computing

Essential characteristics of cloud computing (cont.):

- **Rapid elasticity:**

Cloud computing gives you the ability to expand and reduce resources according to your specific service requirement. For example, you may need a large number of server resources for the duration of a specific task. You can then release these resources upon completion of the task.

8.1 Cloud Computing

Essential characteristics of cloud computing (cont.):

- **Measured service:**

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

8.1 Cloud Computing

Essential characteristics of cloud computing (cont.):

- **On-demand self-service:**

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. Because the service is on demand, the resources are not permanent parts of your IT infrastructure.

8.1 Cloud Computing

Essential characteristics of cloud computing (cont.):

- **Resource pooling:**

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and re-assigned according to consumer demand.

There is a degree of location independence in that the customer generally has no control or knowledge of the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center).

Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

8.1 Cloud Computing

Service models as defined by NIST:

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

8.1 Cloud Computing

Service models as defined by NIST (cont.):

- **Software as a service (SaaS):**

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.

The applications are accessible from various client devices through a thin client interface such as a Web browser.

Instead of obtaining desktop and server licenses for software products it uses, an enterprise obtains the same functions from the cloud service.

SaaS saves the complexity of software installation, maintenance, upgrades, and patches.

8.1 Cloud Computing

Service models as defined by NIST (cont.):

- **Platform as a service (PaaS):**

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.

PaaS often provides middleware-style services such as database and component services for use by applications. In effect, PaaS is an operating system in the cloud.

8.1 Cloud Computing

Service models as defined by NIST (cont.):

- **Infrastructure as a service (IaaS):**

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

IaaS enables customers to combine basic computing services, such as number crunching and data storage, to build highly adaptable computer systems.

8.1 Cloud Computing

Deployment models as defined by NIST:

- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud

8.1 Cloud Computing

Deployment models as defined by NIST (cont.):

- **Public cloud:**

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

The cloud provider is responsible both for the cloud infrastructure and for the control of data and operations within the cloud.

8.1 Cloud Computing

Deployment models as defined by NIST (cont.):

- **Private cloud:**

The cloud infrastructure is operated solely for an organization.

It may be managed by the organization or a third party and may exist on premise or off premise.

The cloud provider (**CP**) is responsible only for the infrastructure and not for the control.

8.1 Cloud Computing

Deployment models as defined by NIST (cont.):

- **Community cloud:**

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

It may be managed by the organizations or a third party and may exist on premise or off premise.

8.1 Cloud Computing

Deployment models as defined by NIST (cont.):

- **Hybrid cloud:**

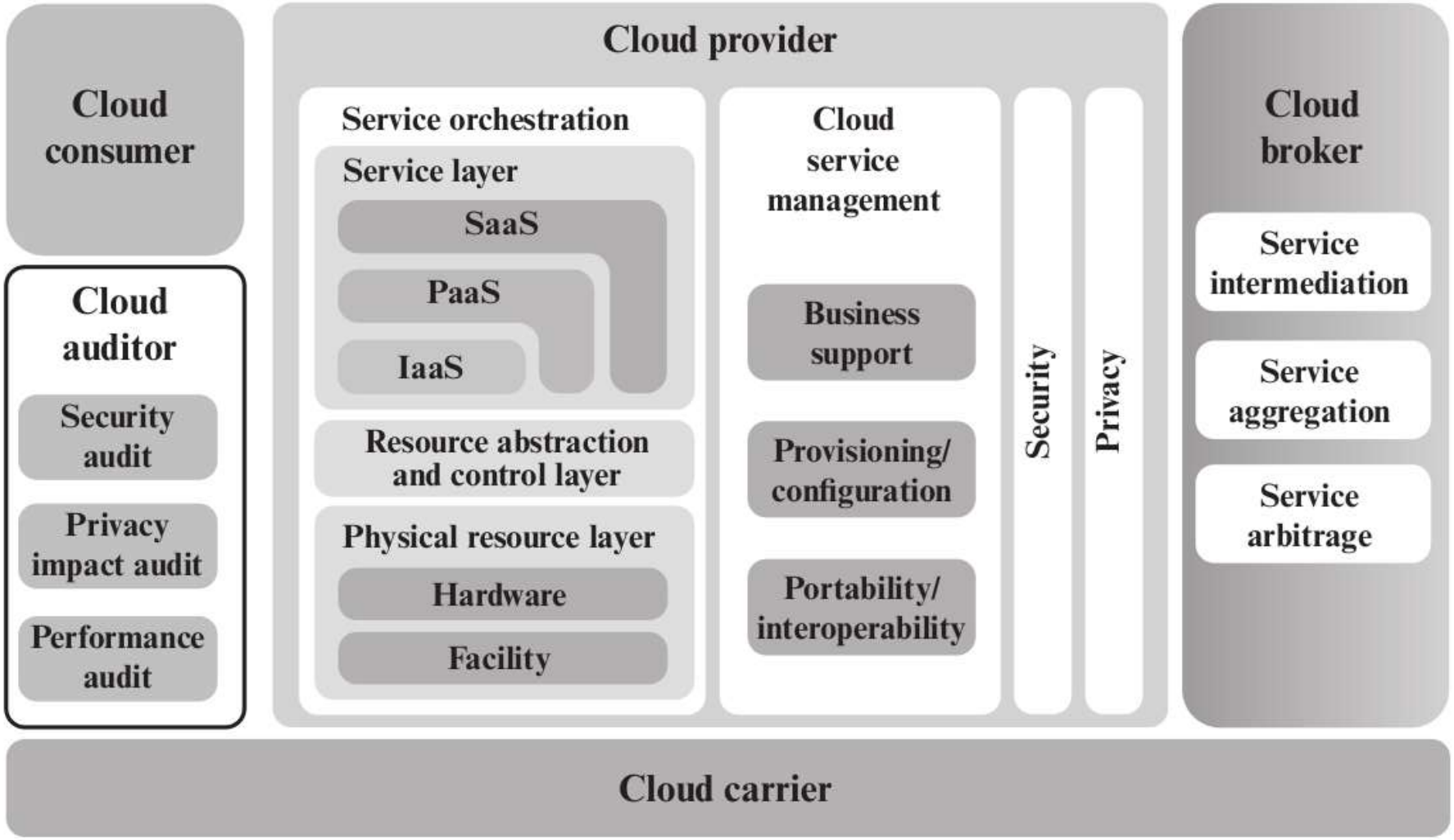
The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

8.1 Cloud Computing

- NIST provides a reference architecture for cloud computing.
- 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.

8.1 Cloud Computing

NIST Cloud Computing Reference Architecture



8.1 Cloud Computing

- Five major actors in NIST reference architecture:
- **Cloud consumer:** Maintains a business relationship with, and uses service from cloud providers.
- **Cloud provider:** Is responsible for making a service available to interested parties.
- **Cloud auditor:** Conducts independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.
- **Cloud broker:** Manages the use, performance, and delivery of cloud services, and negotiates relationships between CPs and cloud consumers.
- **Cloud carrier:** Provides connectivity and transport of cloud services from CPs to cloud consumers.

8.2 Cloud Security Risks and Countermeasures

- Due to the operational models and technologies used to enable cloud service, cloud computing may present risks that are specific to the cloud environment.

- Cloud-specific security threats:
  - Abuse and nefarious use of cloud computing
  - Insecure interfaces and APIs
  - Malicious insiders
  - Shared technology issues
  - Data loss or leakage
  - Account or service hijacking
  - Unknown risk profile

8.2 Cloud Security Risks and Countermeasures

Abuse and nefarious use of cloud computing:

- For many CPs, it is relatively easy to register and begin using cloud services, some even offering free limited trial periods. This enables attackers to get inside the cloud to conduct various attacks, such as spamming, malicious code attacks, and denial of service.

- 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

8.2 Cloud Security Risks and Countermeasures

Insecure interfaces and APIs:

- CPs expose a set of software interfaces or APIs that customers use to manage and interact with cloud services.
- The security and availability of general cloud services are dependent upon the security of these basic APIs.
- These interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.
- Countermeasures:
  - analyzing the security model of CP interfaces
  - ensuring that strong authentication and access controls are implemented in concert with encrypted transmission
  - understanding the dependency chain associated with the API.

8.2 Cloud Security Risks and Countermeasures

Malicious insiders:

- An organization relinquishes direct control over many aspects of security and confers an unprecedented level of trust onto the CP.
- One grave concern is the risk of malicious insider activity.
- 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.

8.2 Cloud Security Risks and Countermeasures

Shared technology issues:

- IaaS vendors deliver their services in a scalable way by sharing infrastructure; the underlying components that make up this infrastructure (CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture.
- The use of isolated virtual machines for individual clients is still vulnerable to attack, by both insiders and outsiders
- 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.

8.2 Cloud Security Risks and Countermeasures

Data loss or leakage:

- For many clients, the most devastating impact from a security breach is the loss or leakage of data. We address this issue in the next subsection.

- 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.

8.2 Cloud Security Risks and Countermeasures

Account or service hijacking:

- Account or service hijacking, usually with stolen credentials, remains a top threat.
- With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity, and availability of those services.
- Countermeasures:
  - Prohibit the sharing of account credentials between users and services.
  - Leverage two-factor authentication techniques.
  - Employ proactive monitoring to detect unauthorized activity.
  - Understand CP security policies and SLAs.

8.2 Cloud Security Risks and Countermeasures

Unknown risk profile:

- In using cloud infrastructures, the client necessarily pass the control to the CP on a number of issues that may affect security; thus the client must pay attention to and clearly define the roles and responsibilities involved for managing risks.

- For example, employees may deploy applications and data resources at the CP without observing the normal policies and procedures for privacy, security, and oversight.

- Countermeasures:
  - Disclosure of applicable logs and data.
  - Partial/full disclosure of infrastructure details (e.g., patch levels and firewalls).
  - Monitoring and alerting on necessary information.

8.3 Data Protection in the Cloud

- There are many ways to compromise data:
  - Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media.
  - Loss of an encoding key may result in effective destruction.
  - Unauthorized parties must be prevented from gaining access to sensitive data.

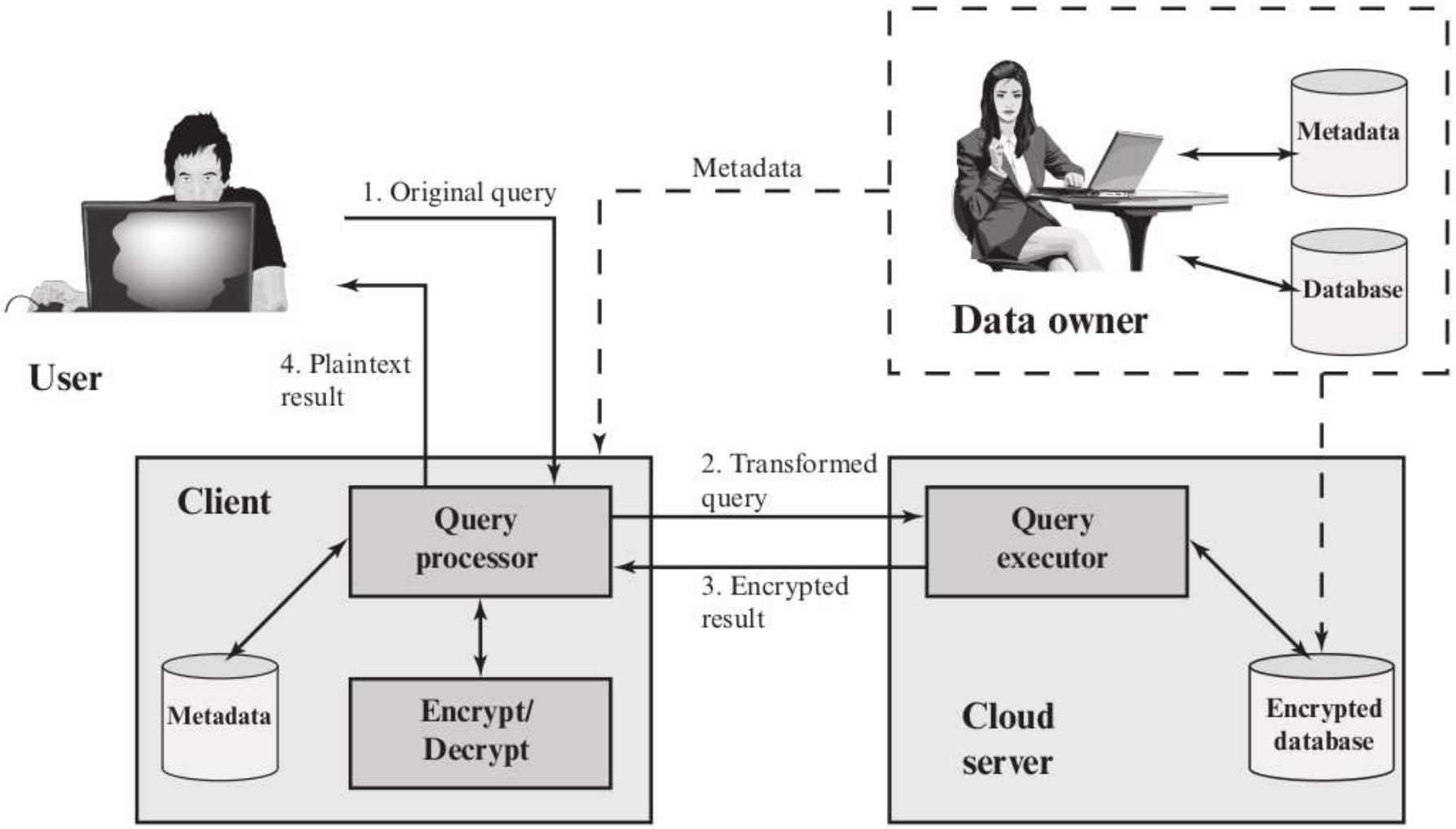
- The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges that are either unique to the cloud or more dangerous because of the architectural or operational characteristics of the cloud environment.

8.3 Data Protection in the Cloud (cont.)

- 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.
- The client can enforce access control techniques but, again, the CP is involved to some extent depending on the service model used.
- 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.
- So long as the key remains secure, the CP has no ability to read the data, although corruption and other denial-of-service attacks remain a risk.

8.3 Data Protection in the Cloud (cont.)

An encryption scheme for cloud-based databases:



8.3 Data Protection in the Cloud (cont.)

An encryption scheme for cloud-based databases:

- **Data owner:** An organization that produces data to be made available for controlled release, either within the organization or to external users.
- **User:** Human entity that presents requests (queries) to the system.
- **Client:** Frontend that transforms user queries into queries on the encrypted data stored on the server.
- **Cloud Server:** An organization that receives the encrypted data from a data owner and makes them available for distribution to clients. The server could in fact be owned by the data owner but, more typically, is a facility owned and maintained by an external provider.

8.3 Data Protection in the Cloud (cont.)

Retrieve a record from the database:

1. The user issues a query for fields from one or more records with a specific value of the primary key of a table.

2. The query processor at the client encrypts the primary key (of the query), modifies the query accordingly, and transmits the query to the server.

3. The server processes the query using the encrypted value of the table's primary key and returns the appropriate record or records.

4. The query processor decrypts the data and returns the results.

8.4 Cloud Security as a Service

- Security as a Service (SecaaS): 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.

- Among the services typically provided are authentication, antivirus, antimalware/-spyware, intrusion detection, and security event management.

- In the context of cloud computing, cloud security as a service, designated SecaaS, is a segment of the SaaS offering of a CP.

8.4 Cloud Security as a Service (cont.)

- **Categories of SecaaS:**
  - Identity and access management
  - Data loss prevention
  - Web security
  - Email security
  - Security assessments
  - Intrusion management
  - Security information and event management
  - Encryption
  - Business continuity and disaster recovery
  - Network security

8.4 Cloud Security as a Service (cont.)

Categories of SecaaS:

- **Identity and access management (IAM):**

Includes people, processes, and systems that are used to manage access to enterprise resources by assuring that the identity of an entity is verified, and then granting the correct level of access based on this assured identity.

Identity provisioning, is providing access to identified users and subsequently deprovisioning, or deny access, to users when the client enterprise designates such users as no longer having access to enterprise resources in the cloud.

Another aspect of identity management is for the cloud to participate in the federated identity management scheme used by the client enterprise.

8.4 Cloud Security as a Service (cont.)

Categories of SecaaS:

- **Data loss prevention (DLP):**

Monitoring, protecting, and verifying the security of data at rest, in motion, and in use.

Much of DLP can be implemented by the cloud client.

The CSP can also provide DLP services, such as implementing rules about what functions can be performed on data in various contexts.

8.4 Cloud Security as a Service (cont.)

Categories of SecaaS:

- **Web security:**

Real-time protection offered either on premise through software/appliance installation or via the cloud by proxying or redirecting Web traffic to the CP.

This provides an added layer of protection on top of things like antiviruses to prevent malware from entering the enterprise via activities such as Web browsing.

In addition to protecting against malware, a cloud-based Web security service might include usage policy enforcement, data backup, traffic control, and Web access control.

8.4 Cloud Security as a Service (cont.)

Categories of SecaaS:

- **Email security:**

Provides control over inbound and outbound email, protecting the organization from phishing, malicious attachments, enforcing corporate polices such as acceptable use and spam prevention.

The CSP may also incorporate digital signatures on all email clients and provide optional email encryption.

8.4 Cloud Security as a Service (cont.)

Categories of SecaaS:

- **Security assessments:**

Third-party audits of cloud services.

While this service is outside the province of the CSP, the CSP can provide tools and access points to facilitate various assessment activities.

8.4 Cloud Security as a Service (cont.)

Categories of SecaaS:

- **Intrusion management:**

Encompasses intrusion detection, prevention, and response.

The core of this service is the implementation of intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) at entry points to the cloud and on servers in the cloud.

An IDS is a set of automated tools designed to detect unauthorized access to a host system.

An IPS incorporates IDS functionality but also includes mechanisms designed to block traffic from intruders.

8.4 Cloud Security as a Service (cont.)

Categories of SecaaS:

- **Security information and event management (SIEM):**

Aggregates (via push or pull mechanisms) log and event data from virtual and real networks, applications, and systems.

This information is then correlated and analyzed to provide real-time reporting and alerting on information/events that may require intervention or other type of response.

The CSP typically provides an integrated service that can put together information from a variety of sources both within the cloud and within the client enterprise network.

8.4 Cloud Security as a Service (cont.)

Categories of SecaaS:

- **Encryption:**

A pervasive service that can be provided for data at rest in the cloud, email traffic, client-specific network management information, and identity information.

Encryption services provided by the CSP involve a range of complex issues, including key management, how to implement virtual private network (VPN) services in the cloud, application encryption, and data content access.

8.4 Cloud Security as a Service (cont.)

Categories of SecaaS:

- **Business continuity and disaster recovery:**

Comprise measures and mechanisms to ensure operational resiliency in the event of any service interruptions.

This is an area where the CSP, because of economies of scale, can offer obvious benefits to a cloud service client.

The CSP can provide backup at multiple locations, with reliable failover and disaster recovery facilities.

This service must include a flexible infrastructure, redundancy of functions and hardware, monitored operations, geographically distributed data centers, and network survivability.

8.4 Cloud Security as a Service (cont.)

Categories of SecaaS:

- **Network security:**

Consists of security services that allocate access, distribute, monitor, and protect the underlying resource services.

Services include perimeter and server firewalls and denial-of-service protection.

Many of the other services listed in this section, including intrusion management, identity and access management, data loss protection, and Web security, also contribute to the network security service.

8.5 Addressing Cloud Computing Security Concerns

- As more businesses incorporate cloud services into their enterprise network infrastructures, cloud computing security will persist as an important issue.

- Cloud computing security failures have the potential to have a chilling effect on business interest in cloud services and this is inspiring service providers to be serious about incorporating security mechanisms that will allay concerns of potential subscribers.

- NIST has recommended various security controls that are relevant in a cloud computing environment.

8.5 Addressing Cloud Computing Security Concerns

Security controls that are relevant in a cloud computing environment:

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

References

- Cryptography and Network Security, Principles and Practice, 7th Edition, William Stallings.