Security and Privacy System Requirements for Adopting Cloud Computing in Healthcare Data Sharing Scenarios

Research-in-Progress

Tatiana Ermakova
Technical University of Berlin
tatiana.ermakova@tu-berlin.de

Benjamin Fabian
Humboldt Universität zu Berlin
bfabian@wiwi.hu-berlin.de

Rüdiger Zarnekow
Technical University of Berlin
ruediger.zarnekow@tu-berlin.de

ABSTRACT

The emerging cloud computing technology enables new essential scenarios in healthcare, in particular those of data sharing among practitioners. Nevertheless, their security and privacy concerns still impede the wide adoption of cloud computing in this area. Although there are numerous publications in the context of cloud computing in healthcare, we found no consistent typical security and privacy system requirements framework in this domain so far. Owing to the lack of those studies and preparing the ground for creating secure and privacy-friendly cloud architectures for healthcare, we survey security and privacy system requirements for cloud-based medical data sharing scenarios using two strategies. We base on a systematic design science approach following the literature-driven requirement elicitation strategy and apply an established security requirement elicitation methodology as part of the scenario-driven strategy. Finally, we evaluate and compare the two security and privacy system requirements elicitation strategies used in this paper.

Keywords

Cloud Computing, Healthcare, Security, Privacy, Requirement.

INTRODUCTION

There are multiple new scenarios enabled through the adoption of the emerging cloud computing technology in healthcare (Loehr et al., 2010), whereas the data sharing scenarios are of high relevance to practitioners (He et al., 2010; Kanagaraj and Sumathi, 2011; Huang et al., 2011; Zhang and Lu, 2010). Nevertheless, cloud computing also faces many security and privacy challenges (Deng et al., 2011; Ekonomou et al., 2011), which raise wide concerns among patients and medical workers (Li et al., 2011b, Li et al., 2012, Chen et al., 2012a; Deng et al., 2012; Shini et al., 2012; Abbadi et al., 2011), in particular the risk of losing control over data (Chen and Hoang, 2011, Li et al., 2010). Many researchers observe a research potential with respect to the existing security and privacy preserving mechanisms (Loehr et al., 2010; Abbadi et al., 2011; Deng et al., 2011; Shini et al., 2012), while Ekonomou et al. (2011) call for establishing human trust campaigns.

Although there are numerous publications in the domain of cloud computing in healthcare, to our knowledge there are few works about general and systematic security and privacy system requirements frameworks so far (Zhang and Liu, 2010; Deng et al., 2011) and none that are elicited by multilateral requirements engineering methods, which would be able to also point out potential conflicts between the requirements. With this background we aim to take first steps to close this research gap.

The present work is aimed to support the TRESOR (TRusted Ecosystem for Standardized and Open cloud-based Resources) research project with healthcare practitioners (TRESOR, 2013) funded by the German Federal Ministry of Economics and Technology. To elicit security and privacy system requirements, we follow literature-driven and scenario-driven strategies. The implication of the first strategy is conducted in accordance with the design science framework proposed by Hevner et al. (2004). Based on the literature search framework introduced by vom Brocke et al. (2009), we systematically review articles published up to year 2012 dealing with security and privacy preserving mechanisms for the use of cloud computing in healthcare, then define system security and privacy requirements, and evaluate them in semi-structured interviews with different experts from the German healthcare industry. We use the requirement pattern presented by Rupp (2005, in German) to formulate the requirements. The second strategy covers security and privacy system requirements arising from specific processes and multiple stakeholders with different interests in healthcare data sharing scenarios and relies on an established security requirements elicitation methodology called Multilateral Security Requirements Analysis (MSRA) (Fabian et al.,

2010; Gürses et al., 2005; Gürses and Santen, 2006; Gürses et al., 2006; Gürses, 2010). Finally, we provide a comparison of the two security and privacy elicitation strategies and further research options in this field.

The paper is organized as follows. The background and work related to the topic is provided in section 2. We introduce our research design in section 3 and present the results in the fourth section. In conclusion, we summarize all findings and present our further research directions.

BACKGROUND AND RELATED WORK

The relatively new technology of cloud computing creates a scenario diversity in healthcare (Loehr et al., 2010), one of them the medical data sharing scenarios remarked by He et al. (2010), Kanagaraj and Sumathi (2011), Huang et al. (2011), and Zhang and Lu (2010) as being of particularly high relevance to practitioners. The wide adoption of cloud computing in healthcare is, however, impeded by many still open security and privacy challenges (Deng et al., 2011; Ekonomou et al., 2011). Li et al. (2011b), Li et al. (2012), Chen et al. (2012a), Deng et al. (2012), Shini et al. (2012). Abbadi et al. (2011) speak about concerns among patients and medical workers, which Chen and Hoang (2011) and Li et al. (2010) in particular relate to the risk of losing control over data. Loehr et al. (2010), Abbadi et al. (2011), Deng et al. (2011), and Shini et al. (2012) call for further research on the existing security and privacy preserving mechanisms, while Ekonomou et al. (2011) propose undertaking campaigns for establishing human trust.

An unsystematic analysis of some related security and privacy threats for medical data sharing scenarios in the cloud computing environment is provided by Nematzadeh and Camp (2010), Shini et al. (2012), and Loehr et al. (2010). There are also some authors who introduce security and privacy-enhancing mechanisms, however without a careful analysis of multilateral security and privacy requirements. Those works elaborate on access control (Basu et al., 2012; Chen and Hoang, 2011; Chen et al., 2012a; Chen et al., 2012b; Li et al., 2010; Li et al., 2012; Yu et al. 2010), keyword search over encrypted records (Li et al., 2011b), unlinkability between the patient and the electronic health record (Li et al., 2011a), and tracing of traitors (Nematzadeh and Camp, 2010). Attempts to elicit security and privacy system requirements with respect to medical data sharing in the cloud were undertaken by Zhang and Liu (2010) and Deng et al. (2011). Deng et al. (2011) relied on the business logic and the architecture of a home healthcare system in the cloud, particularly aimed to support depressed patients. The review of related literature thus shows there is no security and privacy system requirements framework elicited by established security requirement elicitation approaches (Gürses et al., 2005; Gürses and Santen, 2006; Gürses et al., 2006; Gürses, 2010; Fabian et al., 2010), in particular the multilateral ones, which would be able to also point out potential conflicts between requirements.

RESEARCH DESIGN

In our research, we apply literature-driven and scenario-driven strategies to elicit security and privacy requirements.

While applying the first one, we follow the design science framework proposed by Hevner et al. (2004) and elicit system requirements in three cycles, namely rigor cycle, design cycle, relevance cycle. In the rigor cycle, we conduct a systematic literature search on security and privacy friendly mechanisms for the use of cloud computing in healthcare in accordance with the literature search framework proposed by vom Brocke et al. (2009). We base on the AIS ranking list and search in the EBSCOhost, IEEE Xplore, Emerald, ScienceDirect, AISeL, Springer, ACM Digital Library and Proquest literature databases, and apply a combined backward and forward search. Then we evaluate the findings of the literature analysis and define the initial draft in the design cycle. In the final relevance cycle we conduct semi-structured interviews with different experts from the German healthcare industry to evaluate the developed requirements. We formulate the requirements in accordance with the framework presented by Rupp (2005, in German).

To define scenario-driven, multilateral security and privacy requirements, we follow the multilateral security requirements analysis (MSRA) method (Gürses et al., 2005; Gürses and Santen, 2006; Gürses et al., 2006; Gürses, 2010; Fabian et al., 2010). According to Fabian et al. (2010), the paradigm of multilateral security contradicts the traditional view by acknowledging stakeholders' conflicting interests with respect to assets. This is essential in healthcare delivery involving multiple parties. Based on the main functionalities of a data sharing scenario enabled through cloud computing, we identify stakeholders, i.e., parties concerned to the system-to-be, and elaborate on their security and privacy goals. In all the steps, we rely on the expert interviews and the literature analysis. In our further research we are going to identify facts and assumptions as the relevant properties of the environment and refine stakeholder views on the scenario taking them into account, reconcile the identified security and privacy goals by capturing conflicts between them, finding compromises between conflicting goals, and establishing a consistent set of security and privacy system requirements. Finally, we will reconcile them and functional requirements in a real project.

RESULTS

Literature-driven system security and privacy requirements collection

Zhang and Liu (2010) refer to traditional security goals (e.g., Fabian et al., 2010) confidentiality, integrity and availability extended by authentication, non-repudiation, and audit and archiving, as well as ownership of information, patent consent and authorization. These are referred to and used by Chen et al. (2012b) and further extended by Deng et al. (2011).

Type	Concept / Security or Privacy Goal	Source	Requirement
Security	Users' Authenticity and Authentication	Zhang and Liu (2010), Chen et al. (2012a), Chen et al. (2012b)	The system shall verify the identities of users at the entry of every access (Zhang and Liu, 2010).
Security	Non-Repudiation of Users' Actions	Zhang and Liu (2010), Chen et al. (2012a), Chen et al. (2012b)	The system shall ensure that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction (Zhang and Liu, 2010).
Security	Non-Repudiation of Users' Emergency Access	Loehr et al. (2010)	The system shall ensure that one cannot deny having had an emergency access.
Security	Auditability of Users' Actions	Zhang and Liu (2010), Chen and Hoang (2011), Deng et al. (2011), Basu et al. (2012), Chen et al. (2012b)	The system shall record user actions (e.g., in a chronological order by maintaining a log of every access to and modification of data) (Zhang and Liu, 2010).
Security	Users' Sharing and Access without Patient's Involvement	Loehr et al. (2010), Basu et al. (2012)	The system shall enable data sharing and access without the patient's involvement.
Privacy	Users' Anonymity	Loehr et al. (2010), Nematzadeh and Camp (2010), Li et al. (2011b)	The system shall prevent determining the user's identity based on her actions and/or indexes (Li et al. 2011b).
Privacy	Confidentiality of Users' Access Privileges	Chen and Hoang (2011), Yu et al. (2010)	The system shall ensure access privileges information is accessible only to the authorized users.

Table 1. User-Related System Security and Privacy Requirements Collection through a Literature Analysis

The special properties addressed by the authors of security and privacy friendly mechanisms for the use of cloud computing in healthcare data sharing scenarios are formulated as fine-grained access control (Li et al., 2010; Yu et al., 2010; Chen and Hoang, 2011; Li et al., 2011b; Basu et al., 2012; Li et al., 2012), access right revocation (Li et al., 2010; Li et al., 2011b; Li et al., 2012; Basu et al., 2012), flexible data access policies (especially under emergency scenarios) or emergency exceptions (Li et al., 2010; Li et al., 2011a; Li et al., 2012), efficiency, scalability, and usability (e.g., user secret key accountability) of the proposed mechanisms (Li et al., 2010; Yu et al., 2010; Li et al., 2011b; Basu et al., 2012; Li et al., 2012), write access control (Li et al., 2012), record anonymity (Li et al., 2011a), index and query privacy (Li et al., 2011b), and user access privilege confidentiality (Yu et al., 2010). Further related concepts include prevention of security attacks and violations (Nematzadeh and Camp, 2010; Chen et al., 2012b; Shini et al., 2012), data sharing and access without the patient's involvement (Loehr et al., 2010; Basu et al., 2012), secure record's navigation (Basu et al., 2012), confidentiality of a

medical record's existence for a given person (Loehr et al., 2010), client anonymity (Loehr et al., 2010; Nematzadeh and Camp, 2010), and non-repudiation of emergency access (Loehr et al., 2010).

Type	Concept / Security or Privacy Goal	Source	Requirement
Security	Ownership of Medical Record	Zhang and Liu (2010), Chen et al. (2012b), Shini et al. (2012)	The system shall define the creator, author and manager of the data (Zhang and Liu, 2010).
Security	Confidentiality of Medical Record	Zhang and Liu (2010), Yu et al. (2010), Chen and Hoang (2011), Deng et al. (2011), Li et al. (2011a), Basu et al. (2012), Chen et al. (2012b), Li et al. (2012), Shini et al. (2012)	The system shall ensure the data is accessible only to the authorized readers (Zhang and Liu). The system shall ensure the data is accessible only to the unauthorized contributors (Li et al., 2012).
Security	Integrity of Medical Record	Zhang and Liu (2010), Chen and Hoang (2011), Deng et al. (2011), Li et al. (2011a), Chen et al. (2012a), Chen et al. (2012b), Shini et al. (2012)	The system shall preserve the accuracy and consistency of data (Zhang and Liu, 2010).
Security	Availability and Utility of Medical Record	Deng et al. (2011), Basu et al. (2012), Shini et al. (2012)	The system shall ensure the availability and utility of data when needed.
Security	Archiving of Medical Record	Zhang and Liu (2010), Chen et al. (2012b)	The system shall restore data without a loss when needed (Zhang and Liu, 2010).
Security	Patient Consent and Authorization for Medical Record Sharing	Zhang and Liu (2010), Deng et al. (2011), Chen et al. (2012b), Basu et al. (2012)	The system shall allow the patient to grant rights over her or his data to other users (Zhang and Liu, 2010).
Security	Fine-Grained Access to Medical Record	Li et al. (2010), Yu et al. (2010), Chen and Hoang (2011), Deng et al. (2011), Li et al. (2011b), Basu et al. (2012), Li et al. (2012)	The system shall ensure different users are authorized to read and write different sets of data (Li et al., 2010; Li et al., 2012; Li et al., 2011b).
Security	Revocation of Access to Medical Record	Li et al. (2010), Li et al. (2011b), Basu et al. (2012), Li et al. (2012)	The system shall prevent the user from future access when necessary (Li et al., 2010; Li et al., 2012; Li et al., 2011b). The system shall prevent the user from access to future data when necessary (Li et al., 2012).

Table 2. Medical Record-Related System Security and Privacy Requirements Collection through a Literature Analysis

Based on these observations, we derive three system security and privacy requirements collection sets, namely those directly related to users, i.e., medical workers, the flow and storage of medical records and the system itself, which we respectively

present in Table 1, Table 2, and Table 3. An initial observation already reveals some conflicts between the security and privacy goals specified, e.g., patent consent and authorization to medical record sharing and users' sharing and access without the patient's involvement, auditability of users' actions and users' anonymity, as well as confidentiality of medical records and emergency exception. This supports the necessity of a multilateral security paradigm.

Type	Concept / Security or Privacy Goal	Source	Requirement
Security	Flexible or/and Emergency Access to Medical Record	Li et al. (2010), Nematzadeh and Camp (2010), Deng et al. (2011), Li et al. (2011a), Li et al. (2012)	The system shall allow changes to the data access policies (Li et al., 2010; Li et al., 2012).
Privacy	Unlinkability between Patients and Medical Records	Li et al. (2011a)	The system shall ensure the unlinkability between patients and documents (Li et al., 2011a).
Privacy	Patients' Anonymity in Medical Record	Deng et al. (2011)	The system shall prevent determining the patient's or/and owner's identity based on the document (Li et al., 2011a).
Privacy	Confidentiality of Medical Record's Existence	Loehr et al. (2010), Basu et al. (2012)	The system shall ensure information about a document's existence for a given patient is accessible only to the authorized users (Loehr et al., 2010).

Table 2. (cont.) Data-Related System Security and Privacy Requirements Collection through a Literature Analysis

Type	Concept / Security or Privacy Goal	Source	Requirement
Security	Availability and Utility of System	Zhang and Liu (2010), Deng et al. (2011), Chen et al. (2012b)	The system shall serve its purpose and be available when needed (Zhang and Liu, 2010).
Security	Efficiency, Scalability and Usability of System	Li et al. (2010), Yu et al. (2010), Deng et al. (2011), Li et al. (2011b), Basu et al. (2012), Li et al. (2012)	The system shall be efficient, scalable and usable. The system shall support a large and unpredictable number of users (Li et al., 2010; Li et al., 2012; Li et al. 2011b).
Security	Detection and Prevention of Security Attacks and Violations in System	Nematzadeh and Camp (2010), Chen and Hoang (2011), Chen et al. (2012b), Shini et al. (2012)	The system shall detect and prevent any security attacks and violations (e.g., illegal behavior over data) (Chen and Hoang, 2011), e.g. by sending an alert when malicious action is in progress.

Table 3. System-Related System Security and Privacy Requirements Collection through a Literature Analysis

Scenario driven security and privacy requirements elicitation

Following the MSRA framework provided by TAPAS (2004), Gürses et al. (2005), and Fabian et al. (2010) and based on the preliminary literature analysis and expert interviews, we identify direct stakeholders whose information is being exchanged

and indirect stakeholders only interested in the system-to-be. The information exchanged is then specified in an information model.

In the taxonomy of direct stakeholders' roles, we differentiate between the roles of Patient and Clinician who may be a doctor (e.g., intern, senior physician, chief physician, and consultant physician) or a nurse (e.g., nurse, senior nurse, and medical registration). Among indirect stakeholders, we distinguish between a Health Care Cloud (HCC), some independent researcher, the government, Healthcare Certification Authority (HCA), National Health Insurance (NHI) (TAPAS, 2004; Li et al., 2011a) and a non-clinician in a healthcare organization who may perform QA (Quality Assurance) management, administration (e.g., administrative employee, administrative registration, research employee, controlling, data protection officer), IT-administration, or spiritual welfare.

Stakeholder	Information Object	Counter-Stakeholder	Requirement Derived from a Literature Analysis
Patient	Medical Records	Clinician	Confidentiality of Medical Record Integrity of Medical Record Fine-Grained Access to Medical Record Revocation of Access to Medical Record Flexible or/and Emergency Access to Medical Record Patient Consent and Authorization to Medical Data Sharing
		Non-Clinician	Confidentiality of Medical Record's Existence Unlinkability between Patients and Medical Records
	Identification Data	Non-Clinician	Patients' Anonymity in Medical Record
	Patients' Data (possibly) to be revealed from Clinicians' Actions and/or Indexes	Non-Clinician	
Clinician	Actions and Identification Data	Outside	Users' Anonymity
	Access Privileges	Outside	Confidentiality of Users' Access Privileges
	Decisions (possibly) to be revealed from Medical Records	Non-Clinician	
	Local Content	Outside	

Table 3. System Security and Privacy Requirements Collection through a Scenario Analysis

A scenario where information sharing between clinicians with respect to a patient takes place can be described as follows. After completion of treatment, the patient is discharged from the hospital and goes to another hospital or rehabilitation facility. Her doctor sends medical records containing the patients' medical history, diagnosis, medications, allergies etc., whereas the nurse provides other information, e.g., the patient's having an infectious germ. The communication is enabled via cloud. Similar information sharing scenarios are considered in the works by He et al. (2010), Kanagaraj and Sumathi (2011), Huang et al. (2011), Zhang and Lu (2010).

For our main two direct stakeholders' roles, we formulate corresponding information models. The information being shared about a Patient includes:

- medical records;
- patients' identification data (possibly) contained in medical records;
- patients' data (possibly) to be revealed from clinicians' actions and/or indexes.

The information model of a Clinician constitutes:

- clinicians' actions (e.g., data transmission or/and reception) and identification data audited for non-repudiation purposes;
- clinicians' access privileges;
- clinicians' decisions (possibly) to be revealed from medical records;
- local content in case of using local-based services.

Potential security threats may arise from both inside and outside counter-stakeholders driven by curiosity, the expectation of profit making, etc. (TAPAS, 2004; Deng et al., 2011). The potential counter-stakeholders can be other patients, medical personal not involved in the treatment, colleagues of the patient, insurance companies, the public, etc.

In Table 3, we define some requirements suggestions describing which counter-stakeholder's actions should be restricted in respect to which information object of which stakeholder and compare them to the previously derived ones. The possible actions here may include sharing, reading, modifying, and deleting. The table shows, the requirement sets derived through a literature and scenario analysis have many requirements in common as well as contain some unique ones.

CONCLUSION AND FURTHER WORK

The wide adoption of the new cloud computing paradigm facilitating new essential scenarios in healthcare is mainly restricted by security and privacy challenges and concerns.

In the present work, we derived a set of security and privacy system requirements for adopting cloud computing in healthcare data sharing scenarios based on a design science approach in the literature-driven strategy and the multilateral security requirements analysis methodology in the scenario-driven strategy.

Both requirements elicitation strategies gave many common results, but also helped to capture some unique requirements, thus supplementing each other. The common requirements are related to the medical records and identification data of patients, as well as the actions, identification data, and access privileges of clinicians in the system. The scenario analysis also revealed patients' data (possibly) to be revealed from clinicians' actions and/or indexes, decisions (possibly) to be revealed from medical records, and local content in case of using local-based services as protection targets. The literature analysis additionally pointed out users' authenticity and authentication; auditability, non-repudiation of users' emergency and non-emergency actions; users' actions with and without patient's involvement; as well as system's availability and utility, efficiency, scalability and usability, and detection and prevention of security attacks and violations there. Thus, the comparison shows, the scenario-driven strategy provides much more detailed results, whereas the literature-driven strategy gives a more comprehensive varied requirements set, here possibly due to mature state of research in this field.

The observation of the results of the adoption of the literature-derived strategy revealed some conflicts between the security and privacy goals specified, e.g., patent consent and authorization to medical record sharing and user's sharing and access without the patient's involvement, auditability of users' actions and users' anonymity, as well as confidentiality of medical records and emergency exception. Through the application of the principles of the established MSRA method in the information sharing scenario, we identified the concerned parties and their security and privacy information assets to be protected. Our future work here will be aimed at identifying facts and assumptions and refining stakeholder views, capturing conflicts between security and privacy goals and searching compromises between them to make the security and privacy requirements set consistent.

The concluding research goal we see is a more detailed evaluation and comparison of the two security and privacy elicitation techniques used in this paper, namely the literature research focusing on system security and privacy system requirements within a design science framework, and an established multilateral security requirements method that is able to refine the former approach and to point out (and hopefully solve) potential requirements interactions or conflicts in an early system development phase.

REFERENCES

Abbadi, I. M.; Deng, M.; Nalin, M.; Martin, A.; Petkovic, M.; Baroni, I. (2011) Trustworthy Middleware Services in the Cloud, in *Proceedings of the 3rd International Workshop on Cloud Data Management*.

Basu, S.; Karp, A.; Li, J.; Pruyne, J.; Rolia, J.; Singhal, S.; Suermondt, J.; Swaminathan, R. (2012) Fusion: Managing Healthcare Records at Cloud Scale. *IEEE Computer Special Issue on Move Toward Electronic Health Records*.

Chen, L.; Hoang, D. B. (2011) Novel Data Protection Model in Healthcare Cloud, in *Proceedings of the IEEE International Conference on High Performance Computing and Communications*.

Chen, T.-S.; Liu, C.-H.; Chen, T.-L.; Chen, C.-S.; Bau, J.-G.; Lin, T.-C. (2012a) Secure Dynamic Access Control Scheme of PHR in Cloud Computing. *Journal of Medical Systems,* 6.

Chen, Y.-Y.; Lu, J.-C.; Jan, J.-K. (2012b) A Secure EHR System Based on Hybrid Clouds. *Journal of Medical Systems,* 5.

Deng, M.; Petkovié, M.; Nalin, M.; Baroni, I. (2011) A Home Healthcare System in the Cloud - Addressing Security and Privacy Challenges, in *Proceedings of the IEEE 4th International Conference on Cloud Computing*.

Deng, M.; Nalin, M.; Petkovié, M.; Baroni, I.; Marco, A. (2012) Towards Trustworthy Health Platform Cloud, *Secure Data Management*, Lecture Notes in Computer Science, 7482, 162-175.

Ekonomou, E.; Fan, L.; Buchanan, W.; Thüemmler, C. (2011) An Integrated Cloud-Based Healthcare Infrastructure, in *Proceedings of the 3rd IEEE International Conference on Coud Computing Technology and Science*.

Fabian, B.; Gürses, S.; Heisel, M.; Santen, T.; Schmidt, H. (2010) A Comparison of Security Requirements Engineering Methods, *Requirements Engineering Journal*, 15, 1.

Gürses, S. (2010) Multilateral Privacy Requirements Analysis in Online Social Networks, PhD Thesis, HMDB, Department of Computer Science, K.U. Leuven, Belgium.

Gürses, S.; Berendt, B.; Santen, T. (2006) Multilateral Security Requirements Analysis for Preserving Privacy in Ubiquitous Environments, in Berendt and Menasalvas (Eds.) *Proceedings of the UKDU Workshop*.

Gürses, S.; Santen, T. (2006) Contextualizing Security Goals: A Method for Multilateral Security Requirements Elicitation, in J. Dittmann (Ed.) *Proceedings of the Sicherheit 2006 - Schutz und Zuverlässigkeit*.

Gürses, S.; Jahnke, J. H.; Obry, C.; Onabajo, A.; Santen, T.; Price, M. (2005) Eliciting Confidentiality Requirements in Practice, in *Proceedings of the 15th Annual International Conference hosted by the IBM Centers for Advanced Studies*.

Ekonomou, E.; Fan, L.; Buchanan, W.; Thüemmler, C. (2011) An Integrated Cloud-Based Healthcare Infrastructure, in *Proceedings of the 3rd IEEE International Conference on Cloud Computing Technology and Science*.

He, C.; Jin, X.; Zhao, Z.; Xiang, T. (2010) A Cloud Computing Solution for Hospital Information System, in *Proceedings of the IEEE International Conference on Intelligent Computing and Intelligent Systems*.

Hevner, A.R., March, S.T., Park, J., Ram, S. (2004) Design Science in Information Systems Research. *MIS Quarterly*, 28.

Huang, Q.; Ye, L.; Yu, M.; Wu, F.; Liang, R. (2011) Medical Information Integration Based Cloud Computing, in *Proceedings of the International Conference on Network Computing and Information Security*.

Kanagaraj, G.; Sumathi, A.C (2011) Proposal of an Open-Source Cloud Computing System for Exchanging Medical Images of a Hospital Information System, in *Proceedings of the 3rd International Conference Trendz in Information Sciences and Computing*.

Li, M.; Yu, S.; Ren, K.; Lou, W. (2010) Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-Owner Settings. *Security and Privacy in Communication Networks und Social Informatics and Telecommunications Engineering*, 50, Lecture Notes of the Institute for Computer Sciences, 89-106.

Li, Z.-R.; Chang, E.-C.; Huang, K.-H.; Lai, F. (2011a) A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform, in *Proceedings of the IEEE 15th International Symposium on Consumer Electronics*.

Li, M.; Yu, S.; Cao, N.; Lou, W. (2011b) Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing, in *Proceedings of the 31st International Conference on Distributed Computing System*.

Li, M.; Yu, S.; Zheng, Y.; Ren, K.; Lou, W. (2012) Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption, *IEEE Transactions on Parallel and Distributed Systems*.

Loehr, H.; Sadeghi, A.-R.; Winandy, M. (2010) Securing the E-Health Cloud, in *Proceedings of the ACM International Health Informatics Symposium*.

Nematzadeh, A.; Camp, L. J. (2010) Threat Analysis of Online Health Information System, in *Proceedings of the 3rd International Conference on PErvasive Technologies Related to Assistive Environments*.

Rupp, C. (2005) UML 2 glasklar : Praxiswissen für die UML-Modellierung und -Zertifizierung, Carl Hanser Verlag.

Shini, S.G; Thomas, T.; Chithraranjan, K. (2012) Cloud Based Medical Image Exchange-Security Challenges, in *Proceedings of the International Conference on Modelling, Optimization and Computing*.

TAPAS (2004) TAPAS Security Requirements, http://www.opentapas.org/docs/security_requ.html. Accessed February 20, 2013.

TRESOR (2013) TRESOR, http://www.cloud-tresor.com/. Accessed May 10, 2013.

vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Plattfaut, R.; Cleven, A. (2009) Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process, in *Proceedings of the 17th European Conference on Information Systems*.

Yu, S.; Wang, C.; Ren, K.; Wenjing L. (2010) Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, in *Proceedings of the 29th Conference on Information communications*.

Zhang, R.; Liu, L. (2010) Security Models and Requirements for Healthcare Application Clouds, in *Proceedings of the IEEE 3rd International Conference on Cloud Computing*.

Zhang, J.; Lu, J. (2010) The District Medical Data Center Based on Cloud Computing, in *Proceedings of the 5th International Conference on Computer Science & Education*.