Høgskulen
på Vestlandet

10. Cloud Security

ELE130

Nettverkssikkerhet

Guang Yang
D463
Bergen

Outline

- Cloud Computing
  - Cloud Computing Elements
  - Cloud Computing Reference Architecture
- Could Security Risks and Countermeasures
- Data Protection in the Cloud
- Cloud Security as a Service (SecaaS)

Cloud Computing

NIST defines cloud computing (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.”

Cloud Computing

Five essential characteristics:

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

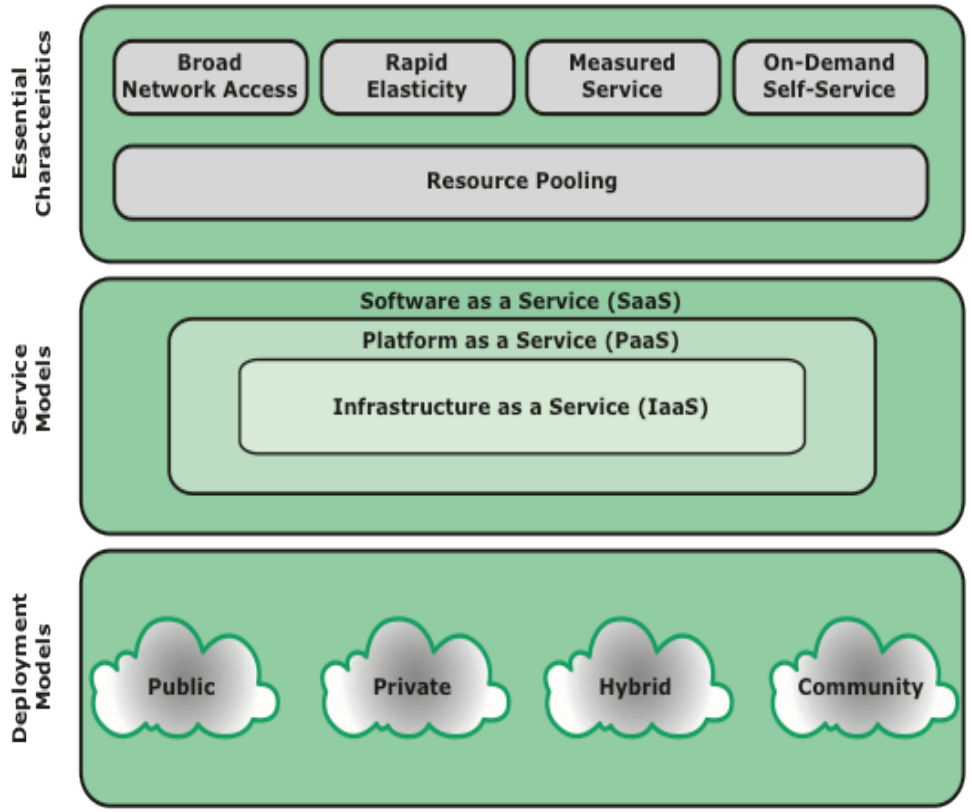


Figure 5.7 Cloud Computing Elements

Cloud Computing

Three service models, which can be viewed as nested service alternatives:

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

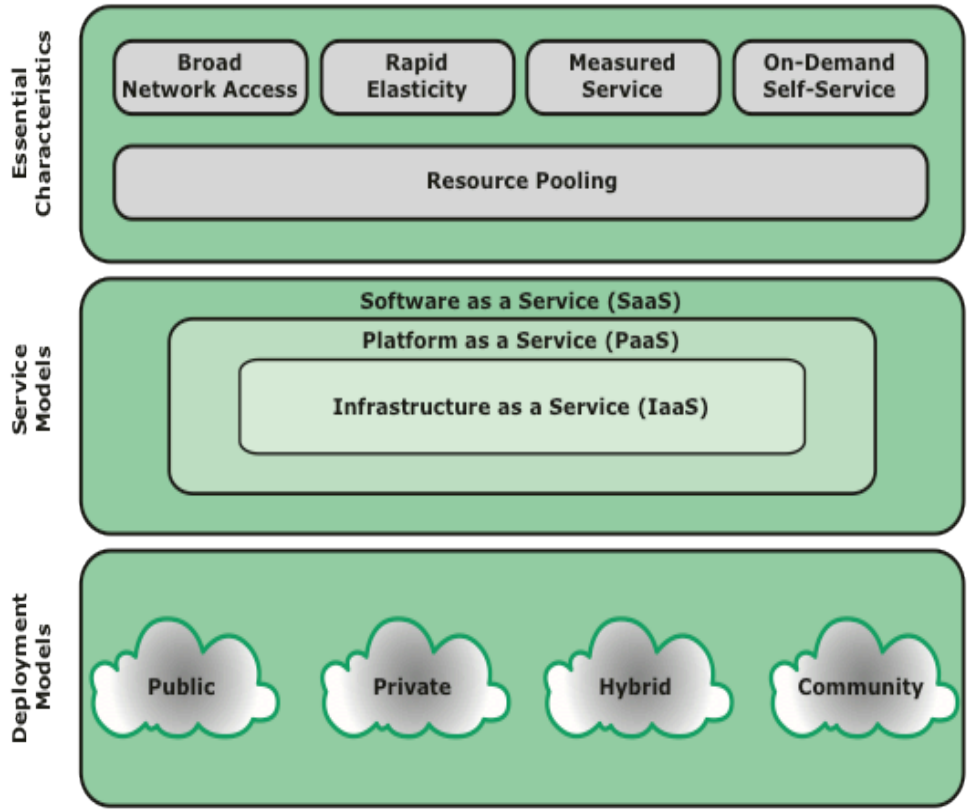


Figure 5.7 Cloud Computing Elements

Cloud Computing

NIST defines four deployment models :

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

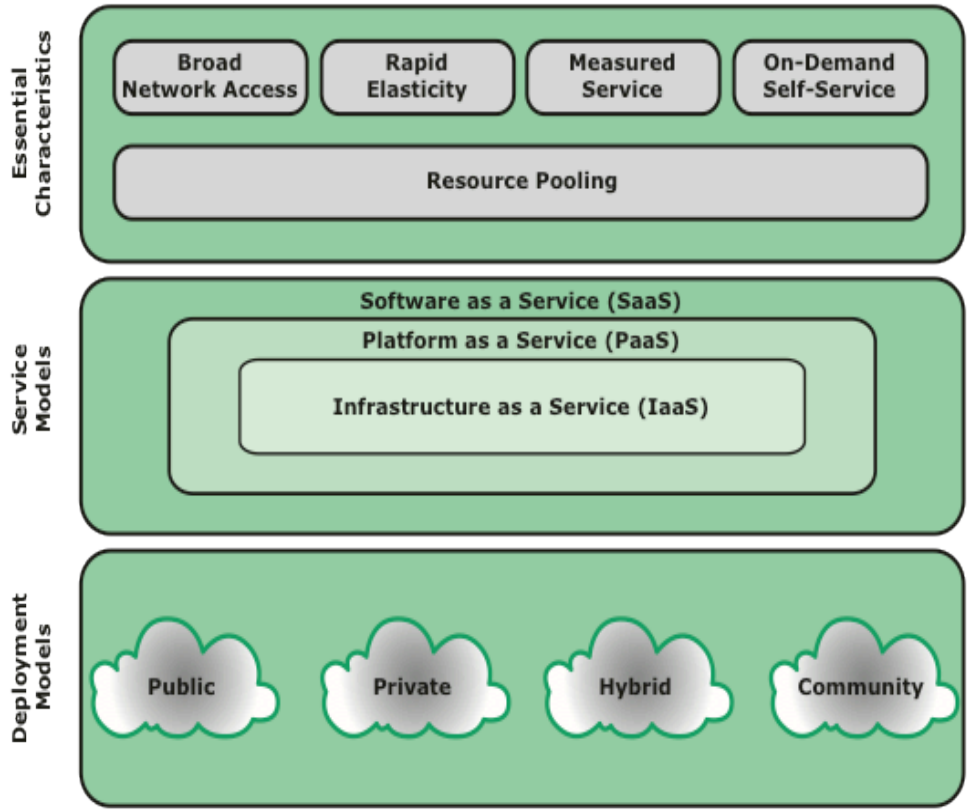


Figure 5.7 Cloud Computing Elements

Cloud Computing

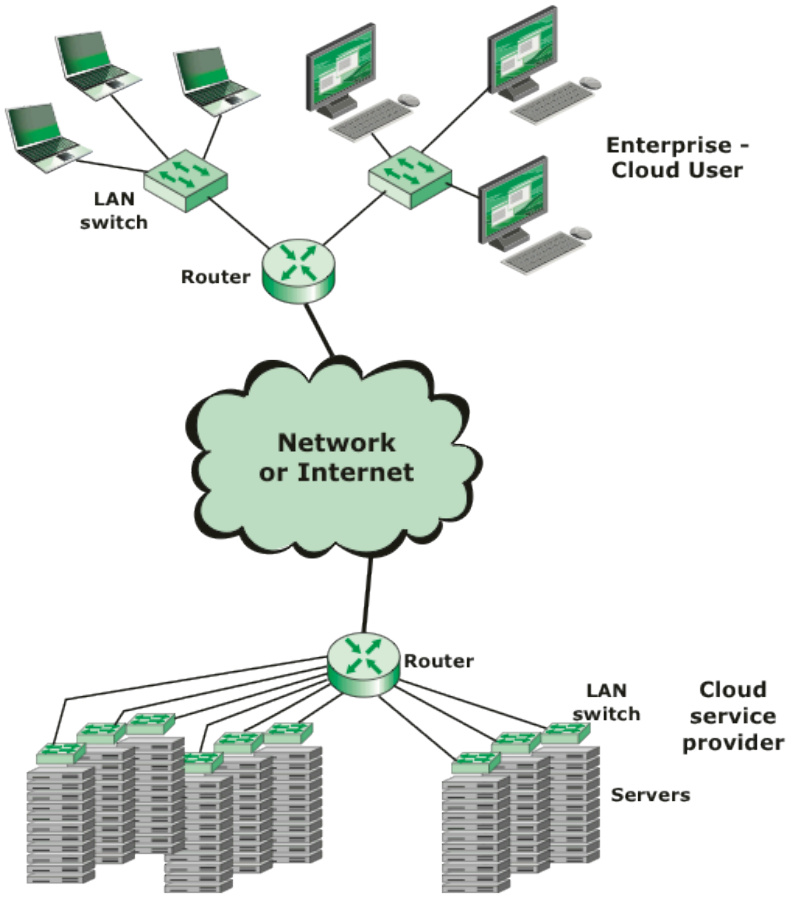


Figure 5.8 Cloud Computing Context

Cloud Computing, the NIST reference architecture

- Consumer
- Provider
- Auditor
- Broker
- Carrier

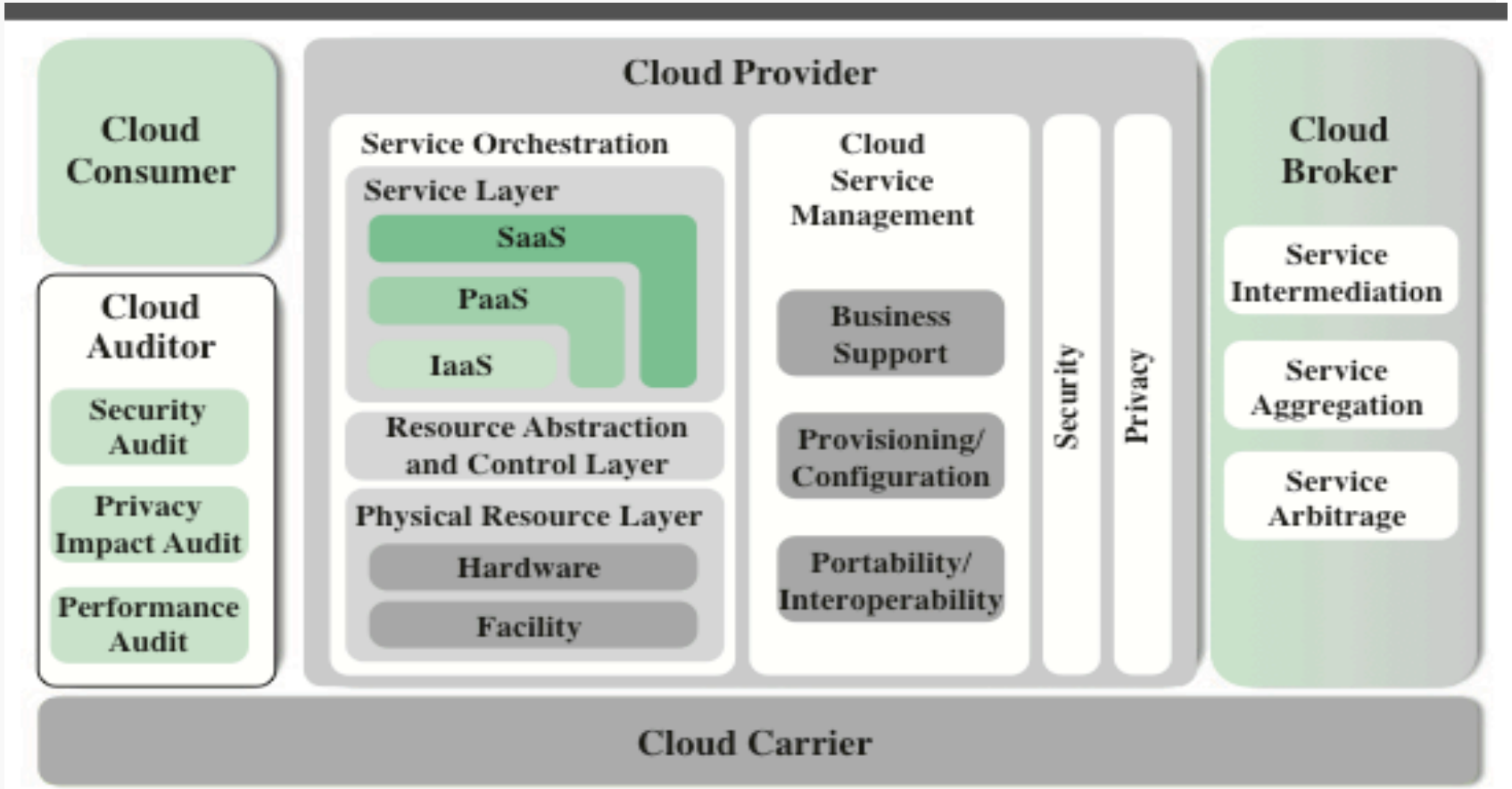
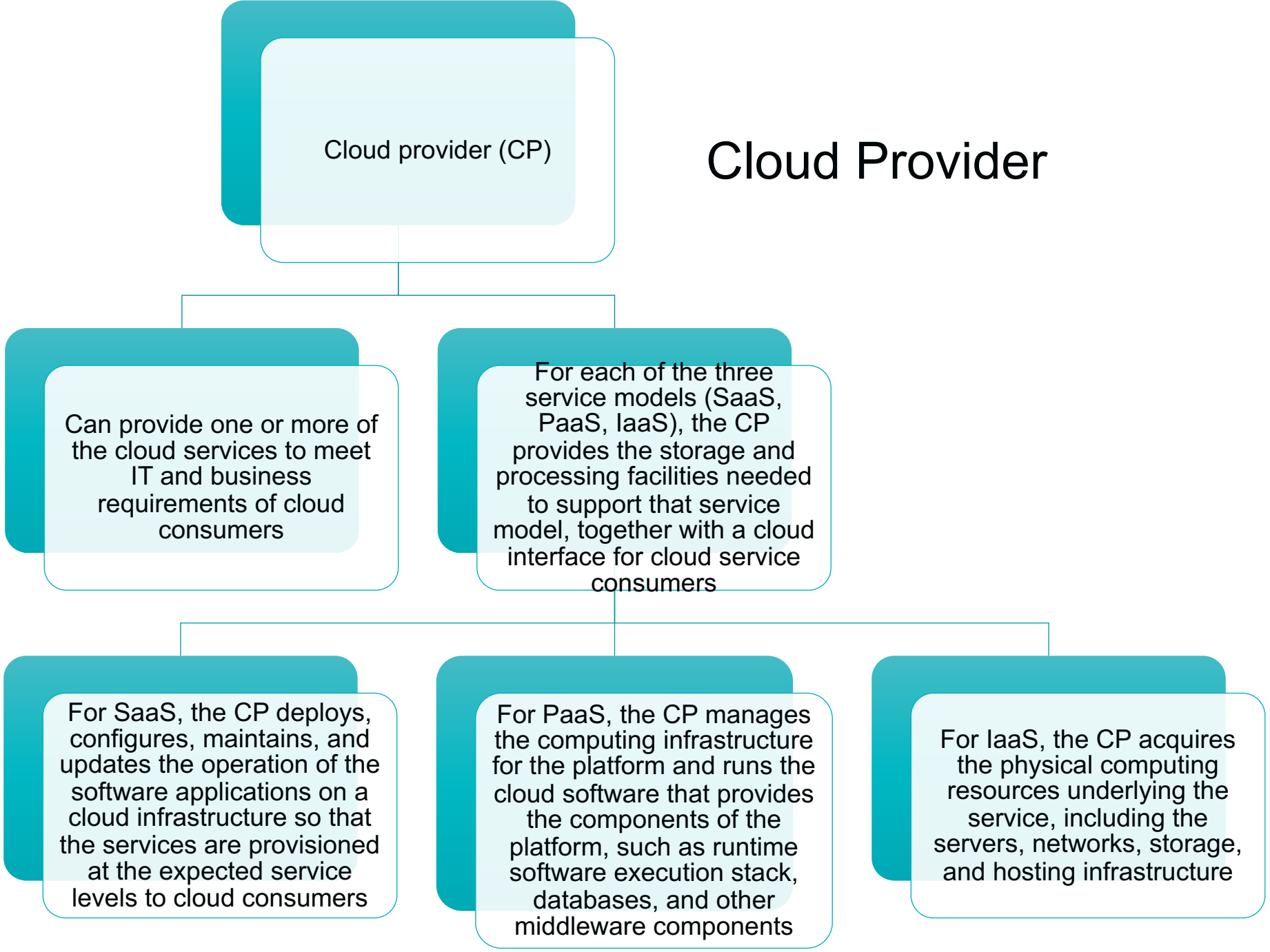


Figure 5.9 NIST Cloud Computing Reference Architecture

Cloud Provider



Could Security Risks and Countermeasures

The Could Security Alliance lists the following as the top cloud-specific security threats, together with suggested countermeasures:

- Abuse and nefarious use of cloud computing
  - Countermeasures:
    1. Stricter initial registration and validation processes
    2. Enhanced credit card fraud monitoring and coordination
    3. Comprehensive introspection of customer network traffic
    4. Monitoring public blacklist for one's own network blocks
- Insecure interfaces and APIs
  - Countermeasures:
    1. Analyzing the security model of CP interfaces
    2. Ensuring that strong authentication and access controls are implemented in concert with encrypted transmission
    3. Understanding the dependency chain associated with the API

Could Security Risks and Countermeasures

- Malicious insiders
  - 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 information security and management practices, as well as compliance reporting
    4. Determine security breach notification processes
- Shared technology issues
  - Countermeasures:
    1. 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 operations
    4. Enforce SLAs for patching and vulnerability remediation
    5. Conduct vulnerability scanning and configuration audits

Could Security Risks and Countermeasures

- Data loss or leakage
- Account or service hijacking
  - Countermeasures:
    1. Prohibit the sharing of account credentials between users and services
    2. Leverage strong two-factor authentication techniques where possible
    3. Employ proactive monitoring to detect unauthorized activity
    4. Understand CP security policies and SLAs.
- Unknown risk profile
  - Countermeasures:
    1. Disclosure of applicable logs and data
    2. Partial/full disclosure of infrastructure details
    3. Monitoring and alerting on necessary information

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

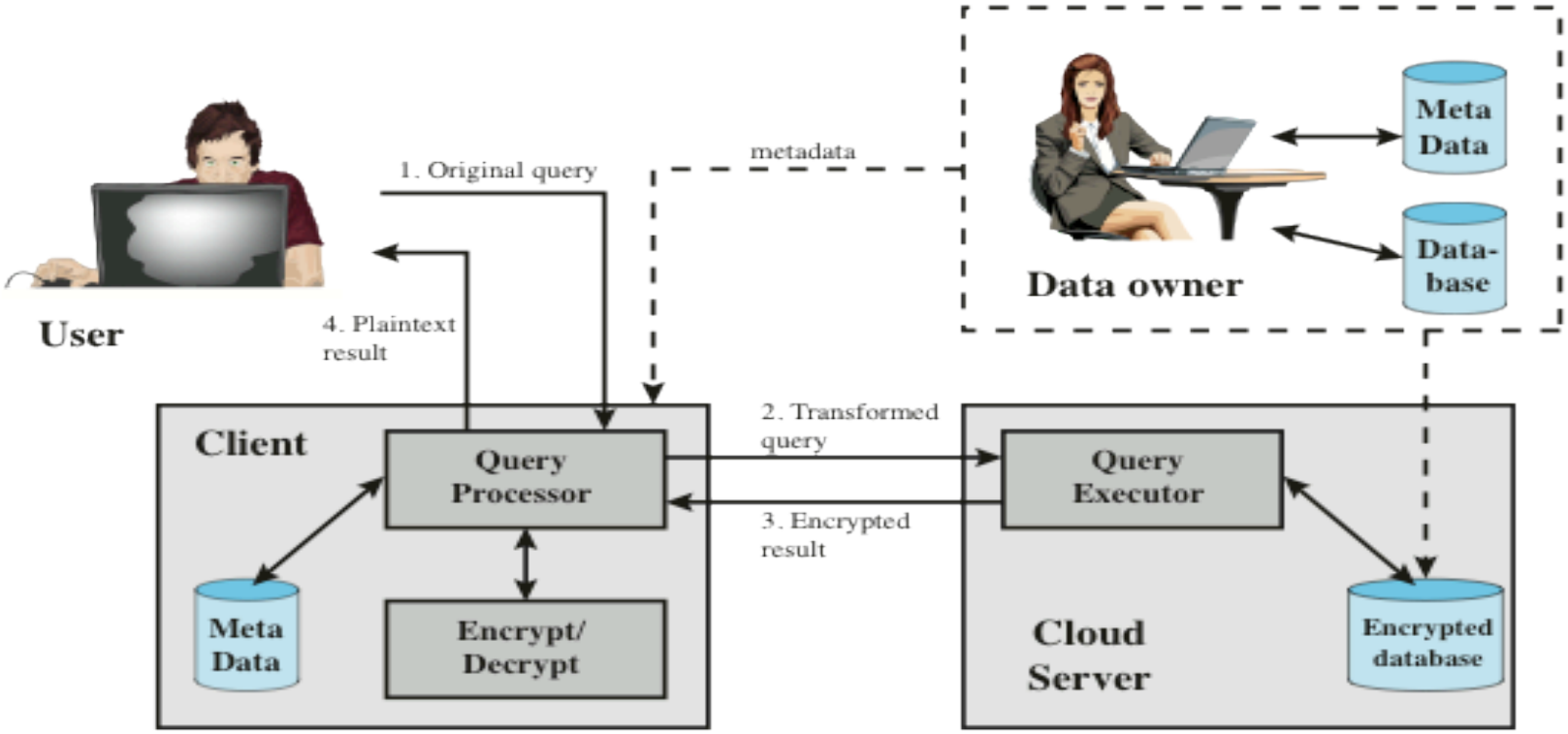


Figure 5.10 An Encryption Scheme for a Cloud-Based Database

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

Cloud Security as a Service (SecaaS)

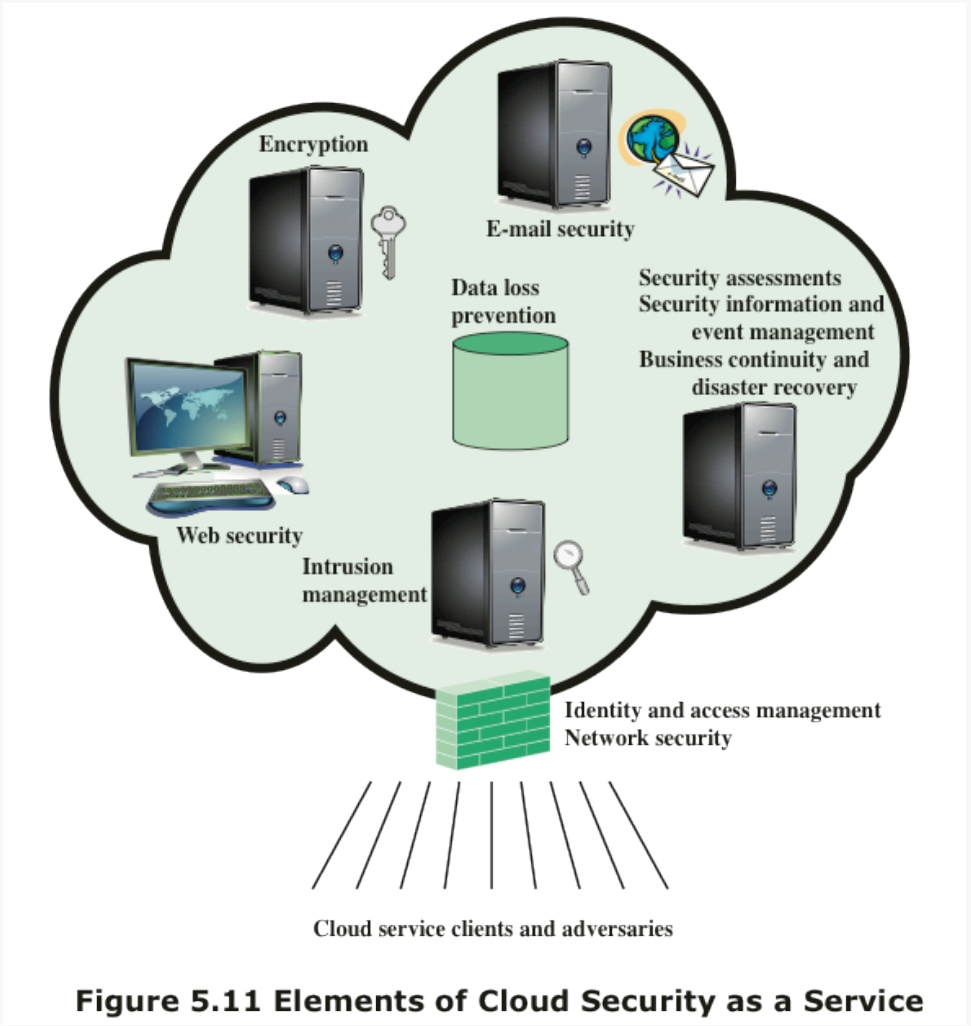


Figure 5.11 Elements of Cloud Security as a Service

Thank you for your attention!