The Magical Cloud

Lennart Franked

Department for Information and Communicationsystems (ICS),
Mid Sweden University, Sundsvall.

2014-10-20

Mittuniversitetet
MID SWEDEN UNIVERSITY

Overview

1. Cloud Computing
   - Definition of Cloud
   - Essential Characteristics
   - Service Models
   - Deployment Models
   - Putting it all in a context
2. Cloud Computing Reference Architecture
   - NIST Conceptual Reference Model
   - Actors within the conceptual reference model
3. Cloud Security Risks and Countermeasures
   - Cloud-specific security threats
   - Data protection in the Cloud
   - (Cloud) Security as a Service ((C)SecaaS)

Mittuniversitetet
MID SWEDEN UNIVERSITY

Literature

The lecture covers chapter 5 “Network Access Control and Cloud Security” in [1]. When finished reading the chapter, you should solve problems 5.2 and 5.3 in [1], note however that in 5.3 instead of writing a brief paper, publish the URL in the forum along with a brief summary of the what the video addresses.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Definition of Cloud

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. This cloud model promotes availability and is composed of *five essential characteristics, three service models, and four deployment models.*"[2]

Mittuniversitetet
MID SWEDEN UNIVERSITY

Cloud Computing Elements

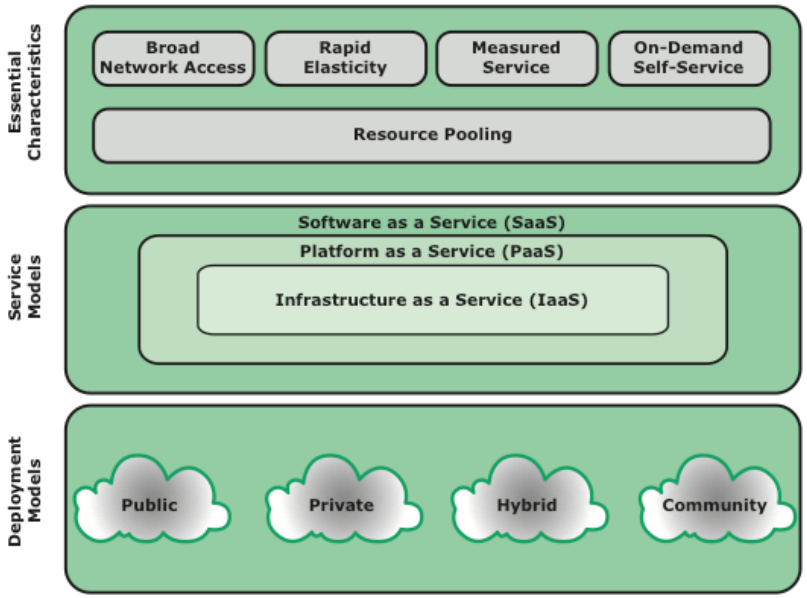

Figure 5.7 Cloud Computing Elements

Figure: Found in [1]

Mittuniversitetet
MID SWEDEN UNIVERSITY

Broad Network Access

Essential Characteristics

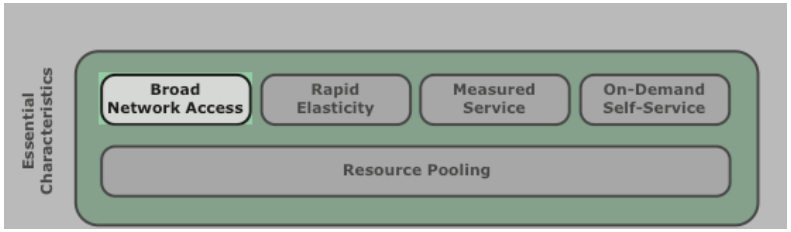

Figure: Broad Network Access [1]

- Available over the network.
- Accessible over standard mechanisms.
- Heterogeneous client platforms.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Rapid Elasticity

Essential Characteristics

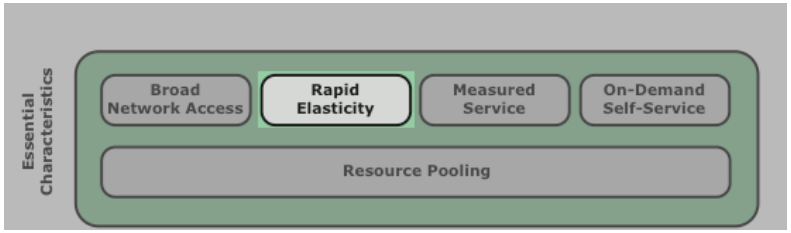

Figure: Rapid Elasticity [1]

- Resources can be provisioned and released based on requirements.
- Either manually or automatically.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Measured Service

Essential Characteristics

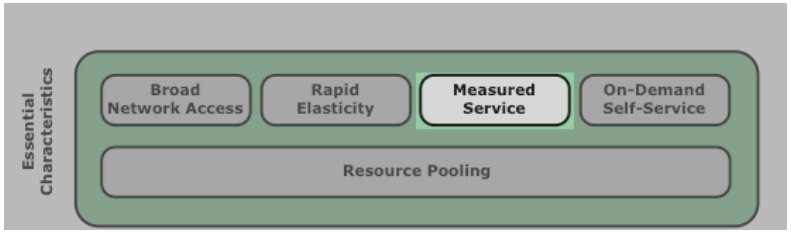

Figure: Measured Service [1]

- Able to measure the usage of each consumer.
- Storage, processing, bandwidth, et cetera.

Mittuniversitetet
MID SWEDEN UNIVERSITY

On-Demand Self-Service

Essential Characteristics

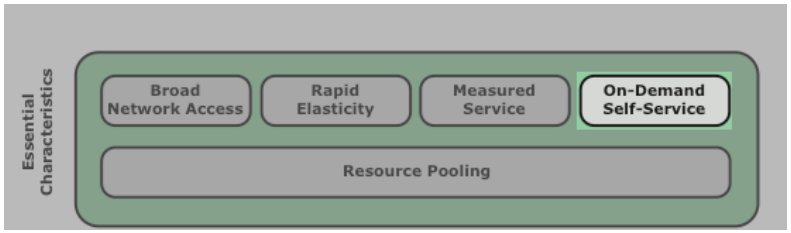

Figure: On-Demand Self-Service [1]

- The consumer should be able to provision computing capabilities as needed without having to involve each service provider.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Resource Pooling

Essential Characteristics

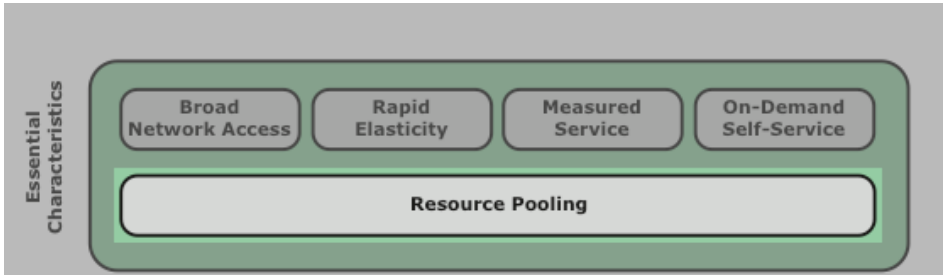

Figure: Resource Pooling [1]

- The providers computing resources are pooled to serve multiple consumers.
- Each consumer could have different physical and virtual resources dynamically assigned and reassigned based on requirements.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Resource Pooling II

Essential Characteristics

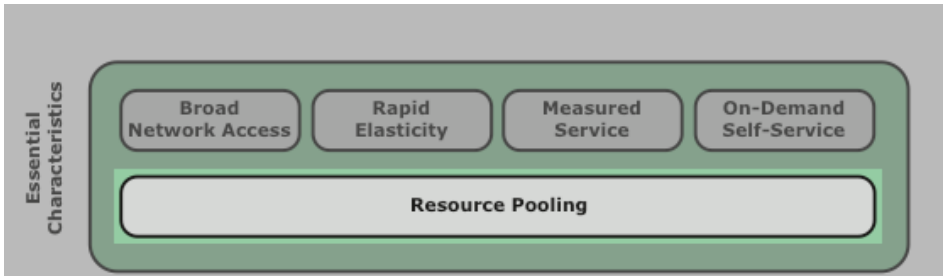

Figure: Resource Pooling [1]

- Location independent – The location of the data is outside the customers knowledge and control.
- Some basic control can exist, such as which country to store the data in.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Software as a Service (SaaS)

Service Models

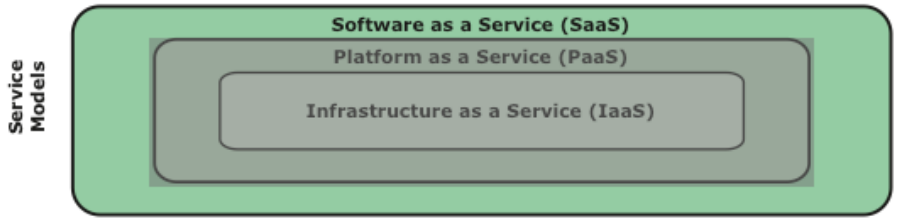

Figure: Software as a Service [1]

- Certain applications that are running in the providers cloud are made available to the consumer.
- Accessible from various clients through a thin interface.
- The consumer do not control nor manage the underlying cloud infrastructure.
- Example: Gmail

Mittuniversitetet
MID SWEDEN UNIVERSITY

Platform as a Service (PaaS)

Service Models

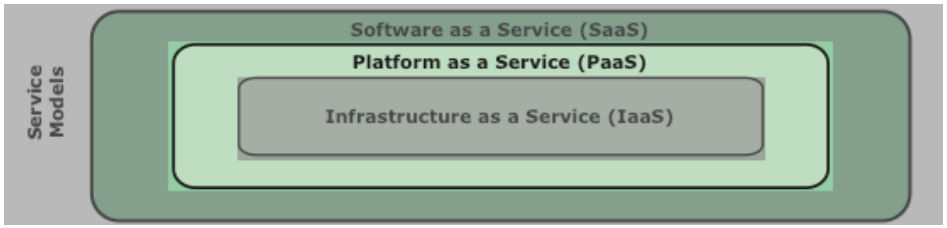

Figure: Platform as a Service [1]

- Allows the consumer to create their own software using tools and libraries provided by the cloud provider.
- This software can then be run using the cloud providers resources.
- Operating system running in the cloud.
- The consumer do not control nor manage the underlying cloud infrastructure.
- Example: Google App Engine

Mittuniversitetet
MID SWEDEN UNIVERSITY

Infrastructure as a Service (IaaS)

Service Models

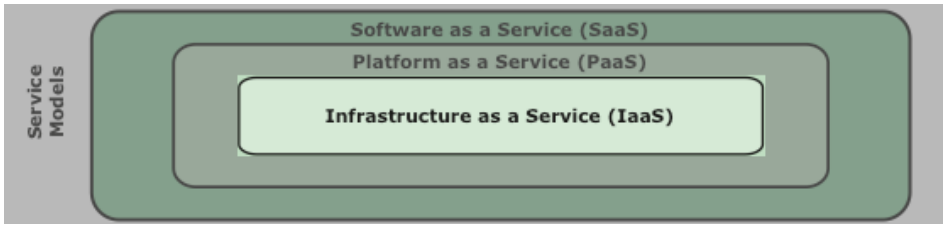

Figure: Infrastructure as a Service [1]

- The cloud provider provides a system infrastructure to the customer.
- Processing power, storage, network, et cetera.
- Often given in the form of a Virtual Machine.
- Example: Amazon EC2

Mittuniversitetet
MID SWEDEN UNIVERSITY

Public Cloud

Deployment Models

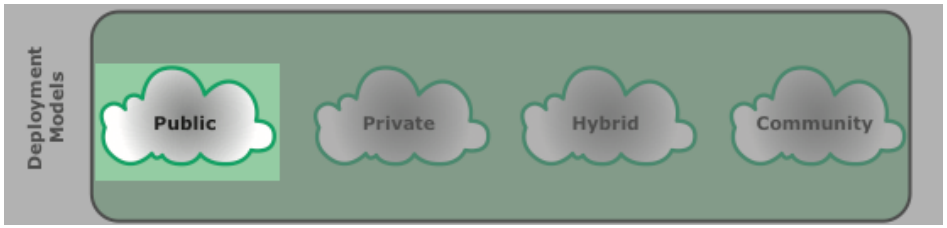

Figure: Public Cloud [1]

- The cloud infrastructure is available for public use.
- Usually owned and managed by a business, academic or goverment.
- Located on the premises of the cloud provider.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Private Cloud

Deployment Models

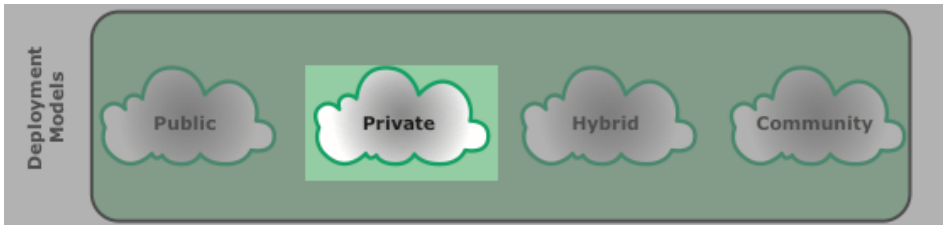

Figure: Private Cloud [1]

- The cloud infrastructure is only available for a single organization.
- Usually both owned and managed by that organisation.
- Located on or off premises.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Hybrid Cloud

Deployment Models

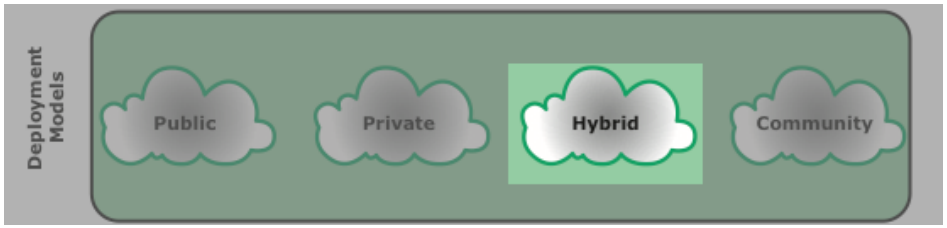

Figure: Hybrid Cloud [1]

- Infrastructure is a composition of two or more deployment models.
- Each cloud infrastructure must be a unique entity.
- Allows resource portability between the cloud infrastructures.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Community Cloud

Deployment Models

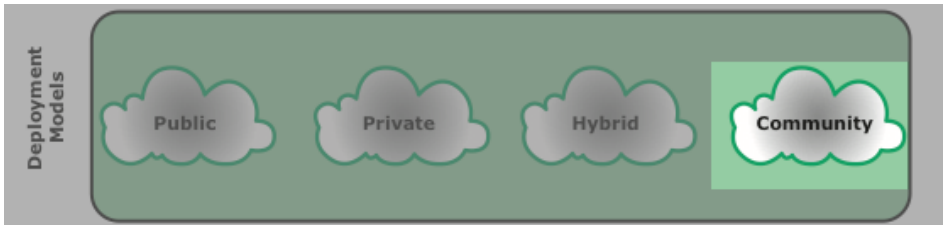

Figure: Community Cloud [1]

- The cloud infrastructure is only available to a specific community.
- Owned by one or more organisations in the community, a third party or combination.
- Exists on or off premises.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Cloud Computing Context

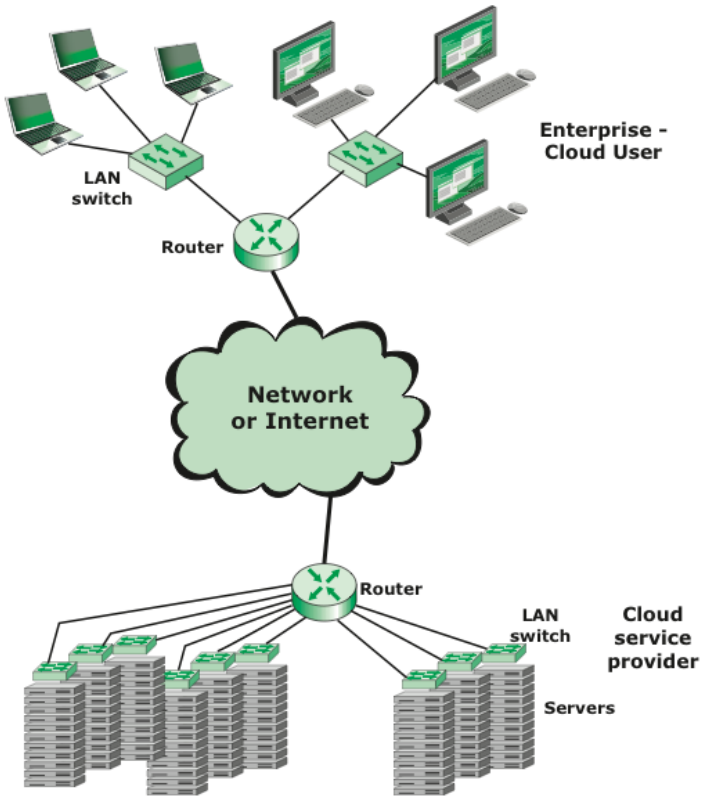

Figure 5.8 Cloud Computing Context

Figure: Found in [1]

Mittuniversitetet
MID SWEDEN UNIVERSITY

NIST Cloud Computing Reference Architecture

Conceptual Reference Model

"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." [3]

Mittuniversitetet
MID SWEDEN UNIVERSITY

NIST Cloud Computing Reference Architecture

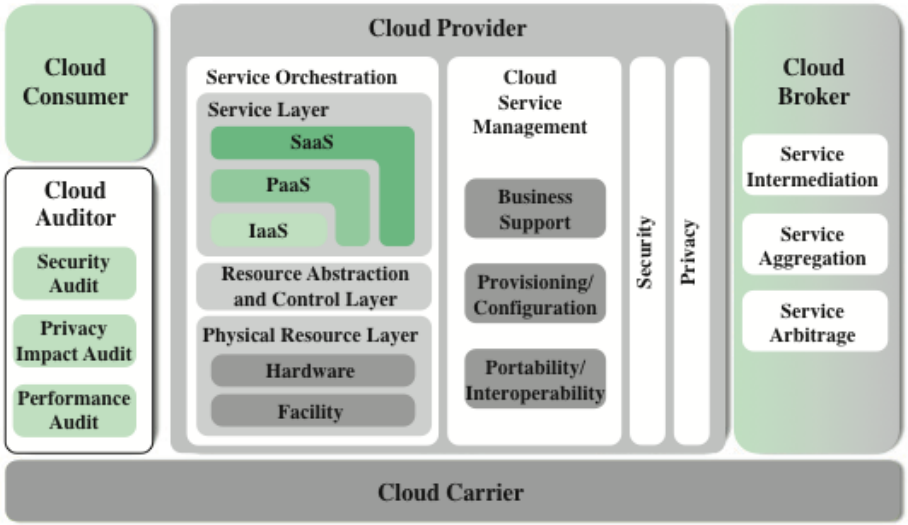

Figure: NIST Reference Architecture[3]

Mittuniversitetet
MID SWEDEN UNIVERSITY

Five Major Actors

NIST Cloud Computing Reference Architecture

Defines five major actors in the Conceptual Reference Model [3]:

Cloud Consumer

A Person or organisation that maintains a business relationship with and uses services from Cloud Providers

Cloud Provider

A person, organization or entity responsible for making a service available to interested parties.

Cloud Carrier

An intermediary that provides connectivity and transport of cloud services from provider to consumer.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Five Major Actors II

NIST Cloud Computing Reference Architecture

Cloud Auditor

A party that conduct independent assessment of cloud services, information system operations, performance and security.

Cloud Broker

An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud provides and cloud consumers.

Mittuniversitetet
MID SWEDEN UNIVERSITY

The Notorious Nine

Cloud Security Alliance

- Cloud Security Alliance list their top nine cloud-security threats. [4]
  - Data Breaches
  - Data Loss
  - Account Hijacking
  - Insecure APIs
  - Denial of Service
  - Malicious Insiders
  - Abuse of Cloud Services
  - Insufficient Due Diligence
  - Shared Technology Issues

Mittuniversitetet
MID SWEDEN UNIVERSITY

Storing data in the Cloud

Data protection in the Cloud

- By storing data in the cloud, the threat for data compromise will increase.
- Data storage implementation may vary depending on cloud provider.
  - Multi-instance model - one DBMS for each subscriber.
  - Multi-tenant model - one DBMS shared among multiple subscribers.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Securing data

Data protection in the Cloud

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

Mittuniversitetet
MID SWEDEN UNIVERSITY

Securing data II

Data protection in the Cloud

How could we ensure protection of our data in transit, at rest and in use?

- Use encryption to protect the data in transit. Problems?
  - Key management with cloud provider.
- Encrypt the entire database to protect data at rest. Problems?
  - Loose the key and all data is lost as well.
  - Difficult to search and access the database.
  - User need to download entire tables or databases to be able to properly work with it.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Encryption scheme for a cloud-based database

Data protection in the Cloud

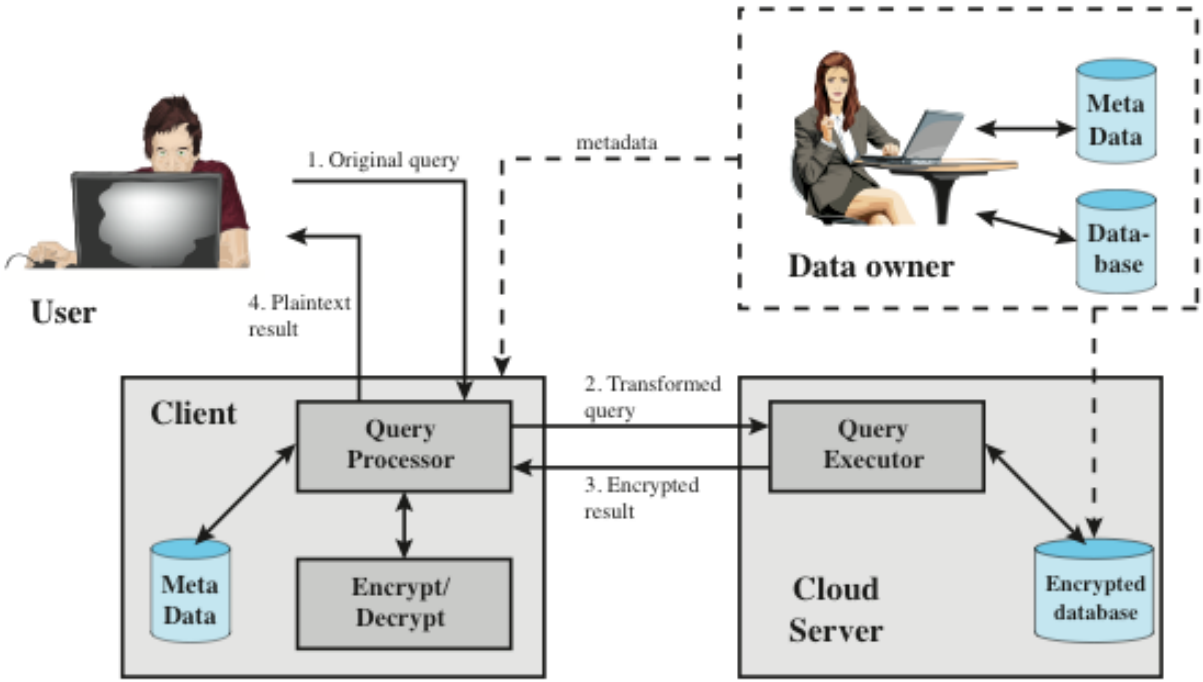

Figure: Encryption scheme for a cloud-based Database [1]

Mittuniversitetet
MID SWEDEN UNIVERSITY

SecaaS

SecaaS

"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" - Cloud Security Alliance

Mittuniversitetet
MID SWEDEN UNIVERSITY

Categories

SecaaS

Identity and access management

Assuring the identity of an entity, and granting correct level of access.

Data loss prevention

Monitoring, protecting and verifying the security of the data.

Web security

Real-time protection to prevent web based attacks. Proxy web traffic through the Cloud Provider.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Categories II

SecaaS

E-mail security

Control over inbound and outbound e-mail. Protection against spam, phishing, malicious attachments et cetera.

Security Assessments

Provides tools to ease the auditing process of the cloud services.

Intrusion Management

IDS/IPS

Mittuniversitetet
MID SWEDEN UNIVERSITY

Categories III

SecaaS

Security information and event management

Aggregates log and event data to be analysed to be able to offer real-time reporting and alerting.

Encryption

Business continuity and disaster recovery

Redundancy and backups of data.

Network Security

General network security.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Referenser

[1] William Stallings. *Network security essentials : applications and standards*. 5th ed. International Edition. Pearson Education, 2013. ISBN: 978-0-273-79336-6.

[2] Peter Mell and Tim Grance. *The NIST Definition of Cloud Computing*. NIST Special Publication 800-145. 2011.

[3] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf. *NIST Cloud Computing Reference Architecture*. NIST Special Publication 500-292. 2011.

[4] Top Threats Working Group, Cloud Security Alliance. *The Notorious Nine: Cloud Computing Threats in 2013*. 2013. URL: http://www.cloudsecurityalliance.org/topthreats/.

Mittuniversitetet
MID SWEDEN UNIVERSITY