AK IT-Security 1

Current Research - Cloud Computing and E-Government

Bernd Zwattendorfer
Graz, 12.11.2014
Overview

» What is Cloud Computing?
   » Definition
   » Models

» Cloud Computing in E-Government
   » Benefits/Drawbacks

» Secure Storage in the Public Cloud
   » Using the Austrian citizen card

» Cloud and eID
   » Cloud Identity Models
   » eID Authentication at Public Clouds
   » A new Identity as a Service Model
Overview

» What is Cloud Computing?
  » Definition
  » Models
» Cloud Computing in E-Government
  » Benefits/Drawbacks
» Secure Storage in the Public Cloud
  » Using the Austrian citizen card
» Cloud and eID
  » Cloud Identity Models
  » eID Authentication at Public Clouds
» A new Identity as a Service Model
What is Cloud Computing?

» Definition of the NIST:
  » “Cloud computing is 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.” (Mell & Grance, 2010)

» Features
  - On-Demand Self Service
  - Broad Network Access
  - Resource Pooling
  - Rapid Elasticity
  - Measured Services
Characteristics

- **On-Demand Self-Service / Self-provisioning of resources**: Management of resources by the user/customer – Resources can be requested on demand and can be provided immediately

- **Broad Network Access**: All resources are broadband connected via the Internet or Intranet

- **Resource Pooling**: Computing resources are pooled in one place and made available to several users

- **Massive Scalability**: Resources can be made available to the appropriate extent depending on requirements

- **Rapid Elasticity**: Resources can be allocated in real-time and (partly) automated according to the changing needs of the user

- **Measured Service / Pay as you go**: Consumption-oriented payment or settlement model

- **Multitenancy**: Resources and services are shared dynamically between all users
Overview

» What is Cloud Computing?
  » Definition
  » Models

» Cloud Computing in E-Government
  » Benefits/Drawbacks

» Secure Storage in the Public Cloud
  » Using the Austrian citizen card

» Cloud and eID
  » Cloud Identity Models
  » eID Authentication at Public Clouds

» A new Identity as a Service Model
Deployment Models

» Models based on operational and organizational aspects

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

Broad Network Access
# Evaluation – Public Clouds

<table>
<thead>
<tr>
<th>Public Clouds</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strengths</strong></td>
<td><strong>Weaknesses</strong></td>
</tr>
<tr>
<td>- High availability</td>
<td>- Compliance with legal regulations</td>
</tr>
<tr>
<td>- Reliability</td>
<td>- Isolation issues due to multi-tenancy</td>
</tr>
<tr>
<td>- High elasticity</td>
<td>- Less detailed logging capabilities</td>
</tr>
<tr>
<td>- Facilitated patch management</td>
<td>- Proprietary interfaces</td>
</tr>
<tr>
<td>- Distribution for failure safety</td>
<td></td>
</tr>
<tr>
<td>- Low costs</td>
<td></td>
</tr>
</tbody>
</table>
# Evaluation – Private Clouds

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Strong control</td>
<td>• Higher costs</td>
</tr>
<tr>
<td>• Detailed logging/auditing</td>
<td>• Specific point to attack</td>
</tr>
<tr>
<td>• Compliance with legal regulations</td>
<td>• Lack of elasticity</td>
</tr>
</tbody>
</table>

![Diagram of Private Cloud](image_url)
# Evaluation – Community Clouds

<table>
<thead>
<tr>
<th>Community Clouds</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strengths</strong></td>
<td><strong>Weaknesses</strong></td>
</tr>
<tr>
<td>⬤ Lower costs than private cloud</td>
<td>⬤ Competition between consumers</td>
</tr>
<tr>
<td>⬤ Elasticity</td>
<td>⬤ Specific point to attack</td>
</tr>
<tr>
<td>⬤ Compliance with legal regulations</td>
<td>⬤ Consensus between involved parties required</td>
</tr>
<tr>
<td></td>
<td>⬤ No accurate prediction on required resources</td>
</tr>
<tr>
<td></td>
<td>⬤ Who is the legal entity in case of liability</td>
</tr>
</tbody>
</table>

![Diagram of Community Clouds](image)

- Classification:
  - Organization
  - Organization
  - Organization

---

*Graz, 12.11.2014*

*Bernd Zwattendorfer*
# Evaluation – Hybrid Clouds

<table>
<thead>
<tr>
<th>Hybrid Clouds</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strengths</strong></td>
<td><strong>Weaknesses</strong></td>
</tr>
<tr>
<td>- Flexibility</td>
<td>- Complexity</td>
</tr>
<tr>
<td>- Stronger control</td>
<td>- Compatibility issues due to different interfaces</td>
</tr>
<tr>
<td></td>
<td>- Classification of data (sensitive data should not be stored in public cloud)</td>
</tr>
</tbody>
</table>

![Diagram of Hybrid Clouds](image)
Service Models

» Models based on technical and service aspects

- Everything as a Service (XaaS)
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
## Evaluation – Infrastructure as a Service

### Infrastructure as a Service (IaaS)

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Operating systems or application runtime can be chosen by the customer</td>
<td>• Increase of administrative complexity</td>
</tr>
<tr>
<td>• Full control over operating system and runtime</td>
<td>• Customers have to maintain updates on their own</td>
</tr>
</tbody>
</table>
### Evaluation – Platform as a Service

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Focus on application development instead of infrastructure</td>
<td>• Existing applications must be amended to provided interfaces</td>
</tr>
<tr>
<td>• Less administrative effort</td>
<td>• Vendor lock-in</td>
</tr>
</tbody>
</table>

**Platform as a Service (PaaS)**

Graz, 12.11.2014

Bernd Zwattendorfer
Evaluation – Software as a Service

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Minimum administrative effort</td>
<td>• Very generic and not easily extendable</td>
</tr>
<tr>
<td>• Quick adoption</td>
<td>• Cost intensive</td>
</tr>
</tbody>
</table>

Software as a Service (SaaS)
Overview

» What is Cloud Computing?
  » Definition
  » Models

» Cloud Computing in E-Government
  » Benefits/Drawbacks

» Secure Storage in the Public Cloud
  » Using the Austrian citizen card

» Cloud and eID
  » Cloud Identity Models
  » eID Authentication at Public Clouds
  » A new Identity as a Service Model
Cloud Computing for the Public Sector

» Benefits
  » Cost Savings
    » “[…] over a 13-year life cycle, the total cost of implementing and sustaining a cloud environment may be as much as two-thirds lower than maintaining a traditional, non-virtualized IT data center.” (Alford, 2009)

» Market Potential
  » Growth rate of 26% for the upcoming years (Deloitte, 2009)
  » Concentration of core business (Khan et al., 2011)

» Already on the agendas of European Bodies
  » ENISA (Priorities for Research on Current and Emerging Network Trends)
  » European Commission
    » Digital Agenda for 2020:
      » “[…] an EU-wide strategy on cloud computing notably for government and science.“
      » "Unleashing the Potential of Cloud Computing in Europe"
  » Cloud for Europe (C4E)
    » Public sector requirements and usage scenarios for cloud computing
Benefits for the Public Sector

» Scalability
  » High load close to deadlines (e.g. elections, tenderings etc.)

» Payment model
  » „Pay-as-you-go“

» Easy implementation
  » No in-house infrastructure, APIs

» Less maintenance efforts
  » Automatic updates and patches

» Availability
  » Spread and multiple computing centers of the cloud provider
Chances and Risks for the Public Sector

» Legal
  » Data Protection and Privacy
  » Influence only via contracts (SLA)

» Structural
  » Vendor Lock-In

» Economic
  » Costs for functional adaptations
  » Operational costs vs. Investment costs

» Technical
  » Standardisation
  » Security
Cloud Computing in Europe

» Austria
  » Emphasize cost savings but struggle with security and data protection
  » Favours private and community clouds over public clouds

» Denmark
  » Decrease cost of IT services
  » Moved services of Danish procurement authority into the cloud (2011)

» Ireland
  » Cloud computing is part of Irish technological action plan
  » Expects 10,000 high value jobs in this area

» United Kingdom
  » G-Cloud installation (Private or community cloud covering all service layers)
Overview

» What is Cloud Computing?
  » Definition
  » Models

» Cloud Computing in E-Government
  » Benefits/Drawbacks

» Secure Storage in the Public Cloud
  » Using the Austrian citizen card

» Cloud and eID
  » Cloud Identity Models
  » eID Authentication at Public Clouds
  » A new Identity as a Service Model
Motivation

» Public Cloud Storage
Motivation

» Secure Public Cloud Storage
Motivation

» Secure Public Cloud Storage using Smart Cards
The Software CCE (Citizen Card Encrypted)

» Platform-independent Open Source Tool
» Encryption and decryption based on software and hardware keys
» Supports Austrian Citizen Card
» S/MIME as container format
» Uses local file-system as a data storage
Implementation

LDAP directory

Austrian Citizens

Citizen Card Encrypted (CCE)

1

2

3

Public Cloud

Dropbox

Google Drive
Implementation

» Inclusion of Cloud Storage Services
  » DropBox
  » Google Drive

» Mapping between Cloud-Credentials and Smart Card
  » Login to cloud automatically

» Connection with the file system
  » By moving a file into a specific cloud folder the file is encrypted automatically
Screenshots - Encryption

- Store files and folders within an encrypted container
- Store container in the cloud
- Unlock device
- Please enter PIN/password for device: My Smartcard
- Store container
- Please enter the name of the container file
Screenshots - Decryption

- Open encrypted_container.cce
- Get access to files or folders stored in an encrypted container
  - Matching key found! Press next to decrypt the container.
  - Depending on the used key store you will be asked for the appropriate PIN or password.

Decryption of files and directories stored in a container

- Select directory: C:samples\1\Dropbox\App\CCE
- Choose the desired directory to decrypt
Evaluation - Advantages

» Usage of external PKI Infrastructure
  » LDAP directory enables encryption for arbitrary Austrian citizens
  » User-Management separated from cloud provider

» Vendor Lock-In Prevention
  » Keys are managed by a trusted external party, not CCE
  » Substitution of cloud provider is easier

» Secure hardware-based decryption
  » Private key cannot be read out of hardware
  » 2-Factor Authentication

» Open Source Implementation
  » Easy to extend
  » Additional cloud providers, different container format, PKI, etc.
Evaluation - Disadvantages

» Web interface and mobile version is missing
  » Use of smart cards with mobile phones difficult
  » Storing private key securely is difficult
» Two way sync with cloud storage
  » First encrypted locally, then upload
» Smart card reader necessary
  » Reducing the systems to be used
Overview

» What is Cloud Computing?
  » Definition
  » Models

» Cloud Computing in E-Government
  » Benefits/Drawbacks

» Secure Storage in the Public Cloud
  » Using the Austrian citizen card

» Cloud and eID
  » Cloud Identity Models
  » eID Authentication at Public Clouds
  » A new Identity as a Service Model
Identity in the Cloud-Model

- Similar to isolated model
- Identity data are managed by the same cloud provider that hosts the application
- No effort or costs for user management
- User management of cloud provider is used
- e.g., Google

[Zwattendorfer et al., 2014 (WEBIST)]
Identity to the Cloud-Model

- Similar to central model
- Identity data are managed by external identity provider
- IdP hosted by external organization
- Existing infrastructure can be re-used
- Higher control on identity data
- e.g., Google Apps Salesforce.com

[Zwattendorfer et al., 2014 (WEBIST)]
Identity from the Cloud-Model

- "Identity as a Service"
- Identity data are provided from external cloud provider
- Hybrid cloud model
- Choose desired provider
- Outsourcing of user management to cloud
- e.g., Intel Cloud SSO, SkIDentity

[Zwattendorfer et al., 2014 (WEBIST)]
Overview

» What is Cloud Computing?
   » Definition
   » Models

» Cloud Computing in E-Government
   » Benefits/Drawbacks

» Secure Storage in the Public Cloud
   » Using the Austrian citizen card

» Cloud and eID
   » Cloud Identity Models
   » eID Authentication at Public Clouds
   » A new Identity as a Service Model
Current Situation

» Main Issues:
  » Username/Password authentication
  » Two separate authentication processes
    » Usually two different credentials
STORK Authentication to the Public Cloud

- Identity to the Cloud Model
- Google Apps und Salesforce.com
- Strong authentication (national eIDs) instead of username/password
- Support of 18 MS eIDs
- Single Sign-On
Screenshots

https://docs.google.com/a/xyz.com/
Overview

» What is Cloud Computing?
  » Definition
  » Models
» Cloud Computing in E-Government
  » Benefits/Drawbacks
» Secure Storage in the Public Cloud
  » Using the Austrian citizen card
» Cloud and eID
  » Cloud Identity Models
  » eID Authentication at Public Clouds
» A new Identity as a Service Model
Motivation – Current Deployment

Service Provider Domain 1

MOA-ID

bPK

Online Application

User

bcard

eg卡
Motivation – Current Deployment

Scalable, but many instances of MOA-ID!
Motivation – Central Deployment
Motivation – Central Deployment

» Advantages
  » Users only need to trust one specific Identity Provider
  » Possibility of Single Sign-On (SSO)
  » No separate Identity Provider installation at the Service Provider (Save Costs)
  » Support of different identity protocols

» Disadvantage
  » Single Point of Failure/Attack
  » Scalability
Motivation – Central CLOUD Deployment
Motivation – Central CLOUD Deployment of an Identity Provider

» Advantages
- Users only need to trust one specific Identity Provider
- Possibility of Single Sign-On (SSO)
- No separate Identity Provider installation at the Service Provider (Save Costs)
- Support of different protocols

» Scalability

» Disadvantage
- Single Point of Failure/Attack
- Privacy (Cloud Provider acts honest but curious)
A user-centric and privacy-preserving Identity as a Service Model for eIDs

(a) Client-side model
Requirements

» Qualified and authentic identity data
  » High quality attributes applicable for eIDs

» Semi-trusted identity providers
  » E.g., public clouds

» Integration effort and complexity
  » Easy integration into existing infrastructures

» Privacy
  » Identity data/attributes must be preserved wrt. to the identity provider

» User-centricity
  » User always remains in full control over her identity data

» Selective Disclosure
  » User can disclose only parts of her identity data
Cryptographic Preliminaries

» Redactable Signatures

» Allow for replacement or removal of (specified) parts of a message after signature creation such that the original signature stays valid (and no interaction with the original signer is required).
**Redactable Signatures**

Receiver of a **conventional signature** gets:

\[
\text{Signature } S = \text{Sign}(\text{Hash}_{\text{TOTAL}})
\]

Total Hashvalue
\[
\text{Hash}_{\text{TOTAL}} = h_1 \| h_2 \| h_3 \| h_4 \| h_5
\]

Receiver of a **redactable signature** gets:

\[
\text{Hashvalue } H(m_4)
\]

This text contains private data

**Summary:**

Redactable signatures allow for the redaction of private data from a message, while still preserving the integrity of the remaining text through a total hash value. The redacted data is then signed, ensuring that any alteration of the message can be detected. This approach provides a balance between security and confidentiality, making it suitable for applications where partial disclosure of information is necessary.
Proxy Re-Encryption

A semi-trusted proxy can alter a ciphertext, which has been encrypted for one party A, so that it may be decrypted by another party B.

The proxy thereby gains neither access to the plaintext of the data nor to the decryption key.
Proxy Re-Encryption

Plaintext → Encrypt → C_A → Proxy → C_B → Decrypt → Plaintext

- A’s Public Key
- Re-Encryption Key A→B
- B’s Private Key
- A’s Private Key
- B’s Public Key
The Model - Registration

- Identity data are issued by a trusted third party
- Registration process depends on the underlying eID approach
- Identity data are encrypted for the user by the registration authority and signed by a redactable signature scheme
The Model - Authentication

1.) User wants to access protected resource

(a) Client-side model
The Model - Authentication

(a) Client-side model

2.) User redacts all attributes which should not be disclosed to the service provider + Re-encryption key generation for SP
The Model - Authentication

(a) Client-side model

1.) & 6.)
3.)
2.) 4.)
5.)
User Control
User

3.) Redacted identity data and re-encryption key are sent to IdP in the cloud
The Model - Authentication

1.) & 6.)
3.)
2.) 4.)
5.)

User Control

(a) Client-side model

IdP verifies identity data and re-encrypts it for the SP
The Model - Authentication

(a) Client-side model

1.) & 6.)
3.)
2.) 4.)
5.)

User Control

User

Encrypted Attributes

Client

Registration Authority (RA)

Service Provider

Identity Provider

Authentication

Transfer identity data to SP based on existing protocol (e.g. SAML)
The Model - Authentication

(a) Client-side model

1.) & 6.)
3.)
2.) 4.)
5.)

6.) Verify and decrypt attributes and provide resource

User

Encrypted Attributes

User Control

Client

Service Provider

Authentication

Identity Provider

Registration Authority (RA)

Registration
Requirements

» Qualified and authentic identity data
  Attributes are signed and certified by trusted authority

» High quality attributes applicable for eIDs

» Semi-trusted identity providers
  Only encrypted data is provided to the IdP

» Integration effort and complexity
  Existing identity protocols already support the transfer of encrypted data and digital signatures out-of-the-box

» Privacy
  Cloud provider sees data in encrypted form only

» User centricity
  Only the user is able to decrypt the data and to generate re-encryption keys

» Selective Disclosure
  User can redact a subset of attributes
Identification and Authentication in Austria

Application

Enrolment

Identity Link

Certificate

SourcePIN

Identity Provider

(MOA-ID)

Service Provider

ssPIN

Citizen Card

security layer

Citizen is uniquely **identified** (Identity Link)

and **authenticated** by verifying a qualified electronic signature

Enrolment

more information
Process Flow - Current Situation

1. Request Authentication

2. SAML AuthnRequest

3. Read Identity Link

4. Verify Identity Link

5. Generate ssPIN

6. Create Signature

7. Verify Identity Link

8. SAML Assertion (ssPIN)

9. Provide Resource

Service Provider

Identity Provider (MOA-ID)

Client Middleware
Identity Link

Current Situation
» SourcePIN and personal data
» Conventionally signed by trusted authority

New Model
» Personal data are encrypted
» All ssPINs (encrypted) instead of sourcePIN
» Signed by trusted authority using a redactable signature scheme

...<saml:SubjectConfirmationData>
  <pr:Person xsi:type="pr:Physical"
    <pr:Identification>
      <pr:Value>123456789012</pr:Value>
      <pr:Type>http://reference.e-g</pr:Type>
    </pr:Identification>
  <pr:Name>
    <pr:GivenName>John</pr:GivenName>
    <pr:FamilyName>Doe</pr:FamilyName>
  </pr:Name>
  ...
  <saml:Attribute
    AttributeName="CitizenPublicKey"
  ...
  <dsig:RSAKeyValue>
    <dsig:Modulus>snW80LC49qNefems</dsig:Modulus>
    ...
Process Flow – New Model

1. Request Authentication

2. SAML AuthnRequest

3. Read Identity Link

4. Return redacted Identity Link and re-encryption key

5. Verify redacted Identity Link + re-encrypt attributes

6. SAML Assertion (re-encrypted attributes)

7. Decrypt attributes

8. Provide Resource

Client Middleware

Service Provider

Identity Provider (MOA-ID)
Conclusions

» Cloud computing can be advantageous for the public sector
  » Cost savings, scalability, etc.
  » But: privacy and security issues

» Use of eIDs and cryptographic technologies can help

» Want to support us?
  » Seminars/Projects:
    » http://www.iaik.tugraz.at/content/teaching/master_courses/seminar_project/
References

» P. Mell, T. Grance, - “The NIST definition of cloud computing” - NIST 2010
» T. Alford - “The Economics of cloud computing” - Booz Allen Hamilton – 2009
» F. Khan, B. Zhang, S. Khan, S. Chen - „Technological leap frogging e-government through cloud computing“ - 2011 - 4th IEEE International Conference on Broadband Network and Multimedia Technology
» Bernd Zwattendorfer, Arne Tauber - "The Public Cloud for E-Government" - IADIS International Conferences Web Based Communities and Social Media and Collaborative Technologies 2012
» Bernd Zwattendorfer, Bojan Suzic, Peter Teufl, Andreas Derler - "Sicheres Speichern in der Public Cloud mittels Smart Cards" - D-A-CH Security 2013
» Bernd Zwattendorfer, Bojan Suzic, Peter Teufl, Andreas Derler - "Secure Hardware-Based Public Cloud Storage" - Open Identity Summit 2013
» Bernd Zwattendorfer, Daniel Slamanig - "On Privacy-Preserving Ways to Porting the Austrian eID System to the Public Cloud" - 28th IFIP TC-11 International Information Security and Privacy Conference (SEC 2013)
» Daniel Slamanig, Klaus Stranacher, Bernd Zwattendorfer - "User-Centric Identity as a Service-Architecture for eIDs with Selective Attribute Disclosure" - 19th ACM Symposium on Access Control Models and Technologies (SACMAT 2014)
Thank you for the attention!

Bernd Zwattendorfer—
bernd.zwattendorfer@egiz.gv.at
www.egiz.gv.at