



openHPI – Internet Security Privacy: Cloud

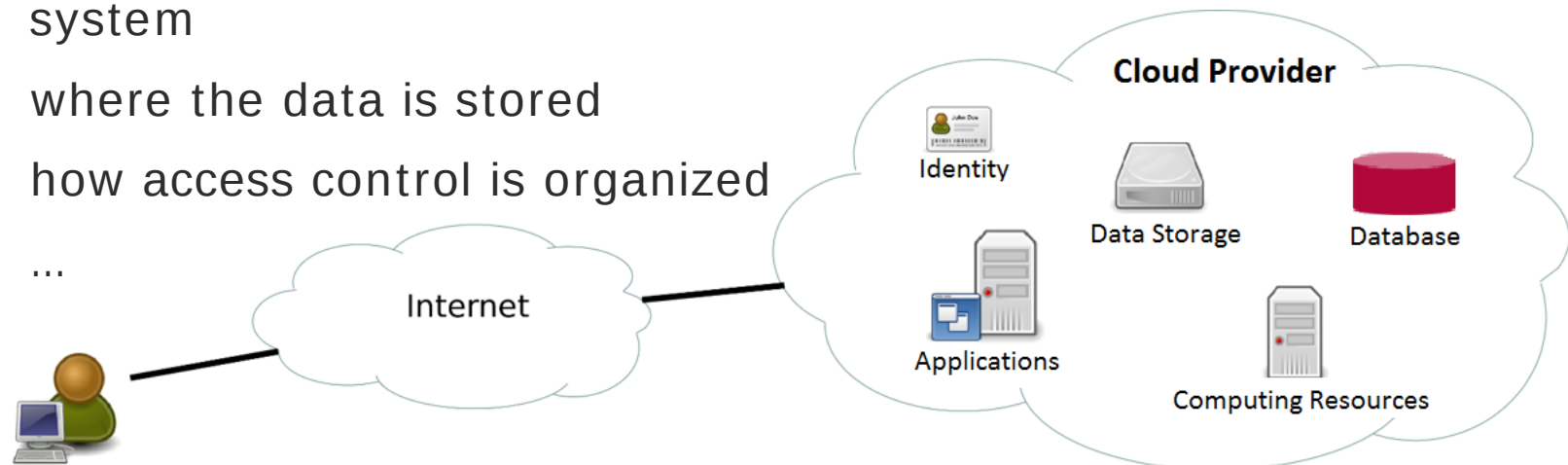
Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

What is Cloud Computing?

"Cloud" is a metaphor which means, that users do not see the technical infrastructure and do not have to worry about it when they use computer resources (computing power, storage space, applications)

Example: Cloud data store

- Users store data without knowing
 - on which server, on which hardware, with which operating system
 - where the data is stored
 - how access control is organized
 - ...



Cloud Technologies Everywhere (1/3)

A Cloud is very attractive to the (IT) industry as well as end users

- There are various **cloud models**:
 - SaaS – Software as a Service
 - PaaS – Platform as a Service
 - IaaS – Infrastructure as a Service

Advantages:

- **Users** do not need a computing infrastructure to use a computing system, to run a software, or to store data. They simply need a device to input data and show results
- **Cloud provider** takes care of the computing infrastructure, installs and updates the programs and offers interfaces to use these infrastructure and programs
- ...

Cloud Technologies Everywhere (2/3)

A Cloud is very attractive to the (IT) industry as well as end users

Advantages:

- Users require less in-depth knowledge, everything is offered as a (managed) service, for example,
 - backup, office, storage, ...
- Users can access their data and software with all their devices and from anywhere via the Internet
- Manufacturers can save on devices because complex calculations take place in the cloud - only data input and display of the results take place on the device
- ...

Cloud Technologies Everywhere (3/3)

A Cloud is very attractive to the (IT) industry as well as end users

Advantages:

- Restoration and exchange of data is made much easier
 - it is relatively hard to organize backups at home at a comparable backup level - and much more expensive (hardware + power + software + time)
- Cloud infrastructures are usually quite professionally protected against attacks and offer various security certificates
 - even employees of cloud service providers that have access to user data must be checked

Integration of Cloud Computing (1/2)

Many IT systems are now closely linked to the cloud, e.g. all modern operating systems use cloud technologies

- **Apple OS X and iOS** are integrated with iCloud: PhotoLibrary, Drive, Keychain (passwords), Backup (including applications and application data), Find My iPhone / iPad / Mac (Anti-Theft)
 - link to Apple ID
- **Android** phones are integrated into the cloud by Google: Settings and contact data, apps and application data can be stored in the cloud
 - link to Google account
- **Windows 10**: OneDrive for photos and (office) documents, backup, notes
 - link to Microsoft account

Integration of Cloud Computing (2/2)

Voice recognition software such as Siri, Cortana and Google Voice Search also work with cloud technology

Further examples:

- Document processing in the cloud (or browser)
 - GoogleDocs
 - Microsoft Office365 (Office WebApps)
- Data storage in the cloud
 - Dropbox
 - Google Drive
- Software Development
 - Cloud9.com
 - Codeanywhere.com
- ...

Privacy and Cloud Computing

In order to enable cloud functionality, computers or smartphones must be connected almost permanently to the Internet

- Although not directly linked to cloud technology, manufacturer surveillance or collection of data and user activity is similar and uses the same technologies

Main risks:

- Without special precautions, operating system manufacturers or cloud service providers have full access to the data and logs stored in the cloud
- Compromising the user account usually offers full access to all data
- Users can not protect themselves against an attack on cloud infrastructure

Target: Cloud Users

Many users do not realize that data synchronization is often done silently in the background and all data like photos and documents are synchronized within the cloud storage

Even users who are informed about cloud technology often underestimate the risks

- Users themselves are the simplest attack target for gaining access to cloud data storage
- **Example:** „Celebgate“ (2014)
 - hacker attack on iCloud storage of celebrities
 - email addresses (e.g., appleprivacysecurity@gmail.com) were used to steal passwords via phishing mails
 - with the password, attackers got full access to the iCloud account, stole private photos and published them on the Internet

Encryption for Cloud Data Storage

Measures to preserve privacy for cloud storage:

- **Encrypt the data before uploading it** to the Cloud

Proprietary solutions with their own client applications, protocols and encryption are not trusted because nobody can view the source code to verify that encryption and protocols are actually secure ...

- Cloud data storage with access via open protocols such as WebDAV (Yandex.Disk, 4shared.com, Box.com, etc.) and independent client software with encryption feature, guarantee data security
 - Duplicati is one popular free (LGPL) software for encrypted incremental backup
- Encryption requires user know-how
 - **Caution:** Keys must never be lost!