Cloud Computing - Starting Points for Privacy and Transparency

Ina Schiering

Ostfalia University of
Applied Science

Wolfenbüttel, Germany

IFIP Summerschool: Privacy and Identity Management for Life, Helsingborg, August 2nd, 2010

Cloud Services

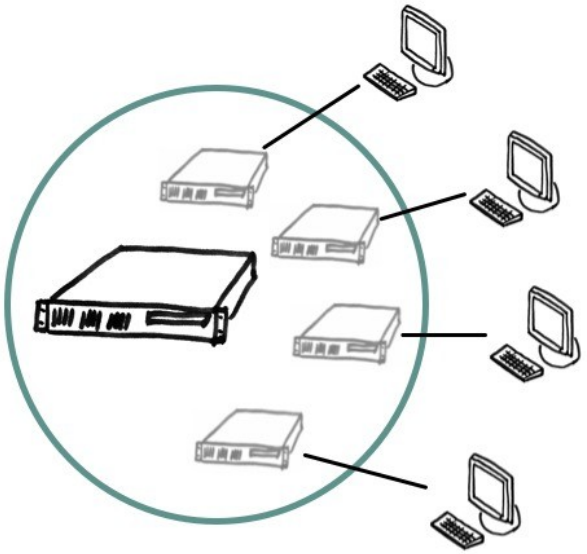
Introduction

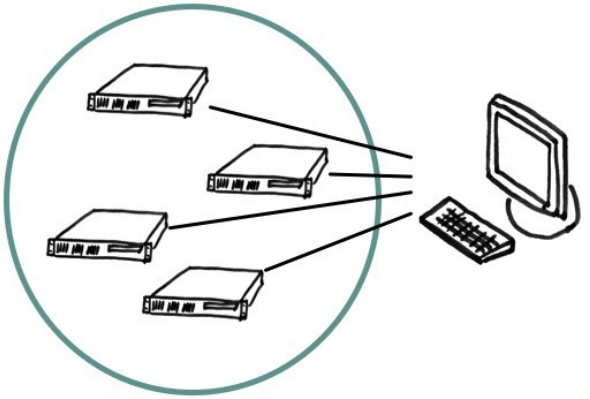
- Interacting Partners
- Service Delivery Model
- Cloud Deployment Model

Privacy in Cloud Services

Audits and Assessments

- Dynamically utilisable, scalable IT services
- Use of **virtualisation** and **scalability**





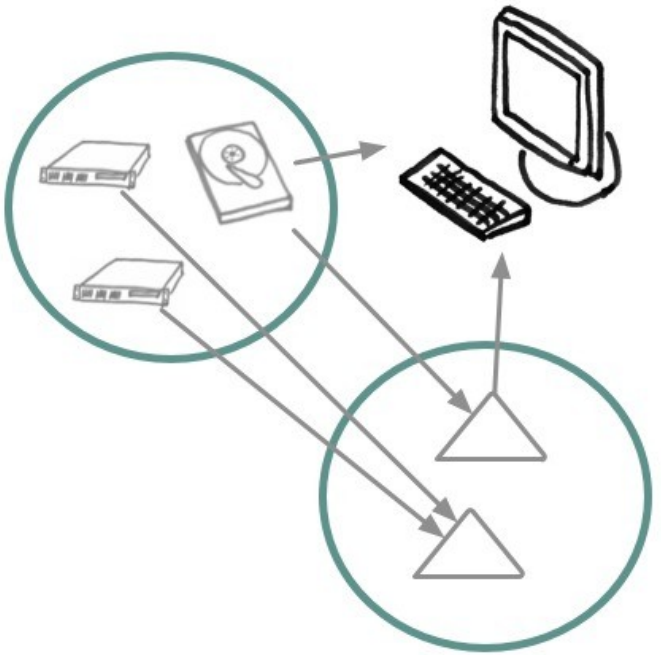
Interacting Partners

The different **interacting partners** in a cloud environment are

- Cloud Users
- Cloud Providers
- Resource Owners

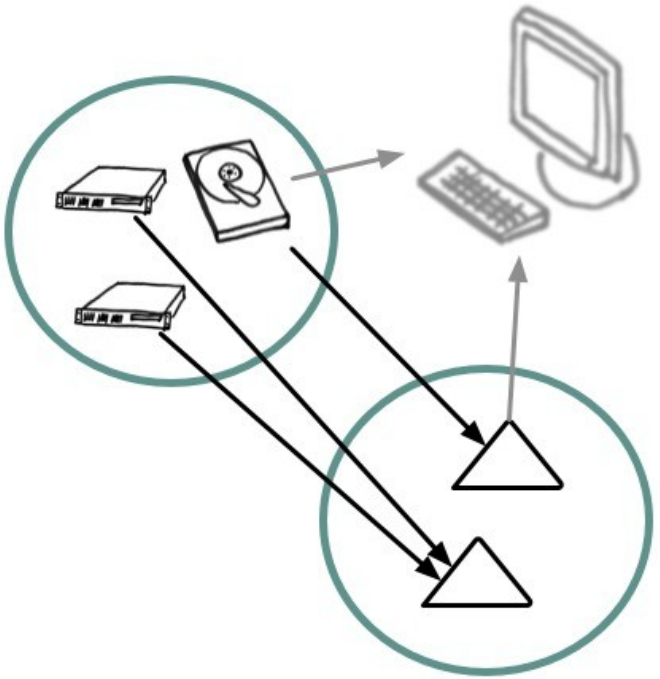
Cloud User

- Uses a cloud service
- A person, a company or an organisation can be a cloud user



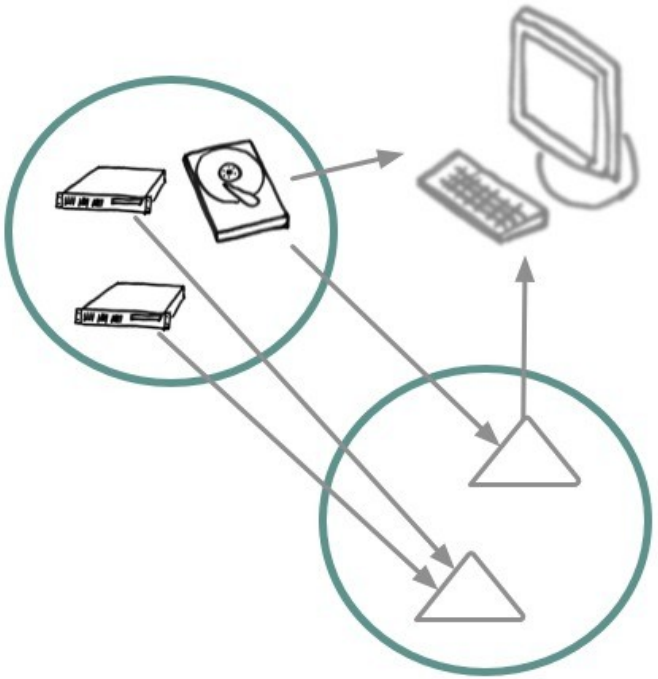
Cloud Provider

- Cloud services are offered by cloud providers



Resource Owner

- Resource Owner is an interacting party who owns resources
- Resources are e.g. virtual instances and storage



Service Delivery Model

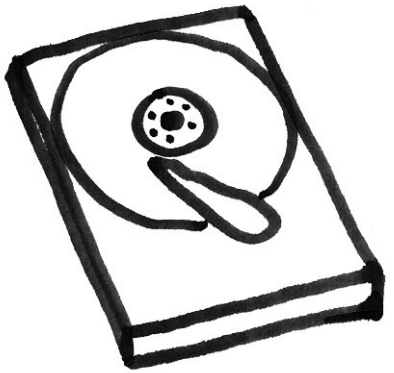
Cloud services are distinguished concerning the complexity of the technology stack they deliver.

Types of cloud services are:

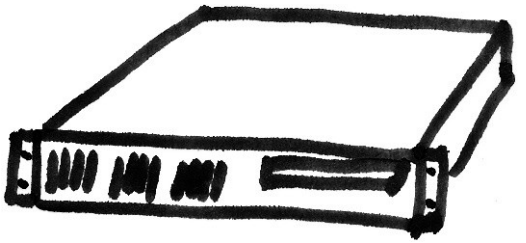
- **IaaS** - Infrastructure as a Service
- **PaaS** - Platform as a Service
- **SaaS** - Software as a Service

Infrastructure as a Service

- Storage
(Amazon S3, ScaleUp)



- Virtual instances
(Amazon EC2)



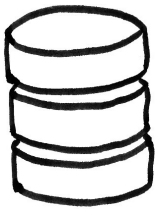
PaaS

Platform as a Service

Infrastructure software as (e.g. LAMP-Stack)

- Web servers, application servers

- Data bases



- Asynchronous queues

(Microsoft Azure, Amazon Web Services, Google App Engine, Force.com)

SaaS

Software as a Service

Software for complex processes e.g.

- Email
- Text Processing
- CRM (Customer Relationship Management)

(Google Docs, Salesforce.com, Facebook, Picasa)

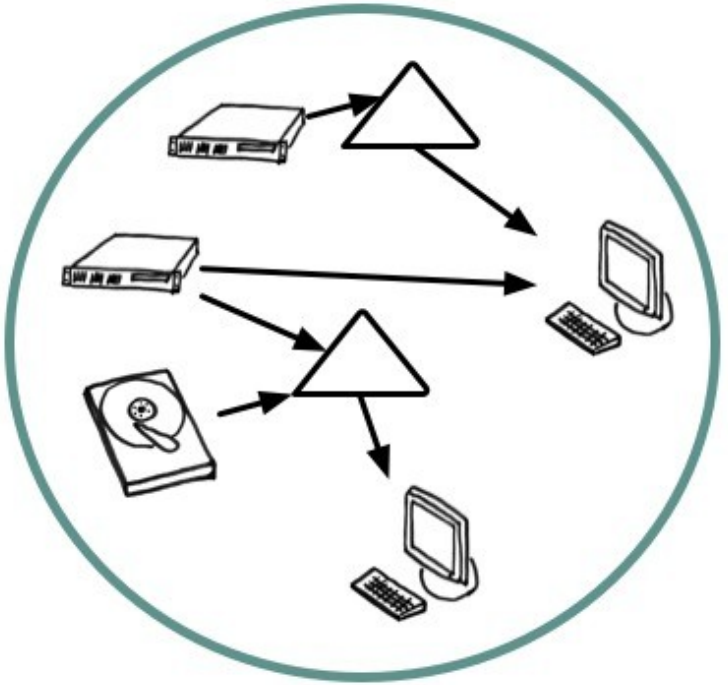
Cloud Deployment Model

Cloud services are distinguished concerning the relation between cloud provider and cloud user:

- Private clouds
- Public clouds
- Hybrid clouds
- Community Clouds

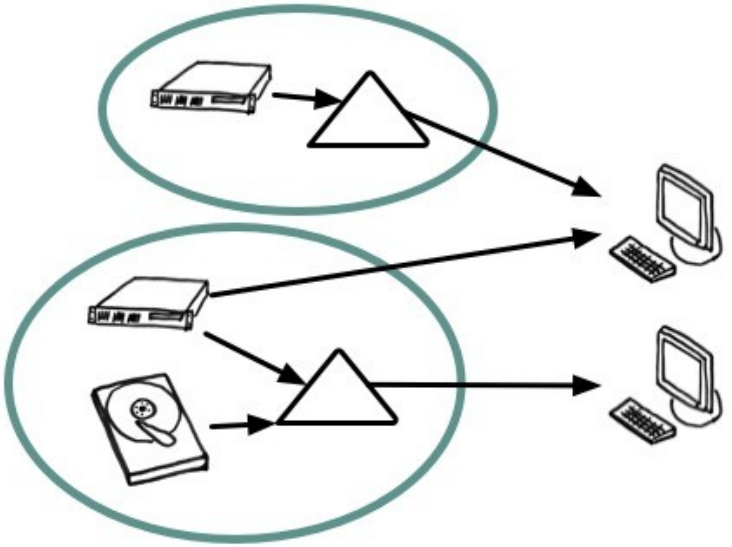
Private Clouds

- Cloud user, cloud provider and resource owner are the same instance



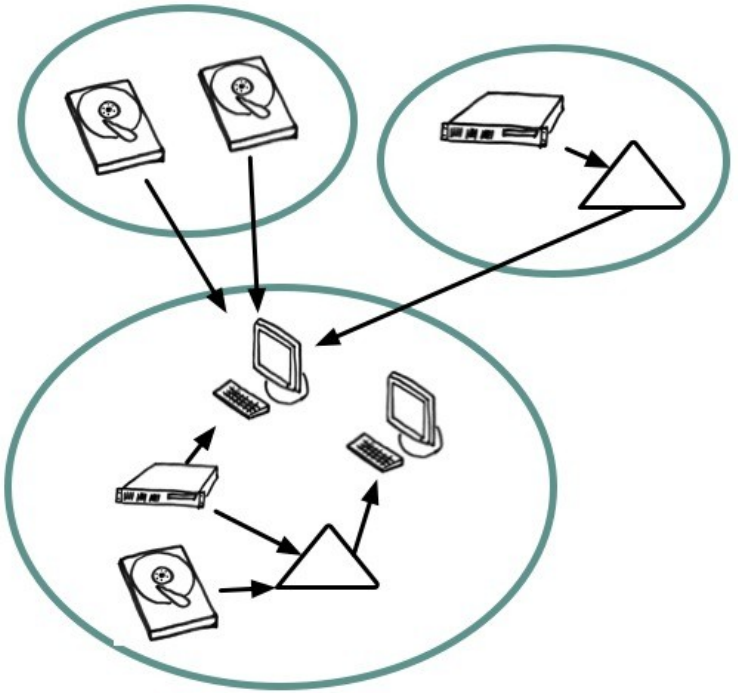
Public Clouds

- Cloud services offered by an external supplier
- **All physical resources are out of reach of the cloud user**



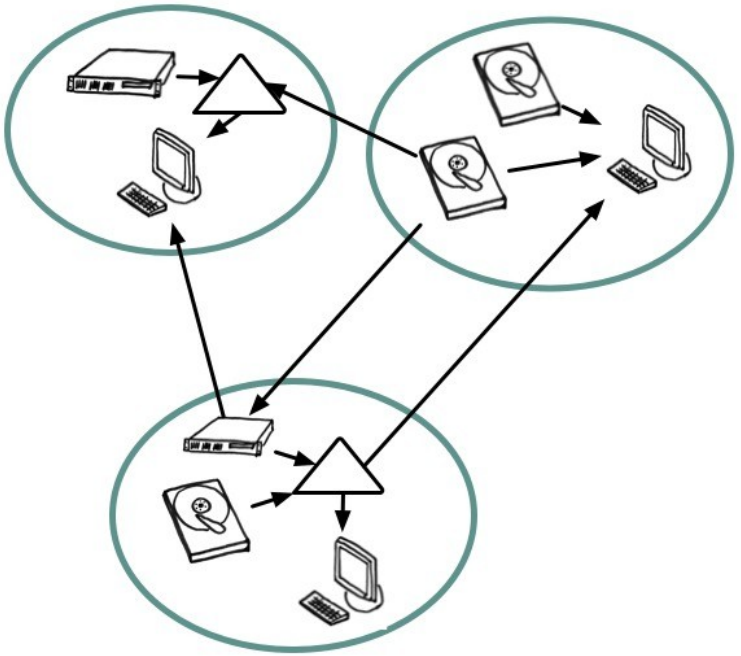
Hybrid Clouds

- Mixture of private and public cloud



Community Clouds

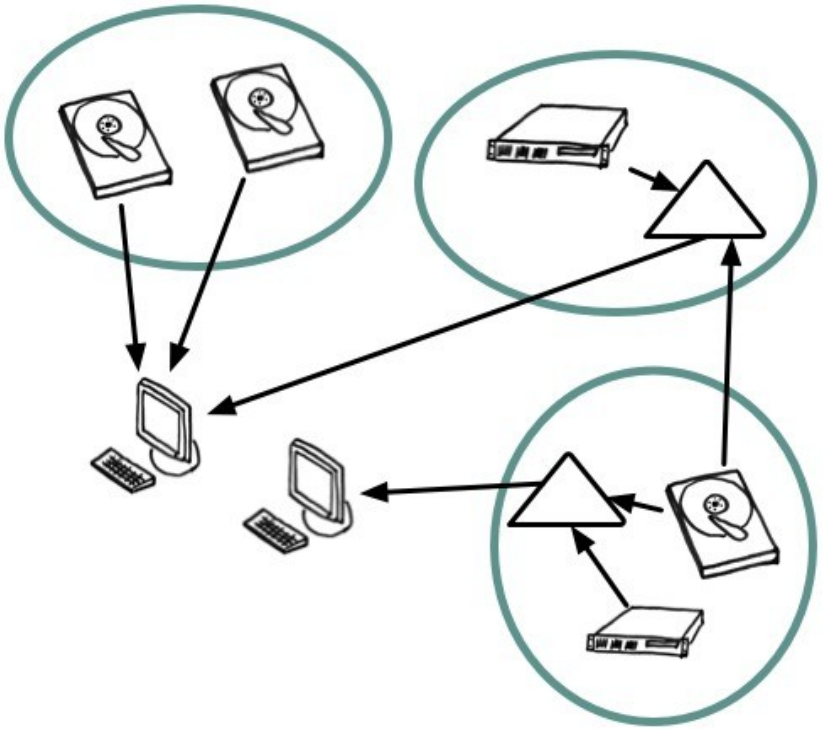
- Several organisations have similar requirements and share the infrastructure (e.g. model for public sector)



Cloud Network

Interacting partners in a cloud can be visualized as a

finite, directed graph



Privacy in Cloud Services

We concentrate

- on cloud services for organisations,
- on technical measures.

What data of organisations?

- Personal data of employees, customers
- Confidential (business-related) data
- Intellectual property

Responsibility rests always with the cloud user.

Responsibility for Personal Data

Personal data

- fairly and lawfully processed
- processed for limited purpose
- adequate, relevant, not excessive
- accurate,
- not kept longer than necessary
- processed in accordance with data subjects rights
- secure

Multilateral Privacy

Allows all parties of an interaction

- **to express their privacy objectives**
- with no party taking precedence over another.

Mechanisms of effective control are needed.

Requirements for Data Privacy

Standard requirements for data privacy:

- Confidentiality,
- Integrity,
- Availability
- Authenticity
- Accountability
- Non-repudiability
- Restrict the location of data

Operational Requirements

- Identity and Access Management
- Monitoring, reporting, logging (e.g. based on service level, legal requirements)
- Backup, archiving of data
- Deletion of data
- Interfaces to other Systems (e.g. data warehouse)

Characteristics of Cloud Services

- Shared resources
- Communication over public networks (Internet)
- Location of resources not transparent
- Operated by third parties

Approach to Requirements

Requirements have to be met by the application, resp. the service:

- **SaaS:** Requirements are actual requirements for the service
- **IaaS, PaaS**: Support the realisation of requirements in applications

Components of an IT-Service

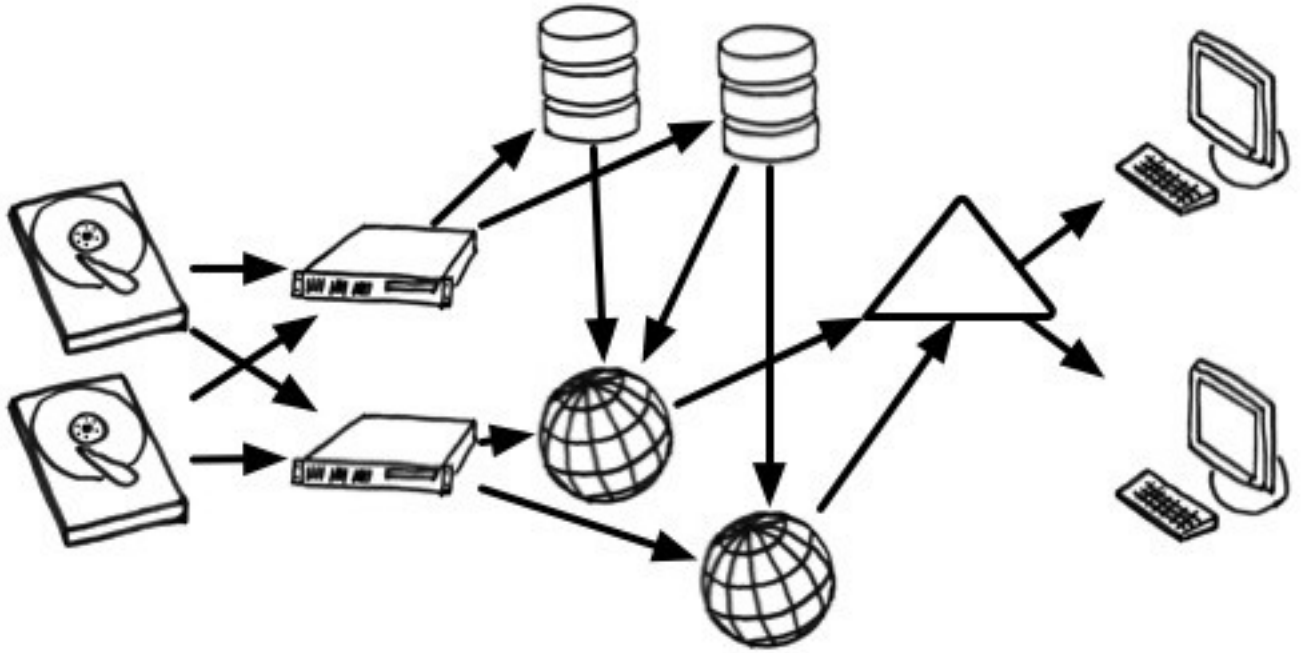
Introduction

Privacy in Cloud Services

- Privacy Requirem.
- **Cloud Services**
- IaaS
- PaaS
- SaaS

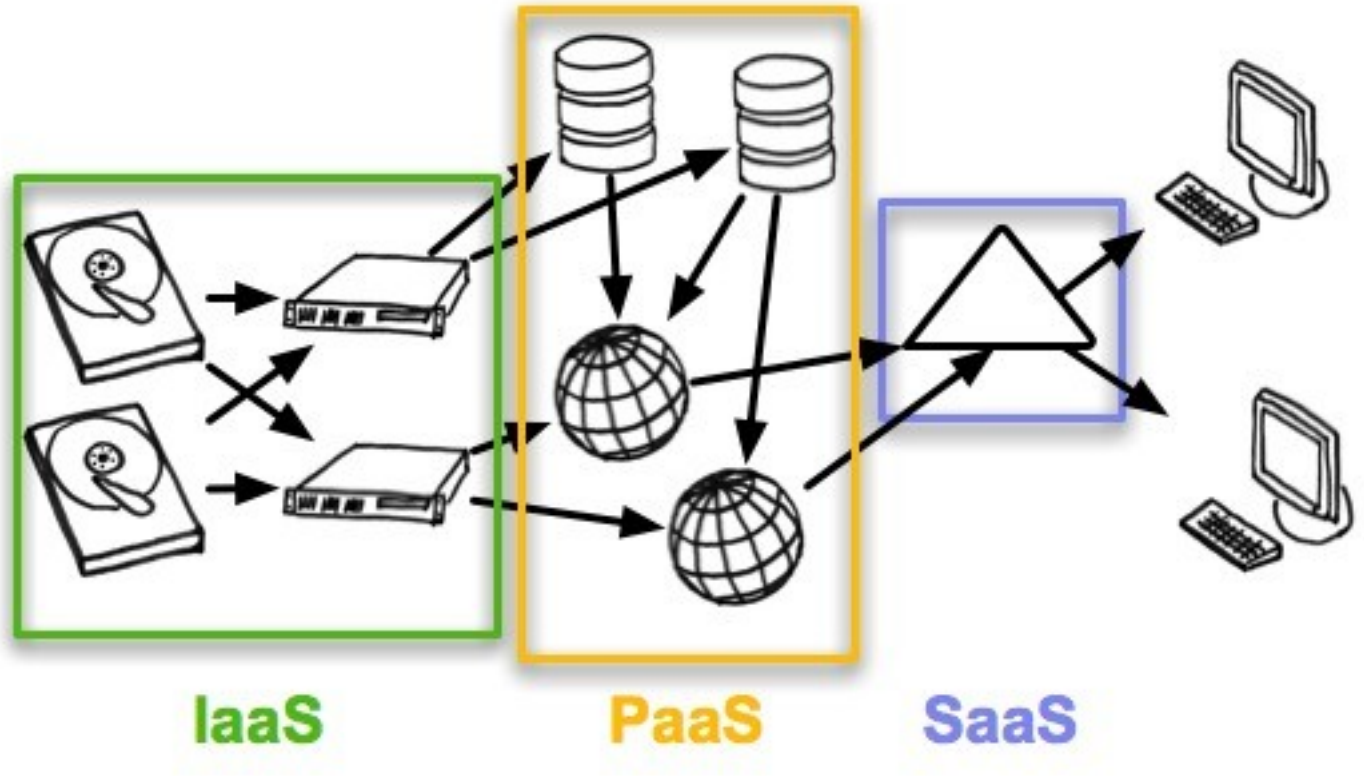
Audits and Assessments

We start with an example of an IT-Service realised *traditional*:



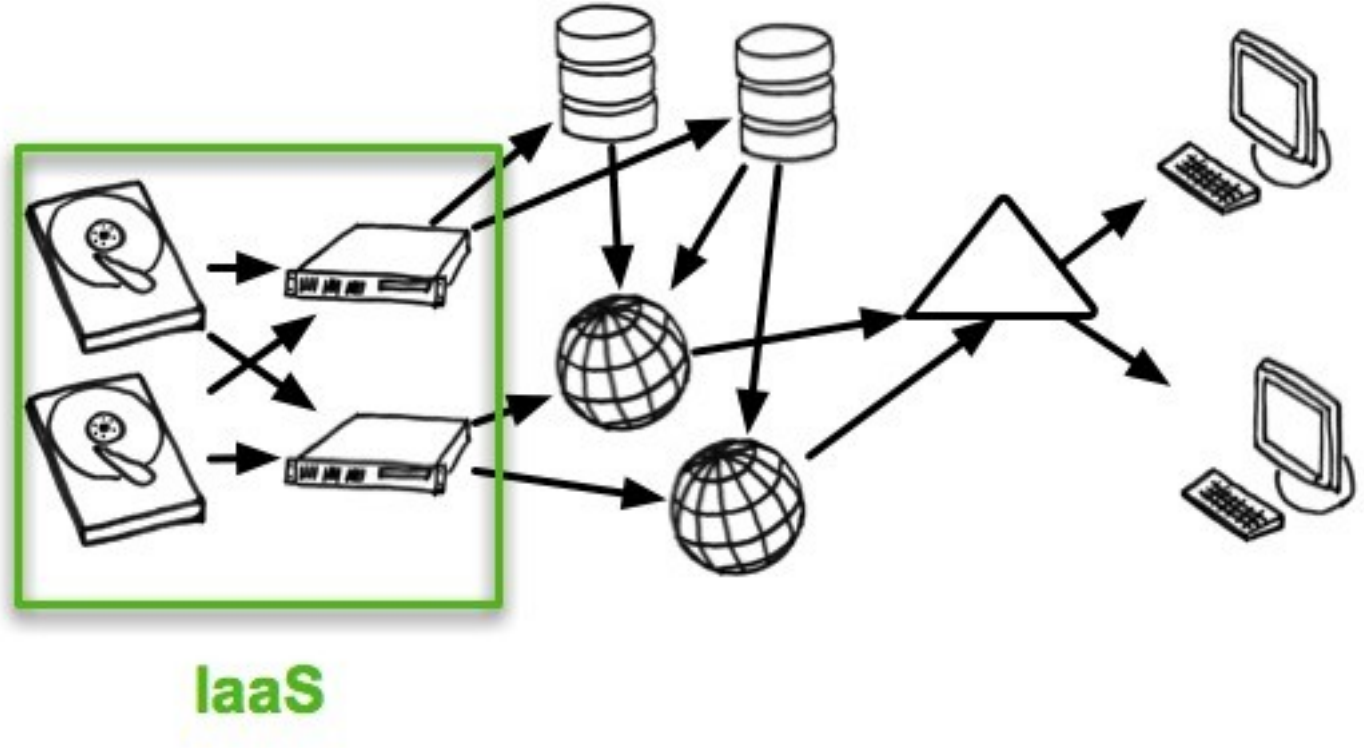
Use Cloud Services

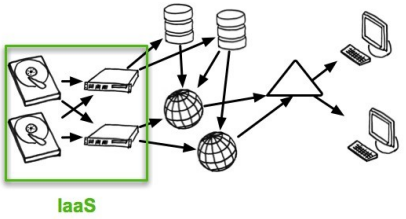
Service delivery models for cloud services:



IaaS

Use IaaS cloud services for storage and virtual instances:



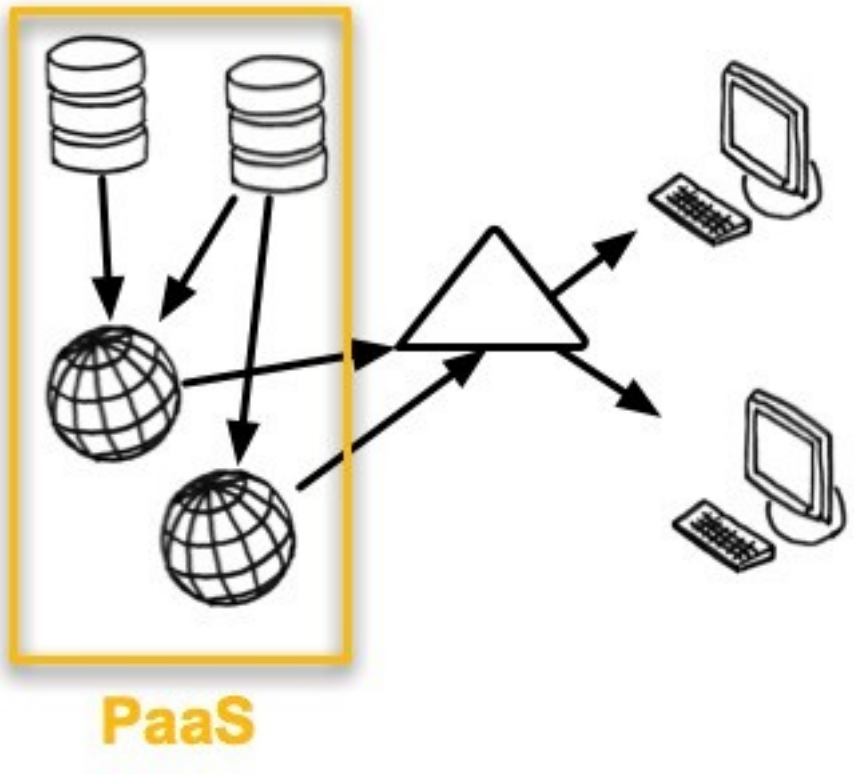


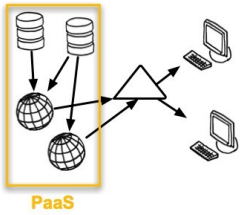
IaaS

- **Host security** instead of network security for access and transfer of data
- **Encryption** (possible for transfer, but not feasible for computation, data bases)
- **Multi-tenancy**
- **Access of cloud provider** restricted by processes and documented
- **Restrict locations**
- **Standardized API**, logging, monitoring, reporting
- **Deletion of Data**

PaaS

Use PaaS cloud services for data base and application server, web server:

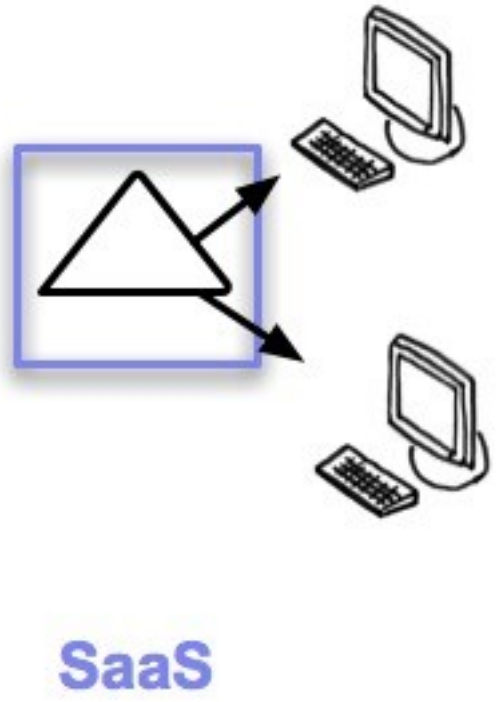


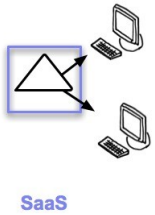


PaaS

- **Support requirements for data privacy in applications** (e.g. data bases)
- **Identity and Access Management** (as feature)
- **Encryption** (possible for transfer, but not feasible for computation, data bases)
- **Multi-tenancy**
- **Access of cloud provider** restricted by processes and documented
- **Restrict locations**
- **Standardized API**, logging, monitoring, reporting
- **Deletion of Data**

Use SaaS cloud services for the IT-service





SaaS

- **Support requirements for data privacy, operational requirements**
- **Identity and Access Management**
- **Encryption** (possible for transfer, but not feasible for computation)
- **Multi-tenancy**
- **Access of cloud provider** restricted by processes and documented
- **Restrict locations**
- **Standardized API**, logging, monitoring, reporting
- **Deletion of Data**

Realising requirements

Host security instead of network security for access and transfer of data (IaaS, virtual instances)

- Allowed by cloud provider, realised by cloud user

Encryption

- For virtual instances (IaaS) realised by cloud user, otherwise by cloud provider

Standardized API, logging, monitoring, reporting

- Standards need to be developed and established (see e.g. DMTF approach)

“Rest of requirements”

- Realised by cloud provider

Checking Requirements

Responsibility for personal data

- Cloud user

Realisation of requirements for processing of personal data

- Cloud provider (often)

To cope with responsibility cloud user needs to assess the requirements regularly

- **Standard assessments and audits**

Audits and Assessments

Audits and Assessments incorporating privacy requirements

- EuroPrise
- PIA (Privacy Impact Assessment, UK)
- BSI IT-Grundschutz
- Common Criteria

EuroPrise - European Privacy Seal

- Certification applicable to IT services or IT products
- Based on Data Protection Directive and E-Privacy Directive of the European Union
- Checked by admitted experts from legal and technical perspective, accredited certification authority checks the evaluation report
- Performed after the close of a project
- SaaS Cloud services with a fixed environment could be checked (outsourcing)

PIA - Privacy Impact Assessment

Introduction

Privacy in Cloud Services

Audits and Assessments

- EuroPrise
- **PIA**
- BSI IT-Grundschutz
- Common Criteria
- Assessments of Cloud Services

PIA - Privacy Impact Assessment of the ICO (Information Commissioner's Office) in the UK

- Assessment applicable to IT services or IT products
- Evaluate and manage risk of IT projects caused by privacy issues already during initialisation phase of the project
- Accompagnies project during all phases, privacy issues are managed as risks
- SaaS Cloud services with a fixed environment could be checked (outsourcing)

BSI IT-Grundschutz

Introduction

Privacy in Cloud Services

Audits and Assessments

- EuroPrise
- PIA
- **BSI IT-Grundschutz**
- Common Criteria
- Assessments of Cloud Services

IT Grundschutz of BSI (Bundesamt für Sicherheit in der Informationstechnik)

- Framework focussed on IT services
- Based on ISO27001, structured in modules, module about privacy
- Define, analyse and document IT service, analyse threats, model safeguards based on IT-Grundschutz catalogues
- Can accompagny project during all phases
- SaaS Cloud services with a fixed environment could be checked (outsourcing), should incorporate cloud technology in threat analysis

Common Criteria standard

- Certification for IT products
- Target of Evaluation (TOE) is defined, protection profiles from standard catalogue or individually defined, intended Evaluation Assurance Level (EAL),
  TOE is checked against a selected protection profile with EAL,
- Performed after the close of a project
- IaaS, PaaS, (SaaS) cloud service to built IT services can be checked concerning privacy requirements, multi-tenancy, encryption, etc.

Assessments of Cloud Services

Common audit in the US:

SAS 70 Type II audit

- American Institute of Certified Public Acountants (AICPA)
- service organisations defines control objectives and corresponding control activities, audit checks these controls
- addresses financial statement audits of cloud users in the US

Assessments of Cloud Services

Introduction

Privacy in Cloud Services

Audits and Assessments

- EuroPrise
- PIA
- BSI IT-Grundschutz
- Common Criteria
- **Assessments of Cloud Services**

Why use cloud providers SAS 70 Type II and not EuroPrise, IT-Grundschutz (ISO 27001), PIA etc. ?

- SAS70 Type II in **needed by cloud users in the US** which is the focus of the cloud market
- SAS 70 Type II is not about services but only about the **whole service organisation**

Assessments of Cloud Services

Introduction

Privacy in Cloud Services

Audits and Assessments

- EuroPrise
- PIA
- BSI IT-Grundschutz
- Common Criteria
- **Assessments of Cloud Services**

Open source initiatives (OpenStack, Eucalyptus):
Broader range of cloud providers, regional adapted cloud services and more possibilities for control

Process oriented standards for cloud operations, based on service operations frameworks like ITIL (see DMTF whitepaper) facilitate assessments

Legal requirements will lead to compliant cloud services

Conclusion

Cloud computing is not a new technology but a new access concept for IT services

- No new problems but known problems
- Impacts are worse because of the dynamic and size of clouds
- Assessments for privacy can be used for cloud services, but restrict flexibility

Possible next steps: Adapt assessments to dynamically changing cloud networks, but standard cloud APIs are needed addressing automated check of requirements

Thank you for your attention

Questions ?