Cloud Computing in Health Care - On effective ways to deal with sensitive patient data in a secure Cloud environment

ISC-CLOUD 2013

24.09.2013

Horst Schwichtenberg, Steffen Claus – Fraunhofer SCAI
Julian Laufer - RHÖN-KLINIKUM AG
Approach

„On effective ways to deal with sensitive patient data in a secure Cloud environment“

■ “effective ways”
  ■ implemented holistic IT-Solution
■ “sensitive patient data”
  ■ General protective goals and challenges
■ “secure Cloud”
  ■ preventive measures
German SMEs and Cloud Acceptance

- Bitkom/KPMG (2012)
  - Just 5-10% of all SMEs (small and medium enterprises) make use of public Cloud services (SaaS, PaaS, IaaS)
  - 99% of all German enterprises are SMEs
  - Positive attitude towards Cloud: 25% (large enterprises: 60%)

![Chart](image_url)

Quelle: KPMG
Program: Trusted Cloud

- Overcome the lack of trust in Cloud by SMEs and Public Services
- Enable new businesses based on Cloud technologies in Germany
Health Care & Cloud Provider?

Challenges and questions:

• No official cloud security regulations for health care
• What is the likelihood and impact of potential risk to health information
• Usage of cloud storage
• Is there any top-notch security to fulfill by the provider to be compliant with regulations for health data
• How to deal with „rights on the data“ and the liabilities
  → different than HIPAA rules for data ownership

• ...

© Fraunhofer SCAI
“Natural Language Processing (NLP) of clinical text for secondary use - as a Service in a Community Cloud “

- **Averbis GmbH:**
  - Coordinator, NLP, Anonymisation

- **Fraunhofer SCAI:**
  - Cloud-Experts, Text- und Data-Mining

- **Universitätsklinikum Erlangen:**
  - Data provider, architecture, data protection officer

- **RHÖN-KLINIKUM AG:**
  - Architecture, operational tests with users
  - Data protection officer

- **TMF e.V.:**
  - Data security in personal data processing, legal expertise
Hip joint prosthesis: Retrospective study

Plausibility checks: Especially focused on economical aspects

Pharmaco-Vigilance: Early warning system for side-effects

Pathologie
Cloud-based Service System: Architecture

„On effective ways to deal with sensitive patient data in a secure Cloud environment“
Classic goals of data protection/security

„On effective ways to deal with sensitive patient data in a secure Cloud environment“

- **Confidentiality**
  - Only authorized persons can access sensitive data
    - → Encryption; access controls

- **Integrity**
  - Data is complete, up-to-date and untampered(?)
    - → Signatures, Hashing

- **Availability**
  - Data can be accessed/processed in a timely manner
    - → e.g. redundancy
Further data protection goals

„On effective ways to deal with sensitive patient data in a secure Cloud environment“

Protective goals:

- Transparencies
  - Replicable IT-Processes
    - documentation, view on processes, monitoring und protocols

- Limited applicability
  - Dedicated data usage
    - Anonymisation, function-/tenancy separation, deletion of data

- Intercede possibilities
  - Person affected rights
    - Allow Actions on Data, Single-point-of-contact

- Revision…
Clinic-Internal Preprocessing

- Challenge
  - Personal patient data
- Approach
  - De-Identification
  - Transfer data base
  - Temp Ids
  - Anonymisation
- Possible attacks
  - Re-Identification

ID → tempID

© Fraunhofer SCAI
Re-Identification

Y. Erlich (01/2013)
- “Identifying personal genomes by surname inference”
- “anonymized” genome sequences were linked with public data bases → re-identification possible

Dankar (07/2012)
- “Estimating the re-identification risk of clinical data sets”
- Allows for estimation of “uniqueness” of data

IMS Health / pharmafakt / VSA
- Business model based on selling receipt data
- Anonymisation / Pseudonymisation
- Conflicting statements of german data protection officers (BayLDA, T. Weichert/ULD)
Data transfer to the Cloud

- **Challenge**
  - Data transfer via insecure and public network
- **Approach**
  - VPN (SSL/TLS)
  - BSI guidelines (key lengths, ciphers)
- **Possible attacks**
  - Div.
Attacks on SSL/TLS

- Weaknesses of ciphers
  - E.g. BEAST, CRIME, Lucky 13, RC4, etc.
- Compromising the trust chain
  - Attacks on CAs (e.g. Diginotar)
  - „loss“ of private keys (maybe forced?)
- End user misuse
  - Short keys
  - careless key handling / PKI
  - Usage of old/broken ciphers
- Weaknesses of PRNGs
  - Implementing backdoors on purpose
  - closed-source PRNGs, hardware based
„On effective ways to deal with sensitive patient data in a secure Cloud environment“

Cloud-Testbed @Fraunhofer SCAI

Development and test environment for Cloud Services

Deployment of use cases

Production environment
Cloud: Multi-tenancy

„On effective ways to deal with sensitive patient data in a secure Cloud environment“

- Separations
  - VPN server
  - VLANs
  - Image-Store
  - App-Layer

E.g. www-01.ibm.com/software/ecm/content-analytics/uima.html
Cloud

- Data non-persistent
- VMs will be deleted after text mining.
- Service/VM is controlled by the user in the clinic
- Limited lifetime of Cloud services, destroy „hanging VMs
- Shutdown immediately after the document processing
- Startup immediately before document processing
- Secure VM image storage, transfer to nodes via SCP
- Prevention of vendor lock-in
- Open standards, migration concepts
- Load- and penetration tests
Cloud Text Mining: Startup

- Challenge
  - Secure deployment
- Approach
  - VM-Template
  - secure storage
  - „reserved“/exclusive nodes
  - Image temporarily located on node
Cloud text mining: Processing

- Challenge
  - Inter-node communication
- Approach
  - VLANs
  - Doc-encryption
  - Exclusive nodes
  - Encrypted Interprocess Communication

Diagram:
- Klinik A
- EP
- VLAN A
- Terminologies
- Cloud storage
- Worker
- Worker
- Worker

© Fraunhofer SCAI
Cloud text mining: Shutdown

- Challenge
  - „cleaning up“
- Approach
  - Deletion of VMS, no patient data is persisted
- Possible attacks
  - E.g. (A. Kolb, 05/2013, Forensics in the Cloud)
IT-Security: Orientation

- BDSG: See attachment for §9 sentence 1
  - Postulates certain security measures that follow the state-of-the-art
- BSI Eckpunktepapier Cloud-Computing (2011)
  - Minimum requirements towards information security
  - 15 areas (security management, data centers, networks, data security, portability, …)
- BSI-Grundschutz (BSI 100-2)
  - Information security management; guideline with concrete security measures
  - Adaption of the standard to Cloud-specifics (e.g. virtual networks, cloud management, cloud Storage), approx. end of 2013
- Requirements of the clinic partners within cloud4health
- Other helpful guidelines and frameworks
  - ENISA (Information Assurance; Benefits and Risks)
  - NIST Guidelines
  - CSA Security Guideance
Generell Approach:

Protect data by making the barriers as high possible

Components:
- Anonymisation, Deidentification at the hospital
- Streaming: Avoid storing data in the cloud
- Encryption
- Secure transfer, even when it is encrypted
- Isolation and no storing of used virtual machines
- Leave control of virtual machines to the hospital
- Store results again in a secure zone (maybe hospital)
Summary

• based on: OpenNebula, Open vSwitch, OpenVPN
  a Community Cloud environment is running at SCAI
• design and implementation is done by RHÖN-KLINIKUM AG IT & SCAI
• the Infrastructure is accepted at the hospital for the use case data
• Services established and first use case is in operation
• Ongoing work: checking middleware and OS to harden, further discussion with data protection officers on different levels.
• Performance Benchmarks
• Future work: Openstack Evaluation; ways to handle malicious insiders (e.g. integrating development from SealedCloud?)
Thanks for your attention!

Horst.schwichtenberg@scai.fraunhofer.de