Identification of IT Security and Legal Requirements Regarding Cloud Services

Constantin Christmann, Jürgen Falkner, Andrea Horch, Holger Kett
Fraunhofer Institute for Industrial Engineering IAO
Stuttgart, Germany
e-mail: {constantin.christmann, juergen.falkner, andrea.horch, holger.kett}@iao.fraunhofer.de

***Abstract*—The adoption of cloud computing holds tremendous potential for small and medium-sized enterprises (SMEs) as it enables them to reduce costs as well as improve flexibility and scalability. In order to choose an appropriate cloud service, it is necessary to carefully identify functional and non-functional requirements. In this regard, the aspects affecting IT security as well as legal requirements are important topics to the users of SMEs. However, the smaller the enterprise, the lower the probability that there is enough expertise to identify the requirements in these subject areas. Addressing this issue, the contribution of this paper is the description of a method for identifying IT security and legal requirements regarding a cloud service in a structured kind of way. The presented method was implemented as a part of a prototype for a cloud service search. Based on this search system, an evaluation with users of SMEs was conducted. The evaluation results attest the search system and its underlying method to successfully assist users regarding the identification of relevant legal and IT security requirements, hence reducing the amount of expertise required by users of SMEs, as well as the associated effort of searching for appropriate cloud services.**

Keywords- cloud computing; cloud services; IT security; legal; requirments; service search.

I. INTRODUCTION

The adoption of cloud computing holds tremendous potential for organizations of all shapes and sizes. Especially small and medium-sized enterprises (SMEs) are highly interested in cloud computing as it enables them to reduce costs as well as improve flexibility and scalability [1]. In order to choose the right cloud service, a thorough identification of functional as well as non-functional requirements regarding such service is necessary. Due to the necessary outsourcing of data – which is often a crucial asset of an enterprise - aspects of cloud services affecting information technology (IT) security as well as legal requirements are important topics to users of SMEs [2][3]. However, the smaller the enterprise, the lower the probability that there is enough expertise to identify the requirements in these subject areas. Hence, the contribution of this paper is the description of a method for identifying IT security and legal requirements regarding a cloud service in a structured kind of way. We did implement this method as part of a prototype for a cloud service search (depicted in Fig. 1). In this search system, the search is based on functional and non-functional requirements. In order to define the non-functional requirements – addressing the subject areas of IT security as well as legal aspects of cloud computing - the user is asked simple questions which are easy to answer without special expertise in both subject areas. These answers serve as an input to the method presented in this paper and the result is a selection of applicable requirements addressing IT security or legal constraints. These requirements then serve as input to a service search which accesses a repository to select appropriate cloud services matching the functional and non-functional requirements. The results of this search are then displayed to the user, making sure that the user will consider only cloud services which satisfy her needs.

The remainder of the paper is structured as follows: Section II gives an overview over the different subject areas of cloud service requirements and justifies the focus of this paper. Section III covers the related work regarding the identification of IT security and legal requirements. Then, in Section IV, the underlying methodology for the development of the presented method is described, and in Section V, the method is explained in detail. Section VI presents the application of the presented method in a website helping users to identify appropriate cloud services. Section VII describes our evaluation efforts and Section VIII concludes with a discussion and an outlook on further research activities.

II. CLOUD SERVICE REQUIREMENTS AND FOCUS

In the field of software engineering, the requirements regarding a software application are typically categorized into functional and non-functional requirements [4]. This schema can also be used for the categorization of requirements regarding a cloud service:

- **Functional requirements:** This category comprises the functions/modules needed by users of the cloud service. Examples are address administration, e-mail or invoice practice. The needed interfaces to other services or applications also fall into this category.
- **Non-functional requirements:** Non-functional requirements typically cover various *qualitative and quantitative aspects* regarding the software (i.e., usability, performance, IT security or documentation). However, for an adequate selection of cloud services we need a broader understanding of non-functional requirements which – along with qualitative aspects – also considers the following:

 ISBN: 978-1-61208-388-9

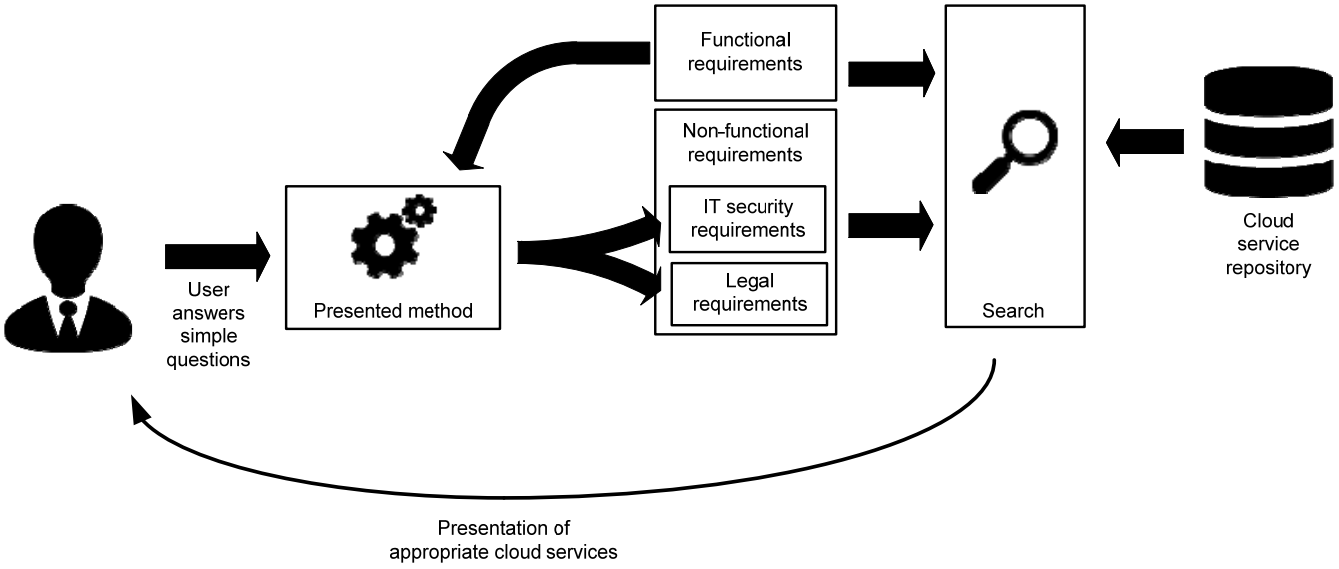

Figure 1. Visualization of the cloud service search

- **Legal requirements:** Depending on the kind of data that is processed by the cloud service, it might be necessary to obey certain legal constraints – i.e., in Germany the Federal Data Protection Act (Bundesdatenschutz-gesetz) regulates the processing of personal data. Such legal requirements may influence (improve) also the IT security of a service; however, primarily they are of a regulatory nature - i.e., they may ensure that fiscal authorities can access service data easily.
- **Economic aspects:** When selecting a cloud service, it might be necessary to also consider economic aspects – i.e., the price of the service should not exceed a given budget or migration cost to a service must be taken into account.

Fig. 2 shows the taxonomy which forms the basis for our understanding of cloud service requirements.

In order to select an appropriate cloud service, all aspects need to be taken into account. However, users from SMEs require varying support in the different subject areas. For example, for reviewing the user experience of certain cloud software not much technical expertise is required. Also, the evaluation of a cloud service from an economic perspective is something users of SMEs should be capable of. However, studies show that such users are especially concerned with IT security as well as being compliant to applicable law [2][3] and these are the topics the users of SMEs in general do not have much experience with. As IT security and law are the areas the users of SMEs need the most support, the focus of this paper lies on the identification of requirements out of these two subject areas.

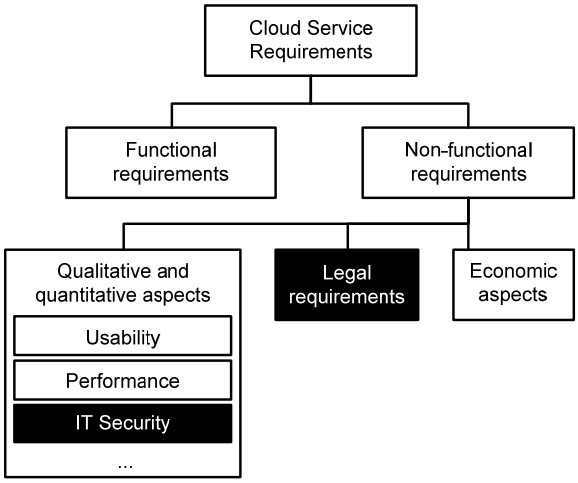

Figure 2. Taxonomy of cloud service requirements. In the diagram the focus areas of this paper has been highlighted.

III. Related Work

As IT security is a highly relevant topic in the context of cloud computing, there exists various literature supporting providers and users to obey important security aspects of cloud computing and cloud services. For example Mather et al. [5] and Krutz et al. [6] cover security aspects of cloud computing mostly with an emphasis on the enterprise perspective. Another example are the security recommendations for cloud providers [7] published by the German Federal Office for Information Security, which can also act as a source for requirements for users of cloud services. On an European Union level the European Union Agency for Network and Information Security (ENISA) offers thread analysis for internet and cloud architectures [8] and, with members from all over the world, the Cloud

 ISBN: 978-1-61208-388-9

Security Alliance (CSA) promotes the use of best practices for providing security assurance on cloud computing for an even broader audience [9]. Furthermore, various certificates formulate requirements affecting the IT security and can be applied in the context of cloud services [10]. Examples are the certification regarding ISO 27001 [11], which addresses IT security management in general or the Euro Cloud Star Audit [12], which explicitly addresses cloud services.

The legal aspects of cloud computing/cloud services do – especially in Germany and the EU as a whole – get great attention and various publications cover relevant aspects for providers as well as users of cloud services [13][14][15].

To sum up, in both areas - IT security as well as law - many resources are available, which can be used by users of cloud computing to formulate their requirements regarding a cloud service. However, to do so, a certain expertise is necessary and in both fields no approach exists, which helps users of cloud services to identify the appropriate requirements without requiring the user to deal with the sometimes rather complicated details.

Recommender systems seek to predict a rating or preference of a user for a specific item. There exist different recommender systems which support the selection of appropriate cloud services [16][17]; however, existing systems mainly focus on quantitative aspects like execution time, response time or budget – hence, leaving out important qualitative aspects with respect to legal constraints or IT security. Furthermore, in these systems the user has to specify the (quantitative) requirements herself which may not be possible for many users of SMEs.

IV. METHODOLOGY

This section covers the individual steps which led to the development of the presented method and its prototypical application. Fig. 3 gives an overview of the different steps involved in this process.

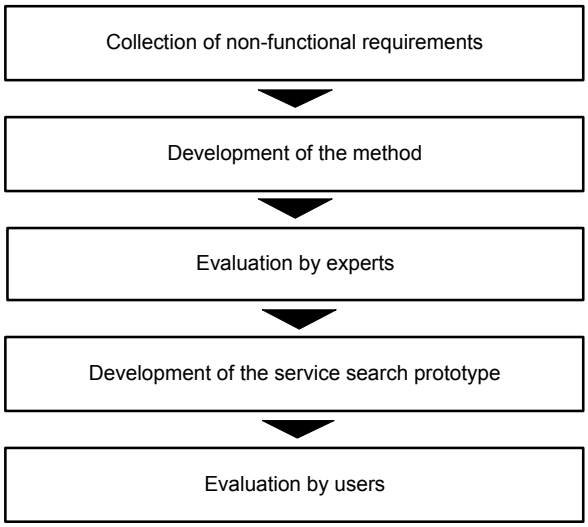

Figure 3. Overview of the different steps which led to the presented method and its prototypical application.

At first, literature reviews in the field of IT security and regarding legal aspects of cloud computing were conducted. Based on [7], [10], [14], [22], [23], and [24] a comprehensive list of non-functional requirements was collected – all of them being relevant regarding the selection of cloud services. The final list of requirements contains 104 entities each being assigned to one of the following subject areas (for examples, see Section V):

- Data center: Infrastructural aspects relevant to IT security, processes, organization of staff (35 requirements)
- Service provider: processes, organization of staff (17 requirements)
- Cloud service: Various aspects of the service relevant to IT security, training and support (35 requirements)
- Legal: contract, legal requirements (17 requirements)

In a next step, strategies regarding IT risk assessment were investigated. As the foundation for our method, we chose the concept of risk analysis [19], which combines the damage a security breach could do to the IT system of a user/organization with its associated probability for occurrence. Then, the list of non-functional requirements as well as the developed method were improved based on discussions with experts with expertise in IT security and regarding legal aspects of cloud computing. The final method is presented in Section V of this paper.

This method was then implemented as part of a prototype for a web-based search system for SMEs which supports the selection of adequate cloud services (see Section VI). The last step comprised an evaluation of this web-based prototype by users from SMEs. The evaluation setting and the results of both evaluation stages (experts and users) are described in Section VII.

V. DESCRIPTION OF THE METHOD

Fig. 4 visualizes the data flow giving an overview over the individual steps of the presented method. The initial input is the set of functional requirements of the user regarding a potential cloud service. The first step performs a preprocessing which results in data types and legal constraints due to the functional requirements. Based on the data types, the protection needs to become qualified. Afterwards, the individual non-functional requirements are derived taking into account these protection needs as well as the legal constraints. The final result is a set of individual non-functional requirements regarding a cloud service. In the following, the different steps of the method will be described in detail.

 ISBN: 978-1-61208-388-9

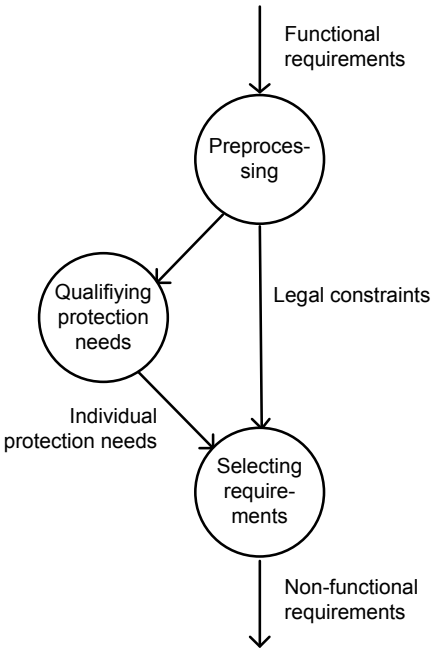

Figure 4. Visualization of the data flow

A. Preprocessing

In the first step a preprocessing is performed, where, based on the functional requirements, the following information is derived:

- The different **data types** which should be processed by a cloud service. As an example, if a functional requirement for the cloud service is *address administration*, then this implies the processing of *address data*.
- The **legal constraints** regarding the cloud service due to the processing of the different data types. These constraints must be derived from national word of law and from regulations applicable to the user's business. Example: In the case of *address data* being a data type, in Germany, the processing of personal data has a legal constraint – due to the fact that the regulations of the Federal Data Protection Act have to be obeyed.

B. Qualifying Protection Needs

Regarding IT security, the most prominent protection targets are availability, integrity and confidentiality of data [18]. In order to qualify the individual user needs regarding these protection targets, our method utilizes the concept of risk analysis [19], which combines the damage a security breach could have to the IT system of a user/organization with its associated probability for occurrence. The risk analysis used by our method comprises the following steps:

1. **Value of protection:** For each data type and protection target (availability, integrity, confidentiality) the value of the protection is qualified using the categories *low, normal, high, very high*. Then, following the maximum principle [20] the value of protecting a target is chosen as the maximum value over all data types.
2. **Threat characteristic:** Then a *threat characteristic* matching the industry sector must be chosen. Based on this threat characteristic, the probability of a security breach affecting one of the protection targets is qualified using the categories *very rare, rare, occasionally, often, very often* (see Table I).
3. **Individual protection needs:** Based on the value of protection and the probability of a security breach, the individual needs regarding the protection targets are derived as being *low, medium, high* or *very high* (see Table II).

TABLE I. THREAT CHARACTERISTIC

Threat Characteristic	**Probability of security breach**		
	Availability	***Integrity***	***Confident-iallity***
Politically explosive, high public interest	very often	occasionally	occasionally
High risk for (industry) espionage	very often	occasionally	very often
No specific characteristic	very often	occasionally	rare

TABLE II. PROTECTION NEEDS

Probability	**Value of Protection**			
	Low	***Normal***	***High***	***Very High***
Very rare	low	low	low	normal
Rare	low	normal	normal	high
Occasionally	low	normal	normal	high
Often	low	normal	high	high
Very often	low	high	high	very high

C. Selecting Requirements

The foundation for this step is a comprehensive list of non-functional requirements relevant to IT security or regarding legal constraints. Examples of such requirements are:

- In Germany, if the processed data is *personal*, then the contract with the cloud service provider must be compliant with the Federal Data Protection Act (Bundesdatenschutzgesetz).
- The computing center of the cloud provider should have a redundancy of N+1 for critical components in order to be able to offer high or very high availability.
- In order to ensure *very high* protection of integrity and confidentiality a strong authentication (i.e., two factor authentication) for users of the service is necessary.

 ISBN: 978-1-61208-388-9

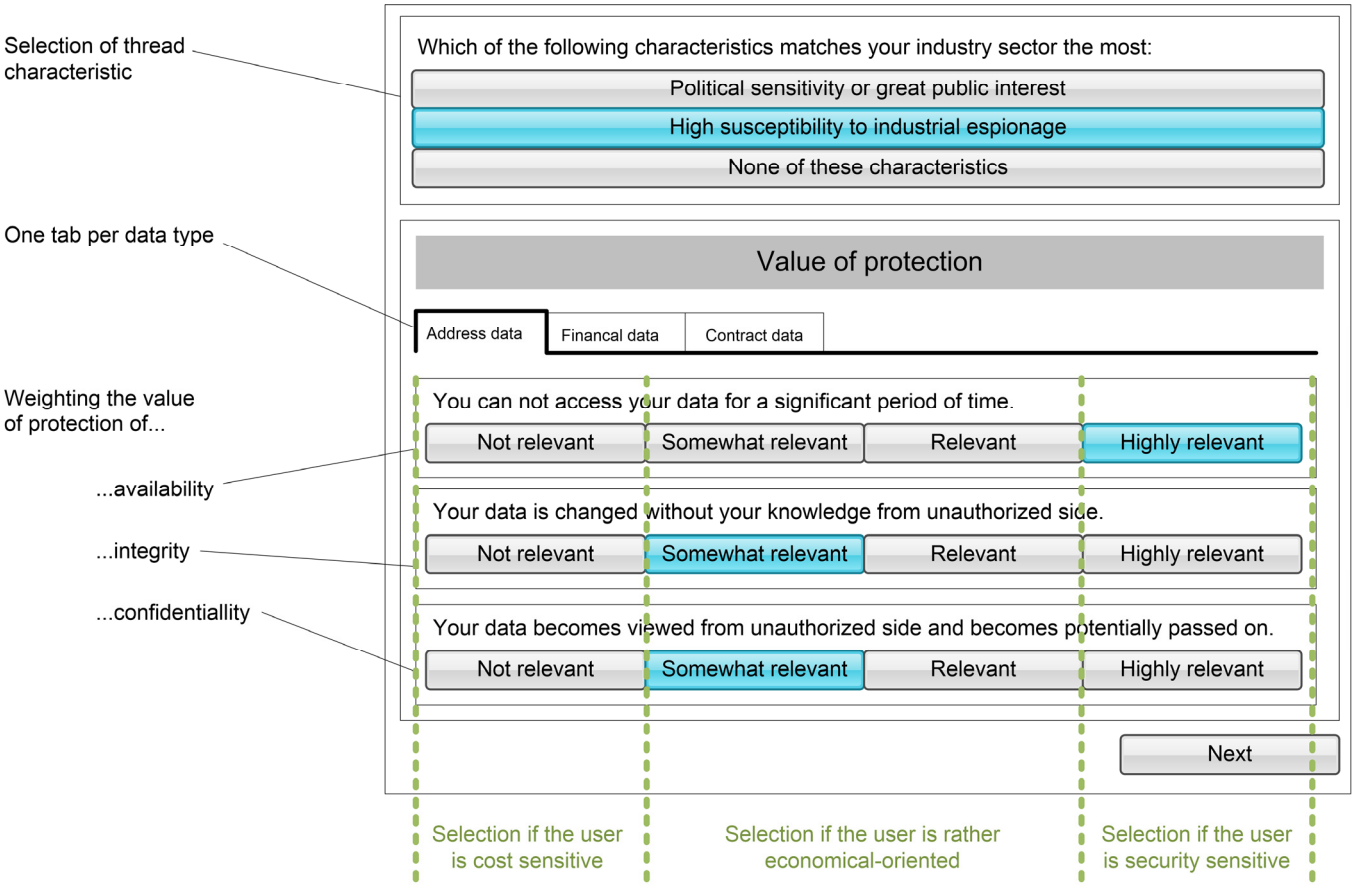

Figure 6. Screenshot of the input elements used to qualify the protection needs

A schema for conveniently expressing that list of requirements is depicted in Fig. 5.

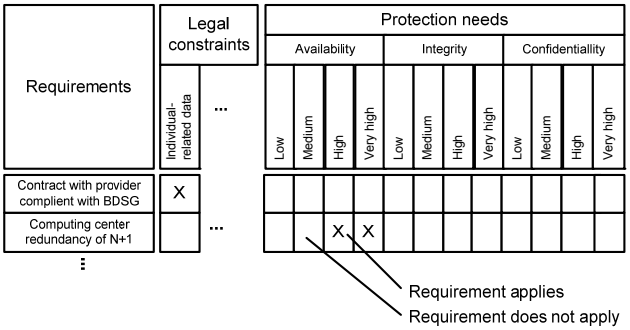

Figure 5. Schema for expressing the set of non-functional requirements

The objective of this last step is the selection of a subset of requirements from this list. This can be achieved by selecting the requirements which do apply when considering the given legal constraints as well as the individual protection needs.

VI. Application

The method described in the previous section was implemented as part of a prototype for a web-based search system for SMEs supporting the selection of adequate cloud services. The central components of this search system are:

- **Fn:** The first component of the system is responsible for the determination of functional requirements regarding a cloud services. In this step, the system supports the user by allowing a semantic extraction of functional terms from product websites specified by the user (i.e., the website of a product the user currently has in use and intends to replace by a cloud service). The technique for this semantic extraction of functional requirements is described in detail in [21]. The functional requirements are represented as a set, detailing for each identified function what kind of data (data types) this function processes and which legal constraints have to be obeyed in this context.
- **Non-Fn:** The second component implements the method described in this paper.
- **Search:** The last component performs a search in the service repository using the search profile defined by

 ISBN: 978-1-61208-388-9

the functional and non-functional requirements. For each service the fulfillment of the individual functional and non-functional requirements was stored in the repository. The search was performed by filtering out services which miss one or more of the identified requirements.

In the following, some background information regarding the implementation of the Non-Fn component will be given.

A. Preprocessing

Data types and legal constraints are automatically determined based on the functional requirements which were identified by the Fn component. In order to achieve this, the system uses a data set which allows a mapping from functional requirements to associated data types. Furthermore, the data set specifies if a data type has one or more legal constraints. The following legal constraints are supported by the system: *personal data, fiscal relevant data* and *security clearance*.

B. Qualifying Protection Needs

In order to gather the value of protection for each tuple *data type* / *protection target* as well as for selecting an adequate threat characteristic, corresponding questions and input elements are presented to the user (see Fig. 6). Then, the individual needs regarding the three protection targets (availability, integrity, confidentiality) are derived based on these inputs.

VII. EVALUATION

The first evaluation comprised the review of the presented method, as well as the list of non-functional requirements by two experts – one with expertise in IT security, one with expertise in both IT security and legal. Both experts did attest the list to successfully cover the necessary aspects of IT security as well as relevant legal aspects regarding the selection of cloud services. Based on the reviewers' feedback the method itself was further improved resulting in the form presented in Section V.

The second evaluation stage involved the assessment of the implemented prototype of the search system by users from five independent SMEs from the craft domain. The prototype was presented to each of these reviewers and afterwards an interview was conducted in order to get the reviewer's opinion regarding the search system and the underlying method. During the interviews, the reviewers attested the search system (together with the underlying method) to successfully assist users with the identification of relevant non-functional requirements. Hence, the system would reduce the amount of expertise required by users of SMEs as well as the associated effort of searching for appropriate cloud services.

VIII. CONCLUSION

In this paper, we have presented a method for identifying IT security and legal requirements regarding a cloud service. Also, details regarding the implementation of the method as a component of a service search as well as evaluation results were given. As the feedback of users of SMEs was quite promising we think that the underlying method is well suited for supporting the identification of cloud service requirements. Hence, we think that by utilizing the method in search systems for cloud services the process of finding appropriate cloud services can be simplified and accelerated as users do not have to identify these requirements on their own. Instead, a search system can handle all these individual requirements under the hood and just present the appropriate services to the user. If users are convinced that such a search system has taken into account all relevant requirements (in particular covering IT security and law) this could further increase the adoption of cloud computing by SMEs as users would have more trust that the selected service is appropriate for them.

Due to these promising results, we plan to further develop the service search system. In addition to improvements to the user experience, we intend to further fill the repository with various cloud services from different domains. This will help us to further asses the relevance of the presented method as well as the relevance of such search system as a whole.

ACKNOWLEDGMENT

This work was funded by means of the German Federal Ministry of Economy and Technology under the promotional reference "01MD11041".

REFERENCES

[1] R. Sahandi, A. Alkhalil, and J. Opara-Martins, "Cloud computing from SMEs perspective: a survey-based investigation," Journal of Information Technology Management, vol. 24, No. 1, University of Baltimore, 2013, pp. 43-49.

[2] H. Kasper, H. Kett, and A. Weisbecker, Potenziale von Cloud Computing im Handwerk. Stuttgart: Fraunhofer Verlag, 2012.

[3] S. Lamberth and E. Hebisch, Sichere Cloud, Technical Report, Stuttgart: Fraunhofer IAO, 2011.

[4] H. Balzert, Lehrbuch der Softwaretechnik – Basiskonzepte und Requirements Engineering. 3rd ed., Heidelberg: Spektrum, 2009.

[5] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Relly, 2009.

[6] R. L. Krutz and R. D. Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis: Wiley, 2010.

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Sicherheitsempfehlungen für Cloud Computing Anbieter*, Bonn, 2012.

[8] C. Lévy-Bencheton, L. Marinos, R. Mattioli, T. King, C. Dietzel, and J. Stumpf, Threat Landscape and Good Practice Guide for Internet Infrastructure, Report, European Union Agency for Network and Information Security (ENISA), 2015.

[9] R. Ko and S. Lee, Cloud Computing Vulnerability Incidents, Report, Cloud Security Alliance (CSA), 2012.

[10] Á. Geréd, A. Weiss, B. Becker, U. Huber, and C. Zeidler, Cloud Computing – Herausforderungen, Qualitätssicherung, Standards und Zertifizierung. Wien: EuroCloud.Austria, 2013.

 ISBN: 978-1-61208-388-9

[11] International Organization for Standardization (ISO): *ISO/IEC 27001:2013*.

[12] EuroCloud: *ECSA - EuroCloud Star Audit*. http://eurocloud-staraudit.eu/ [accessed: 10.07.2013].

[13] M. Bedner, Cloud Computing: Technik, Sicherheit und rechtliche Gestaltung. Dissertation, Kassel: University Press, 2013.

[14] J. Eckhardt, M. Hilber, R. Giebichenstein, F. Niemann, T. Helbing, and A. Weiss, Leitfaden Cloud Computing – Recht, Datenschutz und Compliance. Köln: EuroCloud Deutschland_eco, 2010.

[15] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM): *Cloud Computing - Evolution in der Technik, Revolution im Business*, Berlin, 2009.

[16] M. Zhang, R. Ranjan, S. Nepal, M. Menzel, and A. Haller, "A Declarative Recommender System for Cloud Infrastructure Services Selection," 9th Int. Conf. on Economics of Grids, Clouds, Systems, and Services (GECON'12), 2012, pp. 102-113.

[17] S.-M. Han, M. M. Hassan, C.-W. Yoon, and E.-N. Huh, "Efficient Service Recommendation System for Cloud Computing Market," 2nd Int. Conf. on Interaction Sciences: Information Technology, Culture and Human, 2009, pp. 839-845.

[18] C. Perrin, The CIA triad, techrepublic.com, 2008. http://www.techrepublic.com/blog/it-security/the-cia-triad/ [accessed: 25.12.2014].

[19] C. Eckert, IT-Sicherheit, Konzepte – Verfahren – Protokolle, 8th ed., Munich: Oldenbourg, 2013.

[20] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Standard 100-2*.

[21] A. Horch, C. Christmann, and H. Kett, "Automated Elicitation of Functional User Requirements for Supporting Cloud Service Search," Submitted to: 3rd Int. Conf. on Building and Exploring Web Based Environments (WEB 2015).

[22] V. Avelar, Guidelines for Specifying Data Center Criticality / Tier Levels, White Paper, Schneider Electric, 2011.

[23] Uptime Institute: *Data Center Site Infrastructure Tier Standard: Topology*, Santa Fe, 2010.

[24] J. Wollersheim, P. Hoberg, and H. Krcmar, Merkmale einer Servicebeschreibung für Cloud Services - V 0.9, 2013.

 ISBN: 978-1-61208-388-9